NUCLEAR SECURITY IN SOUTH ASIA: REGIONAL VIEWS ON PROSPECTS AND PRIORITIES

December 2021

STIMSON CRDFGLOBAL South Asian Voices

FOREWORD

I am pleased to present the Stimson Center South Asia program's latest publication, "Nuclear Security in South Asia: Regional Views on Prospects and Priorities." This collection of essays, developed in partnership with CRDF Global, features the work of rising scholars from India, Pakistan, and Bangladesh. Authors were selected through a competitive application process, received grants to support their research, and benefited from two private workshops co-hosted by Stimson and CRDF Global with regional subject-matter experts.

The resulting analysis, first published as a series of pieces on our online policy platform South Asian Voices, explores challenges related to safeguarding nuclear materials and proposes solutions to critical nuclear security issues in South Asia. Policy recommendations range from bilateral and regional security mechanisms, to addressing cyber vulnerabilities, to exploring the potential for advanced reactors in nuclear energy production.

This work follows in the program's long tradition of supporting rising analysts across South Asia and highlighting novel approaches to managing and mitigating some of the region's most complex dynamics.

We are grateful to CRDF Global for making this project possible. For more information on the work of Stimson's South Asia program, please visit our website at https://www.stimson.org/program/south-asia/.

Sincerely,

Elizabeth Threlkeld

Senior Fellow and South Asia Program Director, The Stimson Center

Cover Image: Reetesh Chaurasia via Wikimedia Commons

NOTES FROM CRDF GLOBAL AND SOUTH ASIAN VOICES

A Note from CRDF Global

South Asia, along with every region in the world, is faced with challenges related to safeguarding and securing nuclear material. In this series, eight grantees identified and presented suggestions to address pressing nuclear security issues in South Asia. These articles respond to the larger question which underpinned the scope of this project: How can we mitigate current and future nuclear security vulnerabilities in the subcontinent? The essays propose a variety of solutions including the pursuit of advanced reactors, including Small Modular Reactors (SMRs), addressing cybersecurity challenges, ensuring the safety of nuclear personnel, and developing bilateral security frameworks to enhance regional security. All of the essays are published on South Asian Voices, an online platform that encourages expertise in the nonproliferation field in the region.

CRDF Global is an independent nonprofit organization and leading provider of logistical support, program design and management, and strategic capacity building programs in the areas of threat reduction, CBRNE security and nonproliferation, border security, cybersecurity, global health, technology entrepreneurship, and international professional exchanges.

A Note from South Asian Voices

We are delighted to share this collection of essays, originally featured on South Asian Voices (SAV), with a wider audience.

Since 2013, SAV has provided an online platform for strategic analysis on South Asia's security, political, and economic affairs and featured debate and analysis among scholars, analysts, and policymakers on critical issues in the region.

Thus, it was only fitting for SAV to partner with CRDF Global to offer grants to support research exploring emerging challenges in and possibilities for cooperation on some of the most pressing nuclear security issues on the subcontinent. These essays reflect ongoing analytical work by scholars from India, Pakistan, and Bangladesh, on topics ranging from the impact of nuclear security culture or cyber threats on protection of nuclear materials to regional mechanisms for cooperation and prospects for emerging technologies such as small modular reactors. The essays in this collection, written by Chirayu Thakkar, Sitara Noor, Pulkit Mohan, Palwasha Khan, Md. Shafiqul Islam, Sitakanta Mishra, Tahir Mahmood Azad, and Urvashi Rathore, further understanding of and dialogue on nuclear security risks in the region. They also identify opportunities for collaboration and offer innovative solutions that push the envelope to tackle what are often politically fractious problems.

We are grateful to CRDF Global for their partnership and to all our grantees for their thoughtful and deeply researched pieces. For more analysis on nuclear security issues and other topics related to the subcontinent's strategic affairs, we invite you to visit the South Asian Voices website at southasianvoices.org.

Akriti Vasudeva and Brigitta Schuchert

CONTENTS

Image: Reetesh Chaurasia via Wikimedia Commons

The Kundankulam Nuclear Power Plant (KKNPP) via Wikimedia Commons

1. RETHINKING NUCLEAR SECURITY: THE CASE FOR AN ELITE NUCLEAR FORCE IN INDIA

By Chirayu Thakkar

"Good security is 20 percent equipment and 80 percent people."[1]

—Eugene Habiger, Head of Security, US Department of Energy

Since the early 1960s, India has embraced nuclear energy as a perennial source of power underwriting its development trajectory. After a three-decade-long embargo, India was again integrated into the global nuclear order with the help of the United States in 2008, paving the way for numerous nuclear energy installations across the country. As the worldwide market for nuclear energy shrinks, India remains a bright spot attracting both finance and technology, which coincides with India's technology diversification strategy. With indigenous, Canadian, Russian, French, and U.S./Japanese reactors in action or installation and negotiations underway for the South Korean one, India would have the most diverse reactor portfolio globally in the next decade.[2] Given its subcontinental size, New Delhi might also be interested in harnessing the benefits of modular technology

[1] Eugene Habiger quoted in Rajeshwari Pillai Rajagopalan, *Nuclear Security in India*, (New Delhi: Observer Research Foundation, 2015), 24.

[2] Chirayu Thakkar, "India-U.S. Nuclear Trade and Cooperation: Potential for the Biden Administration," *South Asian Voices*, February 5, 2021. https://southasianvoices.org/india-u-s-nuclear-trade-and-cooperation-potential-for-the-biden-administration/.

currently under experimentation. Along with electricity, nuclear technology's other peaceful uses from the medical to agriculture sectors make nuclear safety and security a pressing concern for India.

This essay first suggests that expansion of the uses of nuclear technology brings the challenge of capacity building for areas ranging from regulatory to forensics, which is neither immediately achievable nor readily acquirable. It then investigates the human factor in physical security by examining security arrangement for all sites throughout the nuclear fuel cycle—what Indian policymakers call "cradle to grave" approach.[3] This paper suggests that an elite nuclear constabulary akin to the one in the United Kingdom can replace the current multi-agency model and fill in some vital gaps. The recommendation to emulate the UK's Civil Nuclear Constabulary has been made on previous occasions; however, this essay dwells upon the necessity, scope, and functions of such a potential force in adequate detail for the first time.[4]

Capacity Gap

The topic of nuclear security usually evokes dramatic events of the Fukushima nuclear disaster, the Stuxnet attack on Iranian facilities, or a potential terrorist attack. Such incidents, although calamitous, are few and far between.[5] The routine challenges of nuclear security are far more mundane. For example, according to the International Atomic Energy Agency (IAEA)'s Incident and Trafficking Database, 36 countries reported 189 cases of "unauthorized activities" such as theft and trafficking of nuclear material in 2019 alone.[6] Most of these countries are parties to the necessary conventions that protect their sites/materials and transparent enough to voluntarily disclose such incidents to an international body indicating the best of their intent. It is not their *intent* but the *state capacity* that determines their success in protecting critical sites and materials. From credible international analysis, India seems to be more challenged by these mundane issues than dramatic events. For example, closely observing the sub-indicator level data of the Nuclear Threat Initiative (NTI)'s Nuclear Security Index, one finds India comfortably ranks third out of 22 countries in its preparedness for cybersecurity vulnerabilities. In contrast, India is much below median ranking on indicators such as controlling and accounting procedures, insider threat prevention, and overall security culture.[7] Combating these challenges is directly related to a state's capacity. This essay adopts a more pragmatic and heuristic definition of state capacity: "a state's ability to accomplish its intended

[3] H.E. Mr. M.J. Akbar, "IAEA Ministerial Conference on Nuclear Security Statement of India," International Atomic Energy Agency (IAEA), December 5, 2016. https://www.iaea.org/sites/default/files/16/12/india_statement_dec_2016.pdf.

[4] This idea was originally mooted by Rajeshwari Rajagopalan. See Rajagopalan, *Nuclear Security in India*, 84. Subsequently, it is echoed by many others. For instance, Sitakanta Mishra and Happymon Jacob, *Nuclear Security Governance in India: Institutions, Instruments, and Culture*. (Albuquerque: Sandia National Laboratories, 2019); also, Raj Chengappa, "The Dirty Bomb", *India Today*, April 6, 2016.

[5] In response to a query on cyberattacks on the Department of Atomic Energy installations in India, the minister responded that no breaches have been reported between 2014 and 2017. See, Q. 1007 of 2017, Lok Sabha.

[6] "IAEA Incident and Trafficking Database: Incidents of Nuclear and Other Radioactive Material out of Regulatory Control: 20202 Fact Sheet," https://www.iaea.org/sites/default/files/20/02/itdb-factsheet-2020.pdf.

[7] NTI Index, "India," 2021. https://www.ntiindex.org/country/india/. It is worth noting here that the Indian government contests the NTI's assessment due to "faulty methodology" and "unreliable information." See Ministry of External Affairs, "Foreign Secretary's media interaction on conclusions of New Delhi Sherpa Meeting," January 17, 2012. https://mea.gov.in/media-briefings.htm?dtl/17957/.

policy actions."[8] Hence, the term state capacity becomes elastic enough to include an array of abilities such as having legislative and regulatory competence, financial resources, technical know-how, proficient workforce, among others, for preventive, monitoring, detection, and punitive purposes in relation to nuclear security.

It is assumed here that with the commitment towards nuclear security in place, enabling legislation, devoting financial resources, and acquiring technology from friendly suppliers becomes significantly easier. However, capacity building is neither immediately achievable nor readily acquirable, making it a momentous task for any state. This concern is frequently echoed by policymakers in India as well. In the aftermath of the Fukushima incident, Jairam Ramesh, then Minister for Environment, wrote Dr. Manmohan Singh raising concerns regarding India's domestic capabilities against its diversification strategy.[9] As Ramesh notes: "Each of the reactor types will call for a certain regulatory procedure, protocol, and capability. *Regulatory expertise takes time to build up and in any case is not available easily*. Gone are the days of Nehru and Bhabha *when public organizations could attract, train, and retain top-flight professional expertise*." (emphasis added)

The capacity gap afflicts the entire span of nuclear fuel cycle, starting from exploration and mining to processing and disposal. Cognizant of these challenges, India instituted the Global Center for Nuclear Energy Partnership in 2011, whose five schools cater to a diverse set of needs for nuclear security in India.[10] There are also dedicated schools such as the National Industrial Security Academy for paramilitary forces guarding nuclear installations and the National Institute of Disaster Management (NIDM) for contingency forces prepared to attend chemical, biological, radiological and nuclear (CBRN) incidents. To pool nationwide resources—both equipment and individuals—NIDM has created an online inventory called India Disaster Resource Network that allows quick identification of necessary resources across state units to pool them in a timely manner.[11] While laudable initiatives, these efforts remain inadequate with chronic shortages of trained workforce. For example, in its latest submission to a parliamentary committee, the Atomic Energy Regulatory Board admitted that with a paltry workforce of 300 scientists and engineers, it is incapable of regulating 57,443 medical X-Ray facilities across India.[12] The response was in reference to a query that pointed out that roughly 91 percent of medical X-Ray facilities remain unregistered and hence, unregulated. In 2013, parliament also underscored the lack of Radiological Security Officers (RSOs), who are primarily responsible for on-site security and regulatory compliance.[13] Some progress has been made on that front for Category I and II radiation sites, where adequate RSOs are now

[8] Mark Dincecco, *State Capacity and Economic Development: Present and Past,* (Cambridge: Cambridge University Press, 2018), 2. For a more conventional discussion on state capacity in the Indian context, see Sumit Ganguly and William R. Thompson "Conceptualizing and Measuring State Strength," in *Ascending India and its State Capacity: Extraction, Legitimacy, and Violence*. (New Haven: Yale University Press, 2017), 53-74.

[9] Jairam Ramesh, *Green Signals: Ecology, Growth and Democracy in India*. (New Delhi: Oxford University Press, 2015), 425.

[10] Government of India: Department of Atomic Energy, 2021. http://gcnep.gov.in/schools/schools.html.

[11] See, "India Disaster Resource Network," https://idrn.nidm.gov.in/. In the remainder of the essay, "state" is used to indicate regional government as is the practice in India. Constitutionally, law and order is a state subject with minimal interference from the federal government.

[12] Department of Atomic Energy, Public Accounts Committee "Activities of Atomic Energy Regulatory Board, Seventh Report," Seventeenth Lok Sabha, February 4, 2021. 13.

[13] Department of Atomic Energy, Public Accounts Committee, "Activities of Atomic Energy Regulatory Board," Ninetieth Report, Fifteenth Lok Sabha, December 9, 2013, 43.

available.[14] Similarly, despite its booming usage of nuclear technology, a 2013 study suggested that India lacked both technical and human capacity for nuclear forensics such as ion mass spectrometry.[15] However, in a paper written subsequently by an Indian scientist, formerly with the Bhabha Atomic Research Center, there was an indication that India has some capacity for research, if not a dedicated nuclear forensic lab.[16]

One can dwell upon each of these individual domains—regulatory, materials accounting, cybersecurity, transportation, forensics, among others, to suggest capacity gaps and ways of strengthening them. The remainder of this essay investigates the human factor in physical security of nuclear installations and make a case for a permanent force responsible for security, transport, and counter-smuggling efforts. Such a permanent force resolves many doctrinal and operational challenges with long-term institutional memory compared to currently practiced multi-agency endeavor.

Physical Security: A Multi-Agency Endeavor

Physical security of nuclear sites in India is a multi-agency endeavor. The phrase "physical security" in this section is narrowly interpreted to include institutional efforts in "averting unlawful removal and usage of nuclear materials."[17] At the highest level, the Atomic Energy Regulatory Board (AERB) is responsible for overseeing India's nuclear security. However, AERB, being a regulatory authority operating under the Department of Atomic Energy (DAE) reporting to the Prime Minister's Office, does not command a force. The actual security of civilian nuclear facilities rests with various agencies, with the Central Industrial Security Force (CISF), operating under the aegis of the Ministry of Home Affairs, remaining the mainstay of protection across installations. Table One encapsulates different phases of the nuclear fuel cycle and corresponding security agencies responsible for protection.

[14] Category I and II radiation sources are the ones with activity ratios of >1000 and 10-1000 respectively. For classification, see the IAEA's "Categorization of Radioactive Sources ". The Atomic Energy Regulatory Board follows the same classification. See, AERB Safety Guide No. AERB/RF-RS/SG-1 (March 2011). All AERB Guidelines cited in this essay are accessible at: https://www.aerb.gov.in/english/publications/codes-guides unless otherwise stated.

[15] National Academy of Sciences, "The Emerging Science of Nuclear Forensics" in *India-United States Cooperation on Global Security: Summary of a Workshop on Technical Aspects of Civilian Nuclear Materials Security*. (Washington, DC, The National Academies Press, 2013), 105-14.

[16] Suresh Kumar Aggarwal, "Nuclear Forensics: What, why and how?" *Current Science* 110, no. 5, (2016): 782-791, 789. See also, S. Mishra and Chaudhary, P., *Proceedings of the National Workshop on Nuclear Forensics: Fundamentals and Applications*

[17] This definition is accepted from the preamble of the Convention on Physical Protection of Nuclear Materials (CPPNM) that entered into force in 1987. See, International Atomic Energy Agency, "INFCIRC/274/Rev. 1," May 1980. https://www.iaea.org/sites/default/files/infcirc274r1.pdf. In a broader sense, physical security would include legal, human, mechanical, and other efforts.

TABLE ONE: NUCLEAR SECURITY ARRANGEMENTS IN INDIA

Stage	Site	Responsible Force
Mining & Processing (UCIL)	Eight mines, three processing plants	CISF and other guards
Storage (Nuclear Fuel Complex)	Two sites	CISF
Solvent and additive production (HWP)	Seven sites	CISF (for radioactive sites), State Police (for non-radioactive sites)
Power Production (NPCIL & Bhavini)	22 plants	CISF (inner perimeter), State Police (outer perimeter)
Vitrification and storage	Three plants	CISF
Transportation		CISF and state police
Post-Disaster		CISF and other agencies
Research Units	Six sites	CISF, as well as the Indian Coast Guard for the Bhahba Atomic Research Center
Strategic Installations	No Information	No Information
Border Surveillance		Individual frontier agencies

To start with, mining and processing of uranium in India is done by the Uranium Corporation of India Ltd. (UCIL) that currently operates eight mines and three processing plants. Apart from the CISF cover, the UCIL website notes the presence of security on its payroll and floats private security tenders on occasion.[18] This can be a recurring feature of many other installations as the exact allocation of duties between CISF personnel and other guards is unknown. Imported uranium pellets and ore concentrate are stored and processed along with other ingredients like Zirconium oxide at two other sites—the National Fuel Complex at Hyderabad and Kota, both secured by CISF. However, the cover provided by CISF to other ancillary units such as seven Heavy Water Plants (HWPs) that are responsible for the production of heavy water (D_2O) and nuclear grade solvents is not uniform. For instance, CISF protects HWP Manuguru and HWP Talcher while state police provide cover to HWP sites at Vadodara and Hazira.[19] The government does not explain this policy, but one can assume that Manuguru and Talcher plants have Boron-10 enrichment facilities, an isotope that is used as a fuel additive in Pressurized Water Reactors and Boiling Water Reactors, necessitating paramilitary level

[18] CISF website lists UCIL Jadugada under the list of protected sites. Similarly, a newer open cast uranium mine in Banduhurang, Jharkhand is under CISF protection see: Atomic Energy Regulatory Board, "Frequently Asked Questions," 44. https://www.aerb.gov.in/images/PDF/f1.pdf. However, observing the UCIL website one finds security staff from guard to manager on its payroll as well as tenders for external security floated from time to time

[19] HWP Manuguru and HWP Talcher are the only two HWP sites that are listed as having CISF stations. See Ministry of Home Affairs, "Central Industrial Security Force: Citizen's Charter," https://www.mha.gov.in/sites/default/files/Citi_Chart111208.pdf. In a question regarding the security of sites at Vadodara and Hazira, the government informed that they were protected by local law enforcement. See Q. 2175 of 2012, Rajya Sabha. Accessible at: https://rajyasabha.nic.in/rsnew/Questions/ShowQn.aspx?tk=8dd47f9e-2db7-480b-939d-d2e44f7f94f9.

security.[20] Like other DAE installations, CISF protects six major DAE research facilities, which houses six operational and two planned research reactors.[21] However, as the Bhabha Atomic Research Center (BARC) is a coastal site, the Indian Coast Guard (ICG) provides aerial and coastal surveillance while CISF protects peripheral cover.[22]

Subhashish Panigrahi via Wikimedia Commons

Coming to the security of nuclear power plants, India has a national Design Based Threat (DBT) plan, based on which each site produces its DBT assessment.[23] Beyond mechanical measures in place for surveillance, detection, delay, response, and access control, the physical security of the perimeter rests primarily with two agencies—the CISF and the state police, for the inner and outer perimeters respectively.[24] For security and contingency purposes, the perimeter and surrounding areas are divided into various zones. The plant itself has three boundaries—coolant boundary, primary and secondary containment boundaries, followed by a 1.6 km Exclusion Zone, which falls under the administrative purview of the plant operator.[25] It is followed by a five km Sterilized Zone and a 16 km Emergency Planning Zone, whose administrative and security responsibilities are with the state police. Both forces—CISF and state police—conduct mock drills periodically for inter-agency coordination.[26] All nuclear power plants have a

[20] Baron, et al. "Fuel Performance of Light Water Reactors" in *Comprehensive Nuclear Materials Vol II* ed. D.D. (Baron & L. Hallstadius. San Diego: Elsevier, 2020), 35-71.

[21] See Department of Energy, "Research and Development Sector," https://dae.gov.in/node/77, and International Atomic Energy Agency, "Research Reactor Database," https://nucleus.iaea.org/rrdb/Content/Geo/Country.aspx?iso=IN.

[22] Mishra and Jacob, *Nuclear Security Governance in India*, 54.

[23] Ministry of External Affairs, "Nuclear Security in India," https://www.mea.gov.in/Images/pdf/Brochure.pdf.

[24] Rajagopalan, *Nuclear Security in India*, 25-26; 40-44.

[25] National Institute of Disaster Management, "Management of Nuclear and Radiological Emergencies," (Government of India: New Delhi, February 2009).

[26] Rajagopalan, *Nuclear Security in India*, 59.

co-located near surface disposal facility for low to intermedial level waste.[27] Apart from on-site waste disposal, the DAE operates three vitrification plants at Trombay, Tarapur (includes storage), and Kalpakkam, which are located with other operational units, and hence, protected by the CISF. As India mostly recycles its spent fuel, it does not currently need a Deep Geological Repository.[28] Similarly, transportation of nuclear material for Type AF and Type B (U/M) F packages as well as irradiated nuclear fuel packages, which demands Level 2 or 3 security, is invariably accompanied by CISF escorts in front and back along with real-time Code Division Multiple Access (CDMA) central monitoring.[29] Apart from CISF, district police also provide necessary reinforcement when such convoys pass through their jurisdiction.[30]

In an event of a nuclear disaster, which includes incidents of sabotage and accidents, a host of agencies from the state to national level get activated (Table Two).[31] However, until such arrangements are in place, CISF personnel are not only responsible for continued protection, but they are also first responders for activities like evacuation.

TABLE TWO: NATIONAL DISASTER MANAGEMENT FRAMEWORK

Severity	Response Level
Severity Scenario I	Radiological Safety Officer/Community
Severity Scenario II	Local Police/Civil Defense/Home Guards
Severity Scenario III	National Disaster Relief Force/Army
Severity Scenario IV	All relevent national level agencies

Apart from the civilian installations discussed so far, there is hardly any information about the security of strategic installations, but it is believed a **specialized force** of the Indian Army is responsible for their physical security.[32] The counter-smuggling efforts on all borders are led by respective frontier forces namely the Border Security Force, Indo-Tibetan Border Police Force, Sahastra Seema Bal, and Assam Rifles, who are usually trained in arresting smuggling efforts of all types. Some of them are also trained in handling CBRN incidents.

[27] PK Wattal. "Indian Programme on Radioactive Waste Management" *Sadhana* 38, no. 5, (2003), 849–857

[28] Department of Atomic Energy, "Re-Cycling Technology for Nuclear Spent Fuel: Lok Sabha Unstarred Question No. 661," September 16, 2020. http://164.100.24.220/loksabhaquestions/annex/174/AU661.pdf.

[29] AERB Guidelines AERB/RF-RS/SG-1 (March 2011); Q. 144 of 2011, Rajya Sabha accessible at: https://dae.gov.in/writereaddata/rssq144_011211.pdf; National Academy of Sciences (2013). "Physical Security at Civilian Nuclear Facilities" in *India-United States Cooperation on Global Security: Summary of a Workshop on Technical Aspects of Civilian Nuclear Materials Security*. Washington, DC: The National Academies Press, 59-70; for packaging classification: AERB/NRF-TS/SC-1 (Rev.1) (March 2016).

[30] AERB Safety Code AERB/NRF-TS/SG-10 (March 2016). For a comprehensive overview of transportation of nuclear materials in India including regulatory, planning, and execution phases, see Reshmi Kazi, *"Post-Nuclear Security Summit Process: Continuing Challenges and Emerging Prospects,"* IDSA Monograph Series No. 59, (New Delhi, Institute of Defence Studies and Analyses, 2017).

[31] National Disaster Management, Authority, *Management of Nuclear and Radiological Emergencies [National Disaster Management Guidelines]*. (New Delhi: National Disaster Management Authority, Government of India, 2009). Apart from the agencies mentioned in the guideline, some have mentioned that India's most elite force National Security Guard (NSG) might be called into action if necessary. See, Rajagopalan, *Nuclear Security in India*, 33.

[32] Sitakanta Mishra, Jacob Happymon, and Shannon Abbott, "Nuclear Security Governance in India: Institutions Instruments and Culture," (Office of Scientific and Technical Information: U.S. Department of Energy, October 1, 2020). https://www.osti.gov/biblio/1678824.

Nuclear Constabulary

As noted earlier, despite CISF being primarily assigned the task of securing Indian civilian nuclear network, their reliance on other forces is telling. The CISF was constituted in reaction to a 1964 fire incident at the Heavy Engineering Corporation Factory, and it is presently responsible for all industrial sites across India and some private organizations after the 2008 Mumbai attacks. It is so thinly stretched that the Ministry of Home Affairs is recruiting veterans to meet the demand.[33] Some have criticized CISF as a threat-based force and not a capability-based force with "conceptual and doctrinal inadequacies."[34] Although no significant security breach has been registered under them, it is unreasonable to expect uniformity of security culture in a rotating force of 140,000 that is deployed across the country protecting VIPs, securing nuclear installation, and providing round-the-clock coverage to software parks.[35] No wonder some serious infractions have been noted in the past; for instance, leaving a uranium consignment unattended on the roadside for a lunch break.[36]

To ensure operational efficiency and instill security culture, it is high time India conceive a permanent nuclear constabulary like the United Kingdom. The Civil Nuclear Constabulary (CNC) in the UK is a dedicated force that ensures the security of all civilian nuclear installations across the country along with transportation and counter-terrorism functions.[37] The UK CNC has only 12 sites to protect. Yet, it operates a force of 1,500 agents with a dedicated command and control center, a search team, an interdiction team, a strategic escort group, a group of police medics, and a team with counter drone capability. With economy of scale on its side—over 30 sites across the country, India should pursue the idea of a dedicated force.

India's civilian nuclear force can entertain the following functions:

- Securing key nuclear installations including power plants and research facilities
- Extending cover to ancillary units like Heavy Water Plants which are under state police
- Adding airborne and seaborne capabilities to protect sites like BARC
- Overtaking transit responsibility of all critical nuclear materials (even private ones)
- Extending protection to private sites on demand

---

[33] Anvit Srivastava, "Ex-Servicemen to help CISF Secure Sensitive Installations," *Hindustan Times*, February 9, 2021. https://www.hindustantimes.com/india-news/exservicemen-to-help-cisf-secure-sensitive-installations-101612828798377.html.

[34] Narendra Kumar, "Paramilitary Forces and Central Armed Police Forces of India: Punching Below Their Capabilities" in ed. Harsh Pant *Handbook of Indian Defence Policy: Themes, Structures and Doctrines*. (New Delhi: Routledge, 2016) 363-384, 380.

[35] IAEA defines security culture as "The assembly of characteristics, attitudes and behavior of individuals, organizations and institutions which serves as a means to support and enhance nuclear security." See IAEA (2008), Nuclear Security Culture: Implementing Guide. IAEA Nuclear Security Series No. 7. Accessible at: https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1347_web.pdf Clearly, such an assemblage of attitudes and behavior would require certain constancy and continuity of personnel.

[36] "Security Escort Leaves Uranium Unguarded, Breaks for Dhaba Meal," *Bangalore Mirror*, May 7, 2012. https://bangaloremirror.indiatimes.com/news/india/security-escort-leaves-uranium-unguarded-breaks-for-dhaba-meal/articleshow/21386362.cms.

[37] Government of United Kingdom, "Civil Nuclear Constabulary: Annual Policing Plan 2021/22," https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/993437/Annual_Policing_Plan_2021-22.pdf.

- Expanding into the counter-smuggling domain
- Deputing trained workforce to frontier forces, airports and seaports, and major cities

One evident benefit of a dedicated force is that instilling security culture in permanent troops is relatively easier than in a rotating force. Moreover, it requires less effort and investment to enhance the technical abilities of a stable force. As mentioned above, such a dedicated force can expand its remit in multiple ways compared to CISF's current role. First, instead of relying on state police beyond the 1.6 km perimeter, the new force can secure the sterilized zone (five km) like the UK CNC. It can also cover existing facilities such as Heavy Water Plants that produce critical additives/solvents and Indian Rare Earths Ltd sites that process monazite sands containing Thorium. Second, for sites like BARC, the premium research cluster for civilian and strategic programs, the new force can add airborne and seaborne capabilities to prevent individual or drone attacks instead of relying on the Indian Coast Guard. In the wake of recent drone attack on Jammu Air Force station, suspected by Pakistan-based Lashkar-e-Taiba using Chinese drones, such preventive capacity of inshore nuclear sites such as Trombay, Kalpakkam, and Kudankulam becomes urgent and inevitable.[38] Third, it can oversee the entire transit arrangement instead of involving multiple agencies. The new force can also provide on-demand, fee-based transit security arrangements to private operators, generating revenue as well as securing equally critical private nuclear assets. It can also include DAE's planned medical isotope co-production facilities on a public-private partnership format.[39] Fourth, in line with its international commitment presented at the 2016 Nuclear Security Summit, India has an inter-agency Counter Nuclear Smuggling Team in place. The new force can lead or overtake this effort.[40] Fifth, such a force can depute nuclear security officers to each frontier (usually made up of three to four sectors and headed by an Inspector General) of major border policing agencies to integrate nuclear security efforts in border management.

Having a unified command would address many doctrinal and operational challenges and create a steady elite force with long-term institutional memory to tackle evolving security challenges. With the economy of scale favoring India, it is time that an amalgam of agencies paves the way for a permanent nuclear constabulary in India to address a vital capacity gap.

[38] Kamaljit Kaur Sandhu, "Jammu IAF base attack: RDX found in IEDs dropped by drones, reveals probe," *India Today*, July 5, 2021. https://www.indiatoday.in/india/story/jammu-iaf-base-attack-rdx-explosives-drones-reveals-probe-air-force-1824002-2021-07-05, and Shishir Gupta, "Pakistan LeT behind drone attack in Jammu, target was ATC and parked IAF helicopters," *Hindustan Times*, June 28, 2021. https://www.hindustantimes.com/india-news/pak-let-behind-drone-attack-in-jammu-target-was-atc-and-parked-iaf-helicopters-101624857978136.html.

[39] Department of Atomic Energy, "BARC Evolves Design of 1st PPP Research Reactor for Production of Nuclear Medicines," Public Information Bureau, January 29, 2021. https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1693211.

[40] "National Progress Report: India" presented at Nuclear Security Summit 2016. Accessible at: http://www.nss2016.org/document-center-docs/2016/3/31/national-progress-report-india; see also, Q. 251 of 2016 Lok Sabha accessible at: http://164.100.47.194/Loksabha/Questions/QResult15.aspx?qref=35170&lsno=16

IAEA Imagebank via Flickr

2. ASSESSING PAKISTAN'S NUCLEAR SECURITY UPGRADES AFTER RATIFICATION OF THE 2005 CPPNM AMENDMENT

By Sitara Noor

The Convention on the Physical Protection of Nuclear Material (CPPNM), adopted in 1987, is the primary legal instrument that forms the basis of global nuclear security regime. The CPPNM along with its amendment that entered into force in 2016, are the only legally binding international instruments in the area of physical protection of nuclear material under the International Atomic Energy Agency (IAEA).[1] Pakistan acceded to the original CPPNM in 2000 after streamlining necessary steps needed to comply with the convention's commitments. In view of evolving nature of threat and renewed global emphasis on nuclear security with the Nuclear Security Summit process, Pakistan began the preparation for ratification of 2005 CPPNM amendment, and on February 24, 2016, the National Command Authority (NCA) of Pakistan approved ratifying the 2005 amendment to the CPPNM—becoming the 94th state to ratify. A little over one month later, following the ratification from Nicaragua on April 8, 2016, the amendment achieved the required number of 102 states and entered into force 30 days later.[2]

[1] "Convention on the Physical Protection of Nuclear Material (CPPNM) and its Amendment," International Atomic Energy Agency (IAEA), https://www.iaea.org/publications/documents/conventions/convention-physical-protection-nuclear-material-and-its-amendment.

[2] Vincent Fournier, "Road Towards Entry into Force of Key Nuclear Security Agreement," International Atomic Energy Agency (IAEA), April 8, 2016. https://www.iaea.org/newscenter/news/road-towards-entry-into-force-of-key-nuclear-security-agreement.

The 2005 amendment's entry into force put in place several new obligations on the member states to bring their physical protection measures in line with the international requirements. To ensure compliance, Pakistan had already initiated several measures in line with the requirements of the amended CPPNM. For instance, Pakistan has incorporated various recommendations of INFCIRC/225/Rev-5, which is considered to be an international standard for the physical protection of nuclear material, and has introduced physical protection measures at its nuclear power plants beyond the scope of the original CPPNM even before the ratification.[3] The formal ratification of the 2005 CPPNM amendment obligated the state to implement additional technical, administrative, and legal measures in line with the amendment's requirements.

This study will provide an assessment of physical protection system upgrades in Pakistan. It will identify the additional obligations under the amended CPPNM and assess how Pakistan has assimilated new requirements in its physical protection measures and what further steps they must take for enhanced compliance.

Evolution of Physical Protection System in Pakistan

The evolution of physical protection of nuclear material and nuclear facilities in Pakistan has coincided with the establishment of the country's nuclear power program and the development of physical protection requirements at the International Atomic Energy Agency (IAEA). At the time of Pakistan's civilian program's initiation, the Pakistan Atomic Energy Commission (PAEC) was tasked with managing the safety and security of the nuclear program. The IAEA's document INFCIRC/225, "Physical Protection of Nuclear Material and Nuclear Facilities," was first published in 1975 and used as the basis for inspection and enforcement of physical protection measures.[4] Pakistan acceded to the original CPPNM in 2000.[5] To fulfill the convention's requirements, an independent body—the Pakistan Nuclear Regulatory Authority (PNRA)—was established in 2001 to ensure the physical protection measures for nuclear material during international transport as required by the original convention.

In the wake of September 11, 2001, as the global security dynamics changed, the risk of nuclear terrorism emerged as a new challenge to the nuclear security regime. Pakistan, like other countries, critically reviewed the existing systems and measures of its physical protection regime. Since the international cooperation and experience sharing in the area of nuclear security was not common, a mechanism was evolved on the basis of a gap analysis of existing physical security measures at the national level and in accordance

[3] Ministry of Foreign Affairs Government of Pakistan, "Pakistan's Nuclear Security Regime," 2020. https://mofa.gov.pk/wp-content/uploads/2020/02/NSRFinal08-02-2020.pdf. INFCIRC/225/Rev-5 is the IAEA publication that intends to assist the Member States in implementing their physical protection regime in line with all international commitments they have undertaken. It explains the basic elements of nuclear security and the recommended requirements to be implemented by the state.

[4] Noreen Iftakhar, "International Nuclear Law: A Case Study of Pakistan," *Strategic Studies*, 38, no. 4. (Winter 2018), 67-89. https://www.jstor.org/stable/48544278.

[5] While acceding to the CPPNM, Pakistan put reservation on paragraph 2 of article 2 regarding domestic use and transport and paragraph 2 of article17 on dispute settlement. "Convention on the Physical Protection of Nuclear Materials: Declaration/Reservations and Objections Hereto," *International Atomic Energy Agency*, March 5, 2021, http://www-legacy.iaea.org/Publications/Documents/Conventions/cppnm_reserv.pdf.

with the IAEA's definition of nuclear security.[6] On the advice of the Government of Pakistan, the Pakistan Nuclear Regulatory Authority (PNRA) initiated the Nuclear Security Action Plan (NSAP) project in July 2006 with the assistance of the IAEA to cover the existing gaps in nuclear security such as security upgradation of the sites, border management, and emergency response. NSAP developed a sustainable system in nuclear security with the established response and recovery capabilities, integrated with national laws, regulations, and procedures.[7] The NSAP project not only enhanced the physical protection of nuclear materials and facilities, but also developed systems for the security of radioactive sources, combatting illicit trafficking, emergency response, and training. Pakistan's nuclear security measures were acknowledged and appreciated by the IAEA.[8] The nuclear security summit process built a new momentum for the ratification and entry into force of the amended CPPNM.

At the 2014 Nuclear Security Summit, the Prime minister of Pakistan announced that it was considering ratifying the 2005 Amendment to the CPPNM and conducting a "review to meet its various requirements."[9] The relevant organizations within the National Command Authority reviewed the existing status of physical protection systems in place, assessed the need for additional measures, and chalked out a plan to fulfill those added requirements of the amended CPPNM. During those deliberations, it was observed that Pakistan was already fulfilling most of the technical requirements of the amendment. However, it was required to formalize the existing measures and review the regulatory framework to add the missing elements such as regulations and guides.

Additional Requirements of the CPPNM Amendment

The original CPPNM covered the physical protection of nuclear material during international transport, whereas the amended CPPNM has a broader scope and coverage.[10] Its role has expanded into the following three areas:

1. **Scope:** Physical protection requirements have expanded to include nuclear facilities and nuclear material in domestic use, storage, and transport.
2. **Offenses:** With the expanded coverage of the convention, the scope of offenses has also expanded to cover the theft of nuclear material as well as the smuggling of nuclear material and the actual or threatened sabotage of nuclear facilities. It also requires the state to minimize the radiological impacts of sabotage and to prevent and combat related offenses.

---

[6] The IAEA defines nuclear security as "the prevention of, detection of, and response to, criminal or intentional unauthorized acts involving or directed at nuclear material, other radioactive material, associated facilities, or associated activities" For further definitions see: IAEA, "IAEA Nuclear Security Glossary: Terminology used in IAEA Nuclear Security Guidance," August 2020, accessed October 6, 2021, https://www.iaea.org/sites/default/files/21/06/nuclear_security_glossary_august_2020.pdf.

[7] Khaliq, M. "Pakistan's Nuclear Security Action Plan," International Atomic Energy Agency, 2009, https://inis.iaea.org/search/search.aspx?orig_q=RN:41011707.

[8] Irfan Haider, "IAEA Praises Pakistan's Nuclear Security Record," *Dawn*, September 27, 2015. https://www.dawn.com/news/1209311.

[9] Mateen Haider, "Pakistan for Global Efforts Against Nuclear Terrorism," *Dawn*, March 24, 2014. https://www.dawn.com/news/1095296.

[10] For the original CPPNM see, International Atomic Energy Agency, "The Convention on the Physical Protection of Nuclear Material," May 1980. https://www.iaea.org/sites/default/files/ infcirc274r1.pdf. For the amended CPPNM see, International Atomic Energy Agency, "Amendment to the Convention on the Physical Protection of Nuclear Material, INFCIRC/247/Rev.1/Mod.1," May 9, 2016, https://www.iaea.org/sites/default/files/infcirc274r1m1.pdf.

3. **International Cooperation:** The amended CPPNM requires the states to expand the scope of cooperation for locating and recovering stolen or smuggled nuclear material. It requires the states to exchange information with each other and the agency and other relevant organizations in case of theft, robbery, and unlawful seizure of nuclear material or credible threat thereof, aiming to recover and protect the material.

Pakistan under the amended CPPNM

Pakistan has made significant progress in its nuclear security initiatives and has received positive feedback from the IAEA for its nuclear security measures.[11] However, with the expansion of the civilian nuclear program and additional obligations from the amended CPPNM, Pakistan must further streamline its efforts to meet international requirements. This will also be helpful in dealing with evolving nature of design basis threats.

The additional requirements of the amended CPPNM broadly fall in the category of administrative, regulatory and legal measures, and international cooperation. To fulfill these requirements, various relevant entities, such as the operator, regulator, and law enforcement agencies, must undertake additional technical, legal, and administrative measures. The following sections will explain these requirements in relevance to Pakistan to determine how Islamabad is faring against the requirements of the amended CPPNM, and what additional measures it needs to undertake to fulfill these requirements in totality.

Administrative and Regulatory Framework

The amended CPPNM requires states to "establish, implement and maintain an appropriate physical protection regime" in the country.[12] The regime would involve various organizations with defined roles and responsibilities. In that context, administrative measures are a prerequisite for identifying these roles and responsibilities in the physical protection process, such as those of the state, licensee, and the regulator.

In Pakistan, the National Command Authority is responsible for establishing a physical protection regime within the state. The PNRA, the national nuclear regulator, is the national contact point for the CPPNM and its amendment. It is responsible for developing the legislative and regulatory framework to ensure the physical protection of nuclear materials and facilities, whereas the Pakistan Atomic Energy Agency is responsible for implementing physical protection measures for nuclear materials and facilities.

The PNRA's mandate is derived from its ordinance (III of 2001) and is declared as the national regulatory body responsible to ensure physical protection of nuclear material and facilities in Pakistan.[13] The requirements of this section are covered in PNRA Regulations PAK/925 as objectives of the physical protection system (Clause 3, 24, 28). However, the PNRA's relationship with other bodies responsible for overall nuclear

[11] APP, "IAEA Chief Praises Pakistan's 'Impressive' Nuclear Security Record," *Express Tribune*, September 27, 2015. https://tribune.com.pk/story/963260/iaea-chief-praises-pakistans-impressive-nuclear-security-record.

[12] Anthony Wetherall and Vincent Fournier, "Key Nuclear Security Agreement to Enter Into Force on 8 May," International Atomic Energy Agency (IAEA), April 8, 2016. https://www.iaea.org/newscenter/news/key-nuclear-security-agreement-to-enter-into-force-on-8-may.

[13] Government of Pakistan: Ministry of Law, Justice, Human Rights and Parliamentary Affairs, "The Gazette of Pakistan: Acts, Ordinances, President's Orders and Regulations," January 22, 2001 (amendment June 27, 2012), https://www.pnra.org/upload/legal_basis/Ordinance%202001(Amennded).pdf.

security in the country needs to be clearly defined as required by the amended CPPNM.[14] This is essential because the Fundamental Principle D of the amended CPPNM requires the designation of a competent authority which is responsible for the implementation of the legislative and regulatory framework, and is "provided with adequate authority, competence, financial and human resources to fulfill its assigned responsibilities."[15] While the PNRA is the competent authority for the regulatory framework, the competent authority(s) for other areas need to be designated clearly.

Samuel Kubani/AFP via Getty Images

The amended CPPNM requires regular national threat assessment and development of Design Basis Threat (DBT). In Pakistan, the NCA with input from other relevant bodies is responsible for conducting the national threat assessment. The DBT is a regulatory tool for planning, designing, and evaluating a physical protection system. The roles and responsibilities of various organizations need to be clearly defined as outlined in the Nuclear Security Series No 13 para 3.35. Similarly, it is also important to set a defined timetable for the review of the DBT.

There is also a need to improve safety and security interface. The PNRA's mandate is to regulate nuclear security from a safety perspective. It has adopted a systematic approach and methodology to deal with the interface of nuclear safety and nuclear security such as unified licensing process; conducting joint safety and security inspections; centralized emergency coordination; rotation policy for employees; transparency and confidentiality of information; modification management; human resource development; safety and security cultures assessment, etc. However, that interface needs to be improved.[16] This is also important from a security culture point of view, which is an important requirement of the amended CPPNM. While PAK-925 covers security culture, there is no document outlining the importance and necessity of a safety and security culture interface.

[14] "Pakistan's Nuclear Security Regime."

[15] "Amendment to the Convention on the Physical Protection of Nuclear Materials," 4.

[16] Tufail Ahmad, "Regulatory Approach for Development and Implementation of Safety-Security Interface," International Atomic Energy Agency (IAEA), https://conferences.iaea.org/event/181/contributions/15327/.

Additionally, Pakistan focuses on nuclear material accounting and control (NMAC) only from a safeguards perspective, but the nuclear security series 13 (para 3.36) additionally stresses the importance of NMAC for nuclear security. This aspect could be included in the PNRA mandate from a physical security perspective. This aspect has been further emphasized in NNS NO 25-G on "Use of Nuclear Material Accounting and Control for Nuclear Security purposes at Facilities" as it underlines the importance of NMAC systems for nuclear security purposes, particularly against insider threats.

Legal Measures

The major development in the legal sphere is the issuance of long-pending regulation on "Physical Protection of Nuclear Material and Nuclear Installations—(PAK/925)" published on July 12, 2019, following the ratification of the CPPNM amendment.[17] With the issuance of this primary technical regulation, major aspects of additional physical protection measures such as nuclear facilities, material in domestic transport, etc., have been covered. Many of the Fundamental Principles in the amended CPPNM, such as security culture, evaluation of threat, graded approach, defense in-depth, quality assurance, and contingency plans, are covered under the PAK/925. Thus, PAK/925 provides the legal basis for the IAEA's "Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Rev.5)" and the technical obligations of CPPNM.

Besides the issuance of relevant regulations, an important second step is the publication of associated regulatory guides that are now in the process of development. These regulatory guides serve as an operating procedure and help the operators to implement relevant regulations. Following the issuance of regulation PAK/925, PNRA has issued the regulatory guide on Format and Content of Physical Protection Plan for Radioactive Sources (PNRARG-926.01). The regulatory guide on Implementation of Access Control System (ACS) measures at Nuclear Installations is under process.

The major technical step resulting from these regulatory improvements was the upgradation of physical protection measures in and around existing and under-construction new nuclear power plants. PNRA's future inspections and issuance/renewal of licenses will be based on compliance of the operators with the new regulations. On ground, these measures have resulted in various upgrades; e.g. physical protection upgrades at Karachi Nuclear Power Plant Unit 1 that were initiated in 2019, are now close to completion with the assistance of the IAEA.[18] Updated physical security of the new K-series plants such as K-1 and K-2 were made part of the construction agreement with China.[19] The C-series Nuclear Power Plants (i.e., C-1, C-2, C-3 & C-4) located at the Chashma site have inbuilt enhanced physical security features such as security by design which is based on additional safety features in the nuclear power plant identified through probabilistic safety assessments that can reduce the possibility of high radiological consequences. This, in turn, helps identify vital areas and their physical protection measures as an additional layer of protection e.g., double containment of the core is one such important feature that has been incorporated in the newly built nuclear power plants in Pakistan.

[17] Government of Pakistan, "The Gazette of Pakistan: Pakistan Nuclear Regulatory Authority," April 20, 2019. https://www.pnra.org/upload/legal_basis/regulations/PAK-925.pdf.

[18] Pakistan Nuclear Regulatory Authority, "Annual Report," 2019. https://www.pnra.org/upload/pnrarpt/PNRA%20Report%202019.pdf.

[19] Asma Khalid, "China-Pakistan Nuclear Energy Cooperation: History and Key Debates," *South Asian Voices*, February 12, 2020. https://southasianvoices.org/china-pakistan-nuclear-energy-cooperation/.

However, there is less clarity on the domestic transport of nuclear material for the K-1, which uses domestic natural uranium as a fuel. The NCA is responsible for developing a mechanism in coordination with the PNRA and licensees for the physical protection of nuclear materials during national transport. The scope of the PNRA ordinance covers the complete fuel cycle, but PAK-925 does not cover the entire fuel cycle and focuses on nuclear facilities only. There is a separate regulation on transport (PAK/916), but in its current form, it does address physical protection measures for domestic material during domestic transport.[20] Nonetheless, since it is under revision, it is important to highlight that the revised regulation should cover this gap.

Most of the offenses added into the CPPNM (amended) such as theft and smuggling of nuclear material and the actual or threatened sabotage of nuclear facilities are covered by the NCA Act and PNRA ordinance. The PNRA Ordinance has a broader scope, and it applies to any person committing an offense, i.e., both the licensee and non-licensee as explained in Section 44 (Offences) of the ordinance. Pakistan, as required by the IAEA also needs to share information regarding laws and regulations adopted to implement the convention.

International Cooperation

The PNRA is the focal point for cooperation with the IAEA, regulatory bodies of other countries, and other international organizations for exchanging regulatory information related to nuclear safety and security. The amended CPPNM encourages the member states to exchange information with each other and the agency in case of theft, robbery, and unlawful seizure of nuclear material. This cooperation is anticipated in case of an event and decision about the nature and level of any cooperation will be decided and determined by the National Command Authority in Pakistan. The level of cooperation can be preventive and proactive and may range from information sharing among member states, border controls, joint investigations of the event, etc. Following the ratification of the amended CPPNM, Pakistan has joined the Nuclear Security Contact Group (NSCG) in 2019 that serves as a platform to develop a strong and sustainable comprehensive global nuclear security architecture.[21] This platform can be used to strengthen and streamline international cooperation in case of a nuclear security incident.

Way Forward

Physical protection of nuclear material and nuclear facilities is one of the most important aspects of the overall nuclear security arrangement. It is, however, crucial to understand that nuclear security and physical protection is not a goal but a process that should continue to evolve incrementally. Therefore, it is critical to do regular analysis on the gaps in physical security and how any gaps are being addressed.

Article 16.1 of the original and amended Conventions provided for a mandated review conference five years after it entered into force. There is also a provision for additional review conference (article 16.2) if majority states vote in favor. States may use the review conference platform to assess the conventions' implementation and efficacy. The first and only review conference was held on September 29, 1992. That review conference did not decide in favor of additional review conferences. With the amendment, the clause of

[20] Government of Pakistan, "The Gazette of Pakistan: Pakistan Nuclear Regulatory Authority Notification," April 20th, 2007. https://pnra.org/upload/legal_basis/Pak-916.pdf.

[21] Nuclear Security Contact Group, "2019 Convener," http://www.nscontactgroup.org/.

review conference has become active again after completing five years of its entry into force in 2020.[22] The IAEA Secretariat has already held an informal meeting of CPPNM Parties in 2018 for a potential review conference in 2021.

To prepare for a potential review conference in 2021, Pakistan may prepare a report on its activities. Besides that, at the International Conference on Nuclear Security: Sustaining and Strengthening Efforts in February 2020, Pakistan announced its intention to host an International Physical Protection Advisory Service (IPPAS) Mission and accession to the International Convention on Suppression of Acts of Nuclear Terrorism (ICSANT).[23] This is a major undertaking and would require additional work and commitments. A three-step approach may be followed to assess the gaps, cover them in a timely manner, and prepare for an international peer review.

- **Self–appraisal**: Firstly, Pakistan may have a dispassionate introspective analysis to find the gaps and potential vulnerabilities internally.
- **Engaging IAEA through workshop or training course:** As the next step, Pakistan may consider requesting the IAEA to offer a workshop or training course on International Physical Protection Advisory Service (IPPAS)to begin with. The workshop will help identify the IPPAS requirements and how to address them.
- **Inviting an IPPAS mission:** Inviting an IPPAS mission i.e., a group of technical experts assessing country's physical protection compliance against international standards, will certainly give a boost to the level of confidence. Pakistan may start with a facility-level review and can assimilate those lessons in its other facilities as well.

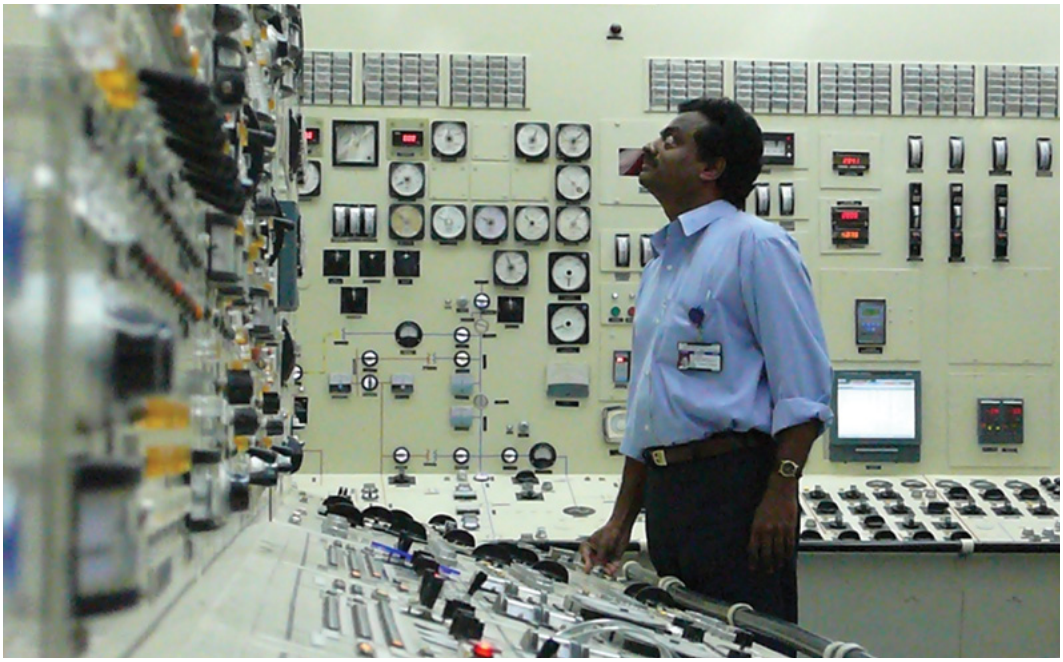
Conclusion

Given the evolving nature of threats in the region and an expanding nuclear power program, Pakistan has paid great attention to ensuring that its nuclear program is fail-safe and meets the international standards of safety and security. Ratification of the amended CPPNM was a manifestation of the country's undiminished focus on nuclear security objectives and desire to comply with international standards. The ratification enabled Pakistan to feature as the "most improved country" on the National Threat Initiative Nuclear Security Index report of 2020.[24] However, the overall score requires further improvement through better information sharing and communication. Hosting an IPPAS mission, even at a facility level, as a next step will not only help bridge the gaps but tremendously boost international confidence in Pakistan's nuclear security architecture.

[22] Australian Government, "The Review Conference for the Amended Convention on the Physical Protection of Nuclear Materials," in *Australian Safeguards and Non-Proliferation Office, Annual Report 2019-20*, 2020. https://www.dfat.gov.au/publications/international-relations/asno-annual-report-2019-20/report/html/section-2-2.html#footnote-5.

[23] International Atomic Energy Agency, "International Conference on Nuclear Security: Sustaining and Strengthening Efforts," (Vienna: February 10-14, 2020). https://www.iaea.org/sites/default/files/20/02/cn-278-pakistan.pdf

[24] Nuclear Threat Index, "Losing Focus in a Disordered World: The NTI Security Index," July 2020. https://www.ntiindex.org/wp-content/uploads/2020/07/2020_NTI-Index_Report_Final.pdf.



IAEA Image Bank via Flickr

3. CAN INDIA ADDRESS THE GROWING CYBERSECURITY CHALLENGES IN THE NUCLEAR DOMAIN?

By Pulkit Mohan

Across the world, cybersecurity architecture is becoming more complex and increasingly requiring advanced safety mechanisms to protect against system vulnerabilities and potential crises. Cyber threats are one of the greatest challenges in terms of security. This is particularly crucial in the case of nuclear systems as cyber infiltration can render safety and security mechanisms ineffective. This is no different in the case of India, as the country has an extensive and growing nuclear program. Over the years, countries, including India have heavily invested in building robust physical protection mechanisms in the nuclear sector and this has made the likelihood of a cyber or blended attack more likely given the rapid technological advancements in the field. As nuclear infrastructure becomes increasingly more integrated with cyber technologies, the risks of its hacking, disruption, and potential for sabotage also increase. The adversarial goal for any cyberattack is to exploit a system's vulnerabilities and then control, execute, and maintain a presence. Cyberattacks may result in theft of nuclear/radioactive materials, radiation release due to malicious intent of adversaries, theft of sensitive information about nuclear facilities, reactor designs etc. Access to nuclear facilities through cyberattacks can result in direct physical access to the facility, materials and information which adds to challenges of interconnectedness of cyber and physical nuclear security. India's civilian

and military nuclear programs have varying security procedures with different priorities and levels of secrecy. However, given the sensitive nature of nuclear materials in general, cybersecurity must be an integral part of the country's nuclear security infrastructure.

To adequately address the cybersecurity challenges faced in the context of India's nuclear program, it is vital to analyze the current policy framework as well as identify vulnerabilities that the systems protecting the country's nuclear facilities may be susceptible to. Additionally, looking at notable incidents of cyber breaches at nuclear systems and the lessons learned would provide useful insights to avoid similar threats for India. India can also learn from best practices developed by countries leading the effort such as United States and Japan. Furthermore, engaging with international organizations such as the IAEA and relevant literature emerging from such institutions is essential to strengthen cybersecurity in nuclear systems. The growing cyber security challenges for India's nuclear facilities require a multi-faceted approach. As the Indian nuclear security and safety infrastructure incorporates cyber technologies, it is essential for policymakers and the industry to engage more deeply with international cyber security practices, collaborate on improving cyber-nuclear security mechanisms with like-minded countries and actively work on building a more robust cyber-nuclear security framework for the country.

The Cyber-Nuclear Security Nexus in India

Cybersecurity gained greater salience in India after the Snowden leaks in June 2013 revealed surveillance by the U.S. National Security Agency (NSA) on multiple countries including India.[1] Since the Snowden leaks and the release of its 2013 Cybersecurity Policy, India has taken steps toward improving its cybersecurity architecture and safeguards. Although cybersecurity does factor into India's nuclear security architecture, it can be argued that there is limited emphasis on building and strengthening the infrastructure to respond to the rapidly growing and evolving cyber threats. India's overall cybersecurity policy has remained inadequate in responding to the risks of cyberattacks and infiltration. Cyberattacks in India reportedly rose by 300 percent in 2020, and in February 2021, India made headlines after power outages across Mumbai in the summer of 2020 were linked to a possible hacking of its power grid by China at the onset of the Ladakh standoff.[2]

In 2013, the Indian government released a first-of-its-kind national cybersecurity policy. However, eight years later, this policy has yet to be updated.[3] Although India's Prime Minister Modi announced that there would be a new national policy outline in 2020 this policy has yet to be released.[4] Additionally, the fact that India's nuclear domain and

[1] Jason Burke, "NSA Spied on Indian Embassy an UN Mission, Edward Snowden Files Reveal," *The Guardian*, September 25, 2013. https://www.theguardian.com/world/2013/sep/25/nsa-surveillance-indian-embassy-un-mission.

[2] See Mayank Mohanti, "Cyberattacks in India Grew by 300% Due to Work From Home: How to Stay Safe," *Indian Times*, July 16, 2021, https://www.indiatimes.com/technology/news/cyberattacks-india-work-from-home-study-545062.html, and David E. Sanger and Emily Schmall, "China Appeared to Warn India: Push Too Hard and the Lights Could Go Out," *New York Times*, February 28, 2021. https://www.nytimes.com/2021/02/28/us/politics/china-india-hacking-electricity.html.

[3] Ministry of Communication and Information Technology, "National Cyber Security Policy—2013," July 2, 2013. https://www.meity.gov.in/sites/upload_files/dit/files/National%20Cyber%20Security%20Policy%20%281%29.pdf.

[4] Ananya Bhardwaj, "India to get new 'robust' cyber security policy soon, says PM Modi," *The Print*, August 15, 2020. https://theprint.in/india/india-to-get-new-robust-cyber-security-policy-soon-says-pm-modi/482356/.

its security architecture is shrouded in secrecy means that there is no explicit mention or focus on the nuclear domain in the 2013 policy. Like nuclear policies, cybersecurity practices remain under-discussed in the public domain. It would be disingenuous to suggest that India's nuclear policy does not have cybersecurity mechanisms in place that are involved in protecting its nuclear systems. India has a Defence Cyber Agency and a National Technical Research Organisation, which are responsible for mechanisms that work to counter cyber risks and threats to the country.[5] Additionally, India has Computer Emergency Response Teams that work with agencies such as the National Critical Information Infrastructure Protection Centre and the National Disaster Management Authority to protect critical cyber infrastructures. The National Cyber Coordination Centre (NCCC) is India's operational cybersecurity and e-surveillance agency, its main role is in screening communications metadata and coordinating intelligence collection among agencies. Further, India has a Computer & Information Security Advisory Group (CISAG) which is responsible "for conducting periodic audits on information systems as well as provide guidelines for countering cyberattacks and mitigating the impact on India's nuclear infrastructure."[6]

India has established several key agencies to counter the growing challenges on cybersecurity. However, the effectiveness of its cybersecurity policies in the nuclear domain lies with the ability to effectively incorporate cybersecurity, cyber infrastructure, and its operating agencies into the larger nuclear security framework. Efficient and effective cybersecurity mechanisms require cohesive inter-agency coordination to strengthen said mechanisms. It is also essential for government authorities to acknowledge, interact with, and evolve cybersecurity protocols and procedures regularly to reflect a rapidly changing security environment. An effective cybersecurity policy also requires clear demarcation of roles, responsibilities, and contingency plans for short and long-term implementation and altering based on circumstances and technological advancements. Additionally, and most importantly, a renewed emphasis on understanding cyber risks and acknowledging the importance of cyber-nuclear security is essential in the Indian context. To address the aforementioned challenges and requirements, a cyber-nuclear policy must take shape and clearly identify roles and responsibilities across agencies as well as create frameworks to address cyber risks and vulnerabilities, build resilience measures, and contribute to robust contingency planning.

The Dangers of Cyberattacks in the Nuclear Domain

Cyber threats in the nuclear domain present a unique challenge that require adaptive and sustainable mechanisms to mitigate the ever-changing risks. There are several instances of cyberattacks on nuclear systems that allow for countries like India to learn and better prepare the security infrastructure for the rising cyber threats in the nuclear domain.

The instance of cyber threats and attacks in Iran, particularly the 2010 Stuxnet attack on the country's Natanz uranium enrichment plant, highlight the dangers of

[5] Pulkit Mohan, "Ensuring Cyber Security in India's Nuclear Systems," *Observer Research Foundation*, October 15, 2020. https://www.orfonline.org/research/ensuring-cyber-security-in-indias-nuclear-systems/.

[6] Rajeswari Pillai Rajagopalan, "Nuclear Security in India," *Observer Research Foundation*, February 2015, https://www.orfonline.org/wp-content/uploads/2016/10/ORF_Monograph_Nuclear_Security.pdf. CERT-In works within Ministry of Electronics and Information Technology, NCIIPC is under NTRO and National Disaster Management Authority (NDMA) comes under the Ministry of Home Affairs. CISAG operates under the Department of Atomic Energy (DAE).

cyberattacks and cyber warfare for a country with nuclear systems.[7] Stuxnet emerged as an extremely sophisticated and dangerous malware and deeply impacted the security mechanisms of several countries. More recently, the attack on the Natanz facility in 2021, which targeted the industrial control systems and destroyed the power supply to centrifuges used to create enriched uranium, underscored the sophistication and capabilities of the cyber domain.[8] Keeping the political considerations and implications of these cyberattacks aside, the security implications for such breaches are worrying on their own. It would be in India's best interest to actively address the imminent risks, drawing from global incidents and using them to further strengthen the country's security mechanisms and improve or replace outdated and vulnerable cybersecurity technologies, whether it may be administrative computer networks (as witnessed by the Kudankulam incident) or security mechanisms that employ identified risky technologies at nuclear facilities.

Kudankulam Nuclear Power Plant (KKNPP) Units 1 and 2 at Kudankulam in Tirunelveli district of Tamil Nadu, India. Reetesh Chaurasia via Wikimedia Commons

As India's nuclear ambitions expand, so does the possibility of gaps and vulnerabilities emerging in the cyber domain. These vulnerabilities were most notably shown in the 2019 malware attack at the Kudankulum nuclear power plant in Tamil Nadu and on the Indian Space Research Organisation headquarters in Karnataka.[9] The cyber breach was an infection of a modification of a malware known as Dtrack, which has been used to attack financial institutions in India in the past and made by to the North Korea-linked

[7] David Kushner, "The Real Story of Stuxnet," *IEEE Spectrum*, February 26, 2013. https://spectrum.ieee.org/the-real-story-of-stuxnet#toggle-gdpr.

[8] Peter Beaumont, "Natanz 'sabotage' highlights Iran's vulnerability to cyber-attacks," *The Guardian*, April 12, 2021. https://www.theguardian.com/world/2021/apr/12/natanz-nuclear-facility-sabotage-iran-vulnerability-to-cyber-attacks.

[9] Debak Das, "An Indian Nuclear Power Plant Suffered a Cyberattack. Here's What you Need to Know," *The Washington Post*, November 4, 2019. https://www.washingtonpost.com/politics/2019/11/04/an-indian-nuclear-power-plant-suffered-cyberattack-heres-what-you-need-know/.

Lazarus group.[10] The incident is a prime example of why countries cannot and must not become complacent with their cyber-nuclear security infrastructure.

Fortunately, the malware was limited to the administrative systems.[11] The failure of the malware to permeate into the plant control or instrumentation is attributed to the preventive access tool known as air gaps. Air gaps refer to "computers or networks that are not connected directly to the internet or to any other computers that are connected to the internet."[12] However, while air gaps helped prevent a more severe breach in the Kundankulam incident, experts have noted that "many of the traditional methods of cyber defense at nuclear facilities—including firewalls, antivirus technology, and air gaps—are no longer enough to match today's dynamic threats."[13] After the incident, CISAG recommended measures for immediate and short-term implementation such as "hardening of internet and administrative intranet connectivity, restriction on removable media, blocking of websites & IPs which have been identified with malicious activity, etc."[14]

While it is reassuring to note that the critical nuclear system was not breached, the incident raises serious concerns about the vulnerabilities exposed in the attack and possibly lessens the already-limited confidence in nuclear power within the public. Short-term measures, although necessary, do little to increase the overall effectiveness of cybersecurity if not matched with larger longer-term policy changes. These short-terms measures, as recommended by CISAG, are important but reactive. A national cyber-nuclear policy can proactively increase resilience of nuclear infrastructure by updating traditional methods—such as air gaps and firewalls—into a more dynamic cyber-security strategy that engages with the rapidly evolving technology environment.

Cyber-Nuclear Security in the Global Context: Lessons and Recommendations for India

Cybersecurity is not just a national challenge. It impacts countries globally and therefore requires global solutions. In the nuclear context, it is imperative that similar, like-minded nations collaborate, exchange useful information, and share best practices to combat the rising threat of cyberattacks. There are several countries, like the United States and Japan, with highly advanced and robust cybersecurity systems in place for their nuclear systems. Such countries actively engage with the developments and advancements in the cyber domain in order to continuously build resilience measures and contingency planning to address the associated risks. Collaboration with such international actors would provide India with the opportunity to learn and incorporate the learnings and best practices into the context of the country's cyber-nuclear infrastructure.

In addition to collaborating with the aforementioned countries, with whom India has signed civil nuclear cooperation agreements, India can also collaborate with partners

[10] Jay Jay, "Lazarus Group's DTrack Malware Infect Indian Nuclear Power Plant," *Teiss*, October 31, 2019. https://www.teiss.co.uk/nuclear-power-plant-dtrack-malware/.

[11] Government of India, Nuclear Power Corporation of India Limited, "Press Release," October 30, 2019. https://npcil.nic.in/writereaddata/Orders/201910301237346960171News_30102019_01.pdf.

[12] Kim Zetter, "Hacker Lexicon: What Is an Air Gap?" *Wired*, December 8, 2014, https://www.wired.com/2014/12/hacker-lexicon-air-gap/.

[13] A Van Dine, "Outpacing Cyber Threats," Nuclear Threat Initiative, https://media.nti.org/documents/NTI_CyberThreats__FINAL.pdf.

[14] Rajya Sabha, "Starred Question No. 109," Government of India: Department of Atomic Energy, November 28, 2019, https://dae.gov.in/writereaddata/rssq109.pdf.

such as the United Kingdom and Russia to better equip its cyber-nuclear infrastructure.[15] These agreements cover several areas of cooperation such as exchange of information, expertise on reactor designs, nuclear safety etc. Given the increasing importance of cybersecurity in the current global nuclear context, India should extend collaboration through these agreements to the cyber-nuclear domain. This can be conducted through technology exchange, exchange of experts, information-sharing agreements, as well as joint exercises and workshops to better equip the security infrastructure at nuclear systems to counter cyber challenges.

Additionally, it would be worthwhile for India to engage more deeply with the private sector in the cyber domain. India has generally limited the involvement of the private sector in the nuclear domain. India's largely indigenously developed nuclear weapons program and nuclear fuel cycle capabilities for civilian use are wholly controlled by the government. Similarly, the nuclear safety and security framework of the country is entirely under governmental agencies. However, in the case of cybersecurity challenges specifically, there is a lot to learn and adapt into the cyber-nuclear security culture. Private actors—whether it is firms or individual actors—are consistently challenging the notions of cybersecurity due to both malicious and ethical intents. Bringing in industry experts from the field has been a part of cybersecurity policies for countries like the United Kingdom, and India should similarly incorporate their involvement into the country's cybersecurity policy.

Finally, the primary point of concern for India's nuclear systems in terms of cyber risks and threats remains the lack of importance given to a clear, concise, and robust policy framework. The lack of a cyber-nuclear policy for India exacerbates issues of vulnerability, lack of education and awareness as well as enhanced inter-agency coordination and response to cyber threats. Cyber threats are constantly evolving, and the dynamic nature of the cyber domain dictates the need for prioritization of cybersecurity in the nuclear security architecture. Cybersecurity requires similar levels of focus and interest within the nuclear domain as issues of insider threat and physical protection.

The Kudankulam incident brought in short-term measures to deal with the problems highlighted by the incident. However, it is imperative that a successful cybersecurity policy works to continually address cybersecurity challenges in a much more dynamic manner which works towards long-term sustainability of said policy to counter cyber risks. India's current cyber-nuclear set-up does not adequately accord importance to a larger policy framework in order to protect against cyber threats. In this regard, India's nuclear infrastructure, through a cyber-nuclear policy, must engage in periodic assessments of its cybersecurity mechanisms and its effectiveness in order to better equip nuclear infrastructure against these threats. Given the sensitive nature of nuclear materials and infrastructures, it is important to create policies that offer both short-term and long-term solutions and accommodate change with changing security needs and contexts. Further, collaboration with allies in the field is key opportunity for India to build, improve and evolve its ability to actively respond to emerging threats and risks that are an unavoidable part of the world.

[15] Pulkit Mohan and Pallav Agarwal, "India's Civil Nuclear Agreements: A New Dimension in India's Global Diplomacy," *Observer Research Foundation*, October 4, 2019. https://www.orfonline.org/research/india-civil-nuclear-agreements-new-dimension-india-global-diplomacy/.

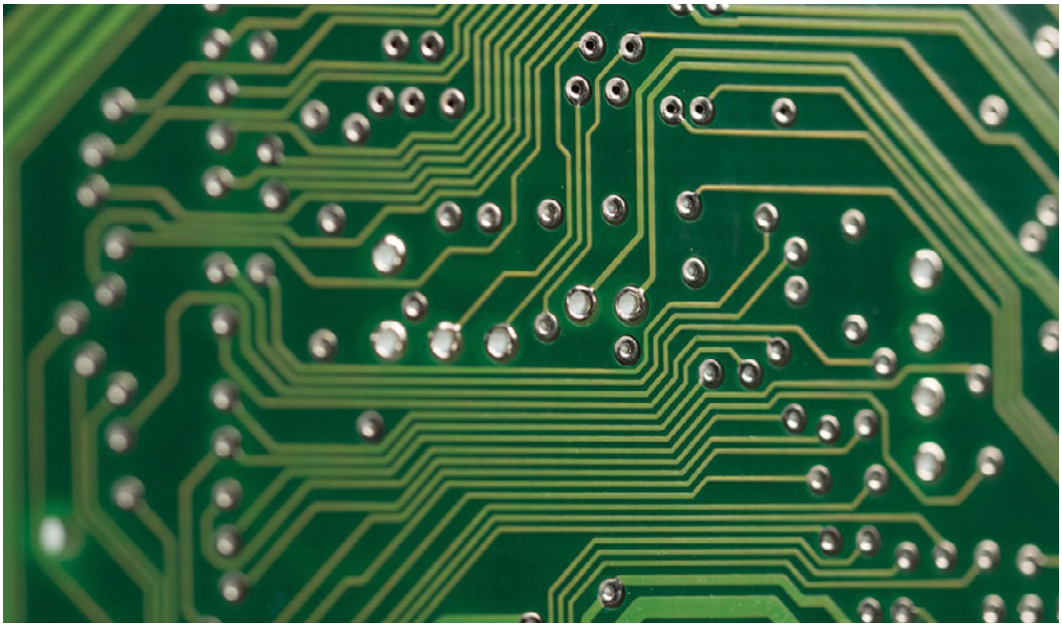


Image via Pixabay

4. BUILDING A BILATERAL FRAMEWORK FOR CYBERSECURITY IN SOUTH ASIA

By Palwasha Khan

In 2019, one of India's largest nuclear reactors located at Kudankulam suffered a malware attack that not only breached the plant's firewalls but also reportedly stole data and information.[1] Though only breaching the administrative network of the plant, and not as catastrophic as other malware attacks such as Stuxnet—the highly sophisticated computer worm most well-known for attacking nuclear centrifuges at Iran's Natanz facility—this attack posed major concerns to safety measures for nuclear installations around the world. While the attack was eventually attributed to a North Korea-based group, speculation and uncertainty underscored the challenges of pinpointing the source of cyberattacks as well as the potential for cyber threats to exacerbate existing tensions in the region.[2]

[1] Debak Das, "An Indian Nuclear Power Plant Suffered a Cyberattack. Here's What you Need to Know," *The Washington Post*, November 4, 2019. https://www.washingtonpost.com/politics/2019/11/04/an-indian-nuclear-power-plant-suffered-cyberattack-heres-what-you-need-know/.

[2] On the DPRK based group see, Harsh V. Pant and Kartik Bommakanti, "Decoding Motives Behind the Kundankulam Intrusion," *Observer Research Foundation*, November 25, 2019, on uncertainty see, Cherian Samuel and Munish Sharma, "Kundankulam: Once Incident, Many Facets," IDSA: Manohar Parrikar Institute for Defence Studies and Analyses, December 16, 2019. https://idsa.in/issuebrief/kudankulam-incident-cherian-munish-161219. On exacerbating threats see, Maj Gen P K Mallick, "Cyber Attack on Kundakulam Nuclear Power Plant: A Wake Up Call," *Vivekananda International Foundation*, December 2019, 27, and Shashi Tharoor, "Kundankulam is Over, But Are We Prepared for the Next Breach: Tharoor," *The Quint*, October 31, 2019. https://www.thequint.com/voices/opinion/kudankulam-cyber-attack-spy-pakistan-china#read-more.

The attack at Kudankulam brought to the forefront not only risks of economic sabotage or data theft from malicious actors, but also questions of India and Pakistan's vulnerabilities to state and non-state actors exploiting weak points in cyber infrastructure. For Pakistan and India these questions are essential in rethinking how they—jointly and independently—aim to address their national security concerns in the 21st century. Kudankulam represents a point in time where both Pakistan and India have a direct interaction with cyber vulnerabilities, which go beyond mere threats of hacking and have the potential the spillover into new security areas. While bilateralism between the two historic rivals will undoubtedly be difficult, as both states look to develop their nuclear energy portfolio and work to secure systems against cyber threats exploring a bilateral framework can be an important first step towards confidence-building measures (CBMs) that begin to address challenges for the future threat environment.

Features of the Cyber Domain

One of the unique features of cybersecurity is that the government's national security interests and the private sector's corporate interests may overlap in terms of fears of stolen data, information, or financial resources. An effective cybersecurity system for sensitive installations and their associated subsystems would closely merge corporate and national security interests. Cyber intrusions have the potential to cause panic and risk the theft and subsequent sale or leaking of sensitive information. Therefore, states are required to physically secure their facilities and protect against cyberattacks. As India and Pakistan move ahead with nuclear energy projects, signing agreements and continuing cooperation with their partners, both states will need to take measures to make sure these sites are secure.[3]

Cyber threats also open the door for potential new pathways of escalation as well as new risks of miscalculation or misperception.[4] For this reason, any form of cooperation that could serve as a confidence-building measure (CBM) between India and Pakistan in the cyber domain may be helpful in risk reduction or preemptive attribution in the event of a future cyberattack. The multiple cyberattacks and data breaches at nuclear facilities underscore the extent that accidental or intentional cyber breaches at nuclear facilities have become a new domain nuclear safety.[5] While international organizations like the International Atomic Energy Association (IAEA) have hosted training programs to enhance cybersecurity at nuclear facilities, India and Pakistan need to review their security regimes concerning nuclear power plants within their respective domestic security frameworks.[6]

---

[3] See Asma Khalid, "China-Pakistan Nuclear Energy Cooperation: History and Key Debates," *South Asian Voices*, February 12, 2020. https://southasianvoices.org/china-pakistan-nuclear-energy-cooperation/, and Aniruddh Mohan, "The Future of Nuclear Energy in India," *Observer Research Foundation*, August 9, 2016, https://www.orfonline.org/research/the-future-of-nuclear-energy-in-india/.

[4] Jason Healey and Robert Jervis, "The Escalation Inversion and Other Oddities of Situational Cyber Stability," *Texas National Security Review*, 3, no. 4. (Fall 2020), 30-53. http://dx.doi.org/10.26153/tsw/10962.

[5] See "Significant Cyber Incidents," Center for Strategic and International Studies, https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents, and "Cyber and Nuclear Security," Chatham House, https://www.chathamhouse.org/about-us/our-departments/international-security-programme/cyber-and-nuclear-security

[6] "IAEA Launches International Training Course on Protecting Nuclear Facilities from Cyber-Attacks," International Atomic Energy Agency, October 24, 2018, https://www.iaea.org/newscenter/pressreleases/iaea-launches-international-training-course-on-protecting-nuclear-facilities-from-cyber-attacks.

Pakistan and India have limited reasons to engage with each other owing to repeated confrontations over the past 50 years, however, as cyber becomes an increasingly important domain any steps towards trust or confidence-building may help mitigate future risks. With foreign technical assistance and partnerships, both Pakistan and India have laid the groundwork for more robust nuclear energy programs.[7] Pakistan and India also have some shared vulnerabilities. Despite significant improvement, both states still are susceptible to insider threats and cybersecurity risks. Illicit activities by non-state actors, weak insider threat prevention, and understanding cybersecurity risks are some of the domains where Pakistan and India could perform better. As highlighted by the Kundankulam incident, these vulnerabilities can be exploited beyond the scope of India-Pakistan's conventional rivalry. Pakistan and India should adopt a joint learning mechanism under the assistance of the IAEA training programs to understand the real-time risk of cybersecurity lapses within their security frameworks. As attribution is a core challenge of cyberattacks, and India and Pakistan may be more likely to attribute a cyberattack to the other due to their standing trust deficit, these training programs are also essential in outlining mutual understanding against non-attributable or delayed attribution from third-party activities that stand to harm both states' interests if successfully executed.

Cybersecurity Challenges to Nuclear Installations: Assessing Vulnerabilities

Civilian nuclear installations are both essential commercial establishments and sensitive strategic sites. Such installations are assisted by a complex matrix of services ranging from transmission of electricity, transportation of nuclear materials, and systems monitoring nuclear reactors. Housing such information requires investing resources in physical security and material transportation and addressing cyber-related commercial risks.[8] New domains of national security threats, such as terrorist organizations potentially targeting civilian facilities, commercial and industrial espionage, commercial theft, and inadvertent information breaches, pose substantial risks to the operability of nuclear installations. International organizations like the IAEA, World Association of Nuclear Operators (WANO), and the Rusatom Automated Control Systems have developed training programs to enhance and expand security measures on nuclear installations beyond traditional understanding. States looking to induct more nuclear power plants or manage existing platforms but lack the financial or technical capabilities to do so, require assisted understanding through international training programs and development of protocols to overcome such challenges. For Pakistan and India, learning from previous cyber-breaches can help preempt vulnerabilities before they can opt for expanding their nuclear power potential.

---

[7] See Shahzadi Tooba Hussain Syed, "Future of nuclear energy in Pakistan," *Foreign Policy News*, October 30, 2015, https://foreignpolicynews.org/2015/10/30/future-of-nuclear-energy-in-pakistan/, and "What is India's Nuclear Energy Future," *Electrical & Power Review*, May 9, 2017, https://www.eprmagazine.com/special-report/what-is-indias-nuclear-energy-future/

[8] See "How to Protect Nuclear Power Plants Against Cyber Attacks," *Chatham House*, https://www.chathamhouse.org/2019/08/how-protect-nuclear-power-plants-against-cyber-attacks, and "Transport of Radioactive Materials," *World Nuclear Association*, April 2021, https://www.world-nuclear.org/information-library/nuclear-fuel-cycle/transport-of-nuclear-materials/transport-of-radioactive-materials.aspx.

Department of Atomic Energy via Wikimedia Commons

In installing more reactors, Pakistan and India stand to face associated risks—such as waste disposal, avoiding civilian contamination, meltdowns and natural disasters, material safety, and security—and cyber vulnerabilities that will be a future cause for concern.[9] Despite China and the United States assisting Pakistan and India, respectively, both recipient states' cybersecurity infrastructure is nascent. Pakistan and India have only announced their cybersecurity policies and both policies can do more to fully address the cybersecurity threats at nuclear facilities.[10] Their policy drafts either generalize nuclear installation security with respect to cybersecurity measures or overlook this dimension.

A further challenge with cybersecurity threats is determining the proper response—particularly to an attack that is difficult to attribute. If a cyberattack is countered by an inappropriate or disproportionate response; this may raise questions on the effectiveness of national security systems in responding to threats or create more uncertainty for future exploitation.[11] Like all other global nuclear facilities, Pakistan and India are also prone to a similar scope of cybersecurity vulnerabilities: theft or financial exploitation, espionage or commercial exploitation, and sabotage or adversarial exploitation. With non-state actor and traditional security concerns operating simultaneously in both countries, cybersecurity vulnerabilities in Pakistan and India require a mutual appraisal of their national security architecture.

[9] See APP "PAEC to enhance nuclear energy share to 8,800 MW by 2030," *The Nation*, June 12, 2020, https://nation.com.pk/12-Jun-2020/paec-to-enhance-nuclear-energy-share-to-8-800-mw-by-2030., and "India Plans Expansion of Nuclear Fleet, Says DEA Chairman," *World Nuclear News*, October 21, 2019. https://www.world-nuclear-news.org/Articles/India-plans-expansion-of-nuclear-fleet-says-DEA-c.

[10] See Ministry of Communications and Information Technology, "National Cyber Security Policy—2013," July 2, 2013, https://www.meity.gov.in/sites/upload_files/dit/files/National%20Cyber%20Security%20Policy%20%281%29.pdf, and Ministry of Information Technology & Telecommunication, "National Cyber Security Policy 2021," Government of Pakistan, January 25, 2021, https://moitt.gov.pk/SiteImage/Misc/files/National%20Cyber%20Security%20Policy%202021%20Consultation%20Draft(1).pdf.

[11] Daniele Hadi Irandoost,"Cybersecurity: A National Security Issue?" *E-International Relations*, May 3, 2018. https://www.e-ir.info/2018/05/03/cybersecurity-a-national-security-issue/.

Framework for Cooperation in South Asia: The Case for Assisted National Security

The idea that Pakistan and India cannot or will not venture beyond their traditional competitiveness is a major impediment in their ability to fully rationalize the impact of cybersecurity vulnerabilities. As the Kudankulam incident highlights, cyber threats to nuclear energy sites are a threat that South Asia must contend with. Given that both states face similar challenges—such as non-state entities conducting nefarious cyber operations—a bilateral, cooperative understanding of nuclear cybersecurity concerns is a mutual interest.[12] Though Pakistan has not suffered reported cyberattacks on nuclear installations, it has endured a significant number of cyber-related incidents ranging from ransomware hacking of large electricity distribution systems, snooping against secure lines of communication to attacks on financial data centers.[13] Since both countries are in the process of improving their cybersecurity frameworks, Pakistan and India should opt for starting a joint cybersecurity initiative.

Pakistan and India have historically engaged in CBMs to reduce traditional security challenges. Such CBMs, however, have not ventured beyond their mutual arrangement of information sharing through Director-General Military Operations which forms their basic information sharing consistently to static ends. India and Pakistan's reliance on Track-II or third-party assisted diplomacy has been more pronounced than conventional bilateralism. However, unlike traditional security domains, cybersecurity vulnerabilities — particularly on nonmilitary installations—present the unique challenge of non- attributable attacks. Traditional bilateralism might not work effectively against cybersecurity threats since such intrusions, attacks, or breaches could likely be non-attributable until extensive investigations report otherwise.

That vulnerabilities are inadequately addressed by both states is in itself an opportunity for India and Pakistan to examine a mechanism to address the issues bilaterally. Previous engagements have mostly attempted to settle strategic issues and were met by rigidness and inflexibility due to each side's national concerns. However, cybersecurity and nonattributable incidents offer a commercial and industrial approach to non-traditional security mechanisms. Cybersecurity focuses on risk reduction and risk aversion, as well as the virtual security of civilian installations that can be bilaterally maintained without influencing each state's national security apparatus by focusing on common threats or vulnerabilities. A bilateral cooperative framework for cybersecurity not only accommodates commercial and industrial security but also stands to prevent traditional security fractures that could be caused by non-traditional, non-attributable incidents.

---

[12] See "Pakistan Army Identifies Major Cyber Attack by India Targeting Mobile Phones of Govt, Military Officials," *The News*, August 12, 2020, https://www.thenews.com.pk/latest/699597-pakistan-army-identifies-major-cyber-attack-by-india-targeting-mobile-phones-of-govt-military-officials, and Eduard Kovacs, "Pakistan APT Group Targets Indian Government," *Security Week*, June 3, 2016, https://www.securityweek.com/pakistan-apt-group-targets-indian-government.

[13] Muhammad Abdul Qadeer, "The Cyber Threat Facing Pakistan," *The Diplomat*, June 6, 2020, https://thediplomat.com/2020/06/the-cyber-threat-facing-pakistan/, and "National Bank of Pakistan gets hit by a cyberattack reports no financial loss or data breach," *Wion News*, October 31, 2021. https://www.wionews.com/south-asia/national-bank-of-pakistan-gets-hit-by-cyberattack-reports-no-financial-loss-or-data-breach-425446, Deeba Ahemd, "Pakistani Power Supplier K-Electric hit by NetWalker Ransomware Attack," *HackRead*, September 9, 2020, https://www.hackread.com/netwalker-ransomware-hits-pakistan-power-supplier-k-electric/, and "Pegasus Snooping: Pakistan Probes whether PM Khan's Phone Hacked," *Al Jazeera*, July 20, 2021, https://www.aljazeera.com/news/2021/7/20/pegasus-snooping-pakistan-imran-khan-phone-hacked, and Syed Talat Hussain, "What Caused Pakistan's Largest Data Centre Attack?" *Gulf News*, August 24, 2021, https://gulfnews.com/opinion/op-eds/what-caused-pakistans-largest-data-centre-attack-1.81758508.

The first level of such a cooperative arrangement can focus on collective learning. Producing a joint academic and technological analysis of cyber-related issues will bolster both countries' understanding of shared concerns. Following the American model designed under the Cybersecurity and Infrastructure Security Agency (CISA), both states can augment their current disaster management architecture to induct separate agencies to address specific challenges to nuclear cybersecurity.[14] Not only would such an arrangement be out of the ambit of India and Pakistan's traditional security framework—which is dominated by a bilateral adversarial environment—but it would also provide international stakeholders a means to offer assistance similar to that extended by WANO mission support programs. A joint-understanding approach focused on academic discourse has the potential to improve risk assessment and gaps in current frameworks without upsetting both countries' national interests. A potential initiative in assisted training programs also allows international stakeholders to combine IAEA assistance and training programs with other possible investors in nuclear technology to increase learning in cybersecurity, computer security, data protection, firewalls and breach incidents, malware, IP spoofing, or inadvertent breaches and related incidents. An academic discussion is a possible first step as it does not require formal state sanction—a challenge in South Asia's security environment—and could provide a base for international involvement, enhance existing literature on the subject, as well as improving confidence between both countries.

The second level would focus on bringing civilian nuclear enterprises to act as Track-II diplomacy mediums. Such a medium will allow both parties to highlight risks posed by nuclear cyberattacks and cyber-related incidents while creating a dynamic platform to continue the conversation over time. Bilateral CBMs, in the eventuality of civilian nuclear enterprises acting as mediums, would address deficiencies in cybersecurity policies of both states from a non-strategic and commercial angle. Cyber CBMs can be three-pronged. First, addressing the commercial necessity of installing bilateral understanding of cyber vulnerabilities. Second, managing standalone and comparative fallout of such an incident on human security aspects.[15] Third, periodically designing and sharing information on possible domestic and international vulnerabilities to such installations from cyberspace. The expansion of nuclear energy projects in India and Pakistan stands to eventually allow the industrial or commercial interests of institutions like the Nuclear Power Corporation of India Limited and the Pakistan Atomic Energy Commission to opt for measures beyond the current ambit of Pakistan Nuclear Regulatory Authority or Indian Atomic Energy Regulatory Board.

The third level of cooperation would involve a joint task force on cyberspace to detect and avert civilian installation threats. This joint task force could be further strengthened if both states provide it with institutional backing, as they have done with the Indus Water Commission to address the issues of water distribution. In the case of the Indus Water Commission, both countries were able to agree that there were performance deficiencies and engage in a joint initiative addressing mutual vulnerabilities. This joint task force would focus on threat assessment concerning cybersecurity vulnerabilities based Pakistan and India's learning on these issues thus far. Given that cyber threats are often anonymous or inadvertent, or focused

[14] "CISA Global: Cybersecurity and Infrastructure Security Agency," February 2021. https://www.cisa.gov/sites/default/files/publications/CISA%20Global_2.1.21_508.pdf.

[15] "Defending Nuclear Power Plants Against a Growing Cyber Threat," *Medium: E-Tech*, February 3, 2020. https://medium.com/e-tech/defending-nuclear-power-plants-against-a-growing-cyber-threat-68ac8d6009c.

on commercial or financial gains, attacks on civilian installations are unlikely to trigger a national security response.[16] With material safety and cybersecurity being one of the most crucial factors in indexing compliance to international safety standards, however, such incidents require a deeper appraisal of security concerns.[17] Acceptance of areas of potential improvement may be an avenue for bilateral learning between Pakistan and India towards cyber-vulnerabilities of nuclear facilities. International organization like the IAEA can assist in any bilateral initiatives. Both India and Pakistan can further enhance this three-pronged approach—collective learning, Track II dialogue, and a joint task force—by using it to reflect the dynamic nature of the ever-changing cybersecurity landscape. Such measures would also contribute to a better understanding of the relationship between cyberspace threat perceptions, nontraditional national security, and vulnerabilities to nuclear installations in South Asia.

Pakistan and India cannot afford nuclear disasters which threaten human security, financial capacity, and may pose escalatory risks. With both states experiencing ransomware attacks, hacking, probing and snooping incidents on sensitive information and risks of theft of commercial and essential data from sensitive installations, their cooperative understanding of the issue should be a top consideration. Both states have improved compliance with international safety standards but still their progress is slow with respect to cybersecurity and insider threat perceptions, a common ground that can be constructed to engage in bilateral—albeit assisted—learning of this threat matrix. Cybersecurity and its impact on national security is significant and it stands to present itself more robustly in comparison to traditional rivalries. Pakistan and India need a working solution where they understand and eventually strive to prevent vulnerabilities that can aggravate challenges to their plans for future nuclear energy production.

[16] Lysa Myers, "Inadvertent Insider Threats Present a Unique Challenge to Organizations," *Security Intelligence*, https://securityintelligence.com/articles/inadvertent-insider-threats-present-a-unique-challenge-to-organizations/, and "Cyber Security Market Soaring as Threats Target Commercial and Govt Organizations," Help Net Security, August 26, 2021, https://www.helpnetsecurity.com/2021/08/26/cybersecurity-market-threats/.

[17] Nuclear Threat Initiative, "About the NTI Index and the Radioactive Source Security Assessment," https://www.ntiindex.org/about-the-nti-index/.

Mahinda Rajapaksa via Flickr

5. THE NEED FOR A REGIONAL MECHANISM FOR NUCLEAR SECURITY IN SOUTH ASIA

By Md. Shafiqul Islam

The growth of nuclear power plants and radiological facilities and activities is increasing rapidly in South Asia. Besides the two nuclear giants, India and Pakistan, smaller countries are exploring nuclear energy options—Bangladesh, for instance, is currently constructing two nuclear power reactors.[1] Sri Lanka has also approved exploring nuclear energy options for power development, while Nepal has invested in nuclear education and passed a bill related to managing nuclear resources after the discovery of high-grade uranium deposits.[2] Along with being home to two nuclear weapons states, South Asia also faces threats from multiple non-state actors and extremist groups—which may rise with the U.S. departure from Afghanistan.[3] Numerous deadly terrorist attacks

[1] "Nuclear Power in Bangladesh," World Nuclear Association, October 2021, https://world-nuclear.org/information-library/country-profiles/countries-a-f/bangladesh.aspx.

[2] Government of Sri Lanka, Ministry of Power, "Nuclear Energy for Sri Lanka," September 21, 2010, http://powermin.gov.lk/english/?p=1949, and Omar Yusuf, "Expanding the Reach of Nuclear Education in Nepal by Training-the-Trainers," International Atomic Energy Agency (IAEA), April 27, 2020, https://www.iaea.org/newscenter/news/expanding-the-reach-of-nuclear-education-in-nepal-by-training-the-trainers, and Rastriya Samarchar Samiti, "Manage Uranium Mines Properly," *The Himalayan,* August 13, 2020, https://thehimalayantimes.com/nepal/manage-uranium-mines-properly.

[3] Kabir Taneja and Mohammed Sinan Siyech, "Terrorism in South Asia After the Fall of Afghanistan," *War on the Rocks*, August 23, 2021, https://warontherocks.com/2021/08/terrorism-in-south-asia-after-the-fall-of-afghanistan/.

in India, Pakistan, Afghanistan, and Bangladesh, in addition to regular features of illicit trafficking of humans, drugs, and arms across the borders demonstrate the vulnerabilities of the security system in this region. With the International Atomic Energy Agency (IAEA) documenting a high number of illegal activities involving nuclear and radiological materials globally, it is not an exaggeration to consider the possibility of terrorist attacks targeting nuclear and radiological facilities in South Asia.[4] As a region that deals with multiple security threats that cross borders, including trafficking and non-state actors, it is imperative to question the effectiveness of the South Asian nuclear security order and revisit existing mechanisms for regional cooperation.

The growth of nuclear energy in the context of the vulnerable security situation, mainly aggravated by extremism and illicit trafficking, compels observers to re-evaluate tools for addressing non-traditional security threats to nuclear materials, including illicit trafficking and extremism, which requires multifaceted national, regional, and international efforts. There are currently no existing regional mechanisms working specifically on nuclear security, however, there are multiple regional frameworks which have the potential to be a starting point for dialogue on cross-border threats that could also pose a risk to nuclear sites—such as targeting transit of illicit materials or cooperation on combating threats from non-state actors. As reported in Table One, there are seven main regional and subregional tools operating in South Asia. This includes four regional tools: The South Asian Association for Regional Cooperation (SAARC), the South Asian Free Trade Area (SAFTA), the South Asian Network for Sustainable Development Goals (SANS), and the South Asia Forum (SAF) and the three subregional tools: the Bangladesh-Bhutan-India-Nepal (BBIN) initiative, the Bay of Bengal Initiative for Multi-Sectoral Technical and Economic Cooperation (BIMSTEC), and the South Asian Subregional Economic Cooperation (SASEC).[5]

These regional/subregional organizations are mainly for the promotion of trade, energy, and socio-cultural ties. While regional forums can offer opportunities for dialogue, shaping norms, and addressing cross-border issues and non-traditional security threats, forums in South Asia have been heavily criticized for not meeting their charter objectives and being derailed by regional rivalries. Furthermore, nuclear security has rarely factored into the scope of these regional mechanisms. However, as many of the threats to nuclear and radiological material in South Asia cut across borders, it is worthwhile to examine the existing mechanisms for regional dialogue. Amongst all regional and subregional tools, SAARC, an economic and geopolitical organization in South Asia founded in 1985 and BIMSTEC, a subregional group providing a link between South Asia and Indo-Pacific region established in 1997, have the mandate to deal with non-traditional security excluding military, political, and diplomatic conflicts and have the potential to serve as forums to address threats to nuclear and radiological materials.[6]

---

[4] Charlotte East and Kendall Siewert, "Incident and Trafficking Database: Combating Illicit Trafficking of Radioactive Materials for 25 Years," *International Atomic Energy Agency*, February 2020, https://www.iaea.org/sites/default/files/6112425.pdf.

[5] There is also a Nepal-based international non-governmental organization, the South Asia Watch on Trade, Economics and Environment (SAWTEE) working on trade, environment, and food security issues in South Asian countries which is not included in Table One.

[6] "Fifth Meeting of the BIMSTEC Sub-Group on Prevention of Illicit Trafficking in Narcotic Drugs, Psychotropic Substances and Precursor Chemicals," BIMSTEC, May 23, 2018, https://bimstec.org/?event=fifth-meeting-of-the-bimstec-sub-group-on-prevention-of-illicit-trafficking-in-narcotic-drugs-psychotropic-substances-and-precursor-chemicals, Nuclear Threat Initiative, "South Asian Association for Regional Cooperation," April 2007, https://www.nti.org/education-center/treaties-and-regimes/south-asian-association-regional-cooperation-saarc/.

Methodology

This study uses both primary and secondary data. Primary data comes from several key informant interviews from subject matter experts, while secondary data includes scholarly articles, reports, and the charters and mandates of existing regional mechanisms in South Asia. Interviews were conducted via email with 16 structured questions. After contacting 35 security experts from India, Pakistan, and Bangladesh, I received six responses, one from India and five from Bangladesh, the gap in informant interviews was supplemented with analysis of secondary sources.

TABLE ONE: CHARTER OBJECTIVES AND MANDATES OF EXISTING TOOLS IN SOUTH ASIA

Organization	Member Countries	Charter Objectives & Mandates
South Asian Association for Regional Cooperation (SAARC)	Afghanistan, Bangladesh, Bhutan, India, the Maldives, Nepal, Pakistan, and Sri Lanka	To promote collaboration among South Asian states in fields that include counterterrorism, disaster relief, and trade, among other areas. No nuclear security mandate.
South Asian Free Trade Area (SAFTA)	Afghanistan, Bangladesh, Bhutan, India, the Maldives, Nepal, Pakistan, and Sri Lanka	To enhance trade and economic cooperation through the free movement of goods within SAARC countries. No nuclear security mandate.
Bay of Bengal Initiative for Multi-Sectoral Technical and Economic Cooperation (BIMSTEC)	Bangladesh, India, Myanmar, Sri Lanka, Thailand, Bhutan, and Nepal	To promote free trade, increase cross-border investment and tourism and promote technical cooperation among littoral and adjacent states in the Bay of Bengal. No nuclear security mandate.
Bangladesh, Bhutan, India, and Nepal (BBIN)	Bangladesh, Bhutan, India, Nepal	To foster connectivity among members and regulate the movement of goods, passengers, and vehicles across borders. No nuclear security mandate.
South Asia Subregional Economic Cooperation (SASEC)	Bangladesh, Bhutan, India, Maldives, Myanmar, Nepal, and Sri Lanka	To develop regional connectivity, trade facilitation and cross-border management. No nuclear security mandate.
South Asia Network on the Sustainable Development Goals (SANS)	Afghanistan, Bangladesh, Bhutan, India, the Maldives, Nepal, Pakistan, and Sri Lanka	To achieve the United Nations Sustainable Development Goals through cooperation amongst SAARC countries. No nuclear security mandate.
South Asian Forum (SAF)	Afghanistan, Bangladesh, Bhutan, India, the Maldives, Nepal, Pakistan, and Sri Lanka	To explore and develop opportunities and policies for expansion of trade and investment. No nuclear security mandate.

Role of existing tools in nuclear security

Tools for Addressing Threats from Non-State Actors

Among these organizations, SAARC's charter and convention indicate that it is the only regional tool that has the multifaceted mandates to strengthen regional cooperation and address security threats, as well as cooperate with international and regional tools with similar aims.[7] Other subregional tools do not have the same scope for maintaining peace and security in this region. However, while SAARC's mandate has the potential to address an array of non-traditional security threats impacting nuclear security—most notably regional threats of terrorism—the regular postponement of summits and frequent disputes between member states has made the organization largely ineffective.[8] For this reason, a South Asian law enforcement representative emphasized forming a new nuclear security platform due to SAARC's ineffectiveness and the gravity of the threat of extremism and terrorism in this region.[9] However, the challenges SAARC has faced are unlikely to vanish with a new mechanism and using existing infrastructure and coordination mechanisms through SAARC is more practical and likely faster than getting each South Asian country to sign on to a separate exclusive tool for nuclear security. SAARC has set terrorism prevention within the organization's mandate and goals and reached additional agreements on curbing terrorist financing (although more can be done to implement these provisions).[10] While SAARC does not address nuclear security in its current objectives, its charter empowers the organization to adapt to new areas of cooperation and develop new coordination mechanisms as deemed necessary of regional importance. Ultimately, the political will of the Indian and Pakistani governments will be the deciding factor.

As South Asia faces ongoing threats from multiple extremist groups across the subcontinent, nuclear security, in turn, becomes more complex and the consequences of nuclear security breaches more severe and borderless. Internationally, fears of nuclear terrorism and the vulnerabilities of radiological material escalated following the 9/11 attacks.[11] Although some have questioned the scope of the nuclear terrorism threat, extremist groups have attacked nuclear energy plants and weapons sites across the globe, including a 2012 air force base attack by Tehrik-i-Taliban in Pakistan on a site thought to house nuclear weapons.[12] In 2013, Indian police also found an improvised explosive device containing 1.5 kilograms of uranium in Assam, which was believed to

[7] "SAARC Regional Convention on Suppression of Terrorism" United Nations Treaties, November 4, 1987, https://treaties.un.org/doc/db/Terrorism/Conv18-english.pdf.

[8] Muhammad Daim Fazil, "The Irrelevance of SAARC," *South Asian Voices*, October 25, 2016, https://southasianvoices.org/the-irrelevance-of-saarc/, and Manzoor Ahmad, "SAARC Summits 1985-2016: The Cancellation Phenomenon," *IPRI Journal* 27, no. 1 (Winter 2017): 43-71.

[9] According to a law enforcement representative of South Asia, "Success or failure of any cooperation depends on the equal importance of objectives set for that cooperation. More so, it also gets preference due to its strategic importance. Since IAEA is coordinating overall nuclear security of the world under the auspices of the UN, and all the countries of South Asia are the more or less perceiving threat of extremism and terrorism which may escalate to nuclear threat in the future, I think, regional cooperation in the field of nuclear security in South Asia may be an effective one."

[10] NTI, "SAARC."

[11] Gwyneth Cravens, "Terrorism and Nuclear Energy: Understanding the Risks," Brookings, March 1, 2002. https://www.brookings.edu/articles/terrorism-and-nuclear-energy-understanding-the-risks/.

[12] Antonia Ward, "Is the Threat of Nuclear Terrorism Distracting Attention from More Realistic Threats?" *The Rand Blog*, July 27, 2018, https://www.rand.org/blog/2018/07/is-the-threat-of-nuclear-terrorism-distracting-attention.html, and Jennifer Rowland, "Militants storm key Pakistan Air Force Base," *Foreign Policy*, August 16, 2012, https://foreignpolicy.com/2012/08/16/militants-storm-key-pakistan-air-force-base/, "Nuclear Facilities Attack Database," National Consortium for the Study of Terrorism and Responses to Terrorism, https://www.start.umd.edu/nuclear-facilities-attack-database-nufad.

be linked to the domestic separatist group the United Liberation of Assam.[13] Osama bin Laden also indicated al Qaeda's interests in nuclear technology, and affiliates of the Islamic State were said to be observing a Belgian nuclear scientist.[14] Both India and Pakistan's nuclear programs have vulnerabilities—with concerns over insider threats and unsafeguarded nuclear materials.[15] The new nuclear power entrants from the region may also fall prey to more vulnerabilities, which motivated non-state actors could exploit in the future.

Beyond SAARC, it may also be within the scope of BIMSTEC to address counterterrorism cooperation—although this is a subregional organization also incorporating countries from Southeast Asia around the Bay of Bengal. BIMSTEC has also established a counterterrorism and transnational crime wing led by India—although also does not deal with nuclear security. A regional tool in Southeast Asia, the Association of Southeast Asian Nations (ASEAN), which has worked with the IAEA in areas including nuclear science, technology, and safeguards may provide a useful starting point for strategies of incorporating nuclear security in SAARC's mandate.[16]

MEA Photo Gallery via Flickr

[13] "Assam: IED, Uranium Recovered, Security Beefed Up," *Outlook India*, January 24, 2013, https://www.outlookindia.com/newswire/story/assam-ied-uranium-recovered-security-beefed-up/787839.

[14] Feroz Hassan Khan and Emily Burke, "Tackling Nuclear Terrorism in South Asia," *Prism* 5, no. 1, 84, and Ward, "Threat of Nuclear Terrorism."

[15] Subir Bhaumik, "India arrests for 'Uranium Theft,'" *BBC News*, September 10, 2008, http://news.bbc.co.uk/2/hi/south_asia/7608984.stm and Hannah Haegeland, "The Terrifying Geography of Nuclear and Radiological Insecurity in South Asia," Henry L. Stimson Center, January 31, 2017, https://www.stimson.org/2017/terrifying-geography-nuclear-and-radiological-insecurity-south-asia/

[16] Alex Nitzsche, "IAEA and ASEAN Strengthen Cooperation in Nuclear Science, Technology and Applications, and Nuclear Safety, Security and Safeguards," International Atomic Energy Agency, September 16, 2019, https://www.iaea.org/newscenter/news/iaea-and-asean-strengthen-cooperation-in-nuclear-science-technology-and-applications-and-nuclear-safety-security-and-safeguards.

Regional Organizations and Monitoring Trade

There is currently no regional/subregional framework or treaty for the safe movement of nuclear materials across borders. SAFTA, a free trade network established under SAARC, mandates trading of all products including manufactures and commodities in their raw, semi-processed, and processed forms. However, SAFTA mainly focuses on tariffs and barriers to trade rather than monitoring what's transferred across the border. The customs cooperation agreement of SAARC countries mainly concentrates on trading regular goods and nuclear material has not been a particular focus. According to the Center for Nonproliferation Studies database, the only open-source database collecting information on trafficking of nuclear material, incidents of trafficking in South Asia are comparatively lower than the rest of the world.[17] However, isolated events—such as the 2014 loss of radioactive material on a bus going across Nepal—underscore the need for regional organizations to play a role in establishing best practices and cooperative mechanisms as nuclear energy expands across the region.[18]

SAARC still has a long way to go to address cross-border crime or trading of illicit materials. Once again, ASEAN's structure can form a potential blueprint in integrating this aspect of security into the SAARC framework. Along with looking for greater opportunities for regional trade, ASEAN has also acknowledged challenges of cross-border crime and worked to set up border liaison offices across Southeast Asia.[19] However, SAARC thus far has not followed this model—for instance, the decision taken in 2006 for the establishment SAARCPOL (modeled off INTERPOL) has yet to function.[20] However, other existing regional/subregional organizations in South Asia are broader in terms of their objectives or sole purposes and they do not even address to monitor and detect illicit trafficking across shared borders including nuclear security issues.[21] As nuclear smuggling may potentially cross-borders, the prediction of high order nuclear security risk is not an exaggeration. As a region with long, shared, and often-porous borders, it is crucial to address and monitor the trade of any nuclear materials—as one expert put it, "pilferage or misappropriate of nuclear materials is a localized event, but its effect bears global dynamics."[22]

One of the top mandated areas of cooperation within SAARC is energy and the SAARC energy center deals with the promotion and utilization of all energy resources, which may provide a further outlet for information sharing and best practices by connecting policymakers and academia.[23] It appears by analyzing charters/mandates and objectives, SAARC is the appropriate institution to take initiative for the formation of a nuclear risk community as member countries are opting for more nuclear and other radioactive materials. It is highly

[17] "CNS Global Incidents and Trafficking Database Archived Reports and Graphics," Nuclear Threat Initiative, July 24, 2018, https://www.nti.org/analysis/articles/cns-global-incidents-and-trafficking-database-archived-reports-and-graphics/.

[18] Bimal Khatiwada, "Radio-active material lost en route to Kathmandu," *The Himalayan Post*, May 1, 2014, https://kathmandupost.com/miscellaneous/2014/05/01/radio-active-material-lost-en-route-to-kathmandu.

[19] "Border Management Overview," United Nations Office on Drugs and Crime, https://www.unodc.org/southeastasiaandpacific/en/what-we-do/toc/border-overview.html.

[20] M. Muzaffar, Iqra Yatool, and Zahid Yaseen; SAARC: An Evaluation of its Achievements, Failures, and Compulsion for Cooperation, Global Political Review, 2, No. 1, (2017), 36-45.

[21] A nuclear security expert opines that: "Our effort of cooperation should be focused on the failures of the regional networks to be nuclear security-focused platforms in South Asia. Other subregional tools like SASEC, BBIN, etc. are particularly focused on trade and environment, energy and conventional security of these countries."

[22] According to a nuclear security expert, "Pilferage or misappropriation of nuclear materials is a localized event, but its effect bears global dynamics. Even a non-nuclear state may fall prey to such terrorism with nuclear involvement". In that sense, South Asian countries should also strengthen their cooperation on the security of nuclear material for peace and security.

[23] "Vision & Mission," SAARC Energy Center, https://www.saarcenergy.org/vision-mission/.

unlikely, there will be a regional cooperation for operating nuclear power plants in South Asia for a responsible and sustainable nuclear future. Keeping in view this, the priority for the SAARC countries is to initiate regional dialogues for ensuring nuclear security in this region.[24]

Policy Implications

South Asian countries have ample reasons to work together for promoting more openness and transparency regarding nuclear security matters. South Asian regional organizations lag far behind groupings like ASEAN in terms of developing nuclear security architecture and global security commitments and standards. While SAARC remains at a standstill, other regional/subregional tools are not prepared to address nuclear security challenges and SAARC remains the best possibility for a regional approach to nuclear security. SAARC should be activated for maintaining the South Asian peace and prosperity by giving impetus to current extremism, terrorism, and global nuclear insecurity dynamics.

SAARC can look at ASEAN for potential avenues for this. For instance, SAARC countries can adopt ASEAN's Network of Regional Bodies on Atomic Energy (ASEANTOM) strategy to unite all member states in nuclear security issues by conducting the heads of state meetings, summits, and dialogues amongst the foreign and home ministers for the formation of a nuclear security working group.[25] SAARC can be used for sharing intelligence regarding information on adversary groups that might have access to illicit materials, border management, and nuclear or radiological emergency mechanisms. It can also be used for sharing experts and best practices, joint training, and coordinating with existing centers of excellence for nuclear security in India and Pakistan.

Subregional tools may also work for improving the intra-regional relationship through resolving unresolved issues i.e., water and border disputes, transit, corridors, for building trust and relationship. Considering the potential consequences of any nuclear security events can be a starting point of dialogues between the two rival countries—India and Pakistan. Nuclear scientists and civil societies within SAARC countries should exert pressure to their respective countries to break the SAARC's stalemate and use other regional tools to work more effectively. On the international level, organizations like the IAEA and the United Nations can urge South Asian countries to be responsive to the international safety and security norms and practices for the enhancement of nuclear security governance.

If these pathways fail to move forward with nuclear security challenges, there is a necessity to form a nuclear security forum in South Asia for maintaining peace, security, and prosperity. It can at least start a trilateral nuclear security cooperation forum (Bangladesh, India, and Pakistan) like the existing tri-nation nuclear cooperation model comprising the three nuclear power countries i.e., Bangladesh, India, and Russia.[26] Under the tri-nation nuclear security forum, member states can work together on terrorism and nuclear security vulnerabilities by taking appropriate strategies, plans, and measures.

[24] According to a security expert, "the agreements should be such that South Asian countries will be responsible to guard the nuclear material when it comes within the area of responsibility of each country."

[25] Tahir Ashraf, Md. Nasrudin, and Md. Akhir, "SAARC as a Tool of Regionalism in South Asia: Lessons from ASEAN," *Journal of Southeast Asian Studies,* 21, (2016), https://doi.org/10.22452/jati.vol21no1.1.

[26] Rana M.S., Islam M.S., "The Logic Behind Trilateral Model for Implementing the First Nuclear Power Plant in Bangladesh," *BIISS Journal*, 42, No.2 (2021),107-129.

IAEA Image Bank via Flickr

6. SCIENTISTS AS ASSETS: THE SECURITY OF NUCLEAR PERSONNEL IN INDIA

By Sitakanta Mishra

Although in many ways a targeted attack on nuclear scientists or engineers is unique to the security situation of each country and cannot be extrapolated to another country's security discourse, attacks on nuclear scientists nonetheless raise essential questions for any nuclear state. Is the security of nuclear personnel—including scientists and engineers—integral to the security of nuclear assets in a country? Are nuclear personnel even considered nuclear assets and given appropriate weight in the nuclear security framework?

While there is increasing awareness today on the security of nuclear installations worldwide, driven in large part by the Nuclear Security Summit initiative initiated by former U.S. President Barack Obama, scant attention seems to have been paid to the status and adequacy of security provided to nuclear personnel who are the main drivers of any nuclear program.[27] Leading scientists, engineers, and personnel are assets whose

[27] Kelsey Davenport, "Nuclear Security Summit at a Glance," Arms Control Association, https://www.armscontrol.org/factsheets/NuclearSecuritySummit.

replacement or elimination can hamper an entire nuclear program. For instance, the killing of Iranian nuclear scientist, Mohsen Fakhrizadeh in 2020, has been said to have "clearly damaged" Iran's nuclear program.[28]

Examining this topic from India's perspective, this essay analyzes the security arrangements in place for the protection of Indian nuclear personnel keeping in mind the sporadic attacks on scientists elsewhere, and reported "unnatural deaths" of scientific personnel in India in the past decade.[29] Using open-source information available on India's current nuclear security framework for nuclear personnel, this essay looks at what is known about the current protections for addressing various threats for nuclear personnel and puts forth recommendations for better addressing potential risks in the future.

The Threat to Nuclear Security Personnel

So far, no major nuclear security-related incidents—that is a Pelindaba break (South Africa, November 2007) style attack breaking into nuclear facilities—has occurred at India's nuclear installations. There has also not been a confirmed targeted killing within India's nuclear scientist community. However, between 2009 and 2013, there were multiple unfounded reports of "unnatural deaths" of Indian nuclear scientists. A number of scientific personnel have reportedly either gone "missing or died under mysterious circumstances."[30] In October 2011, the bodies of K.K. Josh and Abhish Shivam, engineers connected with the building of India's indigenous nuclear-powered submarine, the Arihant, were discovered adjacent to the railway tracks at Penduruthy, near Vishakapatnam Naval Yard.[31] As per answers given in the Lok Sabha, 11 "unnatural deaths" were reported during 2009-13 out of which: "Two cases are due to industrial fire accident, one case of road accident, seven cases of suicide, and one case of murder."[32] It was reported that after a thorough investigation by the police, however, no case was categorized as "mysterious."

Outside the nuclear realm, reports also surfaced in 2009 about the Pakistan-based militant group, Lashkar-e-Taiba's, plans "to kidnap or assassinate some of the prominent scientists" working in India's space industry.[33] Even as many reports remain shrouded in mystery—including alarming reports of the deaths of 680 employees of the Bhabha Atomic Research Center (BARC) over a period of 15 years—and in some cases may be

[28] Ray Takeyh, "What's the Fallout From the Killing of a Top Iranian Nuclear Scientist?" Council on Foreign Relations, November 30, 2020, https://www.cfr.org/in-brief/whats-fallout-killing-top-iranian-nuclear-scientist.

[29] PTI, "11 nuclear scientists died in mysterious circumstances in 4 years," *Economic Times*, October 8, 2015, https://economictimes.indiatimes.com/news/politics-and-nation/11-nuclear-scientists-died-in-mysterious-circumstances-in-4-years/articleshow/49271974.cms?from=mdr.

[30] Vinesh Bansal, "Indian Government's Shameful Neglect of Nuclear Scientists and Their Security," *DNA India*, April 3, 2014, https://www.dnaindia.com/analysis/standpoint-indian-government-s-shameful-neglect-of-nuclear-scientists-and-their-security-1974843.

[31] Special Correspondent, "Detail Hazards to Nuclear Scientists: HC," *The Hindu*, March 4, 2017, https://www.thehindu.com/news/cities/mumbai/detail-hazards-to-nuclear-scientists-hc/article17404318.ece.

[32] Government of India, "Lok Sabha Unstarred Question No. 544: Deaths of Nuclear Scientists," February 12, 2015, https://dae.gov.in/writereaddata/parl/winter2015/lsus544.pdf.

[33] "Incidents and Statements involving Lashkar-e-Taibia: 2009," South Asia Terrorism Portal, 2009, https://www.satp.org/satporgtp/countries/india/states/jandk/terrorist_outfits/lashkar_e_toiba_lt2009.htm and, PTI, "ISRO Chief Madhavan Nair gets Z-category Security," *India Today*, April 5, 2009, https://www.indiatoday.in/latest-headlines/story/isro-chief-madhavan-nair-gets-z-category-security-43616-2009-04-05.

unfounded, they underscore the individual threat faced by scientists, and Indian nuclear scientists are not immune to such threats.[34] The reported mysterious deaths have even prompted questions in the Indian Parliament about the protection of scientists.[35]

In the early years of its nuclear program, India was also under scrutiny for its nuclear development. For years before its civilian nuclear tests in 1974, the U.S. Intelligence Community "was monitoring and analyzing Indian civilian and military nuclear energy activities."[36] Conspiracy theories have also abounded surrounding the death of Homi J. Bhabha on a flight over the Alps in 1966. The official inquiry by France confirmed that the flight had crashed due to pilot error, which failed to convince many. In 2017, a Swiss climber who found remains of the crash while hiking in the Alps noted he thought it was more likely the plane had collided with another aircraft.[37] Unfounded narratives and multiple conspiracy theories of a sabotage plan by the CIA to impede India's nuclear program have also circulated widely, particularly after the publication of the *Conversations with the Crow* (2013) by Reporter Gregory Douglas, which asserted that Bhabha, along with then-Prime Minister Lal Bahadur Shastri, was targeted by the CIA after his statement in October 1965 that India could build an atomic bomb within 18 months.[38] In the interviews for the book, Douglas reports former Assistant Director of Clandestine Operations for the CIA Robert Crowley hinting at an "unfortunate accident" of a bomb going off on the same flight Bhabha was onboard.[39] In the context of targeted attacks on nuclear scientists in other parts of the world, can Indian nuclear personnel not be susceptible to conspiracies, even today?

While one must question the authenticity of media reports, such alarming stories attract attention towards the strength of the protective system for Indian nuclear scientists—especially when New Delhi has embarked on an ambitious nuclear energy expansion plan. Given India's location in a volatile region, threats to nuclear scientists should not be underestimated. The advancement of C4ISR technology also makes it possible to eliminate targets through unmanned remote-controlled stand-off weapons, as was seen in the case of Fakhrizadeh, who was reportedly targeted using a weapon mounted in a pick-up truck.[40]

---

[34] Pitamber Kaushik, "India's Vanishing Nuclear Scientists," *Asia Times*, July 22, 2019, https://asiatimes.com/2019/07/indias-vanishing-nuclear-scientists/.

[35] Lok Sabha, Unstarred Question No. 544.

[36] "U.S. Intelligence and the Indian Bomb," National Security Archive Electronic Briefing Book No. 187, April 13, 2006, https://nsarchive2.gwu.edu/NSAEBB/NSAEBB187/index.htm.

[37] Srijan Shukla, "Mystery of 1966 Air India Crash, that Killed Nuclear Pioneer Bhabha, is Unravelling Bit by Bit," *The Print*, July 27, 2020, https://theprint.in/past-forward/mystery-of-1966-air-india-crash-that-killed-nuclear-pioneer-bhabha-is-unravelling-bit-by-bit/463353/ and Neera Majumdar, "Sabotage or Accident? The Theories About How India Lost Nuclear Energy Pioneer Homi Bhabha," *The Print*, January 24, 2018, https://theprint.in/report/the-theories-india-nuclear-energy-pioneer-homi-bhabha/31233/.

[38] Jayita Sarkar, "Sino-Indian Nuclear Rivalry: Glacially Declassified," *The Diplomat*, June 2, 2017, https://thediplomat.com/2017/06/sino-indian-nuclear-rivalry-glacially-declassified/, and Bharat Karnad, "The Death of a Scientist(s)," *The Citizen*, December 14, 2020, https://www.thecitizen.in/index.php/en/NewsDetail/index/4/19740/The-Death-of-a-Scientists.

[39] Srinivas Laxman, "Operative Spoke of CIA Hand in 1966 Crash: Report," *Times of India*, July 30, 2017, https://timesofindia.indiatimes.com/city/mumbai/operative-spoke-of-cia-hand-in-1966-crash-report/articleshow/59826686.cms.

[40] "Mohsen Fakhrizadeh: 'Machine Gun with AI' Used to Kill Iran Scientists," BBC News, December 7, 2020, https://www.bbc.com/news/world-middle-east-55214359.

India by now is an established de-facto nuclear weapon state, and the fear of sabotage of its nuclear program may sound unrealistic today. However, India's ambitious nuclear energy expansion plan and their considerable scientific manpower are eye-catching; any disturbance in this would derail the expansion plan. Given the triangular strategic competition unfolding in India's neighborhood, there is the possibility of sabotage of the nuclear program in the worst-case scenario. Regional volatility and proliferation concerns in and outside India underscore potential threats.[41] The malware Dtrack attack, linked to North Korea, on the administrative block of **Kudankulam** Nuclear Power Plant in Tamil Nadu in September 2019 hints that India's nuclear assets may be vulnerable to cyber-espionage or sabotage from outside.[42] All these compel one not to overlook the possibility of "systematic outside effort to slow down India's march towards nuclear excellence by killing those involved in the process."[43]

Image via Wikimedia Commons

Security Measures in Place

No amount of security can be security-enough as the threats to scientists are dynamic and evolving, and directly linked to the health and security of the national nuclear program. Any damage to scientists would adversely affect the concerned country's nuclear program, through the loss of knowledge as well as exposing vulnerabilities in a country's security system.

[41] Hannah E. Haegeland and Reema Verma, "The Terrifying Geography of Nuclear and Radiological Insecurity in South Asia," *Bulletin of the Atomic Scientists*, January 22, 2017, https://thebulletin.org/2017/01/the-terrifying-geography-of-nuclear-and-radiological-insecurity-in-south-asia/.

[42] Debak Das, "An Indian Nuclear Power Plant Suffered a Cyberattack. Here's What you Need to Know," *The Washington Post*, November 4, 2019. https://www.washingtonpost.com/politics/2019/11/04/an-indian-nuclear-power-plant-suffered-cyberattack-heres-what-you-need-know/.

[43] Madhav Nalapat, "PMO Unconcerned About Scientist Deaths," *The Sunday Guardian*, October 26, 2013, https://www.sunday-guardian.com/news/pmo-unconcerned-about-scientist-deaths.

Threats to nuclear scientists can be divided into four broad areas based on their station and operation. First, residential areas of the scientific personnel can be vulnerable and possibly be targeted. Staff quarters are normally located inside the facility premise, therefore are well-guarded. The Government of India highlighted its approach to residential safety in a response to a question in the Lok Sabha in 2015, which noted: "security of scientists/engineers of the DAE [at workplace and] in departmental residential colonies are being audited regularly by an agency of Ministry of Home Affairs and as per their suggestions arrangements are in place."[44]

Second, the security of scientists during transit (movements in the locality or outstation travels) is more sensitive and necessitates special attention. In the past, by using remote-controlled weapons and artificial intelligence, most attacks on scientists elsewhere have generally occurred while they were on the move.[45] Top-grade Indian scientists are reportedly provided with extra security cover including while on the move, and normally they stay in their departmental accommodations with special travel arrangements.[46] However, it would be difficult to conclude whether the security cover for them can thwart or withstand a deadly drone attack or attack by automated weapons; or prevent a terror attack on academic events like the one on the Indian Institute of Science premises in Bangalore in 2005.[47]

Thirdly, the possibility of insider threats to nuclear personnel cannot be completely sidelined. Instances of misconduct and "act of sabotage" in the nuclear establishment have been reported. This includes the Kaiga incident in 2009 where a small unit of tritium was deliberately mixed in a drinking water cooler by "disgruntled employees."[48] Although ultimately not a large-scale incident, the Kaiga event does underscore that sabotage of the facility and threat to personnel inside the facility from within is theoretically possible. As this risk falls under broader concerns of rare but costly insider-threat issues—which generally present threats of theft or sabotage—reducing this risk could be done through similar measures such as strengthening security culture and bolstering human reliability programs through employee evaluations and stringent background checks.[49]

Fourth is the possibility of assassination threats from outsiders to personnel working inside the facility. Normally security of nuclear facilities in India are given high priority by the specialized wing of Central Industrial Security Forces (CISF) in coordination with local administration and police.[50] Particularly after 9/11, security in and around Indian

[44] Lok Sabha, Unstarred Question No. 544.

[45] William Tobey, "Overview: Nuclear Scientists as Assassination Targets," *Bulletin of the Atomic Scientists*, November 27, 2020, https://thebulletin.org/premium/2020-11/overview-nuclear-scientists-as-assassination-targets/.

[46] "Scientists Get Extra Security," *Rediff*, December 29, 2005, https://www.rediff.com/news/2005/dec/29isro.htm.

[47] "NIA Court Files Charges Against 2005 IISc Attacker," *The Times of India*, October 4, 2021, https://timesofindia.indiatimes.com/city/bengaluru/nia-court-files-charges-against-05-iisc-attacker/articleshow/86741742.cms.

[48] ET Bureau, "Sabotage in Kaiga: Tritium Added to Drinking Water," *Economic Times*, November 30, 2009, https://economictimes.indiatimes.com/news/politics-and-nation/sabotage-in-kaiga-tritium-added-to-drinking-water/articleshow/5282881.cms, and M V Ramana and Ashwin Kumar, "Safety First? Kaiga and Other Nuclear Stories," *Economic and Political Weekly* 45, no. 7, (2010): 47-54.

[49] Rajeswari Pillai Rajagopalan and Pulkit Mohan, "Nuclear Safety and Security in India: Emerging Threats and Response Preparedness," *Observer Research Foundation*, September 13, 2021. https://www.orfonline.org/research/nuclear-safety-and-security-in-india/.

[50] "Nuclear Security in India," Ministry of External Affairs, https://www.mea.gov.in/Images/pdf/Brochure.pdf.

nuclear facilities have been augmented, taking into consideration all aspects of threat perceptions, including threats from the aerial and waterfront domains.

Due to the sensitivities involved, there is limited information in the public domain except for blanket assurance by the Indian government that stringent security arrangements are in place and regularly audited by the Ministry of Home Affairs.[51] In times of threat, India's top scientists have been provided with some of the highest security categorized as X, Y, or Z/Z+ category security (with Z+ being the highest and mainly reserved for high-level politicians).[52] It is possible other personnel are also provided certain security cover, though not known publicly. However, the security norm seems largely based on "secretive institutional framework."[53] It has been argued that "if secrecy is a matter of life and death, security breaches are likely to be fewer and farther between."[54] Is the strategy of secretiveness or anonymity adequate to ensure security of scientists? This strategy might work for thwarting terrorists but may not be so for foreign intelligence agencies. Surveillance of personnel from designated residential area (if located outside the facility) to their place of work over a period of time would be easy enough to identify pattern of movements and weak spots for attacking or kidnapping.

The security of the "human factor," starting from upper echelon to the rank-and-file in the organization, is integral to nuclear security. Given the susceptibility of personnel, the security of Indian nuclear scientists is normally part and parcel of their selection process, training, and personnel reliability program (PRP). Many layers of the safety and security arrangement are embedded into the day-to-day operation in coordination among departmental security and central security agencies. India's nuclear establishment follows a stringent PRP designed with several lines of inquiry.[55] Generally, continuous background checks of the employee are conducted to verify identity, credit history, criminal history, reputation, and character. A series of psychological and medical screenings are used to evaluate the mental health and stability of the individual, taking into consideration aspects such as depression, schizophrenia, epilepsy, blood pressure, and other disorders. Similarly, the Nuclear Power Cooperation of India Limited (NPCIL), which operates the country's civilian nuclear power plants, and the Atomic Energy Regulatory Board have mandated the Code of Ethics and Conduct requiring "commitment for ethical professional conduct from every director and senior employee."[56] However, suicide as a cause of death of several scientists emphasizes a greater need to evaluate the mental health resources in the PRP.[57]

---

[51] Lok Sabha Unstarred Question No. 544.

[52] "Madhavan Nair gets Z-Category," *India Today* and HT Correspondent, "What is X, Y, and Z security category?" *Hindustan Times*, July 7, 2007, https://www.hindustantimes.com/india/what-is-x-y-and-z-security-category/story-KSyf79JFc3E4gbZVluwS3H.html.

[53] Tobey, "Nuclear Scientists."

[54] Ibid.

[55] Sitakanta Mishra, Jacob Happymon, and Shannon Abbott, "Nuclear Security Governance in India: Institutions Instruments and Culture," (Office of Scientific and Technical Information: U.S. Department of Energy, October 1, 2020). https://www.osti.gov/biblio/1678824.

[56] "Code of Ethic & Conduct," Nuclear Power Cooperation of India Limited, September 6, 2015, https://www.npcil.nic.in/WriteReadData/userfiles/file/15sep06_Code_Ethics.pdf, and "Code of Ethics," Atomic Energy Regulatory Board, https://www.aerb.gov.in/english/about-us/code-of-ethics.

[57] Lok Sabha, Unstarred Question No. 544.

The NPCIL has also instituted a Vigilance Directorate, in line with similar directorates of other agencies, which has the objective "to eliminate or minimize factors which provide (an) opportunity for corruption or malpractices through in-depth examination… [and] regular inspection and surprise visits," ensuring prompt observance of proper conduct and ethics relating to integrity.[58] According to the corporation, it maintains surveillance on employees who have access to sensitive parts of the plants and performs regular and surprise inspections to detect possible misconduct. The Bharatiya Nabhikiya Vidyut Nigam Ltd. (BHAVINI), another public sector undertaking involved in the nuclear program, has its own "code of business conduct and ethics" for board members and senior management along with a Fraud Prevention Policy to provide a system for prevention/detection/reporting of any fraud that is detected.[59]

A Prognosis

Security of human assets in the nuclear industry is a sensitive issue which every nuclear state tries its best to secure—often with utmost secrecy. But real threats remain. There is limited literature or global debate on nuclear scientists as an integral part of security architecture around the nuclear program of a country; rather, the matter is left to individual countries to deal with.

Though individual countries are conscious of the threat, no amount of security can be secure enough, and there is always scope for improvement. Some argue that appropriate attention has not been paid to the perceived threat to scientists in India, and others have highlighted the shortage of security staff and resources.[60] One recommendation, is for India to develop a separate security force similar to that of the United Kingdom's Civil Nuclear Constabulary that can be tasked to secure nuclear facilities and personnel specifically.[61] Moreover, sometimes abduction or "mysterious deaths" are counted as "known risks" that a nuclear scientist understands, or as "work hazards," and such incidents are ignored.[62] Undoubtedly India has evolved and nurtured a coherent nuclear security culture, but any complacency on this particular issue should be dealt with at the highest levels.

Therefore, the urgent need, first, is to change such narratives that exclude personnel from plans to secure nuclear assets. Second, as noted in an Observer Research Foundation by Rajeswari Rajagopalan: "Details of key measures India has adopted such as PRP need to be publicized because, in the absence of such outreach, partners [and the public]… have remained ignorant of India's nuclear security accomplishments. India has to find a fine balance between nuclear security and transparency."[63] Keeping in mind the past attacks on nuclear scientists in various parts of the world, there should also be a global collaborative program to strengthen "nuclear security beyond the installations and

[58] Nuclear Power Corporation of India Limited, "Vigilance," https://www.npcil.nic.in/content/256_1_Vigilance.aspx.

[59] Bhavani, "15th Annual Report, 2017-18" September 28, 2018, https://bhavini.nic.in/writereaddata/AnnualReport/40.pdf.

[60] Nalapat, "PMO Unconcerned," and Bansal, "Indian Government's Shameful Neglect."

[61] Rajewswari Pullai Rajagopalan, Rahul Krishna, Kritika Singh, and Arka Biswas, *Nuclear Security in India: Second Edition*, (New Delhi: Observer Research Foundation, 2016), 78.

[62] Bansal, "Indian Government's Shameful Neglect."

[63] Rajeswari Pillai Rajagopalan, "India's Nuclear Security: Strengths and Gaps," *Observer Research Foundation*, June 14, 2017. https://www.orfonline.org/research/india-nuclear-security-strengths-gaps/.

machines" possibly with the help of IAEA.[64] The priority should be to develop and draw lessons from global best practices involving the security of human nuclear assets. As India makes rapid scientific advancements and furthers its path of self-reliance, a "national scientists' protection act" can be formulated to address possible deaths and assassination threats to scientific personnel.[65] This would establish specific domestic legal framework and fast track legal process to address issues relating to investigation on alleged threats, professional deaths, etc. Ultimately, nuclear security must span beyond securing nuclear installations and address the perceived gaps in the security system in place—including the protection of scientific personnel.

[64] Bansal, "Indian Government's Shameful Neglect."

[65] Sunil Chacko, "Time for Nambi Narayanan Scientists' Protection Act," *Sunday Guardian*, August 22, 2020, https://www.sundayguardianlive.com/news/time-nambi-narayanan-scientists-protection-act.

IAEA Image Bank via Flickr

7. PAKISTAN'S EVOLVING NUCLEAR SECURITY CULTURE

By Tahir Mahmood Azad

In the over two decades since its 1998 nuclear tests, Pakistan has taken important steps to strengthen its nuclear safety as well as develop and enhance its nuclear security culture—defined by the IAEA as: "the assembly of characteristics, attitudes and behavior of individuals, organizations, and institutions which serves as a means to support and enhance nuclear security."[1] As culture is also a product of multiple factors—such as social learning, customs, and history—the process of fostering a strong nuclear security culture in each nuclear weapons state will be somewhat different.

At the core of security culture is the organizational practices around nuclear security, or the "prevention and detection of (and response to) theft, sabotage, unauthorized access, and illegal transfer of or other malicious acts involving nuclear materials and other radioactive substances."[2] In developing a nuclear security culture, the state has a fundamental role to play in adopting and implementing effective laws and legislations in its nuclear program. Internationally defined best practices can also be effective in promoting practices that strengthen the culture of nuclear security. In the past two decades, Pakistan has taken

[1] International Atomic Energy Agency (IAEA), "IAEA Nuclear Security Series No. 7, Nuclear Security Culture," (IAEA: Vienna, 2008), 3.

[2] Ibid.

several steps to enhance its nuclear security by bringing in different stakeholders such as military institutions, nuclear organizations, scientists, and engineers into the country's security to share their inputs. However, there is still space to improve.

This paper examines Pakistan's efforts to enhance its nuclear security culture using the IAEA Nuclear Security Culture Implementing Guide—Nuclear Security Series No. 7 (2008)—as a tool for evaluation. The guide offers practical direction for concerned institutions and regulatory bodies for strengthening nuclear security culture and can be used as a measure to see whether Pakistan's steps are broadly in alignment with international best practices. This essay then examines ongoing challenges that Pakistan faces, which include a lack of public and academic involvement and misperceptions about Pakistan's nuclear security space despite improvements.

Building a Nuclear Security Culture

A strong culture that supports nuclear security and safety is critical for preventing sabotage or theft at nuclear facilities. As noted by the IAEA, universal features at the state, organizational, managerial, and individual level work together to shape the nuclear security culture of a state and its nuclear institutions.[3] A strong nuclear security culture involves each of these actors working to ensure appropriate nuclear safety and security through adherence to guidelines and protection against nuclear threats. As the guide further notes, a culture is "hard to either impose or cultivate, but it can be fostered through role models, training, positive reinforcement, and systematized processes."[4]

Additionally, there are six important multilateral instruments that underpin the emerging nuclear security regime, which include:

1. UN Security Council Resolution 1373
2. UN Security Council Resolution 1540
3. The International Convention for the Suppression of Acts of Nuclear Terrorism (known as the Nuclear Terrorism Convention)
4. The Convention on the Physical Protection of Nuclear Material (CPPNM) and its amendment 2005
5. The Physical Protection of Nuclear Material and Nuclear Facilities INFCIRC/225/Rev.5 (INFCIRC/225)
6. The IAEA Code of Conduct on the Safety and Security of Radioactive Sources (known as the Code of Conduct)

As fears of threats from terrorism and theft of radioactive materials spread, nuclear security—particularly in South Asia—gained growing attention in international politics after September 11, 2001. The Nuclear Security Summits (NSS) in Washington in 2010, Seoul in 2012, the Hague 2014, the final NSS Washington 2016, and their corresponding nuclear experts' meetings and a series of related events have provided an opportunity to develop new strategies and policies for the improvement of global nuclear security.[5] Despite a stronger nuclear security focus in recent years, the Nuclear Threat Initiative

[3] Ibid, 7.

[4] Ibid, 8.

[5] "Nuclear Security Summit 2016," http://www.nss2016.org/.

(NTI) Index of 2020 notes that many states have no regulatory requirements or incentives in place to strengthen nuclear security culture and most of their regulations focus solely on safety culture or subsume security culture within safety culture.[6] As Pakistan—as well as India—was largely isolated immediately following its nuclear tests in 1998, the country has had a steep learning curve for fostering and creating a strong culture around nuclear safety and security.[7]

State Level Steps

According to IAEA **Fundamental Principle A** of INFCIRC/Rev-5, the state should have special responsibility for the "establishment, implementation and maintenance of a physical protection regime."[8] At the state level, legislative and regulatory frameworks have been implemented to support Pakistan's security culture. These include creating autonomous regulatory bodies with sufficient legal authority to fulfill their allocated nuclear security responsibilities. These comprise the National Command Authority (NCA), Pakistan Atomic Energy Commission, Pakistan Nuclear Regulatory Authority (PNRA) and Strategic Export Control Division. The NCA is the top decision-making organization for all nuclear issues including nuclear security (i.e., both military and civilian) and strategic activities. Day-to-day oversight is provided via the NCA's secretariat, the Strategic Plans Division (SPD).[9] To support a strong nuclear security culture, it is the responsibility of a state to define and protect general regulations and is the state's duty to assign work to the relevant organization and keep information safe. With these institutions Pakistan has worked to establish a national nuclear security regime that protects of sensitive information and facilities, and a legal framework for distribution and coordination of responsibilities to secure its nuclear assets.[10]

Pakistan has also stated its commitment to regularly reviewing practices "in light of national obligations, IAEA guidance documents, and international best practices."[11] Former Director General Yukia Amano of the IAEA expressed his appreciation for "Pakistan's cooperation with the IAEA and its active contribution to the Agency's efforts to build capacity in other countries in the region by providing experts and hosting training courses."[12] Pakistan has also adopted international legal instruments including

[6] Nuclear Threat Index, "Nuclear Security Index: Losing Focus in a Disordered World," July 2020, 42.

[7] SAV Editorial Staff, "SAV Explainer: U.S. Response to South Asia's 1998 Nuclear Tests," *South Asian Voices*, July 27, 2018, https://southasianvoices.org/sav-explainer-u-s-response-1998-nuclear-tests/.

[8] International Atomic Energy Agency, "IAEA Nuclear Security Series No. 13, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5)," (IAEA: Vienna, 2011), 5.

[9] Tahir M. Azad and H. Shahid, "Evolution of Pakistan's Nuclear Weapon Programme," *Global Security and Strategic Studies Review* 1, no. 1, 2021, 4-5.

[10] Ministry of Foreign Affairs, Government of Pakistan, "Pakistan's Nuclear Security Regime," 2020, 3. https://www.iaea.org/sites/default/files/publications/documents/infcircs/2020/infcirc932_ar.pdf.

[11] International Atomic Energy Agency, "International Conference on Nuclear Security: Sustaining and Strengthening Efforts," (Vienna: February 10-14, 2020). https://www.iaea.org/sites/default/files/20/02/cn-278-pakistan.pdf

[12] Aabha Dixit, "IAEA Director General in Pakistan: Nuclear Power and SDGs Highlighted," International Atomic Energy Agency (IAEA), March 15, 2018, https://www.iaea.org/newscenter/news/iaea-director-general-in-pakistan-nuclear-power-and-sdgs-highlighted

the Amended 2005 Convention on the Physical Protection of Nuclear Material (CPPNM) and has endorsed "Regulations on Physical Protection of Nuclear Material and Nuclear Installations PAK/925."[13] PAK/925 is in line with INFCIRC 225/Rev 5, and specifically calls attention to security culture as part of the physical protection of nuclear materials.[14]

Ansar Parvez, Chairman, Pakistan Atomic Energy Commission conducts IAEA Director General Yukiya Amano on a tour of the premises during his official visit to Pakistan from March 10-12, 2014.
IAEA Image Bank via Flickr

Organizational Initiatives, Training, and Best Practices

Pakistan proclaims that it has created a strong nuclear security culture, which sustains a national nuclear security regime.[15] In an IAEA Conference in 2020, Tariq Majeed an Inam ul Haq, comprehensively discussed Pakistan's efforts to enhance its nuclear security culture through education of its nuclear scientists and engineers in the Pakistan Institute of Engineering and Applied Sciences (PIEAS).[16] Earlier, in 2019, by recognizing Pakistan's development in nuclear field, the IAEA named PIEAS as an IAEA Collaborating Center to support Member States on research, development, and capacity building in the application of advanced and innovative nuclear technologies.[17] These educational institutions are crucial for developing vigilance, continuous education on best practices, and commitment to nuclear security in Pakistan's institutions. Pakistan also established a Centre of Excellence (CoE) for Nuclear Security in 2012, which consolidates best

[13] Government of Pakistan, "The Gazette of Pakistan: Pakistan Nuclear Regulatory Authority Notification," April 20, 2019, https://www.pnra.org/upload/legal_basis/regulations/PAK-925.pdf.

[14] Ibid, 6, and IAEA, "International Conference on Nuclear Security."

[15] Tariq Majeed, "Nuclear Security Education at Pakistan Institute of Engineering and Applied Sciences (PIEAS): Current Status, Future Prospects and the Lessons Learnt," *International Journal of Nuclear Security* 2, no. 1. https://doi.org/10.7290/v7tb14tx.

[16] Tariq Majeed and Inam ul Haq, "Enhancement of Nuclear Security Culture with Implementation of Nuclear Security Education at PIEAS," International Conference on Nuclear Security: Sustaining and Strengthening Efforts, February 2020. https://conferences.iaea.org/event/181/contributions/15340/attachments/8498/11624/NS_Culture_Enhancement-ICON-2020_-02-A.pdf.

[17] Shant Krikorian, "New IAEA Collaborating Centre in Pakistan to Assist in Application of Nuclear Technologies," International Atomic Energy Agency, December 5, 2019, https://www.iaea.org/newscenter/news/new-iaea-collaborating-centre-in-pakistan-to-assist-in-applications-of-nuclear-technologies.

practices across three nuclear security institutions in Pakistan and collaborated with the IAEA-led Nuclear Security Support Center network.[18]

Brig. Feroz Khan (retd.), has also outlined the evolution of Pakistan's security culture.[19] According to Khan, after the September 11 attacks in the United States, Pakistan developed several important programs including: The Personnel Reliability Program (PRP), Human Reliability Program (HRP), and physical protection of nuclear material and facilities, systems for Nuclear Material Accounting and Control, which increased safety and security procedures for weapons. Pakistan also began a Nuclear Security Action Plan overseen by the PNRA—which is responsible for the control, regulation, and supervision of all matters related to nuclear safety and radiation protection in Pakistan.

Pakistan has also gained some support internationally. According to Naeem Salik and Kenneth Luongo, "Pakistan also has benefited from cooperation and exchanges of information on best practices with friendly countries, including the United States, and has maintained a vibrant, cooperative relationship with the IAEA."[20] This includes a meeting as early as 2000 between Pakistan and U.S. officials to support building Pakistan's nuclear command and control structures.[21] Pakistan has also cooperated with China on nuclear issues and received support in strengthening its nuclear safety and security measures. For example, the PNRA signed agreements for regulatory cooperation with the Chinese National Nuclear Regulatory Authority to coordinate technical trainings for PNRA engineers and scientists.[22] All these trainings and practices are essentials to maintain a safe and secure nuclear program.

In April 2018, the PNRA hosted an International Workshop on Nuclear Security Culture in Practice.[23] The objective of this workshop was: "to emphasize the importance of nuclear security culture to ensure an effective nuclear security" as well as "increase understanding of the key elements of nuclear security culture by internalizing these elements…[and] encourage the participants to review their daily behaviors through the lens of nuclear security culture." The PNRA has also organized various education and training exercises on emergency preparedness and response to train its own staff, licensees and off-site response for capacity building of people involved in nuclear organizations. Some of these activities are arranged in coordination with other national organizations and IAEA under Technical Cooperation projects.[24] In 2020, the PNRA organized ten local training courses on emergency preparedness and response such as regulatory oversight, emergency management system, hazard assessment, public communication, medical response, response to malicious acts.

---

[18] Aabha Dixit, "Pakistan's National Centre of Excellence Contributes to Sustaining Nuclear Security," IAEA Bulletin, December 2016, https://www.iaea.org/sites/default/files/publications/magazines/bulletin/bull57-4/5742222.pdf.

[19] Feroz Hassan Khan, "Nuclear Security in Pakistan: separating Myth from Reality," Arms Control Association, July 2009, https://www.armscontrol.org/act/2009-07/features/nuclear-security-pakistan-separating-myth-reality.

[20] Naeem Salik and Kenneth Luongo, "Challenges for Pakistan's Nuclear Security," Arms Control Association, February 2013, https://www.armscontrol.org/act/2013-02/challenges-pakistan%E2%80%99s-nuclear-security.

[21] Sam Hananel and Laura Rodriguez, "Nuclear Security Cooperation Between the United States and Pakistan: A Survey from 2000-2009," Center for American Progress, June 24, 2009, https://americanprogress.org/article/nuclear-security-cooperation-between-the-united-states-and-pakistan/.

[22] Pakistan Nuclear Regulatory Authority, "Competence Management," https://www.pnra.org/cmpt-mgmt.html.

[23] Pakistan Nuclear Regulatory Authority, "Holding of International Workshop on Nuclear Security Culture in Practice from April 23-26 at PNRA HQs in Islamabad," https://www.pnra.org/NSCP%202018.html.

[24] Pakistan Nuclear Regulatory Authority, "Convention on Nuclear Security: National Report for Eighth Review Meeting, 2020," August 2019.

Individual Attitudes

Each person working within nuclear organizations has a vital contribution and job to perform. Beyond the crucial PRP and HRP, the education components of PIEAS also underscore Pakistan's commitment to the human component of nuclear security.[25] Furthermore, an assessment procedure for nuclear security culture (in the form of a survey) among the scientists and engineers has been introduced, as per guidelines of IAEA. All these exercises have helped develop better understanding of the potential threat scenarios to the nuclear facilities and organizations. Additionally, the PNRA fosters safety and security culture in nuclear installations by certifying that it is on the agenda of the licensee at the highest organizational level. To do this, the PNRA has implemented numerous initiatives for the capability development of regulatory officials in different disciplines.[26]

The Obstacles Ahead

On the basis of recognized global standards and practices, Pakistan has taken this subject seriously and has made significant progress in developing a strong nuclear security culture which has evolved during the last two decades.[27] The IAEA has praised Pakistan's efforts in nuclear security and the NTI has also highlighted Pakistan's progress declaring Pakistan as "the most improved country in the theft ranking for countries with nuclear materials, improving its overall score by 7 points" in 2020.[28] However, there are some areas which need to be improved. Beyond nuclear security culture, Pakistan also needs to take steps to improve its global image and challenge misperceptions about its nuclear security regime. International misperceptions have at times undermined Pakistan's nuclear security efforts. Pakistan does have a robust nuclear safety and security mechanism, but it has to address international perception through productive and proactive nuclear diplomacy. Moreover, countering socio-political vulnerabilities would further enhance Pakistan's credibility.

Conduct Comprehensive Assessments to Address Nuclear Security Culture

At the level of state, organizations, managers and individuals, Pakistan can further conduct a comprehensive assessment to strengthen its nuclear security culture. Furthermore, Pakistan should address socio-political vulnerabilities. As indicated by the NTI Index in 2020, political instability, ineffective governance, corruption, and non-state actors are serious challenges for Pakistan. They can directly and indirectly contribute to a deterioration in Pakistan's nuclear image. A peaceful society and good governance are essential for good security culture. More nuclear security culture workshops, outreach programs, training courses, and international coordination can also support this goal.

Diplomacy Efforts

This is mainly possible through academic writings, publications, and narrative building. The other way Pakistan can project its perspective is through greater involvement of civil society, academics, politicians, and scholars in open discussions about nuclear

[25] Majeed and ul Haq, "Enhancement of Nuclear Security Culture."

[26] Pakistan Nuclear Regulatory Authority, "Competence Management."

[27] Tahir M. Azad, "Pakistan's Nuclear Security: Separating Fact from Fear," Institute for Security & Development Policy, Policy Brief No. 143, February 5, 2014. https://isdp.eu/content/uploads/publications/2014-azad-pakistans-nuclear-security.pdf.

[28] Nuclear Threat Initiative, "Australia Ranks 1st, Pakistan is Most Improved," 2020, https://www.ntiindex.org/news/australia-ranks-1st-pakistan-is-most-improved/.

policies and security. Currently, there are few nuclear experts and analysts in Pakistan. By developing a strong group of nuclear experts at the national and international level, Pakistan can project its perspective ranging from nuclear politics, achievements in peaceful uses of nuclear technology, and efficacy to sustain a deterrence strategy. Nuclear politics has become a specialized subject worldwide and it has attained more attention during the last two decades—Pakistan can do more to be part of this dialogue. Academics may also have an untapped role to play in strengthening the state's nuclear security culture, as they offer recommendations, expertise, diverse opinions, and analysis.

Scholars Exchange Program

Additionally, international cooperation and scholar-exchange programs can support learning about nuclear security culture and best practices. Pakistan has already taken various nuclear safety and security cooperative measures, however, most of these measures are in the scientific, technical, and legal areas. There is a need to expand the horizon of international cooperation with the help of initiatives like the exchange of policymakers, nuclear experts, and security analysts to share knowledge and create institutional and academic cooperation as well as support research opportunities for young scholars at the international level. International cooperation will bring productive results for Pakistan as well as enhance Pakistan's nuclear image. Western research institutions and think tanks in nuclear studies are highly advanced and equipped with rich resources and senior experts. It is the responsibility of the Higher Education Commission of Pakistan, Ministry of Foreign Affairs, and non-governmental organizations/think tanks, particularly working in education and consultancy areas, to provide such funding opportunities for young researchers. Furthermore, international coordination will enhance confidence and will be useful in promoting mutual cooperation and understanding.

Conclusion

Nuclear security culture is a critical component of strengthening organizational best practices and commitments to nuclear security. Pakistan has made strides in establishing nuclear safety and security cultures within nuclear organizations, which gives a positive outlook for the future. The country has worked to align its civilian regulation to international standards as well as re-structured its organizational framework to centralize government oversight.[29] However, less contributions from politicians, civil society, experts, and analysts are continued concerns. In Pakistan, strategic organizations and the PNRA have effectively maintained a safe and secure nuclear program, nonetheless, effective nuclear security culture is achievable only through mutual and sustained coordination from each actor in nuclear security policy and practices.

[29] Senate Secretariat, "The Gazette of Pakistan: Acts, Ordinance, President's Orders and Regulations," March 11, 2010. https://media.nti.org/pdfs/1_20.pdf.

IAEA Image Bank via Flickr

8. PROSPECTS FOR SMALL MODULAR REACTORS IN INDIA

By Urvashi Rathore

Nuclear energy has consistently been a reliable source of power with the benefits of zero carbon emissions and high energy density. Despite this, nuclear energy has never been able to gather adequate backing in the energy sector, which is mostly dictated by fossil fuel industries. The pushback against nuclear energy industries can also be linked to three major nuclear accidents: Chernobyl, Three Mile Island, and Fukushima. Traditionally nuclear energy is generated by massive nuclear reactors of power of 1,000 megawatts electric (MWe) or higher per unit. In large nuclear stations, many of these units are brought together to generate power. However, these large reactors have faced criticism for their significant capital investment, depreciation costs, and lack of robust inherent passive safety features.

Small Modular Reactors (SMRs) have the potential to address several of the issues mentioned above. The International Atomic Energy Agency (IAEA) defines SMRs as reactors producing 300 MWe or less.[1] The size of SMRs facilitates modularized construction in factories and direct assembling on operating sites, and additionally helps in the convenient transportation of reactors to the site. The initial capital and construction time involved in the production of SMRs is much less than a conventional nuclear reactor, which makes them an emerging preference against their larger counterparts in the nuclear energy world. SMRs also come equipped with passive safety features to deal with irregular conditions, whereas the conventional reactors

[1] International Atomic Energy Agency, "Small Modular Reactors," https://www.iaea.org/topics/small-modular-reactors.

require operator intervention to initiate active systems. SMRs can be made to operate underground or as a floating nuclear power unit.[2] The past two decades have seen growing enthusiasm for deploying SMRs as a carbon free source of energy and at the same time addressing safety risks of nuclear energy. SMRs could also be used for other energy exhaustive processes such as cogeneration, district heating, or desalination of sea water. SMR technology has also received substantial research and development funding, which has produced innovative and cutting edge SMR designs.[3]

With India's Department of Atomic Energy (DAE) tracings its start to the vision of India's renowned Nuclear Scientist, Homi Jehangir Bhabha, India's nuclear energy program has only continued to mature over the past seven decades. However, while India's energy demands are set to skyrocket in the coming years, the DAE's vision has yet to be realized, with nuclear energy contributing to only a meagre share of India's electricity generation.[4] This essay analyzes the feasibility of India conceiving SMR research and the challenges involved. Although integrating SMRs into the nuclear power grid is still years away, working on a concept of SMRs that suits India's current nuclear energy regime is a crucial opportunity for India to addresses the factors that have contributed to the lag in nuclear energy growth in the country.

Small Modular Reactors in India

India currently has the world's second largest population, 1.38 billion and counting. As per the population projection report from India's Ministry of Health and Family Welfare, India's population is expected to grow from to 1.52 billion by 2036, an increase in 25.7 percent since 2011.[5] Energy demands will only increase in the coming years—India has been projected to overtake the European Union as the world's third largest energy consumer by 2030. India has a dynamic energy sector mostly dominated by fossil fuel energy plants.[6] The fossil fuel plants have an installed generation capacity of 234,024 MW amounting to 60.2 percent of India's total installed power generation capacity, hydro power accounts for 12 percent, whereas other renewable energy account for 26.4 percent. Nuclear energy shares a meager 1.7 percent of India's total installed power generation capacity.[7] The reasons for backlash include the high capital investment for nuclear projects, long construction times, land acquisition, and safety and public concerns owing to risks of catastrophic accidents. Post-Fukushima, India's nuclear regulatory body, the Atomic Energy Regulatory Board, carried out safety assessments of the nuclear reactors in operation and many new initiatives were introduced in the regulatory process to

[2] Christopher P. Pannier and Radek Skoda, "Comparison of Small Modular Reactors and Large Reactor Fuel Cost," *Energy and Power Engineering* 6, no. 5 (May 2014). https://www.scirp.org/Journal/PaperInformation.aspx?PaperID=45669, and "Russia Connects Floating Plant to Grid," World Nuclear News, December 19, 2019. https://world-nuclear-news.org/Articles/Russia-connects-floating-plant-to-grid.

[3] IAEA, "Advances in Small Modular Reactor Technology Developments," 2020, https://aris.iaea.org/Publications/SMR_Book_2020.pdf.

[4] "Census of India 2011: Population Projections for India and States 2011-20136," National Commission on Population and Family Welfare, November 2019. https://nhm.gov.in/New_Updates_2018/Report_Population_Projection_2019.pdf.

[5] Ibid.

[6] India Energy Agency, "India Energy Outlook 2021," (France, IAE, February 2021), 169. https://iea.blob.core.windows.net/assets/1de6d91e-e23f-4e02-b1fb-51fdd6283b22/India_Energy_Outlook_2021.pdf.

[7] Government of India, Ministry of Power, "Power Sector at a Glance, ALL INDIA," last updated November 15, 2021, https://powermin.gov.in/en/content/power-sector-glance-all-india.

reduce risk of core damage.[8] However, the concerns on expenditures, land acquisition, and long construction times persist and are yet to be fully addressed.

Currently, the Indian nuclear power program uses a closed fuel cycle—meaning that it reprocesses spent fuel to separate fissile material (fuel) from waste products—in a three-stage process.[9] Stage one uses a natural uranium fueled Pressurized Heavy Water Reactors (PHWR), which produces energy and fissile plutonium. The second stage would then use Fast Breeder Reactors (FBRs) that are fueled with enriched plutonium and depleted uranium extracted from the spent fuel in stage one, finally the third stage reactors would use thorium, which is found in vast quantities in the country.

The second stage of India's fuel cycle has been significantly delayed as BHAVINI—a 500 MWe Prototype FBR—has yet to be completed, causing a lag in the three-stage power program.[10] To increase the share of nuclear energy in the country India has also started a parallel acquisition of reactors from foreign countries and plans on increasing the numbers of Indian Pressurized Heavy Water Reactors (IPHWR), a technology that India has mastered. There are currently 22 reactors operating, generating about 6780 MWe, with around 6700 MWe under construction.[11] India has pitched further construction of 10 Indian PHWR of total of 7000 MWe and for the acquisition of two VVER (Vodo-Vodyanoi *energetichesky* reactor; Russian LWR) reactors from Russia of 2000 MWe by 2031 taking the total energy generated by nuclear to 22,480 MWe—three times the current value.[12] This is an ambitious goal facing the same challenges mentioned above for large conventional NPPs. Now is the time India must look beyond traditional nuclear reactors towards the possibility of designing and building SMRs.

SMR Potential

The next steps for SMR production in India can follow the advancements which India has already made in several new nuclear technology projects. India has pitched building an Advanced Heavy Water Reactor (AHWR)-300 MWe-LEU (low enriched Uranium) small reactor and ambitiously plans on building its own IPWR (Indian Pressurized Water Reactor) that would have a capacity around 1000 MWe—too large in MWe to be considered an SMR.[13] The AHWR will demonstrate inherent safety characteristic with several advanced passive safety systems with first or its kind systems. There are no reports on the development status of the IPWR apart from mention of India's intents to produce it. The AHWR core is designed to operate with a mixture of fuel derived from second

[8] Krishna P. Kumar, Hajela, S., Malhotra, P.K., & Ghadge, S.G, "Safety Assessment and Improvements in Indian Nuclear Power Plants," International Atomic Energy Agency (IAEA), 2011.

[9] Niharika Tagotra, "India's Ambitious Nuclear Power Plan – And What's Getting in Its Way," *The Diplomat*, September 9, 2020, https://thediplomat.com/2020/09/indias-ambitious-nuclear-power-plan-and-whats-getting-in-its-way/.

[10] "Indian Government Takes Steps to get Nuclear Back on Track," World Nuclear News, February 11, 2019, https://www.world-nuclear-news.org/Articles/Indian-government-takes-steps-to-get-nuclear-back and Bharatiya Nabhikiya Vidyut Nigam Limited, "Committee on Public Undertakings, Sixth Report (Sixteenth Lok Sabha)," April 28, 2015, https://eparlib.nic.in/bitstream/123456789/65739/1/16_Public_Undertakings_6.pdf.

[11] Government of India Press Information Bureau, "Department of Atomic Energy: Nuclear Power Plants," March 11, 2020, https://pib.gov.in/PressReleseDetail.aspx?PRID=1605939.

[12] Ibid, and Ministry of External Affairs, "India-Russia Relations," June 2020, 9. https://mea.gov.in/Portal/ForeignRelation/India_Russia_Jun_2020.pdf.

[13] Government of India Department of Atomic Energy, "BARC Activities for Indian Nuclear Power Program," http://www.barc.gov.in/randd/artnp.html, and Bhabha Atomic Research Center, "AHWR300-LEU Advanced Heavy Water Reactor with LEU-Th MOX Fuel," Department of Atomic Energy, https://dae.gov.in/node/sites/default/files/ahwr-leu-broc.pdf.

stage reactors, however, as noted above these reactors are often delayed. Consequently, AHWR's construction and operation will be delayed as well.

However, India has shown a huge success in building small Pressurized Water Reactors (PWR) of around 82.5 MW for propelling submarines.[14] Under the Advanced Technology Vessel project, six nuclear powered submarines are planned for construction to bolster India's nuclear triad. The DAE can extrapolate the technology of PWR type reactors already in use with Indian Navy, while combining the design and safety elements from AHWR and IPWR to design Indian SMRs. The SMR design could also be entirely a derivative of propulsion reactor like the Russian KLT-40S, the world's only operating SMR-FNPP (Floating Nuclear Power Plant) which is a derived form of propulsion reactors used in ice-breaker ships.[15] It will be a huge feat on account of DAE if an indigenous SMR design can see light of day, as the current political leadership endorses indigenous technology development through *Atmanirbhar Bharat* (self-reliant India).

Nuclear energy in India has historically been government owned and regulated. However, for SMRs to get off the ground, the DAE must consider a joint effort between government, public, and private players. Once the DAE has the design ready, it could go on to fabricate a prototype SMR in collaboration with industrial giants such as L&T, BHEL, Walchand Nagar, or others. The same concept was used to fabricate the land-based propulsion reactor prototype.[16] The DAE will have to build new or modify existing test facilities to test and demonstrate various design and safety features of SMRs.

Challenges

Incorporating SMRs into India's nuclear energy production is a long-term project, licensing and development time is currently the main consideration for SMRs. Constructing the first prototype and commissioning it may take more than a decade including the time for licensing activities. In India, the Atomic Energy Regulatory Board (AERB) carries out licensing activities related to construction, commissioning, and operation of NPPs. However, the AERB, which currently only overlooks the civilian application of nuclear energy, may not have the experience and knowledge of certifying reactors under strategic use. The DAE will have to frame a collaboration between various organizations involved in research of propulsion reactors, IPWRS, AHWRs, and the AERB to frame a licensing process suitable for SMRs without compromising India's strategic interests. Deriving license and regulation protocols will require substantial research into the design safety parameters catering to SMRs.

Given the number of advantages to SMR technology, this topic has been taken up for discussion globally by various international working groups to discuss the way forward, such as the Cooperation in Reactor Design Evaluation and Licensing.[17] India is also a part of these discussion on SMRs. The topic of licensing and regulation, staffing requirements, and basic safety specifications is something that can be developed with

[14] T.S. Subramanian, "Nuclear Arm," *Frontline*, August 28, 2009, https://frontline.thehindu.com/the-nation/article30188065.ece.

[15] "KLT-40S," International Atomic Energy Agency, Advanced Reactor Information System, April 19, 2013, https://aris.iaea.org/PDF/KLT-40S.pdf.

[16] Subramanian, "Nuclear Arm."

[17] Cooperation in Reactor Design Evaluation and Licensing, "Facilitating International Licensing of Small Modular Reactors," World Nuclear Association, August 2015, http://www.world-nuclear.org/uploadedFiles/org/WNA/Publications/Working_Group_Reports/REPORT_Facilitating_Intl_Licensing_of_SMRs.pdf.

global collaboration as several countries—specifically the United States and Russia—are more advanced phases of licensing. Despite this, licensing difficulties present one of the most difficult challenges on the path of building first SMR prototype. Ideally, licensing activities should not exceed the construction time as this will further burden the capital investment as the reactor will not be operational even after it is constructed.

IAEA Image Bank via Flickr

Once the first prototype successfully demonstrates the SMR technology along with compliance with regulatory protocols it can be transferred to Nuclear Power Construction of India Limited (NPCIL) or any other public sector undertaking for construction and operation in fleet mode. The integration of SMRs in India's existing nuclear power program can be done in both grid and off-grid approach. Multiple SMRs can be grouped together at power plants already housing conventional reactors, and they can be connected to an existing power distribution infrastructure (grid). SMRs can also be made in a distributive manner where grid connections can be closer to promote grid stability and avoid transmission losses. However, due to public concerns over new nuclear sites, the ideal approach for India would be to have multiple SMRs at sites close to already existing NPPs. The off-grid approach maybe suitable for places which lack a grid distribution system for example, the Andaman Islands where power distribution is through stand-alone systems via diesel generators.

SMR development will need a nuclear fuel cycle as well, which can be either a derivative of existing fuel cycles or system dedicated fuel cycle. The fuel cycle for SMRs will have to be developed in an approach that is compatible with India's current fuel cycle—especially the back end of the cycle, which involves reprocessing of spent fuel. However, the reprocessing of SMR spent fuel may only be an option with India if the fuel is indigenous, as fuel imported from abroad will need to be placed in a spent fuel storage facility on an interim basis. No matter how good the strategy is for managing spent fuel, the final disposal of nuclear waste is an ongoing challenge for nuclear energy—whether produced with SMRs or conventional NPPs. The effective management of nuclear waste remains a crucial problem for the nuclear industry and a major concern of the public as well.

One of the key challenges is also the economics factor which also needs to be evaluated carefully. The cost of SMRs can be divided between construction, operation, fuel cycle, and decommissioning. Delays in licensing procedures will have a significant impact on the economic advantages that SMRs have over large reactors. This is something that will have to be considered critical to success of small reactors.

Beyond licensing and economic challenges, the main obstacle that not only SMRs but the whole of nuclear energy industry faces in India is public perception. There is a general lack of trust and concerns from local communities over the addition of NPPs. The anti-nuclear protests outside nuclear power plants in Kudankulam, Tamil Nadu, and Jaitapur, Maharashtra are two significant resistance movements in the last two decades.[18] The major reason of local public distrust is social in nature. To construct an NPP a huge area of land is acquired including the exclusion zone which leads to large displacement of the public from the area. Even well compensated local communities may eventually develop grudges because of various restrictions owing to natural growth zone (five kilometers) around the NPP which mandates only natural growth activities can take place in the region.[19]

These public issues combined with events such as the Fukushima accidents cause concerns about nuclear energy. Although Indian nuclear plants have been able to maintain a generally strong safety record—with experiences gained from few incidents putting their safety features to test—there is always a scope of improvement. The AERB, which is the main responsible authority, has yet to become formally independent. A strong independent nuclear regulatory body can create stronger trust among the public, and allow their voices to be an influence in various regulatory phases of NPPs. The AERB is functionally independent from DAE but an act or law passed by the Indian parliament would strengthen its independence. A bill in this regard "NSRA (Nuclear Safety Regulatory Authority)" was proposed in the parliament but is still yet to see enforcement.[20] This is something that the Indian law makers must look at before trying to concept other established NPP technologies let alone SMRs.

It will take significant dedication to awareness campaigns to build support from the Indian public and trust that SMRs are efficient and safe. This will be a major challenge since the term "nuclear" itself reflects a history of destruction. However, with efficient public outreach the image of nuclear energy can be improved to pave the path for SMRs or future nuclear energy projects. SMRs also require a smaller area for construction and low core inventory, which allows for smaller exclusion zone and emergency planning zone with reduced risks of offsite emergency and may reduce the land acquisition concerns that come with large NPPs.[21] Deploying SMRs in lieu of large reactors will avoid displacement of large populations owing to land acquisition issues. This advantage will

[18] Ajmal Khan A.T., "Anti-Nuclear Protests in India," *The Asia Dialogue*, July 5, 2017, https://theasiadialogue.com/2017/07/05/anti-nuclear-protests-in-india/.

[19] Government of India, "AERB Safety Code: Site Evaluation of Nuclear Facilities," Atomic Energy Regulatory Board, July 2014, https://www.aerb.gov.in/images/PDF/CodesGuides/NuclearFacility/NPPSiting/1.pdf.

[20] Press Information Bureau Government of India, " Nuclear Safety Regulatory Authority," April 12, 2017, https://pib.gov.in/PressReleseDetail.aspx?PRID=1487659.

[21] Nuclear Technology Development and Economics, "Small Modular Reactors: Challenges and Opportunities," Nuclear Energy Agency, 2021. https://www.oecd-nea.org/upload/docs/application/pdf/2021-03/7560_smr_report.pdf.

have to be coupled with initiatives that focus on preferences of local host communities and addressing their safety concerns to enable smooth deployment and acceptance of SMRs. Embedding opportunities for local and regional job creation, will also further help nuclear energy's overall acceptance.

Conclusion

SMRs are in race to become a part of the global energy regime as a competitive low carbon technology component. India, which aims to have economic dominance in South Asia, cannot afford to be behind in this race, however, it has yet to arrive at the starting line. The current nuclear energy regime of India faces several issues which can be directly or indirectly addressed through SMRs. One can simply envisage the difference that deploying SMRs will create in remote regions of India such as Andaman Islands and Northeast regions. SMRs potential deployment around Special Economic Zones surrounding energy exhaustive industries will only boost India's economic growth. It is need of the hour that Indian government vests its time and finances into the SMR program to better address the energy needs of the subcontinent. The road to realizing SMRs will be difficult but not impossible as India's DAE can make it a reality.

CONTRIBUTORS

Chirayu Thakkar is a doctoral candidate in International Relations at the National University of Singapore. Previously, he completed graduate degrees in Modern South Asian Studies from the University of Oxford and Political Science from the Central European University. He has worked for the Margaret Anstee Center, University of Cambridge as an independent researcher on India's foreign aid in Africa. Along with South Asian Voices, his writings have also appeared in The Times of India, The Huffington Post, The Diplomat, and The Asia Dialogue. He has also worked as a political consultant.

Sitara Noor is a Senior Research Associate at the Centre for Aerospace and Security Studies in Islamabad, Pakistan and South Asian Voices Visiting Fellow 2019-2020. Previously, Sitara was the director of a Lahore-based policy consultancy and before that, a Research Fellow at the Vienna Center for Disarmament and Non-Proliferation (VCDNP) in Vienna, Austria. Prior to joining the VCDNP, she worked at the Pakistan Nuclear Regulatory Authority under the Directorate of Nuclear Security and Physical Protection as an International Relations Analyst. She has been a faculty member at the National University of Modern Languages, Islamabad's Department of International Relations for two years. She was also a visiting faculty at the National University of Science and Technology (NUST), Lahore, the Foreign Services Academy of Pakistan, and the Information Services Academy of Pakistan.

Pulkit Mohan is an Associate Fellow with the Centre for Security, Strategy and Technology (CSST) at the Observer Research Foundation, New Delhi. Her research focuses on the intersection of cyber security and nuclear security and nuclear deterrence, with a focus on South Asia. She also works extensively on India's nuclear program and the utilization of nuclear energy. She also helps curate ORF's Kalpana Chawla Annual Space Policy Dialogue. Prior to joining ORF, Pulkit was an Editorial Assistant with a leading development journal. She graduated from the London School of Economics with a master's in International Relations.

Palwasha Khan is a Centre for Security Strategy, and Policy Research (CSSPR) at the University of Lahore Nuclear Scholars Fellow of the 2021 cohort. She holds an MPhil in Strategic Studies from the National Defense University (NDU), Islamabad, with her dissertation focusing on nuclear signaling patterns in South Asia. She has secured a certificate of merit in academic excellence from NDU in MSc. Strategic and Nuclear Studies. Her areas of interest are nuclear deterrence, strategic stability, and nuclear security.

Md. Shafiqul Islam holds a PhD in nuclear safety and is a Professor in the Department of Nuclear Engineering at the University of Dhaka, Bangladesh. He has also worked as Chairman in the said department. His research interests include thermal hydraulics safety, nuclear security culture, nuclear energy economics, and nuclear energy policy. He has nearly eight years of work experiences on research reactor operation and maintenance activities during his past job at Bangladesh Atomic Energy Commission (BAEC). Prof. Islam is working under various capacities of the nuclear power program of the country. He also provides expert services to the IAEA.

Sitakanta Mishra is an Associate Professor at Pandit Deendayal Energy University (Formerly PDPU), Gujarat, India. He was formerly a Research Fellow at the Centre for Air Power Studies (CAPS), New Delhi, and Associate Editor of the Indian Foreign Affairs Journal, New Delhi. He is also the Managing Editor of the Liberal Studies Journal published by PDEU.

Tahir Mahmood Azad is a Visiting Research Fellow at the Centre for Science and Security Studies (CSSS) in the Department of War Studies at King's College London and joined CSSS in 2019.

He previously held fellowships at the Sandia National Laboratories, New Mexico, USA; the SPAIS / Global Insecurities Centre, University of Bristol; the Center for International Trade & Security (CITS), University of Georgia, USA; Centre on Conflict, Development and Peacebuilding (CCDP), Graduate Institute Geneva, Switzerland; the Institute for Security and Development Policy (ISDP) Stockholm, Sweden and Peace Research Institute Frankfurt (PRIF), Germany.

Dr. Azad accomplished a Postdoctoral Research Fellowship (2019-2020) at the School of Politics & International Relations, University of Leicester, UK. He holds a PhD degree from the Department of Strategic & Nuclear Studies, National Defence University (NDU) Islamabad, Pakistan. Previously, he obtained M.Phil. degree with distinction from the same department and M.Sc. in Defence & Strategic Studies from Quaid-i-Azam University, Islamabad, Pakistan.

Urvashi Rathore is a freelance Nuclear Policy Researcher based in India. Her research focuses on nuclear science and technology advancements, as well as nuclear and radiological security culture in India. She is a Robin Copeland Memorial Fellow (2017, India), a fellowship provided by CRDF Global that aims to empower female scientists and engineers from emerging countries. During the fellowship, she worked as a visiting fellow with James Martin Centre for Non-Proliferation Studies, Middlebury Institute of International Studies, Monterey. At CNS, she researched orphan radioisotopes in India and the radiological security culture of the Indian Nuclear Power program. As a Robin Copeland fellow, she also worked at Nuclear Threat Initiative, Washington D.C. on various radiological security issues in India.

She holds a certificate in a semester long non-proliferation training program from the James Martin Centre for Non-proliferation studies, Middlebury Institute of International studies at Monterey. She also worked at Observer Research Foundation, New Delhi, India with the Centre for Security, Strategy and Technology (CSST). She has worked with the Military Affairs Centre on Defence Reforms project at Manohar Parrikar Institute for Defence Studies and Analyses, New Delhi, India. She has a background of engineering with bachelor's degree in Electronics and communications engineering and master's degree in Nuclear Science & Technology engineering from Mody University, India.

South Asian Voices