

SPECIAL **REPORT** no. 160

Nuclear Safety and Security in India: Emerging Threats and Response Preparedness

Rajeswari Pillai Rajagopalan and Pulkit Mohan



S E P T E M B E R 2 0 2 1

Introduction

The nuclear domain is constantly grappling with challenges of existing and emerging threats in terms of both nuclear safety and security. Perceptions around nuclear security threats became particularly serious after the 9/11 terrorist attacks in the United States (US). Since then, the international nuclear community has channeled their efforts to build and strengthen global institutions, norms, and regimes in order to build and/or sustain robust and protective mechanisms in the nuclear security domain.

The International Atomic Energy Agency (IAEA) defines nuclear safety as “the achievement of proper operating conditions, prevention of accidents or mitigation of accident consequences, resulting in protection of workers, the public and

the environment from undue radiation hazards.”¹ On the other hand, nuclear security, according to IAEA is “the prevention and detection of, and response to, criminal or intentional unauthorized acts involving nuclear material, other radioactive material, associated facilities or associated activities.”² Nuclear security also encompasses “The prevention and detection of and response to, theft, sabotage, unauthorized access, illegal transfer or other malicious acts involving nuclear material, other radioactive substances or their associated facilities.”³ While both are aimed at safeguarding nuclear materials and protecting humans and the environment around them, the similarity ends there.

Attribution: Rajeswari Pillai Rajagopalan and Pulkit Mohan, “Nuclear Safety and Security in India: Emerging Threats and Response Preparedness,” *ORF Special Report No. 160*, September 2021, Observer Research Foundation.

Nuclear security is primarily about intentional and malicious actions that could threaten human lives; nuclear safety, meanwhile, is about ensuring that rules, regulations and standard operating procedures (SOPs) are adhered to in order to avoid any accident.⁴

The past decade has seen renewed interest in updating mechanisms to counter nuclear security threats at both the domestic and international levels. The Nuclear Security Summits, and the national pledges made during those events, are manifestations of such focus. In the Indian context, the security environment warrants additional attention to nuclear safety and security mechanisms, specifically the institutional infrastructure in an effort to strengthen policies and practices further.

The growing worries are not unfounded. As of the end of 2019, the Incident and Trafficking Database (ITDB) of the IAEA contained 3,686 confirmed incidents classified as “unauthorised activities and events” that involved nuclear and other radioactive material, going back to 1993.^a In 2019 alone, there were 189 such incidents.⁵

Globally, the Nuclear Security Summit (NSS) initiative, first held in 2010, was an international effort to bring focused attention on the security of nuclear materials across the globe and address the vulnerabilities that might exist in the security practices. Three such other summits have been held since—in 2012, 2014 and 2016. Though this effort was not under the aegis of the United Nations, it helped in getting many countries to make individual pledges in the form of ‘gift baskets’, or voluntary national commitments. Inspired by the in-depth focus at the NSS, Prime Minister Narendra Modi made a promise to play a leading role to keep the discussions going.

A robust discussion on nuclear safety and security requires a deeper look at the various issues that govern the success and improvement of the nuclear safety and security architecture. This report identifies the importance of nuclear safety and security by analysing existing programmes, practices, and infrastructures as well as insider threat, emergency response preparedness, and emerging technology threats.

a The IAEA established the ITDB in 1995 to track nuclear security incidents such as theft, loss of material, and sabotage. The database also monitors incidents of illicit trafficking and other unauthorised activities and events involving nuclear and other radioactive material.

Safety and Security in the Nuclear Power Sector

At present, there are 443 Nuclear Power Reactors in operation in 31 countries, generating approximately 10 percent of electricity worldwide. Additionally, 52 reactors are under construction, mostly in China, India, and Russia.⁶ The massive accident at the Fukushima nuclear power plant in Japan in March 2011 caused no loss of life,^b but disrupted the global nuclear renaissance as several countries decided to phase out their nuclear power programmes.

India is not deterred, though, owing to its large-scale requirements for diversified energy sources. However, the country has been tightening its safeguards to ensure better nuclear security practices. There are 23 nuclear power reactors in

operation today across India, with an additional 11 under construction.⁷ The country has also signed a number of nuclear cooperation agreements with countries including the US, Russia, France, Canada, and UK.⁸

Nuclear power is crucial in many countries' development goals, including India, as renewable energy sources such as wind and solar are not sufficient to meet energy requirements as well as global climate goals. Nuclear power presents India with the opportunity to enhance its energy security and help reduce global CO₂ emissions and minimise global warming and climate change.

^b Following a massive earthquake and tsunami, the power supply and cooling of three reactors, caused a major nuclear accident. This accident caused the three reactor cores to melt and high radioactive release of around 940 PBq. The accident led to all four of the Fukushima Daiichi reactors being written off and required two weeks to stabilise the reactor units with water.

“India was not deterred by the Fukushima accident, given its large-scale requirements for diversified energy sources.”

Indeed, nuclear energy is vital to ensuring that affordable energy is available to all; its role in the promotion of clean energy cannot be ignored. It has emerged as an important carbon-free energy option to generate electricity in a safe and sustainable manner. The 2019 World Energy Council report stated that “nuclear energy will feature in the future global energy mix and make its contribution to sustainable development.”⁹ For nuclear energy to take its place as a major low-carbon energy source,

states must address issues of cost, policy, and safety. Nuclear energy projects must incorporate designs with inherent and passive safety features. Nuclear safeguards are of paramount importance for public acceptance and long-term sustainability of nuclear power. Nuclear facilities also require nuclear security features to prevent clandestine diversion of fissile and fertile materials for non-peaceful use.

Emergency Response Preparedness

Policy and Approach

Emergency response preparedness is an essential aspect of nuclear safety and security. According to the IAEA, emergency response preparedness refers to effective national and global response arrangements and capabilities to minimise the impacts from nuclear and radiological incidents and emergencies.¹⁰

India has an extensive nuclear energy establishment, and as such is required to promptly and adequately determine and effectively undertake appropriate action to protect the public and emergency workers. Emergency response within nuclear facilities operates through three phases: early and intermediate (response), and late (recovery). Emergency management involves different types of exercises. For example, table-top exercises are conducted periodically with an

emphasis on the decision-making processes and protective actions in the early phase of an emergency. These exercises are based on emergency classifications divided across levels of emergency action as well as real-time analyses.

In the Indian atomic energy sector, Integrated Command Control & Response (ICCR) Exercises focus on testing command and control functions, response mechanisms, and communication.¹¹ ICCR exercises also include activation of the emergency response framework and response centres (site emergency center, off-site emergency support center, emergency operation center); execution of response functions by the Nuclear Power Corporation of India Limited (NPCIL),

Department of Atomic Energy (DAE), and district authorities; effectiveness of the liaison between on-site and off-site facilities for sharing information and making decisions; and checking the response timeline for declaration, activation and initial response, as well as coordination between plant and district authorities for the preparation of media briefings and press releases. Additionally, given the proximity of population centres to nuclear facilities, field exercises and public interactions are an important requirement of emergency management in India.

Newer reactors in India are equipped with built-in safety measures that are designed to minimise risks. For example, new light water and heavy water reactors at nuclear plants such as Tarapur nuclear power plant in the state of Maharashtra¹² and the Kudankulam Nuclear Power Plant in Tamil Nadu¹³ have *double containment* to ensure that nuclear material is confined in case of a nuclear emergency. Pressurised water reactors (PWRs) are equipped with steel line double containment that meet international guidelines. These safeguards, based on technology developed in Fukushima, are indigenously developed in India. They form part

of the country's efforts to build robust mitigation measures as well as reduce the risk in evacuation environments and impact on locals in nearby areas.

India has designed a number of control centres responsible for nuclear safety, based on Fukushima safety measures.^c India's DAE and the Atomic Energy Regulatory Board (AERB) have 24x7 emergency control rooms that have a human crew who monitor and respond to emergencies. India's National Disaster Management Authority (NDMA) has its own system as well and coordinates with other agencies on safety measures.¹⁴ Additionally, India has on-site emergency response centres to plan and initiate actions based on the phase and level of emergencies. The safeguards mechanism is designed to interact and coordinate across agencies to effectively identify and respond to emergency situations.

c After the Fukushima accidents, a number of countries reassessed their nuclear safety measures to undertake stronger safety protocols for their nuclear plants. These measures include “‘stress tests’ to reassess the design of nuclear power plants against site specific extreme natural hazards; installing additional backup sources of electrical power and supplies of water, and strengthening the protection of plants against extreme external events; and changes and reforms of organizational and regulatory systems”. In India, safety enhancements included “additional emergency power sources, enhanced onsite water inventories, external water injection arrangements (Hook up points), measures related to hydrogen management, containment venting provision, seismic trip, mobile pumps, onsite emergency support Centre” See: <https://www.iaea.org/newscenter/news/five-years-after-fukushima-making-nuclear-power-safer> & <https://inis.iaea.org/search/searchsingleRecord.aspx?recordsFor=SingleRecord&RN=47088348>

The nuclear power infrastructure in India also has off-site emergency support centres. These centres are responsible for intermediate phase-level emergency and can handle protective action recommendations based on field measurements including changes/lifting of early phase actions, action for identification of actual affected areas through measurement and survey, protective action recommendation based on field survey and assessment, as well as preparation of write-ups for media briefings. Favourable public opinion is an important aspect of confidence-building measures and must be predicated upon continuous and better communication at the local and national levels between nuclear authorities and the public.

Inter-Agency Coordination

The objective of emergency preparedness is to prevent and minimise the impact of any nuclear or radiological incident on both workers and the larger public. The response plan for a nuclear emergency entails notification, activation, request for assistance, and protective action. First responders to such emergencies are required to prevent spread of contamination and restrict entry to the area of accident.^d Key is recognising the

existence of an emergency situation, identifying and characterising the source and origin, monitoring the magnitude, and providing reliable communication to personnel from medical, civil, police and transport agencies.

Responding to emergency situations requires continuous assessment of emergency levels, determining the area for counter-measures, decision-making on protective measures for public and the surrounding environment, as well as prediction of contamination levels. For example, the DAE's Emergency Control Room (ECR)¹⁵ is responsible for the dissemination of authentic information regarding emergencies to the control rooms and response teams across agencies such as the AERB. The nearest ECRs are alerted for response deployment and briefings for further information dissemination. Based on the information provided through timely briefings, the level of emergency and conclusion of the emergency is determined by the AERB.

^d They may also be responsible for lifesaving rescue, emergency first-aid as well as response to loss or theft of material. The first responders include fire personnel, radiation protection experts and officers.

The action plan for emergency response teams involves collection of emergency kits, reaching incident sites, informing other teams about their arrival, identifying all possible hazards, carrying out radiological assessment of the area/ orphan source, determining the cordoned area, assessing contamination level, identifying hotspot or locating the source, identifying the source, advising on decontamination measures, collecting soil, gas, water sampling for analysis and finally, initiating source recovery operation. SOPs are in place that factor in communication, fire, plant, site, offsite, transportation and public emergencies.

India's national emergency response system architecture is a combination of the Indian Environmental Radiation Monitoring Network (IERMON) network,¹⁶ ERC network,^e meteorological

data network, emergency communication rooms, Crises Management Group (CMG), National Technical Research Organisation (NTRO),¹⁷ and NDMA. Effective and procedural communication between all actors and institutions involved in emergency response is a crucial aspect in averting crises as a result of an emergency. Successful inter-agency coordination and provision and dissemination of accurate information are key to handling an emergency efficiently.

e The ERC network consists of 23 DAE ERCs and 7 National Disaster Response Force (NDRF) ERCs.

The Human Factor

Nuclear Security Culture and Personnel Reliability

The roles played by different actors—international organisations, the state, the public, employees, managers, and licensees—are key to shaping a nuclear security culture. Nuclear safety and security require the bridging of divergent cultures as they often involve individuals from diverse backgrounds and experiences. A positive security culture incorporates norms, attitudes, beliefs, and values that determine how people are expected to behave in order to ensure security practices of an organisation to contribute to effective daily operations.

‘Nuclear safety culture’ refers to the assembly of characteristics and attitudes in organisations and individuals, establishing nuclear safety as an overriding priority, wherein nuclear plant safety issues receive the attention warranted by their significance. It also ensures that human actions are consistent, appropriate, and correct, aiming

to prevent human error to the maximum level possible, all of which is predicated upon openness, transparency, and information sharing.

‘Nuclear security culture’, meanwhile, is the assembly of characteristics, attitudes and behaviours of individuals, organisations and institutions which serves as a means to support and enhance nuclear security. This relies on trustworthiness, honesty and integrity of individuals not to engage in malicious acts and is based on compartmentalisation, secrecy, and classifications.

An effective nuclear security culture depends on proper planning, training, awareness, operations, and maintenance as well as on the actions of people who plan, operate, and maintain nuclear security systems. An organisation may be technically competent while remaining vulnerable if it discounts the role of the human factor. Human factor^f is important to maintaining effective nuclear security.

^f The concern is not only the rank-and-file, but also includes the upper-tier of managers and leaders.

Humans either comply with rules-based frameworks or challenge and question them as a result of their attitudes and value systems. In order to promote an effective security culture, it is important to encourage employees to support and contribute to security objectives rather than feeling like they are simply the passive victims of security rules and regulations.

The biggest threat to nuclear security lies in complacency. Such threat may arise because of absence of security-related crises, low priority of security in operational activity, human nature for denial and skepticism, failure of senior management to act as role models, scarcity of resources, outdated procedures, and poor attitude towards those that report faults and flaws or issues from management.

Cross-functional communication is an important pillar of a positive culture, which is based on trust and listening. This requires the establishment of need-to-know levels of information for individuals, on a hierarchical basis and based on security clearances, while also prioritising transparency to the highest possible level. A need-to-know hierarchy allows security departments to share relevant information openly with their cross-functional counterparts within the organisation while still maintaining confidentiality for classified information. Additionally, it is important to seek

common ground between management and security personnel to further promote a positive security culture. A positive need-to-know model would be based on the convergence of position (threat perception and information sharing), interests (jobs, safety, efficiency, preventing crises) and needs (protecting the health and safety of families and communities), where exchanging information and conflict-resolution together is possible.

Personnel reliability programmes

Personnel reliability programmes (PRPs) require basic understanding of what motivates people who are a crucial asset in the workplace. These programmes are developed as a result of careful screening and vetting potential employees in the ‘pre-employment’ stage to observing and assessing employees in the ‘during-employment’ stage, to carefully managing the separation process in the ‘post-employment’ stage. A variety of measures are generally applied on a graded basis.

PRPs include the following:

1. Continuous employee evaluations
2. Behavioural observations
3. Periodic drug and alcohol tests
4. Supervisory interviews
5. Security clearances through comprehensive background checks and vetting process
6. Management reviews
7. Training related to human reliability
8. Financial reviews
9. Security personnel file evaluations
10. Routine or random polygraph testing
11. Medical and psychological evaluations

PRPs require a focus on recognising behaviour that is concerning or deviant, reporting of serious concerns, special considerations for reporting security-related concerns, reporting policy written standards, in-house complaint process, developing employee discussions and focus groups, and a security liaison programme. A security management programme effectively engages with regulatory bodies and civic society.

Security Culture

Trends in nuclear security refers to features that are well-established in security cultures across the world. One example is ‘security by design’, in which facilities and systems are designed from the outset to accommodate the needs and requirements of both security and safety. Similarly, material control and accountancy (MC&A) systems are used to detect and prevent the misuse of nuclear and other radioactive material—both internationally and within a particular State. Modeling and simulation (M&S) and such other approaches contribute to security planning, assessment, training and emergency response and continuous maintenance of security-related aspects in nuclear facilities.

Threat identification in nuclear security occurs through a Design Basis Threat (DBT) system that looks at identifying potential threats in detail so that nuclear security standards and protection measures can be designed and implemented to counter them through a graded approach. Such an approach helps avoid the possibility of ineffective security measures that may leave materials vulnerable, as well as excessive security measures that could unnecessarily impact operations and security measures.

Nuclear security trends emphasise on the “defense-in-depth” principle which involves multiple layers of systems and measures that must be circumvented before physical protection is compromised. Over the years, new challenges to nuclear security continue to emerge such as cyber threats i.e., internet security, mobile devices, The Internet of Things (IOTs) and social media, threats to Industrial Control Systems (ICSs) that comprise devices that control, monitor, and manage critical infrastructure in industrial sectors.

Insider Threat in the Changing Security Context

While rare, insider threat is among the most critical obstacles to maintaining effective nuclear security. Sabotage must be treated seriously as there has been an increase in the number of incidents globally involving employees who may either have been radicalised or coerced, or else motivated by financial greed or simply disgruntled. An insider threat could succeed with a combination of needs and motivations, access, and opportunity, as well as knowledge of assets and operations. Based on clearance levels, an insider may possess in-depth knowledge of systems, procedures and personnel which can be used against the organisation. Personnel reliability programmes are therefore important.

To reduce insider threat, it is important to develop ethical leadership, strengthen synergy between nuclear safety and security, improve security culture, provide clear written procedures and promote its adherence, and establish open communication channels. The establishment of human reliability programmes with continuous employee evaluation, comprehensive background checks, and medical and psychological evaluations further work to reduce insider threat.

The process of background checks and vetting done prior to employment is also essential to verify criminal antecedent behaviors by local law enforcement. Additionally, special verification by central agencies as well as positive vetting or re-vetting undertaken while in a sensitive job is essential. Likewise, for contractors, similar procedures exist.

In recent times, the COVID-19 pandemic has had a massive impact on individuals and given rise to fear and uncertainty on their work front as well as in their personal lives. In this regard, the possible manifestation of an insider threat—theorised as a combination of personal predisposition, stressors, and concerning behaviours—should not be ruled out.

Emerging Cybersecurity Challenges

Cyber threats present a new and unique challenge to nuclear systems and facilities and therefore require appropriate policies. These encompass cyber terrorism, cyber espionage, malware attacks, and distributed denial of service (DDoS). In 2003, for example, the Davis-Besse Nuclear power plant in Ohio, US, suffered a computer worm infection which compromised the safety control system for over four hours; in 2015, hackers targeted the Hanford nuclear site in Washington to gain sensitive information.

A cyber-nuclear security nexus demands an assessment of the origins of the threats. Threats can emerge from state actors, non-state actors (such as terrorist organisations, hackers, lone-actors) and insiders. The severity of an attack can be determined through level of access gained into the systems. Infiltration of malware or viruses into the systems can occur at several stages in the production and supply chain.¹⁸

Cyber-attacks have economic, operational, and reputational costs to a country. Any breach of safety gives rise to distrust of the systems and may negatively impact relations with allies and partners as well as adversaries alike and call into question the reliability of a country possessing nuclear materials.

Insider threat manifestation in the area of cyber vulnerabilities cannot be ruled out either. Nuclear security is predicated upon the human factor and therefore, increases the threats to nuclear systems. As nuclear systems are managed and operated by individuals with different security clearances, insider threats occur in the case of cyber security through possible exposure of the structure to cyber infiltration from within.

The importance of cyber security of the nuclear architecture is not any different for India. In 2013, the Department of Electronics and Information Technology released its first-ever policy framework to articulate a national cyber security policy. India has a number of institutions responsible for cyber security. India's defense cyber agency creates mechanisms within the security infrastructure to battle cyberwarfare and cyber infiltration in India's defense networks.^g

The September 2019 cyber-attack on the Kudankulam Nuclear Power Plant highlighted the importance of strengthening the country's cyber-nuclear security infrastructure. ISRO also confirmed that it was alerted to a breach attempt by the same virus that targeted Kudankulam. The CISAG and CERT-In carried out cyber security audits and argued for further strengthening of the cyber security framework through "hardening of internet and administrative intranet connectivity, restriction on removable media, blocking of websites & IPs which have been identified with

malicious activity etc."¹⁹ Therefore, it is important to strengthen atomic energy infrastructure against cyber threats using preventive access tools and continual assessment and improvement of the cyber security infrastructure in the nuclear domain.

India would do well to draw lessons from the experiences of other countries like the US, UK, and Japan, which have advanced cyber systems to strengthen cyber protection of their nuclear infrastructure. India could also engage in multilateral dialogues, and collaborate with the private sector in order to build a robust cyber security system for its nuclear architecture.

^g Additionally, the NTRO is responsible for India's cyber intelligence and counterintelligence operations. There also exists a network of Indian Computer Emergency Response Team (CERT-In) at the local level which reports to a national level CERT-In for emergency response in the cyber domain. The Computer Information and Security Advisory Group (CISAG) was set up with the DAE to audit IT systems as the risks of potential attacks on systems have increased.

Conclusion

Fostering Safety and Security Practices

The onus of responsibility for nuclear safety and nuclear security remains with the individual sovereign nation. Yet, this is also an issue that requires greater global cooperation. Principles ensuring nuclear security are based on multi-tier protection systems, and involving technological aspects, security framework, and SOPs, all firmly instituted and scrupulously enforced.

National commitment to nuclear security requires legal instruments (conventions and treaties), high-level national engagement (NSS; other global initiatives, e.g., Global Initiative to Combat Nuclear Terrorism (GICNT); IAEA's Ministerial Conference on Nuclear Security (ICONS)); multi-lateral engagement (forum, initiatives by IAEA, GICNT); bilateral cooperation and engagements; as well as track-two platforms.

National systems for nuclear security must work towards legal provision and empowerment through framework and regulatory systems and entities in order to build technological capability and capacity. Effective implementation and enforcement is important in fostering a nuclear security culture that is efficient.

Periodic reviews are essential to ensure improvement of nuclear security systems. India is party to 13 Instruments to combat international terrorism, including the International Convention for the Suppression of Acts of Nuclear Terrorism (ICSANT), and the Convention on the Physical Protection of Nuclear Material (CPPNM). In order to promote India's cooperation with the international community, it supports and voluntarily adopts the IAEA Code of Conduct on the safety and security of radioactive sources and applies IAEA guidance on physical protection of nuclear materials.

India also adheres to NSG guidelines on supply of nuclear items, participates in IAEA's ITDB, and cooperates with Interpol's Radiological and Nuclear Terrorism Prevention Unit & World Customs Organisation. India's proposal at the NSS for a Global Centre for Nuclear Energy Partnership GCNEP-DAE in Bahadurgarh has been viewed as a signal of India's willingness to share its nuclear expertise and cooperate with other nations.

India could strengthen its leadership role in nurturing global governance measures on nuclear security. Legal instruments such as the CPPNM are a case in point. A peer review mechanism was explicitly excluded during the negotiations of the CPPNM 2005 Amendment. However, there is scope for individual Parties to share their experiences on implementation for the benefit of all and to discuss areas where international cooperation, criminalisation or extraditions have been either successful or problematic. The goal is to achieve high standards of implementation, which supports the purpose of the Convention.


Future Trends

Nuclear security is important for India for a number of reasons. As India has a large nuclear programme and its atomic energy facilities are spread across the country, and also considering that the country's immediate neighbourhood is not benign, there are significant vulnerabilities to nuclear terrorism and other threats. There is a growing need for international consensus on how to continually work and improve the nuclear safety and security infrastructure. For example, the CPPNM amendment has brought together different actors on the same platform to take a deeper look at nuclear security.

The paradox is that nations are faced with the dilemma of what level of information should be shared in the interest of nuclear security. At an international level, nations lean towards discussing their achievements more than the shortcomings and subsequent lessons learned. Furthermore, international cooperation is hampered by ongoing geopolitical issues.

“India should strengthen its leadership role in nurturing global governance measures on nuclear security.”

Given the catastrophic consequences of a nuclear security incident, states must come together to frame new rules of the road, akin to the IAEA Convention on Nuclear Safety. This process should ensure the participation of all states and other stakeholders.

Even as there might be compromises to accommodate different stakeholder perspectives, an instrument that has the inclusion of a large number of stakeholders can help in better adherence to global norms. 

This special report is a by-product of the discussions that took place at a virtual closed-door roundtable discussion organised by ORF in December 2020. Due to the sensitive nature of the subject, details of participants are not provided.

Endnotes

- 1 European Nuclear Safety Regulators Group, “What is nuclear safety?”, ENSREG <http://www.ensreg.eu/nuclear-safety#:~:text=The%20main%20objective%20of%20nuclear,environment%20from%20undue%20radiation%20hazards.&text=The%20work%20of%20nuclear%20regulators%20covers%20all%20these%20aspects>.
- 2 International Atomic Energy Agency, “Nuclear Security Series Glossary, Version 1.3,” December 2015, <https://www.iaea.org/sites/default/files/18/08/nuclear-security-series-glossary-v1-3.pdf>, 18.
- 3 IAEA, “Nuclear Security Series”
- 4 Edward Waller, “The Interface of Safety and Security in the Response to a Malicious Act,” Presented at the International Experts Meeting on Assessment and Prognosis in Response to a Nuclear or Radiological Emergency, IAEA Headquarters, Vienna Austria, 20-24 April 2015, <https://www-pub.iaea.org/iaecameetings/IEM9p/Session3/6Waller.pdf>
- 5 International Atomic Energy Agency, “Incident and Trafficking Database (ITDB)- 2020 Fact Sheet,” <https://www.iaea.org/sites/default/files/20/02/itdb-factsheet-2020.pdf>
- 6 World Nuclear Organisation, “Nuclear Power in the World Today,” March 2021, <https://www.world-nuclear.org/information-library/current-and-future-generation/nuclear-power-in-the-world-today.aspx>
- 7 World Nuclear Organisation, “Nuclear Power in India,” Updated June 2021, <https://world-nuclear.org/information-library/country-profiles/countries-g-n/india.aspx>
- 8 Pulkit Mohan and Pallav Agarwal, “India’s Civil Nuclear Agreements: A New Dimension in India’s Global Diplomacy”, ORF Issue Brief No. 320, October 2019, Observer Research Foundation <https://www.orfonline.org/research/india-civil-nuclear-agreements-new-dimension-india-global-diplomacy/>
- 9 World Energy Council, “World Energy Issues Monitor 2019,” <https://www.worldenergy.org/assets/downloads/1.-World-Energy-Issues-Monitor-2019-Interactive-Full-Report.pdf>
- 10 International Atomic Energy Agency, “Emergency preparedness and response,” <https://www.iaea.org/topics/emergency-preparedness-and-response-epr>
- 11 Atomic Energy Regulatory Board, *AERB Annual Bulletin 2019*, https://www.aerb.gov.in/images/PDF/Annual_Bulletin/2019.pdf

- 12 Department of Atomic Energy, “Reactor Unit-3 of RAPP Commences Commercial Power Generation”, Vol. 34/NO.1-2, July-Aug 2000, Government of India <https://dae.gov.in/node/171>; Nuclear Threat Initiative, “Tarapur Atomic Power Station (TAPS),” September 1, 2003, <https://www.nti.org/learn/facilities/77/>
- 13 Nuclear Power Corporation of India Limited, “Kudankulam Nuclear Power Plant,” https://www.npcil.nic.in/content/823_1_KnowaboutKKNPP.aspx
- 14 National Disaster Management Authority, “Nuclear and Radiological Emergency,” <https://ndma.gov.in/Man-made-Hazards/Nuclear>
- 15 Department of Atomic Energy, “Crisis Management Group,” https://dae.gov.in/writereaddata/CMG_contact.pdf
- 16 Department of Atomic Energy, “Indian Environmental Radiation Monitoring Network (IERMON),” <https://dae.gov.in/node/304>
- 17 Government of India, “National Technical Research Organisation”, <https://ntro.gov.in/>
- 18 Pulkit Mohan, “Cyber Security in India’s Nuclear Systems,” ORF Issue Brief No. 412, October 2020, Observer Research Foundation <https://www.orfonline.org/research/ensuring-cyber-security-in-indias-nuclear-systems/>
- 19 Government of India, Department of Atomic Energy, Rajya Sabha “Starred Question No. 109: Cyber-attack on Kudankulam Nuclear Power Plant”, 28 November 2019, <https://dae.gov.in/writereaddata/rssq109.pdf>

About the Authors

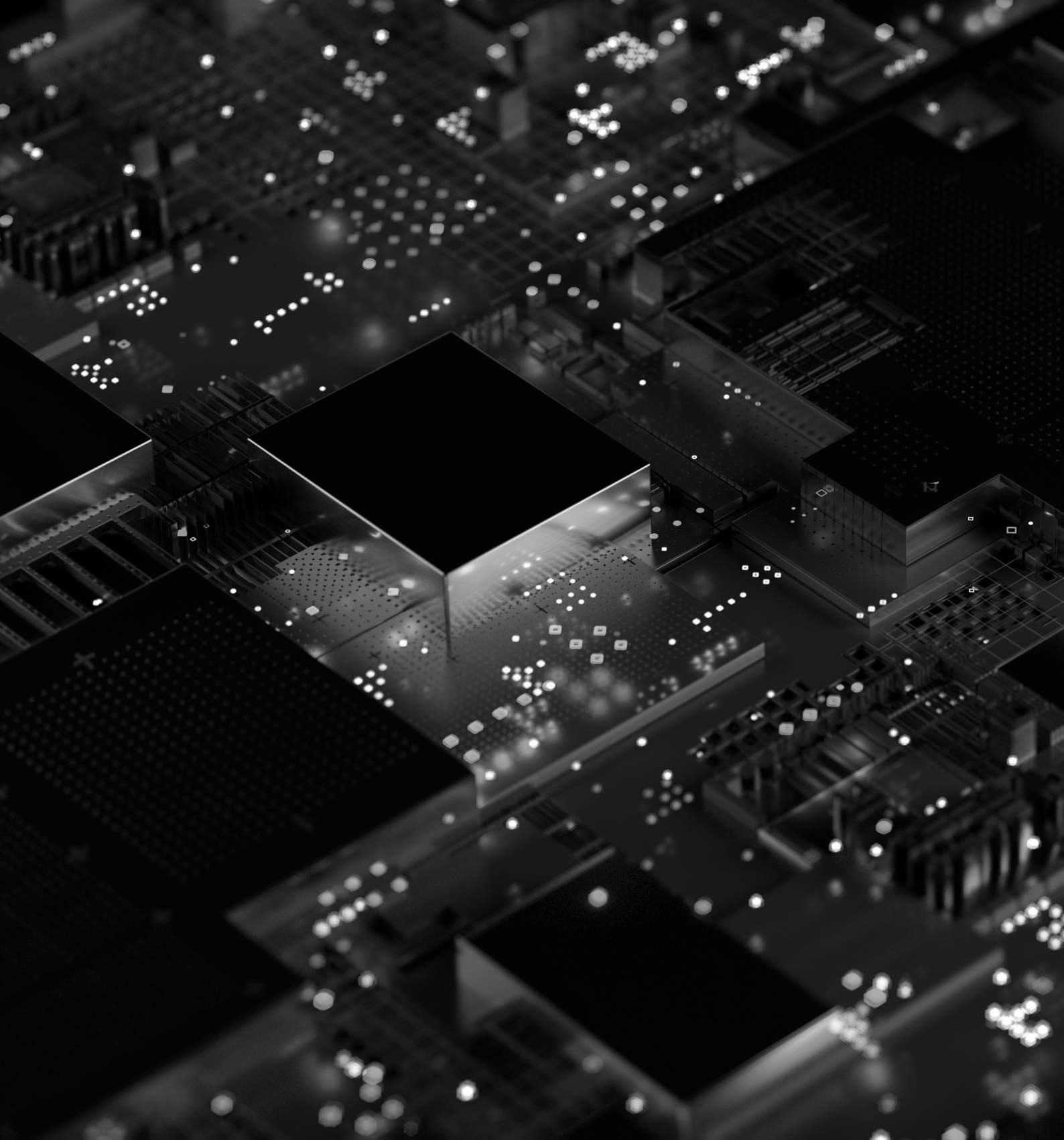
Dr. Rajeswari Pillai Rajagopalan is Director of ORF’s Centre for Security, Strategy and Technology (CSST).

Pulkit Mohan is Associate Fellow at ORF’s CSST.

The authors would like to thank Nitansha Bansal for producing background notes based on an ORF workshop on nuclear security.

Cover image: Getty Images/Rajkumar Nagarajan-EyeEm

Back cover image: Getty Images/Andriy Onufriyenko



Ideas . Forums . Leadership . Impact

**20, Rouse Avenue Institutional Area,
New Delhi - 110 002, INDIA
Ph. : +91-11-35332000. Fax : +91-11-35332005
E-mail: contactus@orfonline.org
Website: www.orfonline.org**