CENTRE FOR SCIENCE
& SECURITY STUDIES

KING'S College LONDON

Exploring nuclear and radiological security in South Asia

A case study handbook

Edited by Dr Zenobia Homan and Amelie Stoetzel

2022

Contents

Commonly used abbreviations

AEC	Indian Atomic Energy Commission
AECH	Atomic Energy Cancer Hospital (India)
AERB	India's Atomic Energy Regulatory Board
AI	Artificial Intelligence
AMD	India's Atomic Minerals Directorate
BARC	Bhabha Atomic Research Centre
BHAVINI	Bharatiya Nabhikiya Vidyut Nigam Limited
CADD	Pakistan's Capital Administration Development Division
CBM	Confidence Building Measure
CENUM	Pakistan's Centre for Nuclear Medicine
CISF	Central Industrial Security Force (India)
CGPC	Cyber Governance Policy Committee
CHASNUPP	Chashma Nuclear Power Complex
CPPNM	Convention on the Physical Protection of Nuclear Materials
CSDS	Pakistan's Cyber Security and Digital Safety Project
DAE	India's Department of Atomic Energy
DPP	Document Preparation Profile (Pakistan)
ECIL	Electronics Corporation of India Limited
FIA	Pakistan's Federal Investigation Agency
FNPP	Floating Nuclear Power Plant
GCNEP	India's Global Centre for Nuclear Energy Partnership
HEC	Higher Education Commission (Pakistan)
IAEA	International Atomic Energy Agency
IGCAR	Indira Gandhi Centre for Atomic Research
INFCIRC	Information Circular (IAEA)
IREL	Indian Rare Earths Limited
IRRS	Integrated Regulatory Review Service (India)
ISO	International Organisation for Standardisation
ISRO	Indian Space Research Organisation
KANUPP	Karachi Nuclear Power Complex
KKNPP	Kudankulam Nuclear Power Plant
NAP	National Action Plan (Pakistan)
NC3	Nuclear Command, Control, and Communication
NCA	Pakistan's National Command Authority
NCCS	Pakistan's Centre for Cyber Security
nCERT	National Computer Emergency Response Team (Pakistan)
NCOC	Pakistan's National Command and Operation Centre
NCSP	National Cyber Security Policy (Pakistan)
NEPRA	Pakistan's National Electric Power Regulatory Authority
NIAB	Pakistan's Nuclear Institute for Agriculture and Biotechnology
NIFA	Pakistan's Nuclear Institute for Food and Agriculture
NIMRA	Pakistan's Nuclear Institute of Medicine and Radiotherapy
NISAS	Pakistan's National Institute of Safety and Security
NNSA	US National Nuclear Security Administration
NPCIL	Nuclear Corporation of India Ltd
NPP	Nuclear Power Plant
NR3C	Pakistan's National Response Centre for Cyber Crime
NRECC	Pakistan's National Radiation Emergency Coordination Centre
NSP	National Security Policy (Pakistan)
NSRA	Nuclear Safety Regulatory Authority (India)
NSS	Nuclear Security Summit
NSS	Nuclear Security Series (IAEA)
NTDC	Pakistan's National Transmission and Despatch Company
OSINT	Open Source Intelligence
PACT	IAEA Programme of Action for Cancer Therapy
PAEC	Pakistan Atomic Energy Commission
PakCERT	Pakistan Computer Emergency Response Team
PANT	Pakistan's Peaceful Applications of Nuclear Technology
PCENS	Pakistan Centre of Excellence for Nuclear Security
PDM	Pakistan Democratic Movement
PECA	Prevention of Electronic Crimes Act (Pakistan)
PIEAS	Pakistan Institute of Engineering and Applied Sciences
PNRA	Pakistan Nuclear Regulatory Authority
PRP	Pakistan's Personnel Reliability Programme
PSDP	Pakistan's Public Sector Development Program
QUANUM	Quality Management Audits in Nuclear Medicine (IAEA)
RANET	Pakistan's Response and Assistance Network
RRCAT	Raja Ramanna Centre for Advanced Technology
RSO	Radiation Safety Officer
SDG	Sustainable Development Goal
SECDIV	Pakistan's Strategic Export Control Division
SKMCH	Shaukat Khanum Memorial Cancer Hospital
SMR	Small Modular Reactor
SOP	Standard Operating Procedure
SPD	Pakistan's Strategic Plans Division
UCIL	Uranium Corporation of India Limited
VECC	India's Variable Energy Cyclotron Centre
VVER	Voda Voda Energy Reactor

Exploring nuclear and radiological security in South Asia

A case study handbook

Edited by Dr Zenobia Homan and Amelie Stoetzel

About the Centre for Science & Security Studies

The Centre for Science & Security Studies (CSSS) is a research centre in the Department of War Studies at King's College London. Since 2003, CSSS has been bringing together multidisciplinary teams of experts from academia, government and industry, with backgrounds in sciences, social sciences and humanities. Members of the centre conduct academic and policy-relevant research on non-proliferation, disarmament, arms control, verification, open source intelligence and mass effect terrorism, with emphasis on the chemical, biological, radiological and nuclear (CBRN) dimension.

About the editors

Dr Zenobia Homan is a project coordinator and Research Fellow in the Centre for Science & Security Studies at King's College London. She organises international professional development courses and related engagements in a number of regions including South Asia. She also conducts research relating to CBRN security, particularly focussing on language and communication.

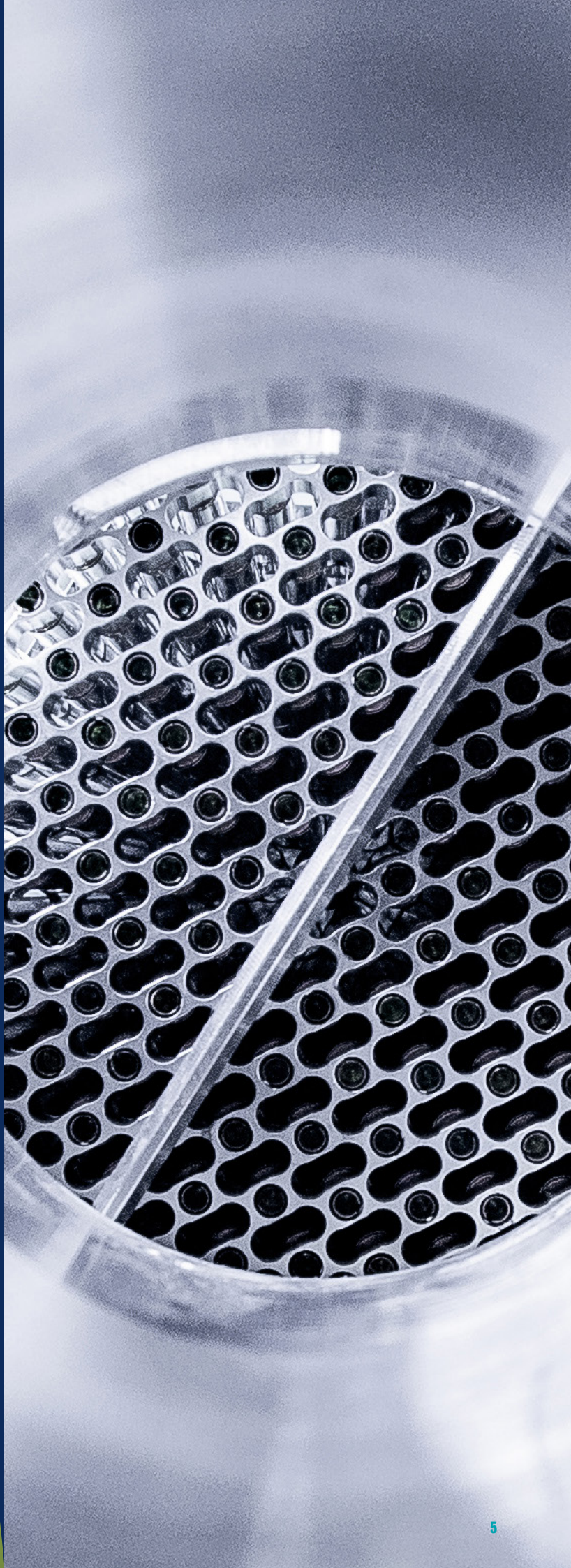
Amelie Stoetzel is a PhD candidate and research assistant in the Centre for Science & Security Studies at King's College London. Her research interests include proliferation risks of small modular reactor designs and related advanced fuel cycle technologies.

Published by King's College London in the Centre for Science & Security Studies.
Centre for Science & Security Studies
Department of War Studies
King's College London
Strand
London WC2R 2LS
United Kingdom

kcl.ac.uk/csss
@KCL_CSSS

I. Introduction

by Dr Zenobia Homan and Amelie Stoetzel



The aim of this handbook is to explore how nuclear security systems have been developed and tested in South Asia.[1] The majority of existing case study handbooks focus on examples from the west – while both India and Pakistan have mature nuclear industries from which much can be learned. King's College London believes that global nuclear security will benefit from diversifying available knowledge and information to enhance nuclear security promotion and education.

This handbook places emphasis on exploring nuclear security through a series of regional case studies. For example, the authors describe how governments in South Asia have sought to develop national regulations relating to nuclear and radiological materials. Specifically, case studies identify potential challenges in implementing a healthy security culture in a range of sectors – including research, policy, healthcare, agriculture, energy, and waste management. Important themes that occur throughout the case studies include the significance of clear communication, adherence to coordinated national and international standards, security awareness among all staff, and the ability to anticipate novel threats.

Background

In the past 20 years, security culture has played an increasingly important role in the protection of nuclear and radiological materials and other sensitive assets, reducing the possibility of terrorism and other threats. Historic cases of theft and sabotage have been attributed directly to weaknesses in personnel behaviour,[2] and it has also been found that disasters as big as the Chernobyl and Fukushima incidents had their roots in the human element.[3,4] Based on Edgar Schein's model of organisational culture and leadership, the International Atomic Energy Agency (IAEA) strongly promotes the importance of nuclear security culture, which it defines as 'the assembly of characteristics, attitudes and behaviour of individuals, organisations and institutions which serves as a means to support and enhance nuclear security'.[5] In tandem, the IAEA also encourages its member states to increase control, accounting and security of radioactive sources to prevent their malicious use and the associated potential consequences.

Attention for nuclear security was heightened following the September 2001 terrorist attacks in the United States and the 2010-16 Nuclear Security Summits (NSS), which lead to high-level cooperation and drastic changes in international security efforts. Pakistan and India were active participants during the NSS process, but both countries rank relatively low on the Nuclear Threat Initiative (NTI) Index for Nuclear Security.[6] The NTI Index emphasises the importance of societal factors, such as the presence of terrorist groups that may attempt to acquire nuclear material, and government malfeasance that could hinder the implementation of security regulations.[7] Pakistan and India continue to produce weapons-usable nuclear materials – while Pakistan has not ratified the International Convention for the Suppression of Nuclear Terrorism and India does not have an independent regulatory agency. They have several challenges in common; both have been called to improve control and accounting measures and to conduct security culture assessments.

1 South Asia is commonly used to refer to the region that encompasses Bangladesh, Bhutan, India, Pakistan, Nepal and Sri Lanka. In this handbook, it is primarily used to refer to the mature nuclear states of Pakistan and India.

2 Christopher Hobbs and Matthew Moran, 'Exploring the Human Dimension of Nuclear Security: The History, Theory and Practice of Security Culture', *The Nonproliferation Review*, 27(5/6).

3 International Atomic Energy Agency, 'Summary Report on the Post-Accident Review Meeting on the Chernobyl Accident', Report by the International Nuclear Safety Advisory Group, Safety Series No.75-INSAG-1, Vienna, 1986, p.76.

4 Committee on Lessons Learned from the Fukushima Nuclear Accident for Improving Safety and Security of U.S. Nuclear Plants; Washington (DC): National Academies Press (US); 29 October, 2014. https://www.ncbi.nlm.nih.gov/books/NBK253947/

5 International Atomic Energy Agency, 'Nuclear Security Culture', IAEA Nuclear Security Series, No. 7, Vienna, 2008. https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1347_web.pdf

6 Nuclear Threat Initiative, 'Nuclear Security Index', accessed 18 July, 2022. https://www.ntiindex.org/

7 Micah Zenko, 'The Hague Nuclear Security Summit: Opportunities for Pakistan and India', March 21, 2014. https://www.cfr.org/blog/guest-post-hague-nuclear-security-summit-opportunities-pakistan-and-india

With that said, it should be noted from the outset that this handbook is not centred around the Pakistan-India conflict and its intricacies, nor does it analyse lessons learned from a military context. Instead, it draws wider conclusions relevant to the security of the global civil nuclear sector. Each case study has been paired with discussion points, to generate debate equally amongst those with years of experience and newcomers to nuclear.

Contributors

This diverse collection of case studies was selected and written by authors from South Asia. Their choices in topics reflect which issues are currently of concern in this region. The research draws on openly available information (spring 2022), reinforced by insight from the contributors and their colleagues.

Dr Tahir Mahmood Azad is a Visiting Research Fellow at King's College London. He holds an MA in Defence & Strategic Studies from Quaid-i-Azam University, Islamabad, and a PhD from the Department of Strategic & Nuclear Studies, National Defence University. Dr Azad has worked at the Institute of Strategic Studies Islamabad and served as a Visiting Faculty Member at Bahria University.

Snekha Gunasekarann is an MSc student in International Relations with a focus on foreign policy at the London School of Economics and Political Science. She has worked with India's national newspaper, *the Hindu*, and conducted research with The Peninsula Foundation, an independent think tank based in Chennai.

Faraz Haider is a Research Associate at Air University, Islamabad. He works on projects that focus on international relations, strategy, and security. He has authored articles for Strafasia.com and has previously worked as a staff writer with *The International Scholar*.

Shayan Hassan Jamy is an MSc student of Strategic Studies at Air University, Islamabad. He has previously worked as an intern at the Arms Control & Disarmament Centre at the Institute of Strategic Studies, Islamabad. He has authored research papers and articles on topics including artificial intelligence, emerging technologies, and global strategic competition.

Aamna Rafiq is a Research Associate in the Arms Control & Disarmament Centre at the Institute of Strategic Studies, Islamabad. She has an BA in Politics and International Relations from the International Islamic University, Islamabad, and an MA in International Relations from Quaid-i- Azam University, Islamabad. Ms Rafiq has worked with the Arms Control and Disarmament Affairs Directorate of the Strategic Plans Division, the Pakistan Institute for Parliamentary Services, and she has assisted the Senate's Standing Committee on Defence Production at the Parliament of Pakistan.

Dr Salma Shaheen is an independent researcher and author. She holds a PhD from the School of Security Studies at King's College London, specialising in the impact of disruptive technologies, nuclear non-proliferation, international security, and deterrence. Previously, she worked as Assistant Director of Research at the Arms Control and Disarmament Affairs directorate of Pakistan's Strategic Plans Division. She regularly writes articles for platforms such as South Asian Voices and The News, Pakistan.

Haleema Saadia is a Lecturer in the Department of International Relations at the National University of Modern Languages, Islamabad. She is currently also pursuing a PhD at the National University of Sciences & Technology, and she is a Research Fellow at the ROADS Initiative, Islamabad.

Chandana Seshadri is an MA student in the School of Security Studies at King's College London. She previously attended Stella Maris College in Chennai, and now works on geopolitical risk analysis and defence research with a particular focus on South Asia.

A brief overview of civil nuclear developments in Pakistan and India

Nuclear power is a sensitive topic in South Asia. Since the 1998 nuclear tests, military discussions dominate the nuclear landscape in India and Pakistan. However, besides their weapon programmes, both countries also have a large civil nuclear sector with full fuel cycles. At the time of writing, Pakistan has six operable reactors,

providing 8% of the country's energy, and two research reactors.[8] India operates 23 nuclear power plants, generating 3% of the country's energy, as well as five research reactors.[9] Furthermore, 80 hospitals in Pakistan use nuclear and radiological substances for medical treatment,[10] and the country's regulator has listed more than 200 industry bodies as nuclear licence holders.[11] On a similar scale, as of 2021 India's regulator listed more than 350 hospital and medical research centres with licences for nuclear and radiological materials.[12]

Pakistan's pursuit of nuclear energy began in 1956 and saw the establishment of the Pakistan Atomic Energy Commission (PAEC). The development of Pakistan's regulatory framework can be traced back to 1965 when the country's first research reactor (PARR-I) was commissioned. After various iterations, the Nuclear Regulatory Authority (PNRA) became an independent body in 2001.[13] The emphasis then was on nuclear safety and licensing and radiation protection. Pakistan has a National Radiation Emergency Coordination Centre (NRECC) and a Response and Assistance Network (RANET). Pakistan has also embraced the 'Centre for Nuclear Excellence' concept, which promotes and shares best practices in nuclear security. This is done through three affiliated institutes: the Pakistan Centre of Excellence for Nuclear Security (PCENS), the National Institute of Safety and Security (NISAS), and the Pakistan Institute of Engineering and Applied Sciences (PIEAS).[14]

India has based the development of its nuclear sector on the idea of self-reliance.[15] It passed its first Atomic Energy Act in 1948, and its Atomic Energy Establishment, now Bhabha Atomic Research Centre (BARC), was set up in the 1950s with the construction of two small boiling water reactors. The following 1962 Atomic Energy Act allowed a central authority to develop, control, and use atomic energy in the country.[16] The main policy body in India is now the Indian Atomic Energy Commission (AEC). The Nuclear Power Corporation of India Ltd (NPCIL) is responsible for design, construction, commissioning, and operation of thermal nuclear power plants.[17] NPCIL is in turn administered by the Department of Atomic Energy (DAE). The institutions established under the Department include the NPCIL, which operates all nuclear power plants and implements projects for power generation based on the schemes and programmes of the government.[18] In addition, the Atomic Energy Regulatory Board (AERB) is responsible for the oversight, which is an executive authority under the President of India with a focus on 'safety and security of civilian facilities'.[19]

8 World Nuclear Association, 'Nuclear Power in Pakistan', Country Profiles, March 2022. https://world-nuclear.org/information-library/country-profiles/countries-o-s/pakistan.aspx

9 World Nuclear Association, 'Nuclear Power in India', Country Profiles, May 2022. https://world-nuclear.org/information-library/country-profiles/countries-g-n/india.aspx

10 Pakistan Nuclear Regulatory Authority, 'PNRA Licensed Medical Radiation Facilities valid upto 15-July-2021', Licensee Data, accessed April 18, 2022. https://www.pnra.org/licenseeData/Medical

11 Pakistan Nuclear Regulatory Authority, 'List of Valid Licensees till 31-03-2022', Licensee Data, accessed May 26, 2022. https://www.pnra.org/licenseeData/WebForm2

12 Atomic Energy Regulatory Board, 'List of Nuclear Medicine Facilities Licensed by AERB (as on 04 03 2021)', Nuclear Medicine, accessed May 26, 2022. https://www.aerb.gov.in/images/PDF/NuclearMedicine/RSD1.pdf

13 Pakistan Nuclear Regulatory Authority, 'History of PNRA', History, accessed June 21, 2022. https://www.pnra.org/history.html

14 Rabia Javed, 'International Community should recognize Pakistan as a Responsible Nuclear State', *South Asia Monitor, May 30, 2020*. https://www.southasiamonitor.org/spotlight/international-community-should-recognize-pakistan-responsible-nuclear-state

15 International Atomic Energy Agency, 'India', Country Profiles, accessed June 21, 2022. https://cnpp.iaea.org/countryprofiles/India/India.htm

16 Simran, 'Are there enough regulatory safeguards against nuclear power?', The PRS Blog, October 30, 2012. https://prsindia.org/theprsblog/are-there-enough-regulatory-safeguards-against-nuclear-power

17 World Nuclear Association, 'Nuclear Power in India', Country Profiles, May 2022. https://world-nuclear.org/information-library/country-profiles/countries-g-n/india.aspx

18 Nuclear Power Corporation of India Limited, 'About NPCIL', About us, accessed May 20, 2022. https://www.npcil.nic.in/content/328_1_AboutNPCIL.aspx

19 M. Aruloli, 'KKNPP 3rd, 4th reactors to go on stream by 2023', *Deccan Chronicle*, March 25, 2018. https://www.deccanchronicle.com/nation/current-affairs/250318/kknpp-3rd-4th-reactors-to-go-on-stream-by-2023.html

Pakistan's civil nuclear framework[20]				
Pakistan Atomic Energy Commission (PAEC)			Pakistan Nuclear Regulatory Authority (PNRA)	
Strategic Plans Division (SPD)				
Institutions and organisations				
Pakistan Institute of Engineering & Applied Sciences (PIEAS)	Strategic Export Control Division (SECDIV)	Pakistan's Centre of Excellence & Nuclear Security (PCENS)	National Institute of Safety & Security (NISAS)	National Command Authority (NCA)
Public sector				
Karachi Nuclear Power Complex (KANUPP)	Chashma Nuclear Power Complex (CHASNUPP)	National Transmission and Despatch Company (NTDC)	National Electric Power Regulatory Authority (NEPRA)	

Table 1: *Pakistan's nuclear infrastructure.*

India's civil nuclear framework[21]					
Atomic Energy Commission (AEC)					
Department of Atomic Energy (DAE)			Atomic Energy and Regulatory Board (AERB)		
Institutions and organisations					
Bhabha Atomic Research Centre (BARC)	Variable Energy Cyclotron Centre (VECC)	Raja Ramanna Centre for Advanced Technology (RRCAT)	Indira Gandhi Centre for Atomic Research (IGCAR)	Atomic Minerals Directorate (AMD)	Global Centre for Nuclear Energy Partnership (GCNEP)
Public sector					
Nuclear Power Corporation of India Limited (NPCIL)	Indian Rare Earths Limited (IREL)	Uranium Corporation of India Limited (UCIL)	Electronics Corporation of India Limited (ECIL)	Bharatiya Nabhikiya Vidyut Nigam Limited (BHAVINI)	

Table 2: *India's nuclear infrastructure.*

Common challenges

The fact that India and Pakistan each have a mature civil nuclear industry sometimes seems forgotten in light of the nuclear weapons related discussions in the region. Despite this, decades of experience developing a large body of civilian nuclear and radiological facilities has certainly resulted in useful observations on best practices and many lessons for security that should be considered in their own right.

It must be acknowledged that there is a relative lack of separation between the civil and military aspects of nuclear materials in both India and

20 Government of Pakistan Ministry of Foreign Affairs, 'Pakistan's Nuclear Security Regime', 2020; International Atomic Energy Agency, 'Pakistan', Country Profiles, accessed June 21, 2022. https://cnpp.iaea.org/countryprofiles/Pakistan/Pakistan.htm

21 World Nuclear News, 'India's Nuclear Regulation Must Improve', August 24, 2012. https://www.world-nuclear-news.org/RS_Indias_nuclear_regulation_must_improve_2408121.html

Pakistan. National security and nuclear security are rarely discussed as two separate issues, which can lead to misunderstandings and increased risks of (nuclear) escalation. What is more, this handbook considers nuclear security in an age of hyper-sensitive media. The nuclear industry, like many others, is regularly affected by the impact of 'fake news'.[22] For example, in 2016, a fake news item famously prompted Pakistan to issue a nuclear warning to Israel.[23] It is therefore essential that both decision-makers as well as the general public understand reliability of sources. While the military sector is usually surrounded by an aura of secrecy and concealment, it is crucial that those working in civil nuclear industry engage in cross-national debates on security considerations. Building mutual understanding and forming working alliances that support each other in security assessment and build-up are essential for an interconnected security system with maximum support and emergency response capacity.

Hence, while the media commonly focuses on weapons, nuclear incidents, destruction and disagreement, 'A far more resonant nuclear story relies on invoking hope instead of fear, vocalising a shared ambition, creating urgency through proximity, and prioritising community-centred perspectives.'[24] The media can then act as an inhibitor or facilitator of open spaces for nuclear security discussions, particularly when it comes to the civil nuclear industry.

Another area for learning and potential collaboration can be found in effective crisis management. This could include, for example, the sharing of incident tracking and reporting, the comparison of legislative measures, and the exchange of accident management lessons. Some of these solutions already exist with the IAEA – such as incident reporting – and many of these have been incorporated in Confidence Building Measures (CBMs) between India and Pakistan – such as crisis communication hotlines (1971 and 1989), the promise not to attack nuclear facilities (1988), and a bilateral agreement to reduce risks relating to nuclear accidents (2007).[25]

The analyses provided in this handbook will show that communication methods and the media play an important role in the civil nuclear sector in South Asia, where effective response strategies and clear messaging are needed to explain nuclear security threats. In the eight cases that follow, regulation transparency, public information, and international cooperation appear as common challenges for both India and Pakistan. We hope that using case studies to link theoretical security concepts to real-life situations can offer practical, new insights in techniques to strengthen the human factor within nuclear security systems.

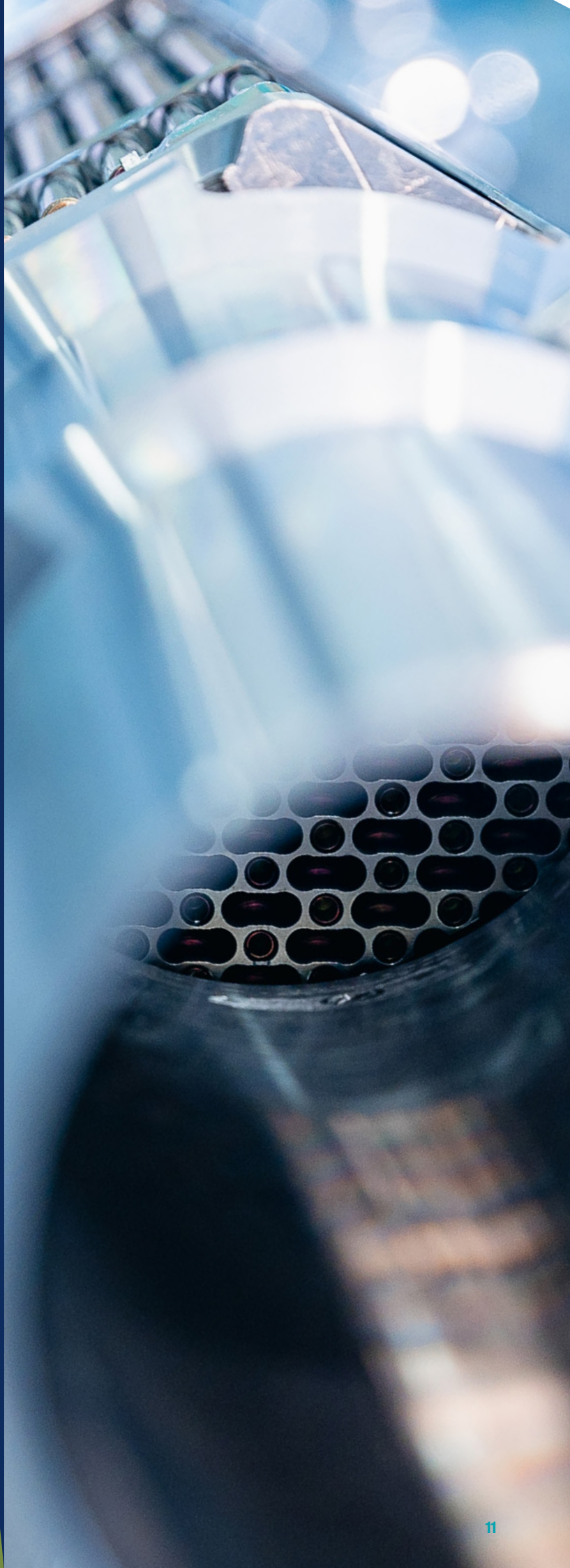
22 False or misleading information presented as news. Also see 'What is "Fake News"?' University of Michigan Library, 20 June 2022. https://guides.lib.umich.edu/fakenews

23 Emma Graham-Harrison, 'Fake News Story Prompts Pakistan to Issue Warning to Israel', *The Guardian*, December 25, 2016. https://www.theguardian.com/world/2016/dec/26/fake-news-story-prompts-pakistan-to-issue-nuclear-warning-to-israel

24 Shazeeda Bhola and Elizabeth Talerman, 'Changing the Nuclear Narrative', *European Leadership Network*, March 15, 2022. https://www.europeanleadershipnetwork.org/commentary/changing-the-nuclear-narrative/

25 Agreement between the Republic of India and the Islamic Republic of Pakistan on Reducing the Risk from Accidents Relating to Nuclear Weapons, 2007. https://mea.gov.in/Portal/LegalTreatiesDoc/PA07B0425.pdf

II. Case studies



Nuclear security practices during the COVID-19 pandemic

by Salma Shaheen

Overview

The COVID-19 pandemic is unique in terms of its global scale, its extended duration, and its direct effects on humans. It has also directly and indirectly affected societies, economies, and international relations. The pandemic – like other events, such as the Chernobyl and Fukushima nuclear incidents and more recently concerns about Zaporozhe in Ukraine[26] – highlighted the importance of communication to a variety of audiences. These include the domestic and international public, as well as national and international stakeholders. However, crisis response and disaster management remain largely dependent on existing plans and systems, including communication, and the development of workflows and processes, even when they do not necessarily fit or apply to the unprecedented situation at hand.

Case summary:

Nuclear security practices during the COVID-19 pandemic in Pakistan

In the case of Pakistan, several measures were put in place to mitigate the impact on safety and security of nuclear facilities, according to the measures implemented globally.[27] However, the authorities in Pakistan, like those in other states, faced challenges in implementing these measures nationwide. One particular challenge was the establishment and maintenance of consistent and clear communication. In absence of publicly available information about the pandemic's effects on nuclear safety and security besides official statements and reports by the IAEA,[28] the examination of this case supports deeper understanding about the pandemic's impact on safe and security management of nuclear operations from national experiences. The following analysis focuses on two response dimensions: communication, and devising and implementing COVID-19 restrictions. While

26 Jake Hecla, Gabriela Levikow and Ksenia Pirnavskaia, 'Minimizing the Consequences of Nuclear Accidents through Effective Communication', *Bulletin of the Atomic Scientists*, August 31, 2020. https://thebulletin.org/2020/08/minimizing-the-consequences-of-nuclear-accidents-through-effective-communication/; 'IAEA concern over communication issues at Zaporozhe', *World Nuclear News*, March 7, 2022. https://www.world-nuclear-news.org/Articles/IAEA-concern-at-communication-issues-at-Zaporozhe; Geoffrey Chapman et. al., *Nuclear Security in Times of Crisis*, Stimson Centre and Centre for Science & Security Studies, 2021. https://www.kcl.ac.uk/csss/assets/nuclear-security-in-times-of-crisis-handbook.pdf

27 Ansar Parvez, 'COVID-19 and Nuclear Power in Pakistan', INSAG Forum 2020. https://www.iaea.org/sites/default/files/20/09/3_parvez_new_insag_forum_npp_operation.pdf

28 Ibid.

assessing these two nuclear security areas, the experiences of other states are thoroughly considered. Finally, the lessons learned will be highlighted.

Communication

In the context of the global pandemic, effective and efficient communication among different stakeholders including the nuclear industry (regulators and operators) and the general public is vital. Effective communication helps mitigate risk, minimise fear, and implementation of protective actions.[29,30] When responding to an emergency or a crisis like COVID-19, it is the responsibility of communicators to employ different communication techniques to engage key stakeholders, and to coordinate consistent messaging at local and international level.[31]

According to the IAEA, important steps in crisis response are to maintain a contact list of people and institutions to be communicated with; to nominate a 'well-trained spokesperson'; and to establish procedures and instructions for effective internal and external coordination.[32] While the IAEA guidelines only mention a single 'well-trained spokesperson', the Fukushima Daiichi incident and the COVID-19 pandemic have highlighted the importance of effective communication by more than one person.[33] Furthermore, past incidents have shown that maintaining trust between communicators and the various audiences is paramount. Two main communication challenges emerged in Pakistan during COVID-19. These affected all sectors, including the nuclear sector.

Firstly, Pakistan's provinces adopted different approaches to tackle the pandemic due to variances in perception and mitigation capacities.[34] This resulted in a disconnect between federal (central) and provincial government communication, thus undermining the national response to the pandemic. A similar lack of transparency in communications was observed in the United States, between the federal, state, and local level, harming national response to the crisis.[35] In Pakistan, symptoms of this communication disconnect between authorities became evident at several points in time. For instance, mass political protests occurred,[36] and confusion amongst the public added to the burden on provincial resources and capacity to enforce measures such as isolation, lockdown, and social distancing.[37,38] However, as the pandemic progressed into a second and third wave, federal and provincial governments sought to develop strategies for more coordinated communication to mitigate the pandemic impact.

Second, although media outlets in Pakistan widely covered and reported information related information,[39] there were instances that undermined the urgency and seriousness required to deal with the pandemic. Several times, government officials tried to downplay

29 International Atomic Energy Agency, 'Communication with the Public in a Nuclear or Radiological Emergency', *IAEA Guidelines 2012*. https://www.iaea.org/publications/8889/communication-with-the-public-in-a-nuclear-or-radiological-emergency; International Atomic Energy Agency, 'Method for Developing a Communication Strategy and Plan for a Nuclear or Radiological Emergency', *IAEA Guidelines 2015*. https://www.iaea.org/publications/10866/method-for-developing-a-communication-strategy-and-plan-for-a-nuclear-or-radiological-emergency

30 Here, communication is defined as 'an interactive process of exchange of information and opinion among individuals, groups, and institutions [involving] multiple messages about the nature of risk and other messages, not strictly about risk, that express concerns, opinions or relations to risk messages or legal and institutional arrangements for risk management.' National Research Council, *Improving Risk Communication*, Washington, DC: National Academy Press, 1989, p. 21.

31 International Atomic Energy Agency, 'IAEA Nuclear Communicator's Toolbox', Resources, accessed June 21, 2022. https://www.iaea.org/resources/nuclear-communicators-toolbox

32 International Atomic Energy Agency, 'Method for Developing a Communication Strategy and Plan for a Nuclear or Radiological Emergency', Vienna, 2015. https://www-pub.iaea.org/MTCD/Publications/PDF/EPR-CommPlan2015_web.pdf

33 Jake Hecla, Gabriela Levikow and Ksenia Pirnavskaia Hecla, 'Minimizing the Consequences of Nuclear Accidents through Effective Communication', *Bulletin of the Atomic Scientists*, August 31, 2020. https://thebulletin.org/2020/08/minimizing-the-consequences-of-nuclear-accidents-through-effective-communication/

34 The 18th Amendment to the constitution in 2010 gave provinces in Pakistan the autonomy to respond and/or mitigate crises, generate resources, control law and order and reform their institutions. For detailed analysis of provincial responses to pandemic see M. Ahsan Ali Raza et. al., 'COVID-19 Pandemic Control and Administrative Issues in Pakistan: How Pakistan Mitigated both Pandemic and Administration Issues?', *Journal of Public Affairs*, 2021.

35 William Hatcher, 'A Failure of Political Communication not a Failure of Bureaucracy: The Danger of Presidential Misinformation during the COVID-19 Pandemic', *The American Review of Public Administration*, vol. 50, no. 6-7, 2020, pp. 614-620.

36 Imtiaz Ahmad et. al., 'COVID-19's Impact on Pakistan's Democratic Process and its Traditional Press', Palarch's Journal of Archaeology of Egypt, vol. 17, no. 7, 2020.

37 Huma Siddiqi, 'Understanding the Causes of Variance in Provincial Response to COVID-19 in Pakistan by Using the Policy Capacity Framework', *South Asian Survey*, vol. 28, no. 1, 2021, pp. 147-48.

38 Madiha Afzal, 'Pakistan Teeters on the Edge of Potential Disaster with the Coronavirus', Order From Chaos, Brookings, March 27, 2020. https://www.brookings.edu/blog/order-from-chaos/2020/03/27/pakistan-teeters-on-the-edge-of-potential-disaster-with-the-coronavirus/

39 Hassan Murtaza, 'Role of Information Technology and Social Media in Deadly COVID-19 Crisis', *Daily Times*, April 6, 2020. https://dailytimes.com.pk/589903/role-of-information-technology-and-social-media-in-deadly-covid-19-crisis/

the risks and challenges of the pandemic by disseminating misinformation and false and insensitive messages such as 'hot and dry weather will curb the spread',[40] 'learn to live with it',[41] as well as 'more people die from traffic accidents'.[42]

The above-mentioned challenges tasked authorities with working toward an informed society, which is key in managing crises, as well as in mitigating risks and fears in the general public, and supporting implementation of standard operating procedures (SOPs). It is important to note here that society itself is a key stakeholder in nuclear security. An incoherent approach among federating units and failure to disseminate correct information in a timely fashion can confuse society – which poses a challenge to nuclear security practices during a pandemic.

Coordination

To ensure the dissemination of timely and accurate information to the wider public as well as nuclear facility employees, the PNRA formed a committee that continuously monitored the evolving situation and advised on future steps. Although it was deemed adequate to shut down most radiological facilities, nuclear power plants remained largely operational to ensure continuous energy production and thus prevent further economic downturn. To protect the health and safety of nuclear facility personnel, the nuclear workforce was reduced to less than 50% of pre-pandemic levels to ensure that social distancing rules could be observed, and local travel was kept to a minimum. On-site staff was equipped with personal protective equipment such as masks and sanitisers. Furthermore, PNRA implemented a work from home concept for the first time in Pakistan's nuclear industry history. Face-to-face meetings were only held in special circumstances. As a result, information transmission was shifted to online platforms. At the end of 2020, contingency plans and response mechanisms were put in place that identified critical functions and ensured that they were performed without risking the health and safety of nuclear facility employees. Surveys were distributed to all nuclear operators to collect information on the status and challenges in each facility. Educational and training courses were shifted to an online setting as well, including e-learning platforms and online courses. Inspections were shifted from a 'Witness Point' focus to 'Record Point',[43] reducing the staff presence required for inspections. To facilitate these services without opening nuclear facilities to an increased cyber risk, PNRA upgraded its IT systems.

However, this shift to an online, low-presence environment resulted in various challenges to the operators. This was largely due to the lack of online availability of critical documents, issues with cyber security concerns, and meetings that took longer in online settings than usual. Furthermore, travel for inspections was largely suspended, compounding matters for the control regime.

These matters show that a country's crisis communication strategy should be devised based on coherence among communicators for efficient management of future crisis or disaster. Examples include successful coherent public

40 'PM Imran hopeful Pakistan's 'hot and dry' Weather will Mitigate Virus Threat', *Dawn*, March 20, 2020. https://www.dawn.com/news/1542413

41 Charlotte Greenfield and Umar Farooq, 'After Pakistan's Lockdown Gamble, COVID-19 Cases Surge', Reuters, June 5, 2020. https://www.reuters.com/article/us-health-coronavirus-pakistan-lockdown-idUSKBN23C0NW

42 'Minister Asad Umar Compares COVID-19 to Road Accidents', *Naya Daur*, May 4, 2020. https://nayadaur.tv/2020/05/minister-asad-umar-compares-covid-19-to-road-accidents/

43 A 'Witness Point' is an identified point in the process where the designated authority, such as the engineer or third party inspector may review, witness, and inspect the method or process of work.

messaging in Vietnam[44] and New Zealand.[45,46] As the pandemic progressed, the coordination between central government and provinces improved in terms of resource allocation and communication in relation to the pandemic. This eventually helped Pakistan to emerge as an example for other countries to follow.[47] One key factor for Pakistan's improvement in crisis management was the gradual implementation of a comprehensive National Action Plan (NAP) working on three dimensions – Preparedness and Response, Containment and Mitigation.[48] All three dimensions contained guidance on communication which demonstrated an enhanced understanding of effective crisis and disaster management by the relevant authorities. In general, the COVID-19 pandemic denotes the critical importance of ensuring non-traditional security, including health security in Pakistan. This was eventually given credence in the country's first National Security Policy (NSP) 2022-26, launched in January 2022. The NSP explicitly focuses on human security with an enhanced emphasis on non-traditional security, and it is a manifestation of the lessons learned.

Lessons learned

A reduction in staff at nuclear facilities can pose risks to efficient management of facility safety and security, as well as administrative work such as licensing. Additionally, remote working raised mental health challenges for nuclear industry – which is known to increase the risk of insider threats. To adjust to lower staff levels in facilities and enhance staff wellbeing, nuclear operators in Pakistan focussed on digital communications. Yet, online communication can result in new security threats if staff are unaware of security practices in a digital setting. Hence, Pakistan's nuclear industry had to increase online security training and threat awareness among its employees.

Pakistan's National Action Plan (NAP) and National Command and Operation Centre (NCOC) were at the centre of the country's efforts to devise and implement COVID-19 restrictions in line with global practice and standards. The NAP highlighted main stakeholders including ministries, armed forces and civil armed forces, key authorities/agencies, health-related departments/institutes, federal and provincial district administration, and international partners.[49] The inclusion of ministries (ministry of foreign affairs, ministry of defence, ministry of finance, and ministry of interior) and armed forces, which are also members of the National Command Authority (NCA) that is responsible for the management of nuclear operations, demonstrates the extent of the NCOC's cascading influence on the nuclear industry through cross-cutting work.

However, to implement pandemic-related restrictions, the authorities faced difficulties related to sociocultural setup, misleading communication, and a limitation of enforcement mechanisms. It is important to be aware of this broader context, because general social contradictions naturally filtered into the nuclear sector as well. Then prime minister, Imran Kahn, asked the public to live with the virus,[50]

44 Emma Willoughby, 'An Ideal Public Health Model? Vietnam's State-led, Preventive, Low-cost Response to COVID-19', *Order From Chaos*, Brookings, June 29, 2021. https://www.brookings.edu/blog/order-from-chaos/2021/06/29/an-ideal-public-health-model-vietnams-state-led-preventative-low-cost-response-to-covid-19/

45 Elle Hunt, 'Words Matter: How New Zealand's Clear Messaging Helped Beat COVID', *The Guardian*, February 26, 2021. https://www.theguardian.com/world/2021/feb/26/words-matter-how-new-zealands-clear-messaging-helped-beat-covid

46 Thinking about an informed society in general, Pakistan's messaging also included popular communicators. For instance, fashion designer Asim Jofa - who developed medical protective suits for front-liners - and celebrities from show business and sports. During the pandemic, they educated the general public about protective measures and communicated to government not to take actions that could potentially put the public in danger. Thus, celebrities have been instrumental in raising awareness about the pandemic among the general public in Pakistan. See 'Asim Jofa Readies Protective Suit for Healthcare Workers in 48 Hours', The Express Tribune, March 30, 2020. https://tribune.com.pk/story/2187150/asim-jofa-readies-protective-suit-for-healthcare-workers-in-48-hours; Kaukab Jahan, 'Coronavirus Pandemic: What Pakistani Celebrities are Saying', Arab News, March 17, 2020. https://www.arabnews.pk/node/1642711/pakistan; '#CancelExams: Pakistani Celebrities Urge Govt to Cancel Exams amid COVID-19 Pandemic', *Daily Jang*, April 27, 2021. https://jang.com.pk/en/news/2705-cancelexams-pakistani-celebrities-urge-govt-to-cancel-exams-amid-covid-19-pandemic.

47 'WHO 'praises' Pakistan's Response Against Coronavirus', *The News International*, July 6, 2020. https://www.thenews.com.pk/latest/682890-who-praises-pakistans-response-against-coronavirus-asad-umar; 'World Economic Forum to Commemorate Pakistan's COVID-19 'Success' on November 25', *Arab News*, November 24, 2020. https://www.arabnews.pk/node/1767666/pakistan

48 Government of Pakistan, *National Action Plan for Corona Virus Disease (COVID-19)* Pakistan, March 2020. https://www.nih.org.pk/wp-content/uploads/2020/03/COVID-19-NAP-V2-13-March-2020.pdf

49 Ibid.

50 Charlotte Greenfield and Umar Farooq, 'After Pakistan's Lockdown Gamble, COVID-19 Cases Surge,' *Reuters*, June 5, 2020. https://www.reuters.com/article/us-health-coronavirus-pakistan-lockdown-idUSKBN23C0NW

while religious scholars (Ulemas) called devoted Muslims to offer Eid prayers in mosques,[51] and the Supreme Court ordered a re-opening of shopping malls.[52] These decisions challenged the implementation of pandemic restrictions including workforce movement. Contradictively, in April 2021, Khan ordered the army to support the policy to enforce the implementation of COVID-19 standard operating procedures (SOPs), such as allowing 50% of staff to be allowed in offices, following low compliance with SOP measures.[53] Some tried to explain this reluctance to follow SOPs with low literacy rates in Pakistan.[54] However, this is difficult to believe because earlier health-based awareness campaigns, such as family planning and vaccination successfully encouraged the Pakistani masses to change their health behaviour.[55] As such, beliefs rooted in political-religious narratives have the power to hinder safety and security campaigns in Pakistan.[56,57]

The Pakistani government's policy to ease general lockdown and impose smart lockdowns was generally lauded in economic terms and it was instrumental in easing off pressures of remote working. For example, Pakistan's nuclear operator, Pakistan Atomic Energy Commission (PAEC),[58] and regulator, Pakistan Nuclear Regulatory Authority (PNRA),[59] used digital platforms for official meetings, educational purposes, training programmes and conferences. The use of digital communication affected the routine performance of the organisational operations of the nuclear industry, which thrive on in-person interaction. Regardless of the COVID-19 restrictions, the nuclear industry continued its work. The PAEC indigenously developed intensive care Unit (ICU) ventilators, called 'i-LIVE', to meet the growing demand for life-saving equipment amid the third wave of COVID-19.[60] PNRA continued its licensing work, but its inspection activities, training courses, emergency exercises, and drills were affected. However, some training courses organised by the IAEA were held virtually.

The Pakistani delegation at the 64th IAEA General Conference informed participants about the implementation of pandemic measures including quarantines, reductions of the workforce, a temporary halt of construction work at nuclear power plants, and working with standard operating procedures to mitigate COVID-19 impact.[61] The delegation underlined the importance of developing the contingency plan in dialogue with employees, as 'it is very important to win the cooperation of the staff.'[62] This indicates that policy measures were important, but human behaviour in terms of social distancing, remote working, and distant communication was key in the management of the COVID-19 pandemic.

Conclusion

Toward the end of 2020, Pakistan was praised internationally for its pandemic management.[63] This reflects that all federating units have learned from the challenges encountered during different stages of the pandemic and have

51 'Doctors Demand Strict Lockdown, Urge Religious Scholars to Review Decision to Open Mosques', *Dawn*, April 22, 2020. https://www.dawn.com/news/1551370/doctors-demand-strict-lockdown-urge-religious-scholars-to-review-decision-to-open-mosques

52 Asif Shahzad, 'Coronavirus 'not a pandemic in Pakistan' says Top Court, Ordering Curbs Lifted', *Reuters*, May 18, 2020. https://www.reuters.com/article/us-health-coronavirus-pakistan-lockdown-idUSKBN22U2NV

53 'PM Imran Calls in Army to Support Police in Enforcing SOPs as COVID-19 Cases Surge', *Dawn*, April 23, 2021, https://www.dawn.com/news/1619906

54 M. Salman et. al., 'Awareness of COVID-19 Among Illiterate Population in Pakistan: A Cross-Sectional Analysis', *Disaster Medicine and Public Health Preparedness*, August 9, 2021. https://www.cambridge.org/core/journals/disaster-medicine-and-public-health-preparedness/article/awareness-of-covid19-among-illiterate-population-in-pakistan-a-crosssectional-analysis/B5E2AAB9EF59C96BC7DB4990F825E4BC

55 Mian Ahmad Hanan et. al., 'Media and Behaviour Change: Effectiveness of Public Health Campaigns in Pakistan', *Isra Med Journal*, vol. 11, no. 4, Part B, July-Aug 2019.

56 Tariq Khan and Javaria Qazi, 'Hurdles to the Global Antipolio Campaign in Pakistan: An Outline fo the Current Status and Future Prospects to Achieve a Polio Free World', *Journal of Epidemiol Community Health*, no. 67, pp. 696-702.

57 Waqar Gillani, 'Dangerous Theories', *The News International*, June 21, 2020. https://www.thenews.com.pk/tns/detail/674847-dangerous-theories

58 Pakistan Atomic Energy Commission, 'PakAtom', *Newsletter*, March 2020 - Aug 2020. https://paec.gov.pk/Documents/PakAtom/P%201-8%20March%202020-August%202020.pdf

59 Pakistan Nuclear Regulatory Agency, *Annual Report 2021*. https://www.pnra.org/reports.html

60 Pakistan Atomic Energy Commission, 'PakAtom,' *Newsletter*, Jan 2021 - Sept 2021. https://paec.gov.pk/Documents/PakAtom/P%201-8%20Jan%20-Sept%202021.pdf

61 'Nuclear Security in South Asia During Times of Crisis', closed roundtable event hosted by King's College London, December 2020.

62 Ibid.

63 World Health Organization, 'WHO Director-General's opening remarks at the media briefing on COVID-19 - September 7, 2020. https://www.who.int/director-general/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---7-september-2020; The World Economic Forum (WEF), 'News Release', 25 Nov 2020. https://www.weforum.org/press/2020/11/pakistan-pm-khan-speaks-with-global-ceos-on-strategic-priorities-in-post-pandemic-era/

gradually improved coordination among each other and communication with all stakeholders. Corrective management of communications became evident with the introduction of the NCOC and its synchronised public messaging, which demonstrates learning in times of pandemic. The outbreak of COVID-19 revealed countries' lack of preparedness for non-traditional security threats as noticeable from poor and inadequate health and social responses worldwide. The pandemic triggered a debate around self-sufficiency and challenged concepts of globalisation.[64] In this context, the launch of Pakistan's first NSP is an encouraging step. However, the implementation of this policy is yet to come.

Remote work and digital communications were a novel experience for Pakistan's nuclear industry and its workers. They had to overcome challenges and learn to embrace the opportunities offered by new trends in their work environment. Both nuclear operators and regulators continued their work whilst following SOPs, illustrating optimisation of nuclear industry during the pandemic. Nonetheless, the pandemic meant that Pakistan's nuclear sector had to learn some difficult lessons in terms of communication and coordination. The ways in which the sector learned to adapt to different modes of work will remain useful in the future.

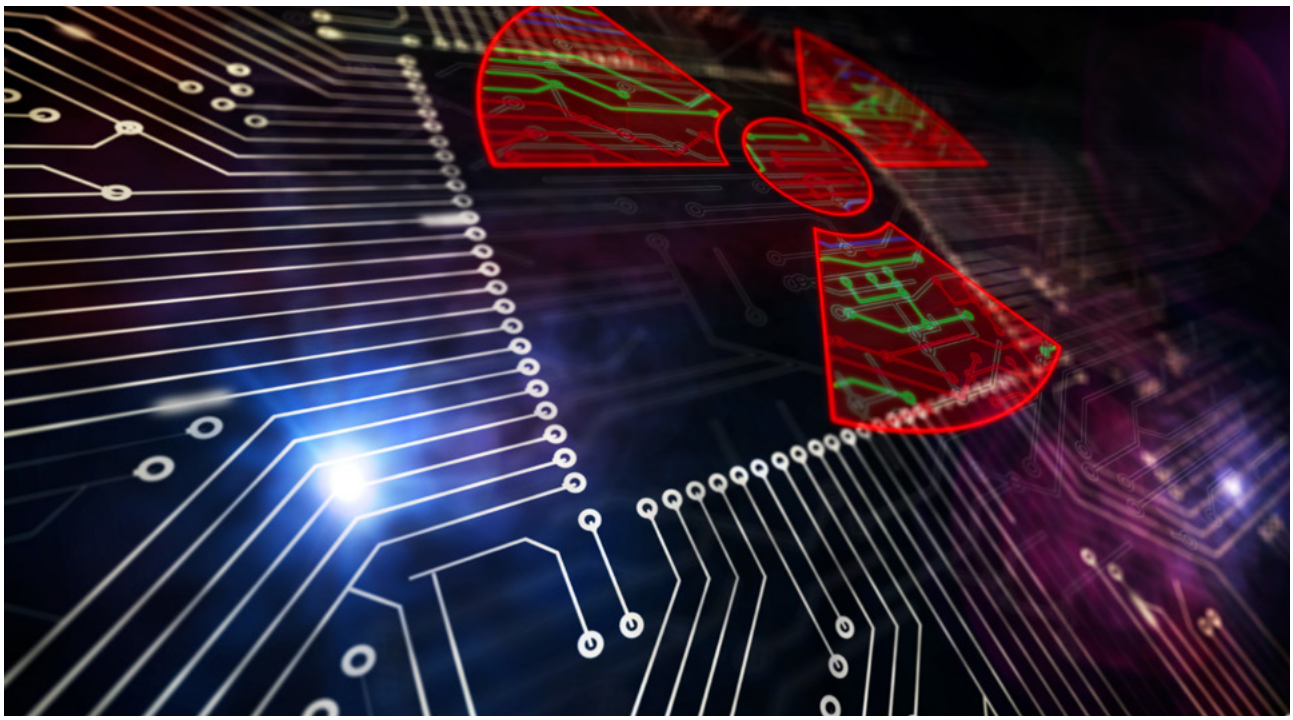
Suggested discussion points

1. How can organisational learning best be facilitated during times of crisis? What does learning from Pakistan's response to COVID-19 tell us?

2. What is the importance of broader public communication for nuclear security during times of crisis? How can nuclear organisations best deal with unhelpful communication by those outside of their control?

3. What does remote working do to nuclear security risks? How can nuclear personnel and organisations best be prepared for remote working, and risks be mitigated? Consider cyber risks, changed working routines, less oversight, less control and so forth – and think about the ways in which Pakistan managed those.

64 Eric Helleiner, 'The Return of National Self-Sufficiency? Excavating Autarkic Thought in a De-Globalizing Era', *International Studies Review*, vol. 23, no. 3, September 2021, pp. 933-957.



Cyber security culture at nuclear facilities in Pakistan

by Haleema Saadia

Overview

Cyber threats pose substantial risks to the safe and secure operation of nuclear facilities. Cyber threats to nuclear activities have evolved in the last two decades as digitalisation and automation have increased amongst nuclear activities. Establishing a strong cyber security culture in addition to and together with implementing nuclear safety and security culture has become a priority for states with nuclear programmes. There is a considerable overlap between these concepts and the measures taken in one area can often improve performance in another. Drawing on experience from Pakistan, this study addresses the question: what lessons and best practices can be learned from nuclear security culture in order to establish a cyber security culture at nuclear facilities?

The first section of this case study will discuss the concepts of nuclear security culture and cyber security culture. The second section gives an overview of the case study. The third section focuses on the attributes and best practices of nuclear security culture that can be used to establish cyber security culture at nuclear facilities, specifically in the context of Pakistan's nuclear programme. The fourth and final section focuses on areas of improvement for establishing a cyber security culture at Pakistan's nuclear facilities.

Nuclear security culture and cyber security culture

The IAEA emphasises the role of people, measures, and systems in establishing an effective nuclear security culture. It thus recognises that a nuclear security regime can fail if the human factor is not addressed.[65] Cyber security culture can be described as 'procedures laid down by an organization to all its employees, directing their course of action in all situations related to data integrity'.[66] Another interpretation of cyber security culture sees it as 'contextualized to the behavior of humans in an organizational context to protect information

65 IAEA, 'Nuclear Security Culture: Implementing Guide,' *IAEA Nuclear Security Series*, no. 7 (2008).

66 Marios Ioannou, Eliana Stavrou and Maria Bada, 'Cyber security Culture in Computer Security Incident Response Teams: Investigating Difficulties in Communication and Coordination', *2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, 2019, pp. 1–4. https://doi.org/10.1109/CyberSecPODS.2019.8885240

processed by the organization through compliance with the information security policy and an understanding of how to implement requirements in a cautious and attentive manner as embedded through regular communication, awareness, training and education initiatives'.[67] Both these definitions likewise emphasise the human element in security.

There are thus considerable parallels between the notions of nuclear security culture and cyber security culture: both focus on fostering security awareness, developing risk perception and, increasing vigilance as regards changes in threats.[68] A key area of overlap in conceptual understanding and practical implementation of nuclear and cyber security culture is the emphasis on treating 'humans as the weakest link'.[69] In both cases – in addition to comprehensive policies, elaborate procedures and technological solutions – organisations depend on the cooperation, compliance, attitude and behaviour of their personnel.[70] The human factor must be addressed to ensure the success and effectiveness of the security culture. The most comprehensive security arrangements and policies can fail if the human factor is not addressed. A sound security culture incorporates this element in procedures and best practices: 'good security is 20% equipment and 80% culture'.[71] This is especially relevant in the case of cyber security culture because it is highly dependent on the cultural tendencies, mindsets, and behaviour of the personnel.

Any security culture requires that all personnel (regardless of seniority or status) are aware of the security requirements of the facility, exhibit commitment to understanding best practices, and have the motivation to implement security regulations and procedures.

Case summary: **Cyber security culture at nuclear facilities in Pakistan**

Pakistan is one of few states that operates a complete nuclear fuel cycle. Pakistan's nuclear programme has a range of nuclear activities and great diversity in terms of nuclear facilities. However, at the time of writing, the PNRA has not issued specific guidelines or regulations for establishing cyber security culture in Pakistan's civilian nuclear facilities and there appears to be no official cyber security policy.

PNRA's Regulation PAK/925 titled 'Regulations on Physical Protection of Nuclear Material and Nuclear Installations' has one clause, which deals with 'protection of computers, communication systems and networks' from cyber-attacks. This clause does not refer to cyber security culture.[72] PNRA, in line with the Government of Pakistan's Public Sector Development Program (PSDP), launched a Cyber Security & Digital Safety (CSDS) project in 2018. CSDS was tasked to set up a team for improving cyber security expertise and to develop the 'regulatory infrastructure for ensuring safety of nuclear installations with digital systems'.[73] Under the project 'Reinforcement of PNRA's Capacity and Regulatory Oversight against Vulnerabilities of Digital Controls and Cyber Threats', PNRA is currently working on the establishment of a Lab on Digital Safety and Cyber Security that is expected to be operational by 2023. This laboratory will be used for training PNRA personnel in digital safety and cyber security, addressing the human element of cyber security. PNRA is also developing Document Preparation Profile (DPP) for 'Regulations for the Licensing of Digital Software Based Safety Systems of Nuclear Installations'.[74] In addition,

67 Moneer Alshaikh, 'Developing Cyber security Culture to Influence Employee Behavior: A Practice Perspective', *Computers & Security*, vol. 98, 2020. https://doi.org/ https://doi.org/10.1016/j.cose.2020.102003

68 Kine Reegård, Claire Blackett and Vikash Katta, 'The Concept of Cyber security Culture,' *29th European Safety and Reliability Conference, 2019*, pp. 4036–4043. https://doi.org/10.3850/978-981-11-2724-3

69 Anna Georgiadou et al., 'A Cyber-Security Culture Framework for Assessing Organization Readiness', *Journal of Computer Information Systems*, 2020, pp. 1–11. https://doi.org/10.1080/08874417.2020.1845583

70 Igor Khripunov, Nikolay Ischenko and James Holmes, eds., *Nuclear Security Culture: From National Best Practices to International Standards*, Amsterdam: IOS Press, 2007.

71 Matthew Bunn, 'Modeling of Nuclear Security: Use the Tool, but Remember Its Limits', *Emerging Issues in Nuclear Security*, Managing the Atom, 2019.

72 Pakistan Nuclear Regulatory Authority, 'Regulations on Physical Protection of Nuclear Material and Nuclear Installations – (PAK/925)', *The Gazette of Pakistan*, 2019. https://pnra.org/upload/legal_basis/regulations/PAK-925.pdf

73 Pakistan Nuclear Regulatory Agency, *Annual Report 2019*, 2019, p.41.

74 Pakistan Nuclear Regulatory Authority, *Annual Report 2021*, 2021.

PNRA is drafting its first cyber security policy. For 2022, one of its targets is to establish laboratories for capacity building of PNRA against vulnerabilities due to digital control and cyber threats. In March 2022, PNRA held a training course for its officials working in NPPs as well as manufacturers of instrumentation, digital safety equipment, and cyber controls for nuclear installations. According to the official press release, this course is 'designed to identify and study the threats to safety and security of Nuclear Power Plants due to the usage of software-based systems and data communication'.[75]

There is limited information about PAEC's developing cyber security policy. PAEC has procedures in place for cyber security but there is no publicly available policy document on its website. For example, PAEC puts a lot of emphasis on air-gapping its digital systems, both in offices and in facilities where nuclear activities are taking place. For instance, there is a strict protocol in place with regards to mobile phone use. Mobile phones are not allowed on the premises of nuclear facilities. There is limited access to internet and only designated workstations have internet connectivity. Previously, the PAEC website contained a variety of useful information, annual reports, data on peaceful applications of nuclear technology, and reports about nuclear power production. However, the PAEC website has been stripped of all this data in the last few years and now only shows minimal information. PAEC has also stopped publicly sharing its Annual Report since 2010-11. This opacity with respect to the procedures and practices of nuclear security and cyber security is not conducive to public trust in its activities and operations.

The Strategic Plans Division (SPD) is responsible for the management of all nuclear matters and activities, including security. The Security Division of SPD provides security and physical protection from all types of threats, which includes insider threats, outsider threats, and cyber threats. The Security Division secures all civilian and military nuclear facilities.[76] SPD has been working on establishing a Cyber Security Division to strengthen this multilayered defence. A two-star general of the Pakistan Army heads the Security Division; it is not known if a military officer of the same rank also heads the Cyber Security Division or the ambit and scope of its activities. Personnel Reliability Programme (PRP) is a key focus of the Security Division and entails extensive oversight and monitoring of all personnel that work in nuclear facilities across Pakistan. PRP has a dual benefit of aiding the Cyber Security Division in the context of addressing the human element and insider threat with regards to cyber security culture. SPD has also established the Pakistan Centre of Excellence for Nuclear Security (PCENS), based on the model of US National Nuclear Security Administration (NNSA), which conducts trainings in security, intelligence, counter-intelligence and technical subjects. PCENS has also conducted cyber security trainings.

Lessons learned

Best practices to establish cyber security culture

The attributes and best practices of nuclear security culture are relevant and applicable to cyber security culture. The stakeholders and their responsibilities are generally similar in both cases. The nuclear regulator is supposed to issue regulations and guidelines for establishing nuclear and cyber security culture, but it is the operator who is considered responsible for implementing these conditions. Literature on nuclear security culture underscores some essential attributes, which include designing 'a risk driven security programme';[77] presence of a comprehensive legislative and regulatory framework; inclusiveness of all personnel of nuclear facilities; importance of addressing the human element; attitudes and behaviours of individuals; comprehension and awareness of personnel; constant monitoring of threats; regular risk assessment; availability of technical

75 Pakistan Nuclear Regulatory Authority, 'Training Course on Digital Safety and Cyber Controls from 14-18 March 2022 at PNRA HQs, Islamabad'. https://pnra.org/TC-DCCC2022.html

76 SPD has merged Intelligence Division and Security Division. Two-star generals of Pakistan Army previously headed both these setups.

77 Nuclear Industry Safety Directors' Forum, 'Key Attributes of an Excellent Nuclear Security Culture', 2013. https://www.nuclearinst.com/write/MediaUploads/SDF%20documents/Security/Key_attributes_of_an_excellent_Nuclear_Security_Culture.pdf

solutions; policies in place for mitigation of threats, etc.[78] These points are equally relevant to establish a cyber security culture.

Pakistan's nuclear security regime consists of three pillars:

- legislative and regulatory framework
- institutions and organisations
- systems and measures.

These three pillars explain how Pakistan has developed its nuclear security culture and are also useful to illustrate how the best practices from this experience can help it establish a cyber security culture in its nuclear program. The following section will focus on the lessons learned from Pakistan's experience in nuclear security that will be helpful in cyber security.

Pakistan's legislative and regulatory framework on cyber security is relatively limited in scope, as there are only two laws remotely related to the cyber sphere. The *Prevention of Electronic Crimes Act of 2016* is largely focused on the prevention of electronic crimes, such as unauthorised access, copying, or transmission of digital information and unauthorised access to a critical information infrastructure system.[79] The *Draft Personal Data Protection Bill of 2021* was approved by the Federal Cabinet in February 2022 but it has yet to be approved by the legislature.[80] The draft bill regulates 'the collection, processing, use, and disclosure of personal data' of a Pakistani citizen by any person, entity or government who 'processes or has control over' any personal data, and defines and criminalises offenses related to data breach or unlawful processing of personal data.[81] It proposes to establish a National Commission for Personal Data Protection (NCPDP) to ensure the implementation of this legislation. The Ministry of Information Technology and Telecommunication (MoITT) issued a *Digital Pakistan Policy* in 2018[82] and Pakistan's first *National Cyber Security Policy* in 2021.[83] Other than the MoITT, the Federal Investigation Agency (FIA) has a National Response Centre for Cyber Crime (NR3C)[84] while the Higher Education Commission (HEC) and Planning Commission have established a National Center for Cyber Security (NCCS). Pakistan's Computer Emergency Response Team (PakCERT) is also in place and provides trainings and services to the public and private sector in infrastructure security and defense against intruder attacks.

There is no dedicated organisation for cyber security for Pakistan's nuclear program. The work of SPD, PAEC, and PNRA appears to be fractional. However, just because there is lack of transparency with regard to measures for cyber security taken by the nuclear establishment should not imply that this area has been ignored. The lack of publicly available information cannot lead to the inference that Pakistan has not taken any steps to promote cyber security and cyber security culture in its nuclear program. It is difficult to walk the fine line between the need for greater transparency to establish public trust and the goal of protecting sensitive information. Pakistan's nuclear establishment appears to err on the side of caution in the context of cyber security measures. As argued earlier, the steps taken for nuclear security can also help improve cyber security. For example, SPD's Personnel Reliability Program (PRP) is by design focused on judging the trustworthiness of the personnel and employees and has inherent markers concerning attitude and behaviour of personnel. PRP can be a key measure in shaping the cyber security culture and is a good example of how measures taken in case of nuclear security can also pay dividends for cyber security.

78 International Atomic Energy Agency, 'Nuclear Security Culture: Implementing Guide', *IAEA Nuclear Security Series*, no. 7, 2008.

79 Government of Pakistan Ministry of Information Technology and Telecommunication, 'Prevention of Electronic Crimes Act, 2016', 2016. https://moitt.gov.pk/Sitelmage/Misc/files/1472635250_246.pdf

80 Kalbe Ali, 'Federal Cabinet Approves Cloud First Policy, Personal Data Protection Bill', Dawn, February 16, 2022. https://www.dawn.com/news/1675330

81 Government of Pakistan Ministry of Information Technology and Telecommunication, 'Personal Data Protection Bill 2021', 2021. https://moitt.gov.pk/Sitelmage/Misc/files/25821 DPA Bill Consultation Draft_docx.pdf

82 Government of Pakistan Ministry of Information Technology and Telecommunication, 'Digital Pakistan Policy', 2018. https://moib.gov.pk/Downloads/Policy/DIGITAL_PAKISTAN_POLICY%2822-05-2018%29.pdf

83 Government of Pakistan Ministry of Information Technology and Telecommunication, 'National Cyber Security Policy 2021', 2021. https://moitt.gov.pk/Sitelmage/Misc/files/NationalCyberSecurityPolicy2021Final.pdf

84 Federal Investigation Agency, 'National Response Centre For Cyber Crime', accessed May 6, 2022. https://nr3c.gov.pk/index.html

Areas for improvement in Pakistan

The following section outlines the steps Pakistan can take to establish a cyber security culture in its nuclear program.

- **Pakistan's state response to cyber security:** Pakistan needs a comprehensive and robust legislative and regulatory framework on cyber security. Just as there are legislative acts for nuclear energy, regulation, and oversight, it is necessary to develop focused legislative acts for cyber security. Nuclear facilities need to be defined as critical infrastructure with respect to information and cyber security.

- **Clarity of roles concerning cyber security:** Which organisation or institution will regulate and oversee cyber security for nuclear facilities: PNRA or SPD? Looking at nuclear programs in other countries, generally the nuclear regulator issues regulations and guidelines on nuclear security, cyber security and cyber security culture. In Pakistan's case, nuclear security is not practically considered a mandate of the PNRA. PAEC has outsourced its nuclear security responsibility to the SPD and its associated organisations (Security Division, which recently had the Intelligence Division merged into it). In this context, it appears logical for the SPD to issue cyber security directives to nuclear facilities. Nonetheless, the SPD is not a regulatory authority. Thus, there needs to be a clarity of roles and responsibilities in this regard.

- **Robust and proactive role of PNRA:** PNRA as an independent regulatory authority needs to take a proactive leadership role in setting regulatory standards for cyber security and in the promotion of cyber security culture. Its cyber security policy needs to cover not only its own facilities but also be broad in scope in order to cover the nuclear facilities operated by PAEC.

- **Cyber security training:** PNRA and PCENS have started conducting cyber security trainings. These trainings must focus on the establishment of a cyber security culture in nuclear facilities and should involve nuclear operators in addition to regulators and security personnel.

- **Collaboration with other industries:** SPD, PAEC, and PNRA need to collaborate with other local industries on cyber security in order to learn from those who are more advanced in this field. For example, Pakistan's banking and aviation sectors have done considerable work with respect to cyber security and can help the nuclear sector in sharing best practices.

- **Transparency:** There needs to be more transparency (without compromising the principles of security) with regards to the processes, procedures, and measures taken by PAEC, PNRA, and SPD for cyber security. Transparency not only creates trust, but also creates an atmosphere in which cyber security culture can be criticised and enhanced.

- **Emphasis on the human element:** This will include a multipronged strategy of building technical expertise of the personnel, shaping their attitudes and behaviours, increasing their competence, introducing incentives for a good cyber security culture, and changing perceptions within organisations allowing them to see their employees as assets instead of liabilities. Practically, this could include (mandatory) trainings and professional certifications for personnel; introducing incentives for good cyber security performance; welcoming suggestions from employees to improve cyber security; giving value to the input of employees with regards to cyber security; introducing guidelines to make it easier and rewarding to follow cyber security protocols; and, introducing technical solutions to help mitigate the consequences of human risk. A key element of nuclear cyber security culture should be to alter the perception of employers and management that their employees are a liability for cyber security. If employees are treated like an asset, there will be reduced chances of them being disgruntled and posing an insider threat.

- **No-blame culture:** PAEC already works on the principle of having a no-blame culture in its nuclear facilities and in context of nuclear safety and security. The same needs to be extended to cyber security culture. The workplace should encourage employees to report weaknesses and vulnerabilities so

remedial measures can be taken. Increased awareness, shared accountability, and improved ability to identify problems and risks will lead to the establishment of a good cyber security culture in nuclear facilities.

Conclusions

Pakistan has established a comprehensive nuclear security regime and has a good nuclear security culture. This has paid dividends for cyber security in nuclear facilities too. However, it needs to take some additional steps to establish a good cyber security culture in its nuclear facilities. There are valuable lessons that can be learned from its experience with regard to nuclear security. Pakistan's cyber security regime could be established based on the same principles as its nuclear security regime by including the three pillars of the legislative and regulatory framework; institutions and organisations; and, systems and measures. Pakistan should issue a national legislation concerning cyber security in nuclear facilities. Specific steps for cyber security culture may also include designating an oversight organisation (eg PNRA or SPD); conducting advanced cyber security trainings for the employees of nuclear facilities; learning from experience of other industries; increasing transparency and instituting a no-blame culture for cyber security in its nuclear facilities. A core element of Pakistan's cyber security culture for nuclear facilities must be the emphasis on human factors.

Moreover, parallels can be drawn in measures for nuclear security and cyber security for nuclear facilities. Best practices and lessons learned in nuclear security can be emulated in cyber security. This case study from Pakistan shows how these two concepts converge and can be helpful in securing nuclear facilities from all kinds of security threats. Ultimately, the human factor is given equal importance as the weakest link in both nuclear security and cyber security.

Suggested discussion points

1. What are similar characteristics held by nuclear and cyber security culture? Are there any differences?
2. What lessons can be learned from the Pakistani experience in developing a cyber nuclear security culture?
3. What does the case tell us about the importance of clarity in organisational and personel responsibilities for nuclear security and security culture?

Information security lessons for nuclear medicine

by Aamna Rafiq

Overview

This case study takes a more in-depth look at nuclear cyber security in Pakistan, focusing on the security of sensitive data. Specifically, it explores security threats in the operational environment of nuclear medicine by analysing the various real-time cyberattacks on medical facilities. It also examines the development of nuclear medicine in Pakistan and the existing state of its adjacent national cyber security framework to identify the gaps. In light of *IAEA Implementation Guidelines for Cyber Security for Nuclear Security*[85] and lessons learned from global case studies, this study proposes recommendations for the enhancement of the national cyber security framework in Pakistan.

As highlighted in the previous case study, computer-based systems perform essential and critical functions in the various operations at nuclear facilities. Cyberattacks with or without inside help on such computer-based systems can result in theft of sensitive information and unauthorised and malicious modifications of operating systems. Cyberattacks combined with non-cyber based attack methods can contribute to nuclear proliferation by non-state entities. Cyberattacks facilitated by emerging technologies like Artificial Intelligence (AI) and quantum computing could potentially cause a major shift in the approach toward information security and nuclear security in the future.[86]

These security challenges require the establishment of a cyber security regime and its integration within the critical components of an established nuclear safety and security landscape. Nuclear and radiological technologies have multiple applications ranging from military to peaceful. In particular, peaceful use in the fields of medicine, energy and industry plays a major role in achieving the Sustainable Development Goals (SDGs). Therefore, a cyber security regime should consist of comprehensive measures relevant to all applications, as well as an exclusive cyber security framework for each sector.

Nuclear medicine: operational environment and threats

Nuclear medicine uses a small amount of radioactive material for diagnosis, evaluation, and therapy of various diseases or to measure the overall or selective functions of a human

85 Ibid.

86 International Atomic Energy Agency, 'Computer Security for Nuclear Security', IAEA Nuclear Security Series No. 42-G, Vienna, 2021. https://www.iaea.org/publications/13629/computer-security-for-nuclear-security

organ. In the area of diagnosis, nuclear radiology provides an extensive, exclusive, and precise set of information that would be unattainable by traditional, non-nuclear imaging techniques. With the help of these detailed images, there is a huge potential to detect various diseases at early stages and to determine the severity of diseases. Information obtained by nuclear medicine assists in planning the course of treatment, including medication, radiation therapy, and so forth. Furthermore, it also helps in assessing the response of disease at different stages of the treatment.[87]

The versatility of nuclear medicine prompted the development of an increasing number of digital medical equipment; Computed Tomography (CT) scans, Magnetic Resonance Imaging (MRI), and digitalised handling of medical grade radioactive materials; all of which are linked to each other through internal networks and to the external world via the internet. Hospitals, unlike nuclear-specific facilities, are often not air-gapped.[88] Valuable digitalised big data generated during diagnosis, treatment, and monitoring is stored not only for every patient but also for future medical research. In addition to medical equipment and nuclear material, this can data be highly vulnerable to internal as well as external cyberattacks.

There are examples that illustrate how cyber incidents can have serious consequences, like the loss of expensive medical infrastructure and human life.

- A healthcare provider may perform a medical treatment by using radioactive materials, using digitally connected devices and medical equipment. If a hacker interferes, they could suddenly lose access to patient medical records, course of treatment, advanced images, and even power controls of the medical equipment.

- A health care provider is performing radiation therapy based on data that they consider authentic. However, the data could be corrupted by an undiscovered cyber security breach. A hacker could potentially reprogram the software, causing a malfunction of medical equipment before or in the middle of the procedure.

In fact, these scenarios are not hypothetical: they became reality during the WannaCry ransomware attack in 2017. This global wave of cyberattacks generated devastating effects on every sector it touched, including government and industry. It infected more than 200,000 Windows systems, including 48 hospital trusts in the United Kingdom and numerous unnamed medical facilities in the United States. It not only affected the administrative systems of the health facilities but also infected their medical equipment. Interestingly, this included advanced radiology equipment, specifically the monitoring device known as the 'power injector' that delivers non-radioactive as well as radioactive 'contrast agents' depending on the requirement of the procedure. Although the systems and their operations were restored within 24 hours, the possible consequences could have been severe.[89]

The number of such cyberattacks increased significantly during the COVID-19 pandemic. Globally, one out of every three healthcare organisations reported being hit by ransomware.[90] Besides computer safety issues (eg machines being hacked) and data protection (eg loss or corruption of medical records), computer systems can contain sensitive information about security systems surrounding radiological materials. As such, healthcare is an area where cyber security and nuclear security meet, overlap and integrate.

Case summary: **Information security lessons for nuclear medicine**

According to the Pakistan Nuclear Regulatory Authority (PNRA), more than 80 licensed healthcare facilities including hospitals,

87 International Atomic Energy Agency, 'Radiation protection in diagnostic nuclear medicine', Resources, accessed April 20, 2022. https://www.iaea.org/resources/rpop/health-professionals/nuclear-medicine/diagnostic-nuclear-medicine

88 A security measure that isolates a digital device or private local area network (LAN) from other devices and networks, including the public internet.

89 Thomas Brewster, 'Medical Devices Hit by Ransomware for the First Time in US Hospitals', *Forbes*, May 17, 2017. https://www.forbes.com/sites/thomasbrewster/2017/05/17/wannacry-ransomware-hit-real-medical-devices/?sh=1299c59f425c

90 'The State of Ransomware in Healthcare 2021', *SOPHOS*, accessed April 22, 2022. https://assets.sophos.com/X24WTUEQ/at/s49k3zrbsj8x9hwbm9nkhzxh/sophos-state-of-ransomware-in-healthcare-2021-wp.pdf

laboratories, research centres, and so forth, are using nuclear or radiological technology in Pakistan.[91] Most of these facilities are run by the Pakistan Atomic Energy Commission (PAEC) (Figure 1).[92]

Share of medical radiological facilities per region

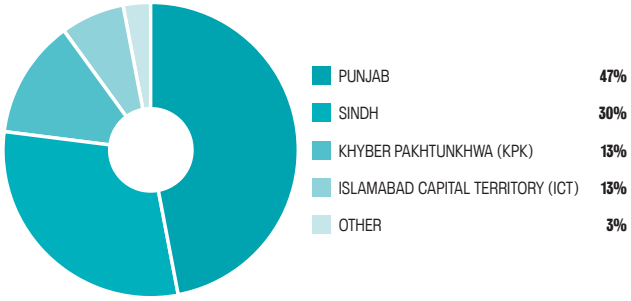


Figure 1: *PNRA Licensed Medical Radiation Facilities, share per region, valid upto 15-July-2021*[93]

In 1957, only one year after its establishment, PAEC secured membership of the IAEA. The core objective of establishing PAEC was the acceleration and enlargement of peaceful uses of atomic energy to achieve health, peace, and prosperity in Pakistan. One of the first applications of nuclear technology in Pakistan was in the healthcare sector. In 1960, PAEC founded its first nuclear medicine facility at the Jinnah Postgraduate Medical Centre, Karachi. PAEC established second and third facilities, the Centre for Nuclear Medicine (CENUM) in the Mayo Hospital Lahore and the Nuclear Institute of Medicine and Radiotherapy (NIMRA), Jamshoro in 1963 and 1965 respectively. Presently, PAEC has 18 hospitals in Pakistan. One more hospital is under construction, while two more hospitals are in the planning phase. With the average of establishing one such hospital every three years, PAEC is working to establish many more facilities across the country[94] (Figures 2 and 3).

Due to the multi-dimensional applications of radiation oncology and nuclear medicine for diagnosis and treatment, PAEC hospitals are notable for their cancer treatments. They are known as Atomic Energy Cancer Hospitals (AECHs). These AECHs are equipped with state-of-the-art nuclear medicine facilities.[95] In addition to modern hybrid imaging, a Stereotactic Radio Surgery (SRS) facility is also available. PAEC also introduced Positron Emission Tomography and Computerized Tomography (PET-CT) as well as a Cyclotron facility in a few of these AECHs.[96]

Along with the Government of Pakistan and the Ministry of Capital Administration, Development Division (CADD), these AECHs of PAEC are major partners of the International Atomic Energy Agency's (IAEA) Programme of Action for Cancer Therapy (PACT). Due to high-quality standards, the International Organization for Standardization (ISO) certified all AECHs. The Nuclear Medicine, Oncology & Radiotherapy Institute (NORI), Islamabad is the first AECH in Pakistan and the third in Asia that got the certification from the Quality Management Audits in Nuclear Medicine (QUANUM) programme by the IAEA.[97]

Atomic energy hospitals in Pakistan

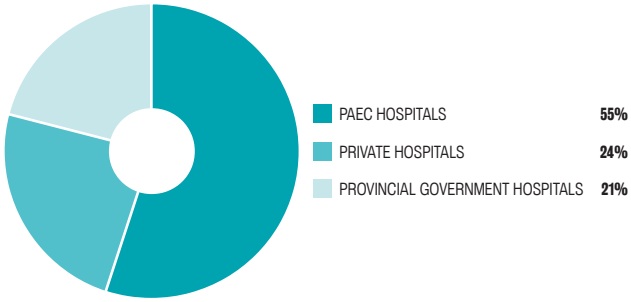


Figure 2: *Atomic energy hospitals in Pakistan*[98]

91 'PNRA Licensed Medical Radiation Facilities valid upto 15-July-2021', *Pakistan Nuclear Regulatory Authority*, accessed April 18, 2022. https://www.pnra.org/licenseeData/Medical

92 'Atomic Energy Cancer Hospitals in Pakistan', *Hilal Magazine*, May 12, 2018. hilal.gov.pk/engarticle/detail/NTg=.html

93 Based on a graph by the Pakistan Nuclear Regulatory Authority, accessed on April 18, 2022. https://www.pnra.org/licenseeData/Medical

94 Pakistan Atomic Energy Commission, Nuclear Medicine and Oncology division, *PAEC Cancer Registry Report* (2015 -20217), accessed April 25, 2022. https://paec.gov.pk/Documents/Medical/PAECR_report_2015-17.pdf

95 Ibid.

96 'Atomic Energy Cancer Hospitals in Pakistan', *Hilal Magazine*, May 12, 2018. hilal.gov.pk/engarticle/detail/NTg=.html

97 Ibid.

98 Based on a graph by Atomic Energy Cancer Hospitals in Pakistan, *Hilal Magazine*, May 12, 2018. http://hilal.gov.pk/eng-article/detail/NTg=.html

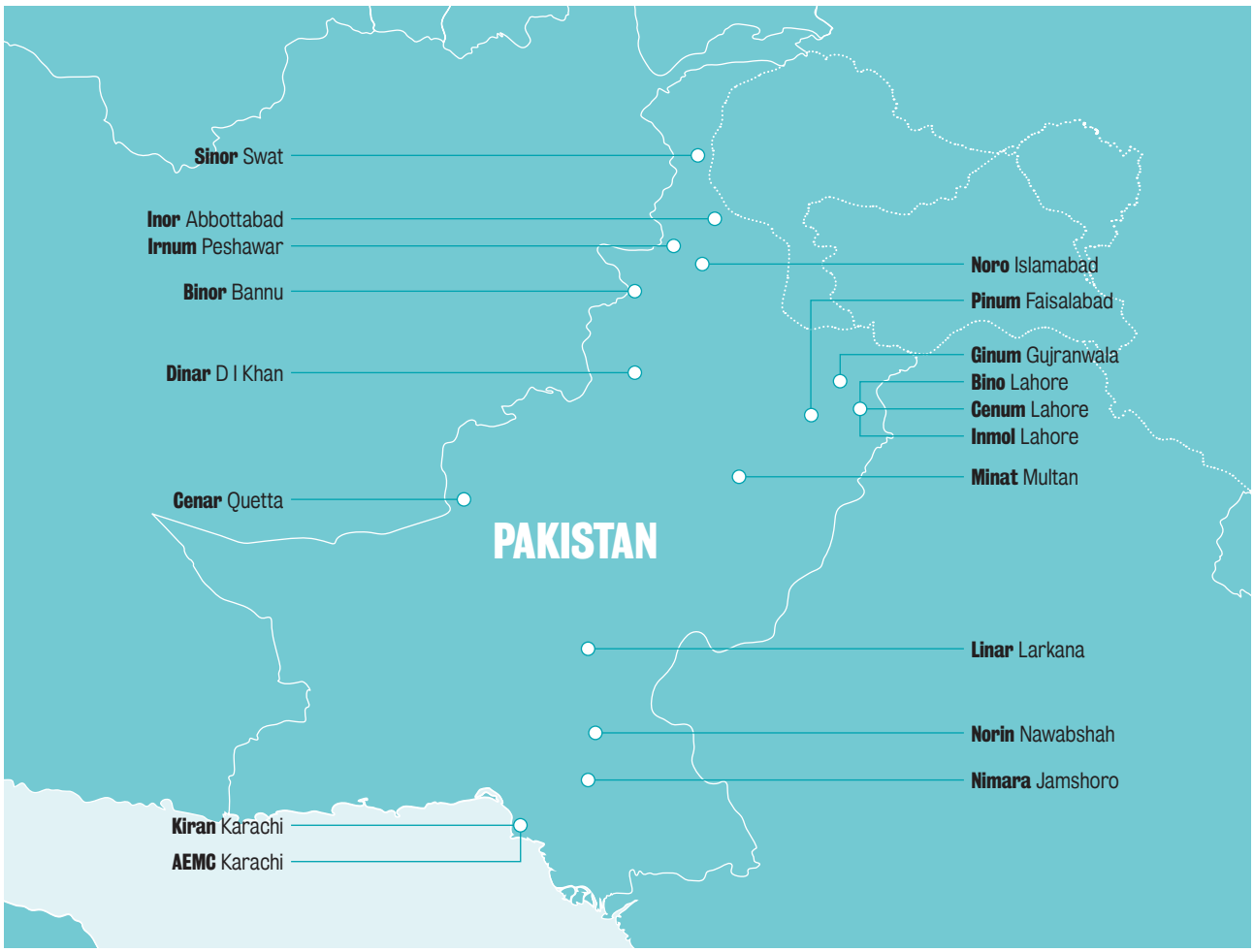


Figure 3: *Atomic Energy Hospitals in Pakistan*[99]

Compared to the number and severity of cyberattacks in hospitals across the globe, cyberattacks on healthcare facilities in Pakistan are – as far as is publicly known – rare. Only one attack of such kind made headlines in May 2017. The Shaukat Khanum Memorial Cancer Hospital (SKMCH) and Research Centre was one of many healthcare facilities around the world to be attacked by the WannaCry Ransomware. The SKMCH approved by PNRA is one of the most advanced and largest private healthcare networks in Pakistan and is famous for its cancer treatment. According to various unofficial news sources, the hospital administration responded to WannaCry Ransomware by sending instructions to all employees to shut down all systems in the network without fulfilling any demands from hackers. The network was restored within a few hours.[100] However, no further information was made public by the SKMCH. This incident gives a snapshot of how things could possibly evolve in the future.

Lessons learned

The security of radioactive materials and associated facilities is a national responsibility. To assist states with this responsibility, the IAEA started its Nuclear Security Series (NSS) in 2006. Especially relevant here is a 2021 update of the Implementing Guide for Computer Security for Nuclear Security[101] It is a consensus-based guiding document that complements the existing international regime on nuclear and radiological security. It is legally non-binding but widely used by IAEA advisory services and review

99 Based on an image by the Atomic Energy Cancer Hospitals in Pakistan, *Hilal Magazine*, May 12, 2018. http://hilal.gov.pk/eng-article/detail/NTg=.html

100 Zubair Ahmed, 'WannaCry Ransomware Cyber-Attack Takes Shaukat Khanum Hospital Into Its Wraps', *Pakwired*, May 17, 2022. https://pakwired.com/wannacry-ransomware-cyber-attack-takes-shaukat-khanum-hospital-into-its-wraps/; 'Shaukat Khanum Hospital also affected by Global WannaCry ransomware Cyber Attack', *Techprolonged*, May 13, 2017. https://techprolonged.com/2017/05/shaukat-khanum-hospital-also-infected-global-wannacry-ransomware-cyber-attack/

101 International Atomic Energy Agency, 'Computer Security for Nuclear Security', IAEA Nuclear Security Series No. 42-G, Vienna, 2021. https://www.iaea.org/publications/13629/computer-security-for-nuclearsecurity

missions.[102] It is also applicable to the peaceful uses of nuclear technology in medicine. In light of this IAEA guidance, the assessment of an existing cyber security regime for nuclear medicine in Pakistan and recommendations for further improvements are given below:

State responsibility

The IAEA guidelines state that the words 'strategy' and 'policy' could be interchangeably used by states. Although Pakistan does not have a National Cyber Security Strategy that deals specifically with nuclear medicine and associated radiological materials, it does have a general National Cyber Security Policy (NCSP) published in 2021.[103] The drafting of NSCP 2021 started before the COVID-19 pandemic, under the 'Digital Pakistan Initiative' to improve Pakistan's cyber security posture and prevent cyber-attacks.[104] According to Microsoft, Pakistan was the second most affected country by malware attacks in 2019[105] – but the increase in malware attacks accelerated the policy-making process.

According to Section 3.17 of the NCSP, the healthcare sector comes under both categories of 'Critical Sector' and 'Critical Information Infrastructure'. Section 3.4 of the NCSP contains various mandatory measures to ensure cyber security and resilience of national critical information infrastructures like development of state-of-the-art security measures for mobile systems and cloud-based solutions, integration of organisational CERT with the relevant sectoral CERTs, align the cyber security risk management methodologies with the international standards, appointment of a Chief Information Security Officer, implement national cyber security standards, and enforce the use of digital accreditation and certifications.

Centralised competent cyber security authority

The IAEA guidelines name the state as the responsible actor for the establishment and empowerment of a competent authority for cyber security. This national authority should be separate from existing or upcoming bodies dealing with other aspects of nuclear security. The state must also ensure that the roles, responsibilities, and functions related to cyber security issues are well-defined and well-coordinated without any overlap. In this regard, the Pakistani government has founded the 'Cyber Governance Policy Committee' (CGPC) which oversees national cyber security issues. The CGPC is responsible for the guidance and formulation of two key national documents: the Cyber Security Act and the above-mentioned NCSP. Furthermore, it is the duty of the CGPC to assist public sector organisations in the determination and design of legal, technical, and procedural measures to ensure compliance with the NCSP 2021. It is also responsible for taking initiatives to harmonise the existing operational environment of organisations with the new cyber security culture. Furthermore, it assigns roles to national institutes for collaborations and official representation at the international level. The federal cabinet directly endorses all decisions and initiatives of the CGPC.

Section 3.1 of the NCSP suggests that a centralised authority would be responsible for the establishment of the National Computer Emergency Response Team (nCERT). It would also be responsible for the establishment and regulations of CERTs of public and private organisations in all sectors, including banking, defence, telecom, healthcare, medicine, etc.[106] Although the establishment of this centralised competent cyber security authority is at the nascent stage, making it mandatory under the NCSP 2021 is a stepping stone to ensure adequate cyber security of critical infrastructure in Pakistan.

102 Ibid.

103 Government of Pakistan, Ministry of Information Technology & Telecommunication, *National Cyber Security Policy 2021*. https://moitt.gov.pk/SiteImage/Misc/files/National%20Cyber%20Security%20Policy%202021%20Final.pdf

104 Aamna Rafiq, 'The National Cyber Security Policy Of Pakistan 2021', *Institute of Strategic Studies Islamabad*, October 15, 2021. https://issi.org.pk/wp-content/uploads/2021/10/IB_Aamna_Oct_15_2021.pdf

105 Microsoft, 'Microsoft Security Intelligence Report (January – December 2018)', accessed May 28, 2022. https://www.microsoft.com/en-ww/security/business/security-intelligence-report

106 Government of Pakistan, Ministry of Information Technology & Telecommunication, *National Cyber Security Policy 2021*. https://moitt.gov.pk/SiteImage/Misc/files/National%20Cyber%20Security%20Policy%202021%20Final.pdf

Regulatory framework and national legislation

The IAEA guidelines also suggest that it is the state's responsibility to design a national legislative framework on nuclear security requirements related to the detection, prevention, and response to an unauthorised activity against the computer-based systems of nuclear facilities. Based on this legislative framework, the government is in a position to develop mechanisms for threat assessment, verification, and compliance with cyber security standards. The state should also establish a sanctions regime for all types of unauthorised activities.

Currently, Pakistan's only legislation that contains sanctions for unauthorised access, transmission and interference with the information or data and critical infrastructure information systems is the 'Prevention of Electronic Crimes Act (PECA)' 2016. The most significant aspect of this act is not the severity but the scope of the sanctions. The act is applicable not only to every citizen of Pakistan regardless of their location but also applicable to every other person who is in Pakistan as well as persons living outside Pakistan but involved in an act committed against the 'person, property, information system or data located in Pakistan and considered as an offense under PECA 2016.'[107]

Conclusions

So far, only one private healthcare network in Pakistan has reported the impact of the WannaCry Ransomware attack. Whether this was an isolated case or not, it illustrates how cyber threats could possibly unfold in the future. Consequently, the PNRA has established and maintained a comprehensive regulatory framework based on related international conventions, IAEA standards, and supplementary guidance for nuclear security.

In Pakistan's future, the government should consider the establishment of a separate centralised competent cyber security authority and nuclear cyber security strategy as recommended by the *IAEA Implementation Guidelines for Cyber Security for Nuclear Security*. Along with CGPC and PNRA, this new cyber security authority will enhance effectiveness of nuclear security culture and produce synergy among information security measures and nuclear security strategies.

Suggested discussion points

1. What are the key cyber security threats that are present in the operational environment of nuclear medicine? What are the key vulnerabilities?
2. How can organisations facing customers or patients best enact radiological security measures and develop a strong security culture?
3. Given the IAEA's computer security guidance is mainly focused on nuclear security, what are the challenges in carrying over recommendations and lessons to radiological security?

107 Parliament of Pakistan, National Assembly, *The Prevention of Electronic Crimes Act 2016*, Art 1; 3 – 8, https://na.gov.pk/uploads/documents/1470910659_707.pdf

Nuclear security in Pakistan's agricultural sector

by Faraz Haider

Overview

In any application of nuclear technology, nuclear security should be paramount in order to prevent accidents. Pakistan's nuclear security infrastructure has gradually developed in close collaboration with the IAEA.[108] A crucial area to consider is climate change – and to address this, Pakistan has employed nuclear technology in a variety of ways. This case study will consider how Pakistan's Peaceful Applications of Nuclear Technologies (PANT) and its associated nuclear security can prevent security incidents. The enaction of tailored regulations and their enforcement by relevant government organisations and authorities in Pakistan's nuclear security regime demonstrate which best practices have helped preserve nuclear security in the PANT sector.

Case summary:

Nuclear security in Pakistan's agricultural sector

Pakistan is faced with numerous and intense challenges related to climate change. Agriculture and associated sectors are threatened due to rising average temperatures, extreme heat, severe flooding risks, and reduced average rainfall.[109] As a result, Pakistan has searched for innovative and effective ways to combat risks to economic and food security caused by climate change with PANT for climate resilience as a crucial component and with a long history through irradiation and plant mutation breeding. Most notably, since 1983, PANT has greatly increased the crop yield of cotton varieties.[110] Other crops, such as sesame and castor, experienced almost doubled yields and improved quality through the application of nuclear techniques as well.[111] The Nuclear Institute for Food and Agriculture (NIFA) and the Nuclear Institute for Agriculture and Biotechnology (NIAB) have been at the forefront of these efforts.

108 Hossein Bidgoli and Mohammad Davand, 'A Review of the Performance of the International Atomic Energy Agency Regarding Pakistan's Nuclear Activities', *Journal of World Sociopolitical Studies*, vol. 1, no. 2, 2017, pp. 228-240. doi.org/10.22059/WSPS.2017.242257.1031

109 World Bank Group, 'Climate Smart Agriculture in Pakistan', 2017. https://climateknowledgeportal.worldbank.org/sites/default/files/2019-06/CSA-in-Pakistan.pdf

110 Carley Willis, 'Cotton in Pakistan: How Nuclear Techniques are Helping the Textile Industry', *International Atomic Energy Agency*, 2021. https://www.iaea.org/newscenter/news/cotton-in-pakistan-how-nuclear-techniques-are-helping-the-textile-industry

111 Nancy Hart, 'Mutant Varieties Satisfy Market and add USD 6 Billion to Pakistan's Economy', *International Atomic Energy Agency*, 2018. https://www.iaea.org/newscenter/news/mutant-varieties-satisfy-market-and-add-usd-6-billion-to-pakistans-economy

In addition to the above-mentioned work, further effort is required to deal with the magnitude of climate change related threats faced by Pakistan. Nuclear techniques using radio isotopes can help assess the ecological impact of climate change on water bodies, groundwater resources, and soils for sustainable water management and agricultural practices.[112] In order for PANT to be effective, it must consider aspects of nuclear security culture alongside its performance in climate resilience. To achieve this, Pakistan has been able to draw valuable lessons from past incidents around the world.

For example, an interesting incident to consider here is the radiological accident in Soreq, Israel. It highlights best practices that Pakistan was able to incorporate in its nuclear security regime and, as a result, prevent similar incidents from happening. The Soreq irradiation facility was built in 1960 and licensed in 1970 under the Israeli Atomic Energy Commission.[113] It was located within the Soreq Nuclear Research Centre but was operating as a separate commercial entity. The facility contained a Model JS6500 gamma steriliser with cobalt-60 gamma source elements.[114] The incident occurred in June 1990, when the facility experienced a jam in the transport mechanism of its irradiator. It was detected through the overdose timer, which automatically tried to lower the nuclear source rack, but was obstructed by a carton that had gotten off track. However, because of a malfunctioning source hoist microswitch, indicators in the facility showed that the source rack was completely lowered into its shielding pool and that the source element was in a safe position. Alarms were heard by on-site staff members, and the duty operator was telephoned and briefed about the problem.[115]

In order to address the issue, one of the senior staff members chose to silence the alarm on their way out by turning off the power unit.[116] They informed the qualified operator about the control console's contradicting indications showing that the source was in its safe position below the water and the gamma radiation alarm indicating a radioactive leak. Then, they left – effectively handing the issue over to the operator, while advising that they call in the Radiation Safety Officer (RSO) for specific instructions. Operators had also been given written instructions in English and oral standing orders in Hebrew that such cases are not to be dealt with alone. However, the on-duty operator chose to disregard the advice and act in violation of the operating instructions by dealing with it themselves. Also, the operator hastily decided that the signal indicating that the source was lowered and safe was correct, thus judging that the gamma radiation signal malfunctioned without calling in a more knowledgeable technician for assistance on the matter.

Based on their flawed reasoning and individual decision-making without the assistance of a qualified technician or the presence of an RSO, the operator took unauthorised actions starting with entering the irradiation room. They bypassed the safety features that had been put in place to prevent such an event. Behind the console, they manually unlocked the doors by compromising their automatic interlocking mechanism and disconnected the radiation monitor cable from the control circuitry and the alarm.[117]

Lessons learned

The incident at the Soreq irradiation facility is an example of nuclear safety failure and radiological exposure due to misjudgment, absence of reasoning, inadequate training materials, and

112 Mohammad Zaman and Monica Exner, 'Combatting Soil Salinisation Using Nuclear Techniques: The IAEA Commemorates 2021 World Soil Day', International Atomic Energy Agency, 2021. https://www.iaea.org/newscenter/news/combatting-soil-salinisation-using-nuclear-techniques-the-iaea-commemorates-2021-world-soil-day; Joanne Liou, 'Impact of Climate Change on Lakes Worldwide Revealed by IAEA Isotope Study', *International Atomic Energy Agency*, 2021. https://www.iaea.org/newscenter/news/impact-of-climate-change-on-lakes-worldwide-revealed-by-iaea-isotope-study; Yuliya Vystavna, 'World Water Day 2022: Making Invisible Visible – Using Nuclear Techniques to Assess and Manage Groundwater in Critical Situations', *International Atomic Energy Agency*, 2022. https://www.iaea.org/newscenter/news/world-water-day-2022-making-invisible-visible-using-nuclear-techniques-to-assess-and-manage-groundwater-in-critical-situations

113 International Atomic Energy Agency, 'The Radiological Accident in Soreq', Vienna, 1993, p. 2. https://www-pub.iaea.org/MTCD/Publications/PDF/Pub925_web.pdf

114 Ibid., p. 3.

115 Ibid., p. 18.

116 Ibid., p. 19.

117 Ibid., pp. 19-20.

general lack of guidance.[118] However, intentional protocol violation and unauthorised access by the operator present valuable lessons for nuclear security, as there is a significant overlap between safety and security mechanisms and procedures, which are shown below.

There are certain key lessons to be drawn from the Soreq facility incident that are directly transferable to nuclear security:

- There is a need for improved control systems that cannot be compromised.
- Increased access and action authorisation controls must be put in place to eliminate any unauthorised operation for the misuse of nuclear material or technologies.
- Irradiation rooms in the facility or research institutes must not be entered by an operator alone. Instead, a two-person rule should be introduced.

Personnel in a comparable irradiation facility or nuclear institute, such as NIFA and NIAB, could compromise safety mechanisms and disregard protocols with malicious intent for the purpose of misuse. However, a stringent nuclear security regime, developed and implemented according to international standards of the IAEA and international conventions, has prevented any similar incident from taking place in Pakistan.

Applicable regulatory framework

Both NIFA and NIAB are bodies under the Pakistan Atomic Energy Commission (PAEC) and under the regulatory oversight of the Pakistan Nuclear Regulatory Authority (PNRA). They are licensed under the PNRA PAK/908 regulation, which stipulates specific nuclear security requirements for the licensee, and operate according to its regulatory framework and guidelines.[119]

Pakistan's nuclear security framework has developed over the years in close cooperation with the IAEA, incorporating various conventions, codes of conduct, and guidelines. Specifically, Pakistan is a part of the Convention on the Physical Protection of Nuclear Materials (CPPNM), as well as its amendment, and subscribes to the IAEA code of conduct on the safety and security of radioactive sources.[120] Pakistan also committed to INFCIRC/899 to become a part of the Nuclear Security Contact Group.[121] PNRA has issued regulations to that effect as well, incorporating the elements of the said international nuclear security instruments into the national regulatory framework. It has also issued a regulatory guide to outline nuclear security operating procedures for nuclear institutes under its umbrella such as NIFA and NIAB.[122] This applicable regulatory framework includes the following:[123]

- Regulations on Physical Protection of Nuclear Material and Nuclear Installations (PAK/925).
- Regulations on the Security of Radioactive Sources (PAK/926).
- Format and Content of Physical Protection Plan for Radiation Facilities having Radioactive Sources Regulatory Guide (PNRA-RG-926.01).

The PAK/925 and PAK/926 regulations cover and prevent the highlighted lessons from the Soreq incident through articles that address the following:[124]

118 Ibid., pp.16-19.

119 Pakistan Nuclear Regulatory Authority, 'List of Valid Licenses till 31-03-2022', Licensee Data, accessed May 30, 2022. https://www.pnra.org/licenseeData/webform2; Pakistan Nuclear Regulatory Authority, 'Regulations for the Licensing of Radiation Facility(ies) other than Nuclear Installation(s) - (PAK/908) (Rev.1)', 2019. https://www.pnra.org/upload/legal_basis/Pak-908.pdf

120 Government of Pakistan Ministry of Foreign Affairs, 'Pakistan's Nuclear Security Regime', 2020.; https://mofa.gov.pk/wp-content/uploads/2020/02/NSRFinal08-02-2020.pdf; Sitara Noor, 'Assessing Pakistan's Nuclear Security Upgrades after ratification of the 2005 CPPNM Amendment', *The Stimson Center*, 2021, https://www.stimson.org/2021/assessing-pakistans-nuclear-security-upgrades-after-ratification-of-the-2005-cppnm-amendment/

121 Nuclear Threat Initiative, 'What Are Nuclear Security INFCIRCs?,' Nuclear Security Index, 2020. https://www.ntiindex.org/story/what-are-nuclear-security-infcircs

122 Pakistan Nuclear Regulatory Authority, 'Format and Content of Physical Protectiomn Plan for Radiation Facilities Having Radioactive Sources – Regulatory Guide', 2021. https://pnra.org/upload/guidelines/RG-926.01.pdf

123 Government of Pakistan Ministry of Foreign Affairs, 'Pakistan's Nuclear Security Regime', 2020. https://mofa.gov.pk/wp-content/uploads/2020/02/NSRFinal08-02-2020.pdf; Pakistan Nuclear Regulatory Authority, 'Format and Content of Physical Protectiomn Plan for Radiation Facilities Having Radioactive Sources – Regulatory Guide', 2021. https://pnra.org/upload/guidelines/RG-926.01.pdf

124 Pakistan Nuclear Regulatory Authority, 'Regulations on Physical Protection of Nuclear Material and Nuclear Installations — (PAK/925)', 2019, pp. 9-14. https://www.pnra.org/upload/legal_basis/regulations/PAK-925.pdf; Pakistan Nuclear Regulatory Authority, 'Regulations on Security of Radioactive Sources - (PAK/926)', 2018 , pp. 5-8. https://www.pnra.org/upload/legal_basis/regulations/PAK-926.pdf

- Physical protection systems to deny unauthorised access.
- Insider mitigation measures to check initial and continuing trustworthiness and reliability of individuals.
- Unauthorised action detection through electronic intrusion detection, constant surveillance, two-person rule, tamper detection devices, or measures similar to that effect.

Similarly, the PNRA-RG-926.01 addresses the following applicable nuclear security aspects for NIFA and NIAB as PNRA licensees:[125]

- Trustworthiness of personnel.
- Security measures related to detection and access control in connection to PAK/926.
- Response arrangements to neutralise a security event.
- Nuclear security training programs.
- Detailed implementation procedures for nuclear security measures.

Training framework

The regulatory framework and its enforcement by the PNRA are accompanied by a rigorous and extensive nuclear security training setup. Pakistan's Nuclear Security Centre of Excellence has been commended internationally by the IAEA and consists of three affiliated training institutes that work in harmony and cover different but interconnected approaches to nuclear security.[126] Each training institute shares best practices and provides a particular dynamic of nuclear security training, education, and technical support.[127]

- Pakistan Centre of Excellence for Nuclear Security (operator perspective).
- National Institute of Safety and Security (regulatory perspective).
- Pakistan Institute of Engineering and Applied Sciences (academic perspective).

Conclusions

Pakistan has a good record of maintaining nuclear security and preventing incidents similar to those at the Soreq irradiation facility. This has been made possible through a comprehensive and targeted nuclear security regime, as well as its enforcement. In order to further strengthen the nuclear security setup and PANT for climate resilience, relevant stakeholders (PAEC, PNRA, NIFA, and NIAB) should increase collaboration with the IAEA's various climate change related initiatives. For example, breeding plant mutations to increase crop yield and resilience will help to tackle the threats from climate change facing Pakistan. Other applications of nuclear technology for adaptation and resilience should be given increased attention.

Suggested discussion points

1. What kind of nuclear security measures will be required as the need for PANT increases with growing climate change threats?
2. How can adherence to nuclear security protocols be ensured through comprehensive training to create a robust nuclear security culture?
3. What can be learnt from this case about the interplay between regulations and enforcement in order to create an effective nuclear security regime?

125 Pakistan Nuclear Regulatory Authority, 'Format and Content of Physical Protection Plan for Radiation Facilities Having Radioactive Sources – Regulatory Guide', 2021, pp.3-9.

126 Aabha Dixit, 'Pakistan's National Centre of Excellence Contributes to Sustaining Nuclear Security', *International Atomic Energy Agency*, 2017. https://www.iaea.org/newscenter/news/pakistans-national-centre-of-excellence-contributes-to-sustaining-nuclear-security

127 I. Khan, N. Iftakhar and T. Ahmad, 'Pakistan's Approach for Development of Human Resource for Secure Management of Radioactive Sources', *International Atomic Energy Agency*, 2018, p. 350. https://inis.iaea.org/collection/NCLCollectionStore/_Public/51/006/51006827.pdf?r=1

Image: Reetesh Chaurasia

India's Kudankulam nuclear power plant

by Chandana Seshadri

Overview

As one of the fastest growing economies in the world, India is torn between meeting the demands of increasing energy consumption and developing a sustainable source of energy. On the one hand, India's energy consumption is projected an increase of 156% between 2017 to 2040.[128] This will result in a greater dependence on coal, which currently accounts for 55% of India's energy production.[129]

On the other hand, there has been a policy push for sustainable development as a tangible alternative. This has resulted in the adoption of renewable sources, predominantly solar power, and is gradually reducing dependence on coal. Additionally, albeit in smaller quantities, India is expanding its total nuclear energy production capacity (Figure 1).

128 BP Energy, 'BP Energy Outlook, 2019 Edition', accessed June 21, 2022, p.135. https://www.bp.com/content/dam/bp/business-sites/en/global/corporate/pdfs/energy-economics/energy-outlook/bp-energy-outlook-2019.pdf

129 India Ministry of Coal, 'Coal-Indian Energy Choice', Major Statistics, accessed May 20, 2022. https://coal.nic.in/en/major-statistics/coal-indian-energy-choice#:~:text=It%20accounts%20for%2055%25%20of,in%20the%20last%20four%20decades

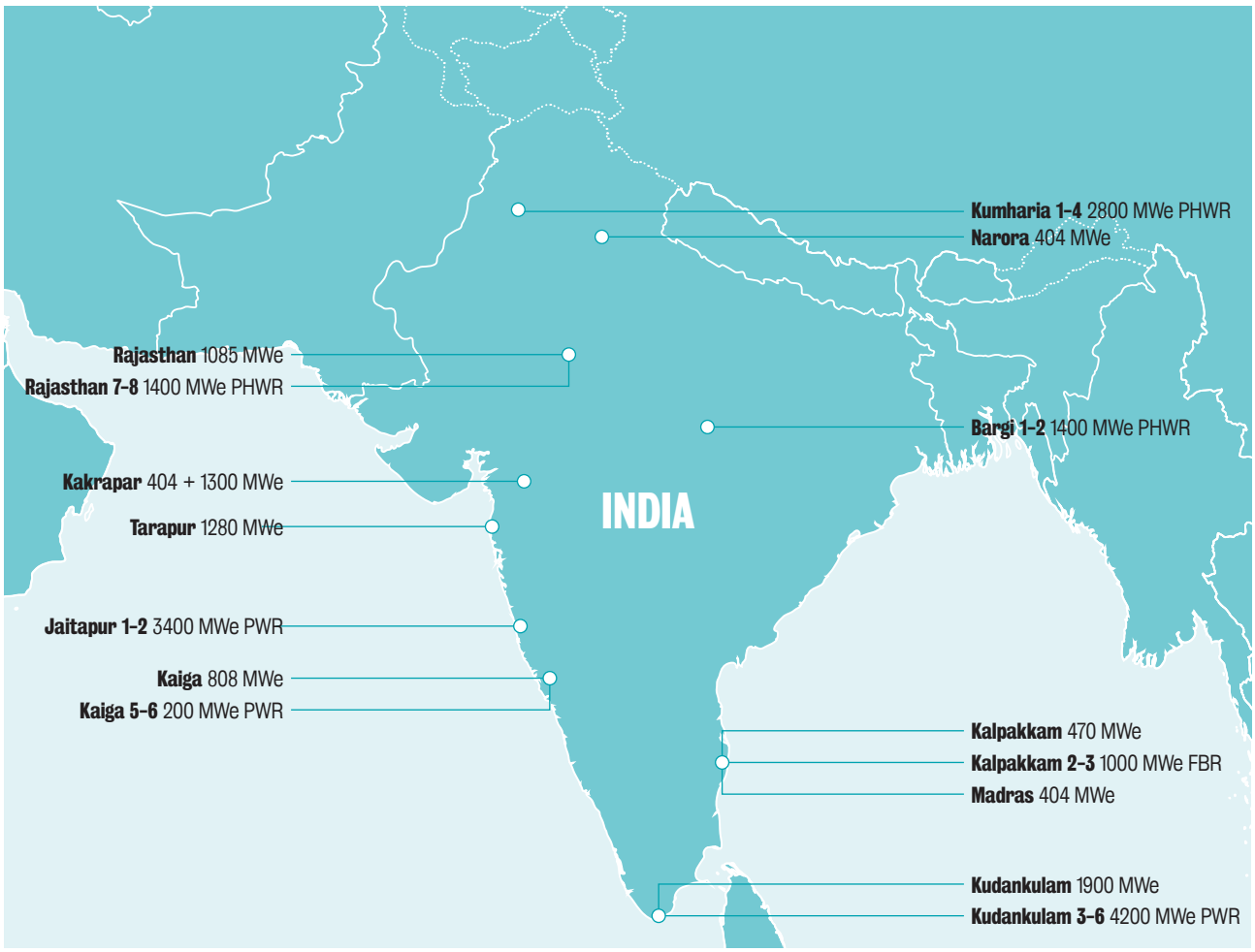


Figure 1: *Nuclear power plants in India*

India's nuclear energy programme is a crucial element in its overall national energy infrastructure.[130] The foundation of India's nuclear energy programme is the 'three stage progression', aimed at optimally utilising the natural resources available in the country, including an abundance of thorium and modest amounts of uranium.[131] The Kudankulam Nuclear Power Plant (KKNPP) plays a vital role in this larger nuclear energy programme.[132] Located in the southern state of Tamil Nadu and the small township of Kudankulam, the KKNPP has two operational units with an additional two Light Water Reactors of 1,000 MWe under construction with technical cooperation from Russia. The expected date of commercial operation of the final two units is March 2023.[133] However, KKNPP has been a contentious plant since its inception. This case study will illustrate how activism and misinformation can affect characteristics, attitudes, and behaviors of individuals and communities in terms of nuclear security.

Case summary:
Kudankulam nuclear power plant

Following the sanctions faced by India after its nuclear tests, in 1988 the USSR entered into an agreement with India to set up high-capacity Voda Voda Energo Reactors (VVER) in the country. After the fall of the Soviet Union, the agreement was later extended in 1998, and a VVER-1000 model reactor was to be built in Kudankulam with technical support from

130 Mohammad Haaris Beg, 'India's nuclear capacity to reach 22,480 MW by 2031: Govt', *Business Today India*, March 24, 2022. https://www.businesstoday.in/latest/trends/story/indias-nuclear-capacity-to-reach-22480-mw-by-2031-govt-327205-2022-03-24

131 A. Gupta, 'India's Nuclear Energy Programme: Prospects and Challenges', *Strategic Analysis*, vol. 35, no. 3, 2011, pp.373-380.

132 Nucler Power Corporation of India Limited, 'All Plants', Plants, accessed May 20, 2022. https://www.npcil.nic.in/content/302_1_AllPlants.aspx

133 S.K. Jain, 'Nuclear Power in India–Past, present and future', *CMD Paper*. Mumbai, 2010. https://management.ind.in/forum/attachments/f2/26502d1456565724-history-npcil-ntpcil-history.pdf

Atomstoyexport, a Russian state-owned entity. The first unit was scheduled to operate from 2009 but it began operations only in 2011. The local population expressed major fears regarding the safety and security of the KKNPP with large-scale anti-nuclear protests across the state and the country.[134]

Environmental concerns

Obstacles that delayed full operationalisation began with apprehensions including but not limited to contamination and pollution of marine ecology, particularly affecting the livelihoods of local residents involved in the fishing industry.[135] The flashpoint, however, was the Fukushima nuclear accident. The east coast of India, particularly Tamil Nadu, was previously hit by a major tsunami in 2004, which killed almost 7000 people and flooded the state.[136] Although new studies in the region indicate a higher tsunami threat probability for the western coast of India, where coastal states also house NPPs, concerns around nuclear power plants are deeply rooted in natural disaster-prone areas. It has been argued that 'all nuclear plants can be subject to severe accidents due to purely internal causes' and 'natural disasters like earthquakes, tsunamis, hurricanes, and storm surges make (these) accidents more likely.'[137]

Environmental activism has been known to benefit from lapses in security culture. Most notably, in the case of the 2012 break-in at the Y-12 National Security Complex in the US.[138] A combination of misunderstanding of security protocols, poor communications, and weaknesses in contract and resource management meant that trespassers were able to gain access to the protected security area. If any security detail is overlooked or underestimated at KKNPP, activists may benefit from this.

Misinformation campaigns

A crucial aspect that could have had serious consequences for nuclear security – but was not the centre of focus of the courts, protesters, and the media – were the misinformation campaigns that spread and garnered more tractions during the anti-nuclear movements. The NPCIL stated that certain 'vested interest groups' were spreading 'unscientific and incorrect information' which, as a result, spread 'fear of nuclear power among the masses.'[139] This statement shows concern regarding the serious push from groups that were initially against nuclear energy. Anti-nuclear misinformation campaigns included rumours of negative consequences of the operation of the plant that could displace the local community and questioned the additional safety features that were incorporated in the plant, which widened the anti-nuclear movement in the state.[140] This phenomenon has been observed throughout the world. For instance, while Poland debated nuclear power, fake messages appeared regarding an accident at the Świerk nuclear reactor.[141] Indeed, activists in India repeatedly made comparisons to countries which closed their nuclear power plants following anti-nuclear protests. However, to date only Germany has successfully shut down its nuclear energy programme, while, France, US, Sweden and the UK still actively maintain their programmes despite waves of anti-nuclear protests.

Almost all aspects of nuclear security culture can be affected by misinformation: information visibility, such as published security policy and

134 M.P. Ram Mohan and A. Shandilya, 'Nuclear energy and risk assessment by Indian courts: analysis of judicial intervention in the Kudankulam Nuclear Power Project', *Journal of Risk Research*, vol. 18, no. 8, 2015, pp. 1051-1069.

135 A. Khan, 'Anti-Nuclear Movement in India: Protests in Kudankulam and Jaitapur', *South Asia Research*, vol. 42, no. 1, 2021, pp. 7-20; 'The story of Kudankulam: From 1988 to 2016', *The Hindu*, December 4, 2021. https://www.thehindu.com/news/national/The-story-of-Kudankulam-From-1988-to-2016/article60528215.ece

136 'Tsunami victims remembered on 15th anniversary in Tamil Nadu', *The Economic Times*, December 26, 2019. https://economictimes.indiatimes.com/news/politics-and-nation/tsunami-victims-remembered-on-15th-anniversary-in-tamil-nadu/articleshow/72976972.cms

137 C.P. Rajendran, M. Heidarzadeh, J. Sanwal, A. Karthikeyan and K. Rajendran, 'The Orphan Tsunami of 1524 on the Konkan Coast, Western India, and Its Implications', *Pure and Applied Geophysics*, vol. 178, no. 12, 2021, pp. 4697-4716.

138 Geoffrey Chapman *et al*. 'Security Culture An Educational Handbook of Nuclear & Non-Nuclear Case Studies', *Centre for Science & Security Studies Occasional Papers*, King's College London, 2017. https://www.kcl.ac.uk/csss/assets/security-culture-handbook.pdf

139 'Vested interests at work in Koodankulam, says NPCIL', *The Indian Express*, September 29, 2011. https://indianexpress.com/article/news-archive/web/vested-interests-at-work-in-koodankulam-says-npcil/

140 'Former Atomic Energy Commission chief M R Srinivasan cautions against scrapping Kudankulam Nuclear Project', *The Economic Times*, September 21, 2011. https://economictimes.indiatimes.com/news/politics-and-nation/former-atomic-energy-commission-chief-m-r-srinivasan-cautions-against-scrapping-kudankulam-nuclear-project/articleshow/10063795.cms?from=mdr

141 Karolina Baca-Pogorzelska, 'How Chernobyl fake news poisons nuclear energy debate in Poland', *Notes from Poland*, April 25, 2020. https://notesfrompoland.com/2020/04/25/how-chernobyl-fake-news-poisons-nuclear-energy-debate-in-poland/

facts about performance measurement; processes, such as feedback, assessment, and coordination with relevant stakeholders; principles for guiding decisions and behaviours, such as staff trustworthiness, exemplary leadership, individual motivation, professional conduct, personal accountability, and effective teamwork; and also beliefs and attitudes, such as the belief that a credible threat exists. Furthermore, the IAEA also reports on the consequences external to nuclear facilities. Communicators are concerned that misinformation distributed online in a nuclear emergency could undermine the reach of and trust in official sources of any information, and respect for authorities and decisionmakers. As a result, people may not follow the advice on how to stay safe, worsening the consequences of the emergency.[142]

Cyber attacks

As outlined in other case studies, cyberattacks are another particular concern at the moment. Examples include the 2003 Slammer Computer worm attack in the Davis-Bae NPP in the US, the 2010 Stuxnet malware attack that affected over 15 nuclear facilities in Iran, the 2015 cyber hacking that took place in the Hanford nuclear site in the US and the 2016 W32, Ramnit and Conficker virus attacks in the Gundremmingen NPP in Germany. These have initiated drastic changes in the perception of security within nuclear and critical infrastructure systems.[143] In October 2019 the KKNPP itself faced a malware attack that was confirmed by the NPCIL. The government statement described that the plant was subject to a malware infection in its administrative network. The statement also assured that the malware infection did not gain any control of the plant.[144] However, some did note the attempted landing of India's second lunar research vehicle, Chandrayaan-2, shortly before the cyberattack – and the Indian Space Research Organisation (ISRO) was alerted of a probable threat to its systems.[145] Although a tangible country or organisation is yet to be identified as the perpetrator of this attack, several key stakeholders have expressed concerns about possible future attacks on systems in nuclear facilities.

Despite the courts' faith in the scientific community, the 2019 cyberattack further affected public perception about the KKNPP. When this happened, it was initially denied by the KKNPP – while the NPCIL later released a statement admitting to the occurrence of a malware attack. The investigations were conducted by the DAE Computer & Information Safety Group and the Indian Computer Emergency Response Team. Further analysis by other institutions such as Kaspersky revealed that the malware was DTrack, which was used in the 2016 ATM breach of financial data, including debit and credit card information of millions in the country. Significantly, Kaspersky, as well as Issue Makers Lab – South Korean based malware analysts – highlighted the possible involvement of the Lazarus group.[146,147] There is no verifiable information pertaining to the motivation of the Lazarus group, but speculations include theft and access of technological and technical data of the KKNPP, and the exchange of data to key stakeholders that work against India's interests.[148]

The groups' involvement insinuates a deeper concern for the Indian nuclear energy programme in terms of cyber defence. According

142 Peter Kaiser, 'Can You Trust Your Newsfeed? New IAEA CRP Studies How to Mitigate the Harm of Misinformation in Nuclear Emergencies', *International Atomic Energy Agency*, 29 January 2019. https://www.iaea.org/newscenter/news/can-you-trust-your-newsfeed-new-iaea-crp-studies-how-to-mitigate-the-harm-of-misinformation-in-nuclear-emergencies-j15001

143 Pulkit Mohan, 'Ensuring Cyber Security in India's Nuclear Systems', *ORF Issue Brief*, no. 412, October 2020. https://www.orfonline.org/wp-content/uploads/2020/10/ORF_IssueBrief_412_Cyber-Nuclear-Security.pdf; Alexandra Van Dine, Michael Assante and Page Stoutland, 'Outpacing cyber threats – Priorities for Cyber security at Nuclear Facilities', *Nuclear Threat Initiative*, Washington DC, 2016. https://media.nti.org/documents/NTI_CyberThreats__FINAL.pdf

144 Uptal Bhaskar, 'India confirms malware attack at Kudankulam nuclear power plant', *Livemint*, November 20, 2019. https://www.livemint.com/news/india/india-confirms-malware-attack-at-kudankulam-nuclear-power-plant-11574262777163.html

145 Jay Mazoomdaar, 'Not only Kudankulam, ISRO, too, was alerted of cyber security breach', *The Indian Express*, November 6, 2019. https://indianexpress.com/article/india/not-only-kudankulam-isro-too-was-alerted-of-cyber-security-breach-6105184/

146 Stephanie Findlay and Edward White, 'India confirms cyber attack on nuclear power plant', *The Financial Times*, October 31, 2019. https://www.ft.com/content/e43a5084-fbbb-11e9-a354-36acbbb0d9b6

147 Sushovan Sircar, 'Exclusive: N Korea Stole Data From Kudankulam Attack, Says Expert', *The Quint*, November 7, 2019. https://www.thequint.com/news/india/kudankulam-nuclear-power-plant-cyber-attack-malware-north-korea-stole-information-data; IssueMakersLab, Twitter, November 3, 2019, 5:12am, accessed June 21, 2022. https://twitter.com/issuemakerslab/status/1190846548415959040

148 Harsh V. Pant and Kartik Bommakanti, 'Decoding Motives Behind the Kudankulam Intrusion', *Observer Research Foundation*, November 25, 2019. https://www.orfonline.org/research/decoding-motives-behind-the-kudankulam-intrusion-58083/

to a 2018 data report published by Symantec, a security software company, India is one among the top five nations subject to cyber threats, including targeted attacks.[149] Given multi-dimensional implications, the threat thus extends beyond the cyber defence in the nuclear energy programme, as it also involves command, control and communication (NC3) for nuclear weapons.[150] The threat of terrorism remains a vital concern for India, arising out of the situation on India's borders and intentions expressed by terrorist organisations. Increasing sophistication of these cyber threats can overwhelm internal agencies and affect coordinated strategies in case of emergencies.[151] Although there is no one-stop solution or golden standard guidance that could be adopted, the initial efforts for reform and adaptation begin with proactiveness.

Lessons learned

To ease protesters' concerns and local agitation, the Madras High Court and the Supreme Court in India undertook judicial intervention.[152] The Supreme Court endorsed reports presented by expert committees on relevant safety standards practiced in the KKNPP, showing that these were not compromised. The courts also clarified that all licenses were obtained in accordance with the law. The courts suggested the implementation of the National Disaster Management Guidelines of 2009 and to execute regular emergency exercises both on and offsite as a measure of proactiveness.[153]

From an emergency preparedness perspective, the key driver that could minimise the impact of any disaster is to bridge communication gaps between the state government and the central government and inter-agency gaps. Given the present context, operation in unison is crucial to reducing any opportunities for the spread of misinformation. For instance, the probability of a malware attack was initially raised by a third-party in September 2014. When the attack occurred, the KKNPP denied it in the beginning, although it was later confirmed by the NPCIL.[154] In the future, this lack of coordination could have serious consequences on the established system in the country and further on both the government and industry credibility.

In turn, the cyber incidents identify crucial gaps in India's nuclear energy sector. The integration of cyber networks and systems into the nuclear infrastructure require an automatic incorporation of security measures and practices against possible resultant threats and risks. Traditional forms of security in the nuclear infrastructure domain previously revolved around physical attacks, but a rising sophistication of cyberattacks on the broader connected systems require urgent action to incorporate cyber security mechanisms into the nuclear security structure. This begins with proactiveness to bring about reforms to established regulations. Proactiveness accompanied with adoption of a culture that incorporates the planning, attitude, awareness, and training throughout the management hierarchy in all agencies ensures an efficiency in the established systems.

Conclusion

The rise of new risks and threats raises crucial questions regarding the existing regulatory framework. How can government and relevant stakeholders contribute to nuclear security? This is especially relevant in India, which is developing energy alternatives backed by ambitious plans for self-sufficiency. The contentious KKNPP case has revealed broader security and safety conditions that need to be addressed. KKNPP is India's 'largest civil

149 'India ranks 3rd among nations facing most cyber threats: Symantec', *The Economic Times*, April 4, 2018. https://economictimes.indiatimes.com/tech/internet/india-ranks-3rd-among-nations-facing-most-cyber-threats-symantec/articleshow/63616106.cms

150 The Nuclear Threat Initiative, 'Addressing Cyber-Nuclear Security Threats', About, accessed June 21, 2022. https://www.nti.org/about/programs-projects/project/addressing-cyber-nuclear-security-threats/

151 Rajeswari Pillai Rajagopalan, Rahul Krishna, Kritika Singh and Arka Biswas, 'Nuclear Security in India – second edition,' *Observer Research Foundation*, 2016, p. xiii. https://www.orfonline.org/wp-content/uploads/2016/10/ORF_Monograph_Nuclear_Security.pdf

152 M. Bhawna, 'Nuclear Energy, Development and Indian Democracy: The Study of AntiNuclear Movement in Koodankulam', *International Research Journal of Management Sociology and Humanity*, vol. 7, no. 6, 2017, pp. 219-229.

153 M. P. Ram Mohan and A. Shandilya, 'Nuclear energy and risk assessment by Indian courts: analysis of judicial intervention in the Kudankulam Nuclear Power Project', *Journal of Risk Research*, vol. 18, no. 8, 2015, pp. 1051-1069.

154 P.K. Mallick, 'Cyber Attack on Kudankulam Nuclear Power Plant – A Wake Up Call', *Vivekananda International Foundation*, 2019. https://www.vifindia.org/sites/default/files/cyber-attack-on-kudankulam-nuclear-power-plant.pdf

nuclear facility,' where two units of the plant are operational and two are under construction.[155,156] However, public perception about the plant and its capability is tarnished due to the large anti-nuclear protests and the even bigger nuclear resistance movements that took place predominantly in Tamil Nadu but also in India as a whole.

The case of KKNPP illustrates that gaps in nuclear security culture can be linked to weak public relations, and a failure to address nuclear apprehensions. While general concerns against advancing nuclear energy as an alternative exist, misinformation, protests, and judicial intervention have made the KKNPP case even more contentious. Unlike Sweden or the UK, India is yet to manifest a change in public opinion, despite extensive debates since the inception of the plant.[157] Various key agencies and think tanks in the country have proposed reforms that aim to counter misinformation. It is now up to policy makers and key stakeholders to push for a change in public perception on nuclear power plants to achieve the ambitious goals of self-sufficiency, sustainable development, and a strong nuclear security culture.

Suggested discussion points

1. How can misinformation create security vulnerabilities? Are there steps that nuclear operators and governments can take to mitigate against these risks?

2. Can protest against nuclear facilities create security issues? How can these risks best be managed?

3. Who should be responsible for cyber security at nuclear facilities? How can operators, regulators and government ensure there are clear roles and responsibilities in this area?

155 P.K. Mallick, 'Cyber Attack on Kudankulam Nuclear Power Plant – A Wake Up Call', *Vivekananda International Foundation*, 2019. https://www.vifindia.org/sites/default/files/cyber-attack-on-kudankulam-nuclear-power-plant.pdf

156 Jack Unwin, 'The top seven nuclear power plants in India', *Power Technology*, February 26, 2019. https://www.power-technology.com/analysis/nuclear-power-plants-in-india/; Nuclear Power Corporation India Limited, 'Kudankulam Atomic Power Project', Plants, accessed May 30, 2022. https://www.npcil.nic.in/content/320_1_OperatingPerformance.aspx

157 John B. Ritch, 'Will The Nuclear Power Industry Regain Public Trust?', *Forbes India*, December 29, 2011. https://www.forbesindia.com/article/biggest-questions-of-2012/will-the-nuclear-power-industry-regain-public-trust/31592/1

Nuclear theft in India

by Snekha Gunasekaran

Overview

India's integration into the global nuclear order in 2008 – following 30 years as an outsider – paved the way for an increasing number of nuclear installations across the country.[158] While the market for nuclear energy has gradually been shrinking worldwide, India has gained support for its technological diversification strategy. Taking into consideration the geographical size and location of the subcontinent, India has opened itself up to modular technology experimentations. These factors as well as the usage of nuclear and radiological materials in the medical and agricultural sectors make nuclear safety and security increasingly difficult and, as a result, a pressing concern.

While some have argued that India needs to drastically improve its practices with respect to safety and security of nuclear and radiological materials,[159] a recent study conducted by the Modi government argued the opposite.[160] It claims that India follows some of the best practices with regard to nuclear security in the world, equivalent to nuclear facilities in the UK, Japan, and France. Given India's geo-political situation, it is not surprising that nuclear security measures have been a key issue for the country. Particularly everyday challenges pose a common threat: according to the IAEA Incident and Trafficking Database, 36 countries reported 189 cases of 'unauthorised activities' such as theft and trafficking of nuclear and radiological material in 2019 alone.[161] The following case study will explore how this has affected India, focussing on IAEA guidance for materials outside of regulatory control.[162]

Case summary: Nuclear theft in India

Like most countries, India has made radiological materials easily available as it recognises the

158 Eugene Habiger quoted in Rajeshwari Pillai Rajagopalan, 'Nuclear Security in India', New Delhi: Observer Research Foundation, 2015, p. 24.

159 Nuclear Threat Initiative, 'Nuclear Security Index', accessed 18 July 2022. https://www.ntiindex.org/country/india/

160 Foreign Secretary's media interaction on conclusion of New Delhi Sherpa Meeting, January 17, 2012. https://mea.gov.in/media-briefings.htm?dtl/17957/

161 IAEA Incident and Trafficking Database, 2020 Fact Sheet. https://www.iaea.org/sites/default/files/20/02/itdb-factsheet-2020.pdf

162 IAEA Nuclear Security Series No. 1, 'Nuclear Security Recommendations on Nuclear and Other Radioactive Material out of Regulatory Control', 2011. https://www.iaea.org/publications/8622/nuclear-security-recommendations-on-nuclear-and-other-radioactive-material-out-of-regulatory-control

large-scale usage of such sources in the medical and commercial sectors. The protection of these materials for those purposes is less rigorous than protection of nuclear materials. This increases the risk of happenstance discoveries of scrap materials as well as fraudulent procurement.

Uranium ore and scrap metal incidents

The need for improved strategies and policies for nuclear and radiological security has been augmented by recurring theft and sale of such materials in India. These thefts and illegal sales of nuclear and radioactive materials are not isolated and have contributed to India's flourishing uranium market. A recent incident, in February 2022, saw two Indian nationals apprehended in Nepal for illegally possessing and attempting to sell uranium smuggled from India.[163] The police received a tip about a car parked outside a 5-star hotel on the outskirts of Kathmandu, which contained the illegal substances. In related incidents, it has been possible to trace back the materials to India's uranium mines, with miners stealing unprocessed uranium ore both in an attempt to quickly make some money and as part of larger international networks.[164,165]

In May 2021, reports suggest that seven kilograms of radioactive uranium worth 210 million Indian Rupees were seized from scrap dealers who were attempting an illegal sale. The perpetrators even went so far as to test the uranium in a private lab facility.[166] In this case, a private investigator received a tip and the Maharashtra Anti-Terror Squad (ATS) set up a trap to catch the dealers. They had been trying to sell off the materials online, and ATS sent a dummy customer to secure a sample of the substance. BARC confirmed the material in question was natural uranium, and the National Investigation Agency (NIA) began an investigation.[167] While the outcomes of the investigation have not been publicly announced (yet), it has been suggested that the uranium was found by chance on a truck containing factory waste that was sold to a scrap yard.[168] Globally, it is not uncommon for radiological materials to – often accidentally – end up in scrap yards.[169,170] This is a risk for those who do not recognise the materials; but it can also pose an opportunity to those who do.

Overall, a staggering amount of over 200 kilograms worth of nuclear and radioactive material has reportedly gone missing from government facilities over the past two decades. This raises serious concerns about security measures on multiple levels, and it also creates a serious threat of nuclear terrorism.[171] Indian government has released brochures summarising the various efforts and steps taken on nuclear security.[172] However, the NTI Security Index highlights irregularities as well as inconsistencies in official incident follow-ups. India has traditionally followed an opaque policy when it comes to its nuclear and radiological security, with the argument that publishing the details of endeavors to rectify these situations would draw attention to nuclear-related issues and could potentially result in further thefts or missing cases.

As per global standards, practices, and guidelines pertaining to nuclear energy, each facility is required to have a comprehensive and rigorous

163 The International News, 'Two Indians held in Nepal for selling N-material', February 17, 2011. https://www.thenews.com.pk/print/934333-two-indians-held-in-nepal-for-selling-n-material

164 NDTV, '2 Indians Among 8 Arrested in Nepal For Possessing Uranium-Like Substances', February 15, 2022. https://www.ndtv.com/india-news/2-indians-among-8-arrested-in-nepal-for-possessing-uranium-like-substances-2770415

165 BBC News Calcutta, 'India arrests for 'uranium theft', 10 September 2008. http://news.bbc.co.uk/1/hi/world/south_asia/7608984.stm

166 India Today, 'Two men arrested with 7kg radioactive uranium in Mumbai', 6 May 2021. https://www.indiatoday.in/cities/mumbai/story/two-men-arrested-with-7-kg-radioactive-uranium-in-mumbai-1799552-2021-05-06

167 India Today, 'NIA takes over probe into seizure of 7kg uranium worth Rs 21 crore in Mumbai', 9 May 2021. https://www.indiatoday.in/india/story/nia-probe-recovery-7kg-radioactive-uranium-maharashtra-ats-mumbai-1800551-2021-05-09

168 The Indian Express, 'Explained: ATS seizes 7kg uranium worth Rs 21 crore from a scrap dealer; here's what happened', 11 May 2021. https://indianexpress.com/article/explained/explained-ats-seizes-7kg-uranium-worth-rs-21-crore-from-a-scrap-dealer-heres-what-happened-7305856/

169 Graham Diggines, 'Scrap metal dealers on 'nuclear alert' ', *The Guardian*, 25 April 2000. https://www.theguardian.com/uk/2000/apr/25/nuclear.world

170 Lenka Dojcanova, 'Behind the Scenes of Scrap Yards: IAEA Launches Online Tools on the Control of Radioactive Material Inadvertently Incorporated into Scrap Metal', IAEA, 10 June 2020. https://www.iaea.org/newscenter/news/behind-the-scenes-of-scrap-yards-iaea-launches-online-tools-on-the-control-of-radioactive-material-inadvertently-incorporated-into-scrap-metal

171 The International News, 'Over 200kg uranium theft in India poses threats of nuclear terrorism', 5 September 2021. https://www.thenews.com.pk/print/888297-over-200kg-uranium-theft-in-india-poses-threats-of-nuclear-terrorism

172 'Indian Diplomacy at Work: Nuclear Security in India'. https://www.eoiukraine.gov.in/pdf/NUCLEAR%20SECURITY%20IN%20INDIA%20English.pdf

system to control material to ensure that no small amount of material is unaccounted for. These international standards are specified by the IAEA.[173] However, uranium mines and hospitals will have different and fewer security measures than, for example, sites with nuclear reactors. The nature of the incidents indicates that there could be a certain degree of inside involvement of those who have access to the materials in the facilities. They could be working independently, or colluding with individuals externally.[174] This could prove to be dangerous for the entire South Asia region and beyond.

An absence of strict protocols could further embolden terrorist outfits and individual actors to acquire nuclear materials. This bolsters the necessity of international redressal to ensure the adherence of guidelines and regulations pertaining to nuclear security on a regular basis as it will continuously evolve and improve. Given its long history dealing with nuclear and radiological materials, India has the potential to pioneer best practices.

Regulation and incident response

Regulation of nuclear and radiological materials in India cannot be compared to any other country. Following the Fukushima accident, the Indian government under Prime Minister Manmohan Singh introduced the Nuclear Safety Regulatory Authority (NSRA) Bill. This was done primarily to alleviate international pressure and growing domestic concern over nuclear safety – but the aim of the bill was to establish an independent nuclear regulator. The proposed bill, however, was widely criticised as an autonomous regulatory body was regarded ineffective by members of the Standing Committee of Science and Technology and was subsequently lapsed.[175] In 2015, India hosted an Integrated Regulatory Review Service (IRRS) mission of the IAEA to review the country's regulatory framework for the safety of its Nuclear Power Plants (NPPs). During this review mission, the idea of an independent regulatory body was suggested again. Reintroducing the NSRA Bill was under negotiation but there has been no new development in that regard at the time of writing.

Instead, currently the Central Industrial Security Force (CISF) is primarily responsible for regulating and securing Indian civilian nuclear networks, including all industrial sites across India. The Ministry of Home Affairs is actively recruiting veterans to meet the demands of the force, and they are assisted by other forces as well as private organisations.[176] The CISF has been criticised for its 'conceptual and doctrinal inadequacies.'[177] It consists of a rotating force with approximately 140,000 members deployed across the country which sometimes makes it challenging to develop expertise and knowledge needed to address constantly evolving security issues in the long-term. The IAEA states that a nuclear constabulary would require 'the assembly of characteristics, attitudes and behavior of individuals, organisations and institutions which serves as a means to support and enhance nuclear security.'[178] Such a body requires a level of permanence with respect to personnel. Therefore, establishing a unified command would address some of the issues faced by a force like CISF. This would be more efficient than a rotating force, as it requires less effort and investment to train new members and enhance their abilities.

Lessons learned

Steps can be taken to combat theft of nuclear and radiological materials. This includes improving legislation, regulation and technical efficiency, as well as nurturing a trustworthy and proficient workforce. This will allow India to employ better monitoring, detection, and preventive policies regarding nuclear and

173 International Atomic Energy Agency, 'Nuclear Security Series'. https://www.iaea.org/resources/nuclear-security-series

174 Foreign Secretary's media interaction on conclusion of New Delhi Sherpa Meeting, January 17, 2012. https://mea.gov.in/media-briefings.htm?dtl/17957/

175 Sonali Huria, 'In a Season of Impetuous Lawmaking, whither Nuclear Safety?', The Leaflet, 22 January 2020. https://theleaflet.in/in-a-season-of-impetuous-lawmaking-whither-nuclear-safety/

176 The Hindustan Times, 'Ex-servicemen to help CISF secure sensitive installations', 9 February 2021. https://www.hindustantimes.com/india-news/exservicemen-to-help-cisf-secure-sensitive-installations-101612828798377.html

177 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, pp. 363-384.

178 IAEA (2008), Nuclear Security Culture: Implementing Guide. IAEA Nuclear Security Series No. 7. https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1347_web.pdf

radiological security. Capacity-building as suggested above, for any state, is a monumental task that is neither immediately achievable nor are the resources readily acquirable. To fill in the gaps, one course of action would be to replace the current multi-agency model and diversify by establishing a constabulary. This was deliberated by Jairam Ramesh, then Minister for Environment, in the aftermath of Fukushima.[179] As such, individual domains like material accounting, cyber security, transportation, regulation, and so forth, can each be tackled to the fullest extent.

An important resource to consider here is the IAEA's *Nuclear Security Recommendations on Nuclear and Other Radioactive Material out of Regulatory Control*.[180] Recommendations for preventative measures include:

- Ensuring that offences established under its laws for criminal or unauthorised acts with nuclear security implications are punishable by appropriate penalties.
- Using nuclear forensics for assisting authorities in determining the origin and history of seized material.
- Public dissemination of appropriate information as part of deterrence. Within this, the state should specify what nuclear security information could be misused by a possible offender and therefore should be protected.
- Ensuring that the personnel involved in nuclear security activities in the areas of detection and response, are explicitly deemed trustworthy, to the appropriate levels for their roles, by a formal process.

India adheres to most of these suggestions, but could improve when it comes to policies relating to public dissemination of information, and ensuring trustworthiness of personal – especially at less high-security sites and facilities.

With that said, international cooperation on nuclear and radiological security on a government-to-government level could be most beneficial to address smuggling and theft of materials. However, cooperative relationships can only be achieved over time and when there are no interfering external factors. Increased involvement by the IAEA and other international experts could lead to cooperation, security upgrades, funding, and generally building common interests with other countries and securing nuclear capabilities.

Conclusions

Even before the events of 9/11 and the Nuclear Security Summits, India was greatly invested in the development of its nuclear and radiological security policies and practices. The threat of terrorism had always forced India to be mindful of security challenges in the region. These measures resulted in the use of a hybrid approach, alternating between technology and policy prescriptions around nuclear and radiological materials. However, there is always room for improvement. India could undertake more comprehensive reviews and adopt further regulatory practices, while involving stakeholders who have a vested interest in radiological materials.

Suggested discussion points

1. Are there any options for cooperation between India and neighboring countries on countering nuclear trafficking?
2. Are there wider security culture challenges that need to be addressed in order to sustainably improve radiological security in South Asia?
3. How could the IAEA assist India in realising its nuclear and radiological security goals?

179 Jairam Ramesh, *Green Signals: Ecology, Growth and Democracy in India*. New Delhi: Oxford University Press, 2015, 425.

180 IAEA Nuclear Security Series No. 15, 'Nuclear Security Recommendations on Nuclear and Other Radioactive Material out of Regulatory Control', 2011. https://www.iaea.org/publications/8622/nuclear-security-recommendations-on-nuclear-and-other-radioactive-material-out-of-regulatory-control

Fake news and nuclear security in South Asia

by Tahir Mahmood Azad

Overview

Political and social dimensions of nuclear technology have always been controversial. This is exemplified by mass media propaganda and campaigns against other states' nuclear programmes.[181]

Adding to this problem, recent innovations in media technology have transformed propaganda mechanisms and strategies. These media tools and tactics have blown existing issues out of proportion, and the resulting challenges are beyond any state's control or regulation. Furthermore, social media – mainly YouTube, Twitter, WhatsApp, Facebook, Google and Instagram – have boosted reach and amount of information by building communication proxies.[182] Fake news through reliable media sources is easily accessible to internet users – followed by repetition of false statements and destructive and incorrect content. False information enhances disturbance, apprehension, and irritation and it can channel negative feelings towards those who are propagated to be adversaries. Today, media disinformation and fake news have become effective tools against rival states. This is an age of media warfare.[183]

Although 'both nuclear safety and nuclear security consider the risk of inadvertent human error, nuclear security places additional emphasis on deliberate acts that are intended to cause harm.'[184] The international community is mandated to take action to address nuclear

181 For example, the Institute of Strategic Studies, Islamabad, has criticised numerous think tanks, research institutes and the media in the US and UK to 'constantly stir [...] the paranoia and propaganda against Pakistan's nuclear weapons program.' Malik Qasim Mustafa, 'Pakistan's Nuclear Weapons Programme: Criticism, Propaganda and Response', *Strategic Studies*, vol. 37, no. 4, 2017, p.40. https://www.jstor.org/stable/48537571

182 See for example, Anthony R. Dimaggio, *Mass media, mass propaganda: examining American news in the 'War on Terror'*, Lexington Books, 2008; David L. Altheide, 'The mass media and terrorism', *Discourse & Communication*, vol. 1, no. 3, 2007, pp. 287-308.

183 Jarred Prier, 'Commanding the trend: Social media as information warfare', In *Information warfare in the age of cyber conflict*, pp. 88-113. Routledge, 2020.

184 International Atomic Energy Agency, 'Nuclear Security Culture', IAEA Nuclear Security Series, No.7, Vienna, 2008, p.5. https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1347_web.pdf

security matters. The IAEA has initiated several legal instruments to make security regimes gradually more effective and robust. Member states have largely constructed mutual harmony in this regard. Specifically, there are various threats which are associated with nuclear technology. The largest of these is the danger of nuclear terrorism.[185,186] The international community has taken this very seriously and the IAEA has charted a path to preventing and countering such actions. This case study will call into question the definition of nuclear sabotage and terrorism: do these comprise only physical attacks or should we be considering the power of media as well?

Case summary: **Fake news and nuclear security in South Asia**

Nuclear terrorism comprises terrorist actions against nuclear facilities, military or civilian, including vehicles transporting nuclear weapons, components, or material; and those in which nuclear weapons, explosive devices, or materials are used to threaten or kill people and abolish infrastructure.[187] It is plausible that terrorist or non-state actors can originate nuclear aggression by methods including deception.[188] For example, terrorists might be able to provoke a nuclear exchange in South Asia by perpetrating a conventional attack in India or Pakistan to increase the risk of state involvement.[189]

After the nuclear tests in 1998, a new era of war tactics and planning emerged in Southern Asia focusing specifically on information warfare. Both Pakistan and India are continuously engaged in various kinds of bilateral conflicts, disputes, and media wars. In recent years, mainstream media channels and newspapers of both states have been involved in reporting aggressive stories. Now, social media is being used for disinformation and 'hate politics.'[190]

Nuclear issues are very sensitive, and any information related to nuclear technology can have physical as well as psychological implications. However, mass media campaigns have been carried out as part of hybrid warfare – and in South Asia this can be traced back to as early as 1980.[191] While hybrid warfare is not a direct war, it makes use of a mixture of irregular strategies, including media propaganda, fake news, and misinformation campaigns.

Media reports on nuclear facilities and fissile material

Pakistan has run a nuclear program since the 1950s. However, the program has always faced international critique and global opposition. Media narratives and campaigns from other countries pose a big challenge for Pakistan. In particular, there have been series of articles, reports and media campaigns that were developed on the basis of hypothetical assessments and data.[192] Yet, according to Pakistan's official records, there is not a single statement made by the government regarding the exact quantity of nuclear material or nuclear fuel on Pakistani soil. At the same time, it has repeatedly been stated that nuclear facilities are under tight security control and responsible institutions are fully prepared to counter any threat.[193]

In 2019, after the Pulwama incident (see the final case study in this handbook for further details), Pakistan and India were on the verge of war. Mainstream media, especially social media, played negative roles on both sides. Social media users on platforms such as Twitter, Instagram and YouTube were spreading incorrect information and hate speech. Indians called for

185 Jack Boureston and Tanya Ogilvia-White, 'Seeking Nuclear Security through Greater International Coordination', *Council on Foreign Relations*, 2010, p.1.

186 Ibid.

187 Peter DeLeon, Bruce Hoffman, Konrad Kelien, and Brian Jenkins, *The Threat of Nuclear Terrorism: A Re-examination*, Santa Monica: *RAND Corporation*, 1998, p.3.

188 Charles D. Ferguson, William C. Potter, *The Four Faces of Nuclear Terrorism*, London: Routledge, 2005, p.3.

189 William C. Potter, 'Countering the Threat of Nuclear Terrorism', in Jean du Preez (ed.), *Nuclear Challenges and Policy Options for the Next U.S. Administration*, James Martin Center for Nonproliferation Studies, Occasional Paper No. 14, December 2008, p.31.

190 Tahir M. Azad, 'Understanding International Propaganda Patterns against Pakistan', in the Institute of Regional Studies (IRS), *Fake News & Facts*, IRS: Islamabad, 2020, pp.210-211.

191 Ibid., p.212.

192 T. M. Azad and M. Rehman, 'International Misperceptions about Pakistan's Nuclear Security', *Global Strategic & Security Studies Review (GSSSR)*, vol. V, no. IV, Fall 2020, p.10.

193 Tahir. M. Azad and H. Shahid, 'Evolution of Pakistan's Nuclear Weapon Programme', *Global Strategic & Security Studies Review (GSSSR)*, vol. VI, no. I, Winter 2021, p.7.

nuclear attacks on Pakistan; Pakistanis called for nuclear attacks on India.[194] However, tension was defused by level-headed decisionmakers in both countries.

An important case regarding fake news and disinformation was revealed by the Brussels-based EU DisinfoLab, which is working to fight disinformation against the European Union. It has uncovered 'a 15-year-old operation run by an Indian entity ANI that used hundreds of fake media outlets and the identity of a dead professor to target Pakistan.'[195] The EU DisinfoLab partially uncovered the network – but admitted the process is much bigger and more resilient than it first assumed.

On 19 November, 2021, Indian media reported a 'seizure of possible radioactive material' by Indian port authorities at the Mundra Port on containers loaded on a Shanghai bound commercial vessel from Karachi Port.'[196] According to the Ministry of Foreign Affairs in Pakistan, concerned authorities of the Karachi Nuclear Power Plant were informed that these were empty containers. These containers were being returned to China, and earlier they had been used for the transportation of fuel from China to Karachi for the K-2 and K-3 Nuclear Power Plants. Both K-2 and K-3 Nuclear Power Plants and fuel used in these plants are protected by IAEA safeguards. Pakistan consequently stressed that such fake reporting and disinformation 'is symptomatic of malicious intent to twist procedural customs issues to bring into disrepute an IAEA safeguarded nuclear power program.'[197]

There are various other fake news stories and disinformation examples which have been articulated by other states to malign Pakistan's nuclear security. These fake news and disinformation campaigns have created serious challenges for Pakistan. Pakistan should address these fake news threads, especially those against its nuclear program. However, changing the nuclear narrative is not an easy task in the Southern Asian region.

Lessons learned

Countering misinformation

To reduce the impact and amount of misinformation, particularly on the internet, both Pakistan and India should be in close contact with information providers and platforms such as Twitter and YouTube. Similar to approaches during the COVID-19 pandemic and other fast-paced information wars with high levels of misinformation, social media platforms should be informed of the possible consequences if such content remains unrefuted on their websites, and they should be incentivised to either flag wrong content, remove it entirely, block accounts strategically spreading misinformation, or remove them from their platforms. Videos or messages uploaded by terrorists and terrorist organisations such as Al-Qaeda have shown that, with the support of Artificial Intelligence (AI), Facebook, YouTube and Twitter have been able to find and remove illicit content relatively quickly. After the removal of former-US President Trump's account from Twitter – following his user rights violation by providing misinformation and calling for the storming of the Capitol in January 2021 – it can be assumed possible that accounts spreading nuclear-related misinformation can be shut down as well. Local providers in South Asia can consider taking the same actions.

Establishing joint verification mechanisms

Ideally, Pakistan and India both can work together to establish a joint monitoring and verification committee to avoid any miscommunication about nuclear issues. This regional media monitoring committee should play a role in capacity building, to strengthen media in each country. It should further play a role in public advocacy in its respective countries. By establishing a joint media forum that discusses and provides real-time information, the public in both countries could easily judge whether information obtained is accurate and

194 Mikail Shaikh, 'The Pulwama Incident Part Two: Pakistan And India Have Much To Learn', *Global Security Review*, June 07, 2019. https://globalsecurityreview.com/pulwama-pakistan-india-conflict-much-learn/

195 EU Disinfo Lab, 'Indian Chronicles', December 09, 2020. https://www.disinfo.eu/publications/indian-chronicles-deep-dive-into-a-15-year-operation-targeting-the-eu-and-un-to-serve-indian-interests/

196 Ministry of Foreign Affairs Pakistan, 'Pakistan rejects Indian media reports claiming 'seizure of possible radioactive material', November 20, 2021. https://mofa.gov.pk/pakistan-rejects-indian-media-reports-claiming-seizure-of-possible-radioactive-material/

197 Ibid.

up to date. Establishing such a forum could also contribute to trust building measures between India and Pakistan by providing a platform for information exchange and verification, particularly when tensions are high.

Academia, journalism, and research institutes – including those conducting OSINT – could contribute to this forum by providing information and assisting in high-quality media production. As such, the joint verification and monitoring mechanisms would reinforce the social-media-based mechanism to counter misinformation discussed above. The EU DisinfoLab can stand as a model for such a forum.

Conclusion

Misinformation campaigns and fake news have gained new traction with the development of highly sophisticated distribution mechanisms. These are increasingly being used as tools of hybrid warfare. In high-risk and fast evolving situations such as trans-border incidents between Pakistan and India – with nuclear implications – preventing the spread of misinformation and generating trust among political decision-makers and the public on both sides of the conflict lines is crucial to avert escalation. Communication involving officials from both sides would help to establish factual discussions and facilitate trust between the two countries. Embedding information structures into trans-national communication is thus crucial for the improvement of nuclear security. Additionally, such structures can render a beneficial advantage for knowledge exchange of lessons learned between India's and Pakistan's advanced civil nuclear sectors.

Suggested discussion points

1. What role does nuclear disinformation play in international relations?
2. What is the impact of fake nuclear news in hybrid warfare?
3. What are the psychological implications of nuclear misinformation?

Nuclear security and crisis communication

by Shayan Hassan Jamy

Overview

This handbook has so far focused exclusively on the civil nuclear sector in South Asia. However a lack of separation between civil and military remains in India and especially Pakistan, and there is no way around the fact that both countries also possess nuclear weapons. While nuclear threats and risks are usually analysed through a geopolitical lens, it certainly influences the civil sector in each country as well. Dangers such as terrorist threats and sabotage of nuclear and radiological facilities are very real on both sides, and as such civil nuclear security cannot be considered in isolation of other issues. A particularly significant area of overlap can be found in crisis communication, which is what this case study will focus on.

In any crisis or conflict involving nuclear armed states, effective communication is crucial in order to mitigate the potential risks of nuclear use. Even though a conflict may begin with conventional weapons, the presence of nuclear weapons on both sides severely complicates the matter, with nuclear escalation always being considered a possible last resort option. Nowhere is this more relevant than in South Asia, where multiple conflicts between India and Pakistan have put tremendous strain on the nuclear security systems in the region; the most recent incident being the 2019 India-Pakistan conflict, which consisted of a series of armed clashes, cross-border airstrikes and exchanges of gunfire between India and Pakistan across the disputed border in the Kashmir region. Although the incident ended without nuclear escalation, the lack of formal crisis management structures between the two states was clearly highlighted. This chapter explores the importance of crisis communication for nuclear security, and examines the lessons we can learn from the 2019 India-Pakistan conflict for nuclear security

culture.

Since their independence in 1947, India and Pakistan have been mired in conflict. While India already tested nuclear weapons in 1974, the relationship with its neighbour took a new turn in 1998 when both states tested nuclear weapons. Between then and 2019 the two countries were involved in four conflicts, none of which has come close to crossing the nuclear threshold. It is important to note, though, that any conflict between nuclear armed states has the potential to escalate and result in the use of nuclear weapons. Therefore, every India-Pakistan conflict since 1998 has been fought under the nuclear shadow.

A major cause of most India-Pakistan conflicts since 1947, has been the unresolved Kashmir dispute. For this, and other reasons, ties between the two states had already deteriorated prior to the 2019 conflict. In terms of the global strategic environment, the international system had been moving away from the unipolarity that had been seen in the post-World War II era. In addition, the US-India strategic partnership had been growing steadily, as had Pakistan-China relations. These factors have contributed to making an India-Pakistan conflict more likely.

Case summary:
Nuclear security and crisis communication

On 14 February 2019, more than forty Indian police personnel were killed by a suicide bomber in Pulwama, located in India-administered Kashmir.[198] This precipitated what would become known as the 2019 Pulwama/Balakot crisis. Pakistan-based terrorist organisation Jaish-e-Muhammad (JeM) claimed responsibility for the attack.[199] India subsequently blamed Pakistan for the attack, an accusation Pakistan denied. India responded to the Pulwama incident by carrying out a cross-border airstrike near Balakot, Pakistan, on 26 February.[200] This was the first airstrike to take place on Pakistani soil since the 1971 war. India claimed to have killed 'a very large number' of JeM terrorists in the airstrike, while Pakistan stated that there had not been any casualties or damage.[201] India's claims were later refuted by local accounts of the airstrike as well as various independent international sources.[202] In the midst of the conflict, however, none of this was clear.

Pakistan's response was immediate. On 27 February, Pakistan conducted a retaliatory airstrike on Indian-administered Kashmir, which led to a fight with the Indian Air Force.[203] The Pakistan Air Force shot down an Indian fighter jet, and Indian Wing Commander (WC) Abhinandan Varthaman was subsequently captured by Pakistan.[204] In the midst of the conflict, an Indian military helicopter was also brought down by friendly fire, which resulted in the death of all six on board.[205]

What followed was a short period of significant tension between India and Pakistan. Ultimately, nuclear escalation was avoided. As a peace gesture, Pakistan returned WC Abhinandan to India on 1 March, which brought an end to the conflict.[206] Although we now have more clarity regarding the details of the conflict, as events unfolded, there was contradictory information on both sides. It would certainly have been possible for the conflict to escalate even further and reach a point where crossing the nuclear threshold would become a possibility for both states.

Significance of nuclear context during the 2019 conflict

Although the 2019 India-Pakistan conflict did not cross the nuclear threshold, the nuclear context during the crisis was certainly worrying. During the conflict, there was aggressive rhetoric

198 'Kashmir attack: Tracing the path that led to Pulwama', *BBC*, May 1, 2019. https://www.bbc.com/news/world-asia-india-47302467

199 Ibid.

200 'Balakot: Indian air strikes target militants in Pakistan', *BBC*, February 26, 2019. https://www.bbc.com/news/world-asia-47366718

201 Ibid.

202 Simon Scarr, Chris Inton and Han Huang, 'An air strike and its aftermath', *Reuters*, March 6, 2019. https://graphics.reuters.com/INDIA-KASHMIR/010090XM162/index.html

203 M Ilyas Khan, 'Between a rock and a hard place', *BBC*, December 24, 2019. https://www.bbc.com/news/world-asia-50826419

204 Ibid.

205 'India admits friendly fire downed Mi-17 helicopter in Kashmir', *The Defense Post*, August 14, 2019. https://www.thedefensepost.com/2019/10/04/india-mi-17-helicopter-kashmir-friendly-fire/

206 Michael Safi and Mehreen Zahra-Malik, 'Pakistan returns Indian pilot shot down over Kashmir in peace gesture', *The Guardian*, March 1, 2019. https://www.theguardian.com/world/2019/mar/01/pakistan-hands-back-indian-pilot-shot-down-over-kashmir-in-peace-gesture

exchanged between India and Pakistan, both of whom directly and indirectly signalled their willingness to use nuclear weapons. India reportedly threatened to launch missile strikes against Pakistan, to which Pakistan promised a response 'three times over.'[207] While these would have likely been conventional missiles, it would have been easy for the conflict to spiral out of control. During the conflict, Pakistani Prime Minister Imran Khan stated that 'given the weapons we have, can we afford miscalculation?'[208] Despite the fact that this was responsible nuclear signalling from PM Khan, it reminded the world of the presence of nuclear weapons on both sides. It showed that even the state leadership was aware of the risk of miscalculation associated with nuclear weapons, especially in South Asia. Indian Prime Minister Narendra Modi later, in April 2019, said India would have responded with a 'night of murder' if WC Abhinandan had not been returned by Pakistan.[209] He also threatened Pakistan by openly stating that India's nuclear weapons were 'not for Diwali.'[210] Such statements were likely made by PM Modi to appeal to his voter base, with the Indian general elections taking place soon after. Whatever the reason, such statements exchanged between nuclear armed states decrease the trust between them, leading to further deterioration of crisis communication in any future India-Pakistan conflict.

Also, the Indian Navy confirmed that it had shifted its major combat units from exercise to operational deployment mode.[211] These included the ballistic missile-armed submarine INS Arihant and the Russian nuclear-powered submarine INS Chakra.[212] There was also a meeting of Pakistan's Nuclear Command Authority, on 27 February.[213] With these events taking place during the conflict, the risk of miscalculation or incorrect threat perception by both conflict parties could have led to serious escalation of the situation.

Ultimately, WC Abhinandan was returned to India and the crisis moved towards de-escalation. However, what could have happened if the Indian pilot had been killed? What if there had been any significant casualties or damages as a result of the airstrikes? India and Pakistan would perhaps not have been so willing to move the conflict towards de-escalation. In that case, the conflict could have easily escalated out of control. When nuclear weapons are involved, neither state can afford the slightest miscalculation or error.

Implications of the 2019 conflict

The 2019 India-Pakistan conflict had a number of implications. Following the conflict, and after Indian actions in Kashmir in August 2019, India and Pakistan downgraded diplomatic ties, and suspended several trade and travel ties and confidence building measures (CBMs).[214] This deterioration of ties makes a future conflict more likely. In any future India-Pakistan conflict, the risk of nuclear escalation would again be present.

Lessons learned

Various lessons were learned from the 2019 India-Pakistan conflict for better nuclear security practices. These lessons do not only apply to India and Pakistan, but to any nuclear armed state.

The clash made clear that any third-party mediation would be difficult in a future India-

207 Sanjeev Miglani, Drazen Jorgic, 'India, Pakistan threatened to unleash missiles at each other: sources', *Reuters*, March 17, 2019. https://www.reuters.com/article/us-india-kashmir-crisis-insight-idUSKCN1QY03T

208 'Imran Khan calls for talks, urges India to avoid miscalculation', *Al Jazeera*, February 27, 2019. https://www.aljazeera.com/news/2019/2/27/imran-khan-calls-for-talks-urges-india-to-avoid-miscalculation

209 Jeffrey Lewis, 'Night of Murder: On the Brink of Nuclear War in South Asia', *Nuclear Threat Initiative*, November 6, 2019. https://www.nti.org/analysis/articles/night-murder-brink-nuclear-war-south-asia/

210 'Our nuclear weapons are not for Diwali, Modi threatens Pakistan', *The Express Tribune*, April 21, 2019. https://tribune.com.pk/story/1956023/nuclear-weapons-not-diwali-modi-threatens-pakistan

211 Imran Hassan, 'Nuclear South Asia: Three Years After the February 2019 Kashmir Crisis', *South Asian Voices*, February 28, 2022. https://southasianvoices.org/nuclear-south-asia-three-years-after-the-february-2019-kashmir-crisis/

212 Ibid.

213 'NCA under PM reviews nuclear capability amid rising tensions', *Geo News*, February 27, 2019. https://www.geo.tv/latest/229439-pm-chairs-national-command-authority-meeting

214 'India-Pakistan relations plumb new depths in 2020', *Economic Times*, December 23, 2020. https://economictimes.indiatimes.com/news/defence/india-pakistan-relations-plumb-new-depths-in-2020/articleshow/79917285.cms

Pakistan conflict.[215] Historically, the US had played a major role as a mediator between the two states and has played its part in de-escalating previous India-Pakistan crises. However, the recent US withdrawal from Afghanistan and the growing US-India strategic partnership would make it difficult for the US to act as a mediator. China, or any other major state, would also find it difficult to be involved in any mediation. Hence, the onus lies on India and Pakistan to communicate effectively with each other.

However, the conflict highlighted the lack of effective crisis communication between the two states. Without proper communication between India and Pakistan, a future conflict could spiral out of control due to miscommunication. This needs to be addressed urgently. The lack of crisis communication between India and Pakistan was again on display in March 2022, following the misfiring of an Indian Brahmos missile into Pakistani territory.[216] It took 48 hours for communication to be established by India, when they acknowledged the misfire was due to a 'technical malfunction.'[217] Such miscommunication cannot be afforded in a nuclear-charged environment.

In most previous conflicts since 1998, both states had maintained a certain level of communication, either through bi-lateral dialogue or leadership hotlines.[218] The importance of crisis communication between nuclear states, especially in the age of emerging technologies, is crucial. Due to the proximity of the South Asian neighbours, the reaction time during a conflict would be minimal. A misfiring of a missile or any other error could be perceived to be a serious escalation, and could possibly lead to the conflict crossing the nuclear threshold. The risk of nuclear escalation in South Asia is too high for there not to exist effective crisis communication between India and Pakistan.

Both India and Pakistan want to maintain a positive perception of themselves on the international stage. Therefore, one state maintaining a responsible nuclear posture during conflict could increase the de-escalation potential in a future crisis. In this scenario, Pakistan's return of WC Abhinandan to India portrayed it as a responsible nuclear weapon state on the international stage. India could not have responded with further escalation of the conflict, as it would have risked losing its image as a responsible nuclear weapon state. Therefore, the international community has a major role to play in any potential conflict between nuclear armed states.

Also, major territorial disputes, like Kashmir, remaining unresolved increases the risk of conflict escalation.[219] CBMs and stable relations are crucial to avoid any conflict from crossing the nuclear threshold, or even stopping the conflict before it can develop. Bilateral CMBs between India and Pakistan would lead to gradual building of trust between the two states, which is currently missing. With that said, measures such as these seem unlikely due to the current geo-political climate. However, we can learn valuable lessons for nuclear security from this situation. Resolution of any long-standing disputes along with maintaining stable relations would prevent any serious escalation of conflict between nuclear armed states. Ultimately, maintaining effective crisis communication during any conflict between nuclear armed states should be the minimum standard to set.

Conclusions

Overarching national interests and geopolitical events will always impact important infrastructure. The IAEA's *Nuclear Security Culture Implementing Guide* (NSS 7) emphasises numerous aspects of clear and effective communication and notes the significance of principles for guiding decisions. It also underlines that it is crucial to understand that a credible threat exists, in order to prevent theft, sabotage,

215 Sitara Noor, 'Pulwama/Balakot and the Evolving Role of Third Parties in India-Pakistan Crises', *Stimson*, March 25, 2020. https://www.stimson.org/2020/pulwama-balakot-and-the-evolving-role-of-third-parties-in-india-pakistan-crises/

216 Daryl G. Kimball, 'India accidentally fires missile into Pakistan', *Arms Control Association*, April 2022. https://www.armscontrol.org/act/2022-04/news/india-accidentally-fires-missile-into-pakistan

217 Ibid.

218 Zafar Khan, 'Crisis Management in Nuclear South Asia', *Stimson*, 2018. http://crises.stimson.org/nuclear/

219 Moeed W. Yusuf, 'The Pulwama Crisis: Flirting with War in a Nucle ar Environment', *Arms Control Association*, May 2019. https://www.armscontrol.org/act/2019-05/features/pulwama-crisis-flirting-war-nuclear-environment

unauthorised access, illegal transfer or other malicious acts including terrorism.

What is more, in the event of any conflict between nuclear armed states the risk of nuclear escalation is always present. The lack of crisis communication between India and Pakistan was a major problem during the 2019 conflict and could have led to unwanted escalation. A strong nuclear security culture relies on attitudes and behaviors – of individuals and organisations, including policymakers and government representatives.

Suggested discussion points

1. What does this case tell us about the importance of crisis communication for nuclear security?

2. What was the actual risk of use of nuclear weapons during the crisis? Why have both India and Pakistan never resorted to crossing the nuclear threshold in their five conflicts since 1998?

3. How would the conflict have played out had there been any significant casualties or damages on either side?

III. Conclusion

by Dr Zenobia Homan and Amelie Stoetzel

This handbook has shown that both India and Pakistan are confronted with nuclear challenges in an evolving threat landscape. While the regional focus is usually on nuclear weapons and conflict, the analyses in this handbook have emphasised civil aspects of nuclear security and lessons from national regulation, legislation and communication.

As has been demonstrated, both countries have large and highly regulated nuclear sectors. However, the case studies in this handbook have exemplified how nuclear security systems in Pakistan and India have been put under strain by tangible and intangible threats. While some threats have proven to be recurring themes for nuclear installations, others are newly emerging and introduced by novel technology.

Although the regulatory structure is different in India and Pakistan and threats inevitably vary across sectors, some recurring themes can be observed across the case studies:

- **Communication:** As multiple case studies have shown, communication can have a vital impact on nuclear security. For example, communication between the regional and national regulatory bodies was essential to develop clear and effective guidance for nuclear operations during the COVID-19 pandemic. Where communication gaps emerged, nuclear security was at risk due to high levels of uncertainty. In other crisis situations, communication is equally important. For example, effective de-escalatory conversations between India and Pakistan have helped to decrease tensions between the two nuclear weapons states during times of confrontation. This requires restraint in rhetoric, and the fast opening of communication channels on both sides. It furthermore requires a high degree of honesty and mutual trust. Because the media plays a decisive role in such crisis communication as well, current developments regarding misinformation and fake news are particularly worrisome.

- **Culture:** The human element can be considered the weakest link in the chain of nuclear and radiological security. Hence, planning, training, awareness of risks, and a drive for maintenance and improvement create a better security culture. For decades, accidental disposal of radiological materials has posed an issue in terms of international smuggling networks. Another challenge is theft of radioactive materials from sites such as mines or hospitals, which may have different security measures and a weaker security culture than nuclear facilities. An interesting new factor was underlined by the global COVID-19 pandemic: an increase in remote working. This has affected nuclear security in all areas, including energy and research.

- **Anticipating novel threats:** In particular, cyber security has become increasingly important – facilities face a broad spectrum of threats and challenges in this realm, including actions by non-state actors. Cyber laws are being developed to deal with these issues, and slowly best practices are beginning to emerge. However, the cyber domain is a rapidly developing field, and methods are quickly outdated – especially with developments in AI. In a fast-paced technological environment such as the nuclear sector, anticipating novel threats to nuclear security is at the heart of good security practices. Threats evolve, and answers must be found – ideally before these threats materialise. It was found that it can be helpful to expand on existing international and national regulatory frameworks to do so. Furthermore, drawing parallels between nuclear security and other high-security sectors can help to develop security solutions that anticipate future threats.

From the case studies, several areas for future consideration also emerged. Namely:

- **Interaction between India and Pakistan:** Notably, 'lessons learned' from the case studies rarely included insights from comparable regional incidents. Analyses in this handbook focussed primarily on national response, or other global examples. It can thus be concluded that regional information exchange can and should be increased – particularly with emphasis on positive outcomes. Instead of underlining mistakes or placing blame, the civil nuclear sectors of both India and Pakistan can be

strengthened by sharing examples of good security culture. Of course, realistically there are many political obstacles to overcome before positive and enriching exchange can take place. However, sharing best practices would be beneficial for both sides and it could contribute to building confidence in other areas of the relationship.

- **Cultural differences:** Culture is not homogenous. Although there are useful IAEA guidelines to follow, there is no 'one size fits all' for a strong nuclear security culture. This is especially noticeable in South Asia, with both India and Pakistan being home to thousands of small ethnic and tribal groups and several hundred languages within their own territory. Navigating resulting cultural differences in training can be challenging, especially when training material is designed and delivered by educators from other countries and yet different cultural backgrounds. To bridge cultural gaps, it will be beneficial to see more pedagogic materials – such as further handbooks, case studies, and exercises – tailor-made for the nuclear sector in South Asia. This could also help in the development of culturally aware training material and course delivery.

- **Universal lessons:** Similarly, there is much the rest of the world can learn from the civil nuclear sector in South Asia. Currently, many case studies are contributed by the US and the UK. Yet, India has a mature nuclear industry across many sectors including energy and research, and much more can be written about Pakistan's Centres of Excellence. While secrecy and opaqueness are necessarily a part of maintaining good national security, global nuclear security would benefit from diversifying its sets of examples and sources of information – and, as the case studies in this handbook have shown, both India and Pakistan are in an excellent position to contribute. Providing a platform to non-Western voices is thus a crucial element of nuclear security promotion and education.

To return to the opening remarks: India and Pakistan have mature nuclear industries from which much can be learned. Both states have considerable experience and expertise in operating and managing nuclear programs. As Asian and middle income countries, both states offer an alternative understanding to Western examples of managing nuclear industry operations. Both have developed nuclear and radiological security systems that are unique to their geographic and economic requirements.

These lessons can be useful to other historical nuclear states, but also especially to emerging nuclear states – in particular, neighbours in South Asia. Looking toward the future, several countries are considering nuclear energy as an option, in the form of large NPPs but also SMRs and FNPPs. What is more, many South Asian countries already have excellent nuclear medicine programmes and industrial sectors making use of a range of radiological materials. It will be useful to continue collecting regional cases of best practice and expanding on local lessons learned, so that national regulators, legislators, operators and other nuclear and radiological practitioners can rely on relevant and applicable examples and more compatible information exchange.

Centre for Science & Security Studies
Department of War Studies
King's College London
Strand
London WC2R 2LS
United Kingdom

kcl.ac.uk/csss
@KCL_CSSS