INITIATIVES IN STRATEGIC STUDIES: ISSUES AND POLICIES

The Challenges of Nuclear Security

U.S. and Indian Perspectives

Edited by S. Paul Kapur
Rajeswari Pillai Rajagopalan
Diana Wueger

OPEN ACCESS

palgrave
macmillan

Initiatives in Strategic Studies: Issues and Policies

Series Editor
James J. Wirtz, International Relations, Naval Postgraduate School, Monterey, CA, USA

This important series on topical and timeless issues relating to strategy studies provides a link between the scholarly and policy communities. The focus is on conceptually sophisticated analyses of political objectives and military means. Strategy, the focus of strategic studies, revolves around core and perennial concerns: protecting the country and people, influencing friends and opponents, using a variety of military tools in various ways, including to deter or coerce other actors. Strategy deals with problems of national policy and the nexus of political, diplomatic, psychological, economic, cultural, historic and military affairs. Central to strategic studies is an understanding of the environment, including increased comprehension of other strategic actors.

S. Paul Kapur · Rajeswari Pillai Rajagopalan · Diana Wueger
Editors

The Challenges of Nuclear Security

U.S. and Indian Perspectives

palgrave
macmillan

Editors
S. Paul Kapur
Naval Postgraduate School
Monterey, CA, USA

Rajeswari Pillai Rajagopalan
Observer Research Foundation
New Delhi, India

Diana Wueger
Naval Postgraduate School
Monterey, CA, USA

ISSN 2945-7130 ISSN 2945-7149 (electronic)
Initiatives in Strategic Studies: Issues and Policies
ISBN 978-3-031-56813-8 ISBN 978-3-031-56814-5 (eBook)
https://doi.org/10.1007/978-3-031-56814-5

Cover credit: Nuclear Reactor@XH4D

This Palgrave Macmillan imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Foreword by Ambassador Rakesh Sood

An Indian Perspective

The advent of nuclear weapons in 1945 fundamentally challenged the ideas of conflict between peer rival states as well as the notion of deterrence; it is a challenge that continues to preoccupy strategic thinkers and political leaders. The contradiction inherent with nuclear deterrence is that while credibility requires a demonstratable willingness to use nuclear weapons, rationality, which is the bedrock of deterrence, requires that neither side crosses the nuclear threshold.

Just because nuclear weapons were never used during four decades of the Cold War when U.S.-Soviet rivalry created a bipolar world, it lulled strategic thinkers into believing that the postulates of nuclear deterrence, non-proliferation, and arms control were the answer to maintaining nuclear peace. However, twenty-first-century developments, both geopolitical and technological, have jolted the strategic community out of its comfort zone, forcing them to reassess the entire gamut of nuclear threats and risks.

The end of the Cold War and the break-up of the Soviet Union created a new proliferation risk—that of "loose nukes," of nuclear materials and even weapons being left without the earlier security checks. 9/11 seared the threat of international terrorism into global consciousness, linking it to weapons of mass destruction.

In 2002, India introduced a new resolution at the UN General Assembly, UNGA 57/83, Measures to Prevent Terrorists from Acquiring

Weapons of Mass Destruction. The resolution was adopted unanimously. Subsequent reports by the UN Secretary General helped sensitise the international community and in 2004, the UN Security Council unanimously adopted Resolution 1540 under Chapter VII of the UN Charter that made it binding on all members to adopt and enforce laws criminalising the possession and acquisition of all weapons of mass destruction, their means of delivery, and related materials by non-state actors, as well as efforts to assist or finance such activities. All states were also obliged to put into place appropriate domestic laws. This was essential to prevent the burgeoning nexus between transnational criminal networks and terrorist groups.

President Barack Obama took the initiative to host a Nuclear Security Summit (NSS) in Washington in 2010. Three international organisations and 47 states attended. The initiative did not undertake any negotiations but concentrated on recognising the common threat of vulnerable facilities and materials, sharing of best practices as a community, and taking unilateral initiatives in the form of "gift baskets" to reduce stockpiles of fissile materials. Three more summits were held in 2012 in South Korea, in 2014 in the Netherlands, and in 2016 again in Washington, to sustain the momentum.

The new risks and these meetings focused attention on nuclear safety and nuclear security afresh. It is clear that safety and security are equally applicable to both military and civilian facilities and nuclear assets. Second, nuclear safety is a subset of nuclear security. Sometimes, safety is explained as preventing internal nuclear risks from escaping and creating an external impact while security is protection of a facility against external threats though this is an oversimplification. Safety features can be inbuilt into the design of the facility and safety drills enhance the overall security. In case there is a nuclear incident, the first priority is to address the public fallout, both political and radiological. Linked to it is ascertaining the cause of the incident—whether it was an equipment failure, a genuine human error or deliberate sabotage or hostile intent. Determining the cause behind the incident also requires intelligence inputs and a calculated assessment that will be undertaken by the security agencies, irrespective of whether the incident has taken place in a civilian or a military facility.

Since the India-US Civil Nuclear Agreement concluded in 2008, there has been a steady increase in exchanges between the two nuclear establishments, gradually nurturing a habit of working together. It has not been easy as exchanges had ended abruptly in 1974. India participation in the

NSSs had also helped the trust building process. It is this growing trust that led to the project helmed by the Observer Research Foundation and the Naval Postgraduate School, resulting in this volume.

The volume takes up six issues and on each, the reader is treated to an Indian and a U.S. perspective. The six issues are carefully chosen and cover insider threat and personnel reliability; role of organisational culture; crisis communication and managing emergency responses; physical security and protection of nuclear materials in use, transport or storage at both civilian and military facilities; risk management and risk reduction in managing radioactive sources; and, cybersecurity threats to nuclear infrastructure.

The perspectives provided interesting insights and are a rich seam to mine for the nuclear security experts in both countries. While federal structures in both countries are different as are organisational hierarchies, yet it is worth exploring if one or the other possesses inherent strengths or weaknesses. Similar differences will show up in crisis communication strategies in a multilingual society like India. There are bound to be differences in response structures too. Yet on others like cybersecurity threats, there would be greater common ground. Though U.S. cybersecurity infrastructure is more developed, the nature of threats would be similar and provide an avenue for further cooperation. Societal structures and hierarchies are different and this is bound to reflect in variations in organisational cultures. Notwithstanding due sensitivity towards these differences, an objective assessment is bound to throw up lessons for learning.

What makes this compendium interesting is the accumulated expertise that the practitioners-cum-authors bring to their respective chapters. The six Indian authors and the dozen U.S. authors have broken bread together while bringing this project to fruition and helped build mutual trust while also gaining each other's respect.

Finally, while the strategic community grapples with the challenges of nuclear deterrence in an era of multipolar nuclear rivalries marked by asymmetry, it is useful to remember that nuclear security is critical to preserving the nuclear taboo.

New Delhi, India
May 2023

Ambassador Rakesh Sood

Ambassador Rakesh Sood has over 38 years of experience in the field of foreign affairs, economic diplomacy, and international security issues and is a frequent speaker and contributor at various policy planning groups and reputed think tanks in India and overseas. He set up the Disarmament and International Security Affairs Division in the Foreign Ministry, which he led for eight years. He then served as India's first Ambassador—Permanent Representative to the Conference on Disarmament at the United Nations in Geneva; he was also a member of UN Secretary General's Disarmament Advisory Board from 2002 to 2003. In September 2013, Ambassador Sood was appointed Special Envoy of the Prime Minister for Disarmament and Non-Proliferation Issues; a position he held till May 2014. From 2016 to 2022, Ambassador Sood held the position of Distinguished Fellow at the Observer Research Foundation (ORF). Ambassador Sood is a Distinguished Fellow at the Council for Strategic and Defense Research (CSDR), where he directs the work of CSDR's Space Technologies and Policy Program.

Foreword by Dr. Christopher Ford

A U.S. Perspective

From the perspective of a policy practitioner, there is perhaps little novelty in being concerned about nuclear security. Several successive U.S. administrations, after all, have highly prioritized it. In the wake of the terrorist attacks upon the United States in September 2001, American officials focused intently upon ensuring that future terrorists never gained access to nuclear material out of which they might be able to fashion a crude nuclear weapon or a radiological dispersal device, or—worse still—access to a usable nuclear device itself.

In the 2010s, nuclear security became a high-level diplomatic priority. In fact, three major international summits—at the head-of-government level, no less—were held on the topic in 2010 (Washington, D.C.), 2012 (Seoul), and 2014 (The Hague), at which governments issued a succession of pledges to secure what was termed "vulnerable" nuclear material worldwide. Toward the end of that decade, the emphasis shifted from using summits to elicit promises of progress to trying to institutionalize and routinize nuclear security "best practices" as the almost reflexive, day-to-day "new normal" of the international community, but the focus on these issues remained strong.

Nevertheless, despite all this attention from practitioners, the subject of nuclear security has received comparatively little scholarly attention. It may have been pursued by national security technocrats, but what it

wasn't was written much about, and there has not yet developed a real literature on the topic.

Hence the importance of this volume, which performs two signal services for the international security community. First, it compiles a number of thoughtful papers that begin to redress this longstanding lack of a nuclear security literature, and makes these papers widely available. Second, this book does not simply compile the thoughts and research of *one* country's experts, but instead brings together experts on nuclear security who are international as well as interdisciplinary. It draws them, moreover, not from just anywhere, but from two countries of tremendous systemic importance: the United States and India. These are, of course, the world's two largest democracies, but each of them also has a sizeable civil nuclear sector, a highly sensitive nuclear weapons establishment, and a history of facing grave terrorist threats.

This book thus does both its readers and the broader policy community an important service, for as we seek to make nuclear security best practices into something as reflexive as breathing—or perhaps more aptly, as "second nature" as it now is in the developed world to fasten one's safety belt when driving in an automobile—we need to make the nuclear security sector more *reflective*. We need it to develop a rich corpus of literature in which experts are able to share perspectives, learn from each other's experiences and research, argue with each other wherever needed, and generally advance the state of the art, in both *theoria* and *praxis*, as the nuclear security community grows and matures around the world.

The development of such a literature is especially important given the real risk that a nuclear-related disaster could stem, as noted in the Introduction, not from a breakdown of deterrence or from nuclear proliferation—dangers that *are* the subject of substantial scholarly attention—but rather "from a peacetime mishap or a terrorist operation at a power plant." Events in Ukraine involving the Zaporizhzhia Nuclear Power Station—so alarmingly occupied and essentially held hostage by the Russian invasion force, and continually at risk of grave damage in the fighting caused by Vladimir Putin's war of aggression—simply highlight this concern.

That is why this volume is so welcome, and so timely.

I had the distinct honor of being part of the conference in New Delhi where some of the chapters that go into this book were first workshopped, and I was at the time enormously impressed with how much it was actually possible for U.S. and Indian experts to discuss and exchange

information and views on this important, but sensitive, topic. It was not always thus.

These issues were ones with which I was myself closely engaged when in government, but for a variety of reasons they were never easy ones to discuss. To see them addressed with such frankness and candor in a "Track 1.5" dialogue was a delight, and it is even more gratifying to see these contributions now mature into a book that will be of considerable value to policy, academic, and operational communities around the world devoted to ensuring that the kind of mishaps and problems considered herein never occur.

To be sure, this is complex terrain for the neophyte. The chapters in this book cover a range of topics, from insider threats and personnel reliability programs to nuclear crisis management, from physical protection of materials and facilities to the control and regulation of radioactive sources, and even to cybersecurity in nuclear facilities. Even simply to enumerate these topics, however, illustrates the importance of not getting these issues *wrong*—and hence also the value of building a scholarly literature and making it available to a wide audience.

As Patrick Lynch and Todd Burbach note in their contribution to this volume, making real progress in this arena does not necessarily have to be "expensive or revolutionary." Moreover, as Narendra Joshi also makes clear later, *sustaining* effective nuclear security requires the adoption and maintenance of an "[e]ffective nuclear security culture." And cultural change is indeed needed, in the broadest sense, to make state-of-the-art nuclear security best practices into the everyday "new normal" for everyone, everywhere who is involved with managing nuclear power, radiological sources anywhere—not to mention those involved in managing nuclear weapons themselves.

This book thus makes a very important contribution, both in the substance it compiles and conveys to the reader, and in the model that it sets for developing a scholarly literature in the field.

Bethesda, Maryland
April 2023

The Hon. Christopher Ford

Dr. Christopher Ford is a visiting fellow at Stanford University's Hoover Institution and a visiting professor at Missouri State University's Graduate Department of Defense and Strategic Studies. From January 2018 until January

2021, he served as U.S. Assistant Secretary of State for International Security and Nonproliferation, where he was responsible, among other things, for State Department nuclear security policy, relations with the International Atomic Energy Agency, and nuclear security-related capacity-building programming. The views he expresses here are Dr. Ford's own, and do not necessarily represent those of anyone else, in the U.S. Government or elsewhere.

Acknowledgement

We are deeply grateful to the many individuals and organizations in India and the United States that provided the time, expertise, and financial backing necessary to bring this volume to life. We especially thank the Defense Threat Reduction Agency (DTRA), including Hunter Lutinski, Robert Pope, Patrick Becker, Patrick Marzluff, Steve Gunther, and Dave Fishman, for their unfailing support over the years. The volume grew out of an annual U.S.-India Track 1.5 Strategic Dialogue, which provided a forum for discussing sensitive subjects forthrightly and respectfully. DTRA's steadfast support for that ongoing project, in addition to this one, enabled us to develop the relationships and trust that eventually made this work possible.

Producing this volume would have been impossible without the support of the Office of the Secretary of Defense's Office for Nuclear and Countering Weapons of Mass Destruction Policy and the Cooperative Threat Reduction Program. There, John Masten guided us through substantive and procedural obstacles with patience and aplomb. We are also grateful to the National Nuclear Security Agency (NNSA), notably Allison Johnston, Karen Gaitan, and Mahmoud "MJ" Jardaneh, for their enthusiastic endorsement of this project and for supporting the participation of lab-affiliated authors.

Finally, this volume could not have been written without the support of the editors' home institutions, the U.S. Naval Postgraduate School (NPS) and the Observer Research Foundation (ORF). We are especially indebted

to Christopher Ketponglard, NPS Faculty Associate for Research, for his tireless efforts, on multiple fronts, to shepherd this manuscript through to publication. We want to thank also Sunjoy Joshi, ORF Chairman, and Samir Saran, ORF President, for their unflinching support to this project in so many ways.

All ideas expressed in this volume are solely those of the individual chapter authors and editors, expressed in their private capacities. They do not represent official positions or policies of any Indian or U.S. governmental organizations.

S. Paul Kapur
Rajeswari Pillai Rajagopalan
Diana Wueger

Contents

Notes on Contributors

Mr. Christopher Boyd has worked over the past 25 years with federal, state, and city agencies; elected officials; and global NGOs to secure the adoption of policies that promote public health, safety, and environmental sustainability. He is the former assistant commissioner for Environmental Sciences & Engineering with the New York City Department of Health where he was the chief regulator for radioactive materials, the New York City water supply, and oversaw responses to environmental outbreaks. He currently serves as a senior consultant for MARC Strategic Solutions, where he advises clients including Brookhaven National Laboratory (BNL), Pacific Northwest National Laboratory (PNNL), and the Office of Radiological Security (ORS) on matters relating to the oversight, management, and regulation of radioactive materials and radiation-producing equipment, as well as adoption of alternative technologies.

Mr. Todd Burbach is the inspector general specialist at Department of the Air Force Inspection Agency, Inspections Directorate, Kirtland Air Force Base, New Mexico. He is responsible for inspecting and reporting high-end readiness and critical compliance by providing oversight of Major Command inspection teams. Additionally, he is an adjunct faculty for the United States Air Force School of Aerospace Medicine, Personnel Reliability Assurance Program (PRAP) course.

He enlisted in the Air Force in October 1982 as a cryptologic linguist technician later serving as an Independent Duty Medical Technician. He

held numerous leadership positions in Special Operations, Medical Treatment Facilities, and various emergency operations and inspections special duties. His assignments include Tactical Nuclear Battery, Intercontinental Ballistic Missile Wings, Prime Nuclear Airlift Force, and Munitions and Maintenance Storage. He retired from active duty in March 2011. Prior to his current position, he was a Nuclear Weapons technical inspector, PRAP, Computer-based Training PRAP course director, and program manager for the Defense Threat Reduction Agency. He currently holds certifications in Basic and Intermediate Nuclear Weapons, Advanced Nuclear Weapons-Surety, and Nuclear Matters.

Dr. Rajeswari Pillai Rajagopalan is the director of the Centre for Security, Strategy & Technology (CSST) at the Observer Research Foundation, New Delhi. Dr. Rajagopalan was the technical advisor to the United Nations Group of Governmental Experts (GGE) on Prevention of Arms Race in Outer Space (PAROS) (July 2018-July 2019). She was also a non-resident Indo-Pacific fellow at the Perth USAsia Centre from April to December 2020. As a senior Asia defence writer for *The Diplomat*, she writes a weekly column on Asian strategic issues. Dr. Rajagopalan joined ORF after a five-year stint at the National Security Council Secretariat (2003-2007), Government of India, where she was an assistant director. Prior to joining the NSCS, she was a research officer at the Institute of Defence Studies and Analyses, New Delhi. She was also a visiting professor at the Graduate Institute of International Politics, National Chung Hsing University, Taiwan in 2012.

Dr. Rajagopalan has authored or edited nine books including *Global Nuclear Security: Moving Beyond the NSS* (2018), *Space Policy 2.0* (2017), *Nuclear Security in India* (2015), *Clashing Titans: Military Strategy and Insecurity among Asian Great Powers* (2012), *The Dragon's Fire: Chinese Military Strategy and Its Implications for Asia* (2009). She has published research essays in edited volumes, and in peer-reviewed journals such as *India Review*, *Strategic Studies Quarterly*, *Air and Space Power Journal*, *International Journal of Nuclear Law and Strategic Analysis*. She has also contributed essays to newspapers such as *The Washington Post*, *The Wall Street Journal*, *Times of India*, and *The Economic Times*. She has been invited to speak at international fora including the United Nations Disarmament Forum (New York), the UN Committee on the Peaceful Uses of Outer Space (COPUOS) (Vienna), Conference on Disarmament (Geneva), ASEAN Regional Forum (ARF), and the European Union.

Dr. S. Paul Kapur is a professor in the Department of National Security Affairs at the U.S. Naval Postgraduate School and a visiting fellow at Stanford University's Hoover Institution. From 2019 to 2021, Kapur served on the State Department's Policy Planning Staff, working on issues related to South and Central Asia, Indo-Pacific strategy, and U.S.-India relations.

Previously, he taught at Claremont McKenna College, and was a visiting professor at Stanford University. Kapur is the author of *Jihad as Grand Strategy: Islamist Militancy, National Security, and the Pakistani State* (Oxford University Press, 2016); *Dangerous Deterrent: Nuclear Weapons Proliferation and Conflict in South Asia* (Stanford University Press, 2007); and the co-author of *India, Pakistan, and the Bomb: Debating Nuclear Stability in South Asia* (Columbia University Press, 2010). His work has appeared in leading academic journals such as *International Security*, *Security Studies*, *Asian Survey*, and *Washington Quarterly;* in more popular outlets such as the *Wall Street Journal*, the *National Interest*, and RealClearPolicy; and in a variety of edited volumes. Kapur also manages consultancy and engagement projects for the U.S. Department of Defense. He received his Ph.D. from the University of Chicago and his B.A. from Amherst College.

Ms. Diana Wueger is a faculty associate for Research in the Department of National Security Affairs at the Naval Postgraduate School and a Ph.D. candidate in Political Science at the University of Chicago. Her dissertation project examines the international politics of secrecy and transparency in conventional arms transfers, and her research interests include the politics of naval and nuclear force structures; great power competition and power projection strategies; and global weapons proliferation and the political economy of security. At NPS, she works with senior faculty to organize government-sponsored Track 1.5/Track 2 strategic dialogues and tabletop exercises with China, Russia, India, and Pakistan. She has assisted in developing a series of operational/strategic South Asian war games in collaboration with the Center for Naval Warfare Studies, and has conducted extensive research on naval strategy for the U.S. Navy.

Ms. Wueger's research has appeared in numerous outlets, including *The Nonproliferation Review, Washington Quarterly*, *Democracy Journal*, *The Atlantic Online*, and *War on the Rocks*, among others. Prior to joining NPS, Diana worked for the Brookings Institution and the Center for the Study of Services in institutional advancement and business development.

She holds a B.A. in Politics from Oberlin College and an M.A. in National Security Affairs from NPS, with a focus in Strategic Studies.

Ms. Daniela Helfet Cooper is the chief of operations (COO) for the Nonproliferation and Disarmament Fund (NDF) at the U.S. Department of State. NDF is a U.S. Government contingency fund responsible for rapidly responding to unanticipated or unusually challenging, urgent, and complex nonproliferation, counterproliferation, weapons destruction, and/or disarmament priorities when and/or where no other USG entities can. This includes threats posed by WMDs, other CBRNE, and advanced or destabilizing conventional weapons, materials, technology, and delivery systems. Dani previously served as the deputy director of NDF before fully shifting in the COO role.

Prior to joining NDF, Dani served as the deputy team chief for Foreign Consequence Management (FCM) in the Office of WMD Terrorism. Prior to FCM, she worked in several capacities throughout the International Security and Nonproliferation Bureau, including various policy and strategy portfolios and two tours in the ISN Front Office as an acting chief of staff and a special assistant to the Assistant Secretary.

Dani is also a former marine officer who was privileged to serve as the Operations Officer for a forward-staged active duty infantry unit, as the headquarters platoon commander and logistics officer for two reserve artillery units, and with the Joint Improvised-Threat Defeat Organization (JIDO) working predominantly on C-ISIS activities in Iraq and Syria. Upon concluding her time with the infantry unit, she returned to civil service with no further service in the Marine Corps Reserves until very recently; she is now a reserve attachment to II Marine Expeditionary Force, G-5.

She holds a B.A. and an M.A. but quickly realized that nobody (including her) cares. She's received a number of military and civilian awards—none of which mean as much as her Marines saving her favorite chow when there was no time to eat or hearing that something jointly learned or experienced by her teammates/marines changed the course of their lives.

Above all else, Dani is most proud of and fulfilled by her family: She is married to the best husband ever (Andy) with whom she has three children—Charlie, Wes, and Grace.

Mr. Alan Evans in his position as a senior research and development nuclear engineer in the International Nuclear Security Engineering

(INSE) department at Sandia National Laboratories, Alan Evans co-leads the Department of Energy (DOE) National Nuclear Security Administration (NNSA) Office of International Nuclear Security (INS, NA-211) Physical Security Functional Team responsible for collaborating with partner countries, industry, academia, and other subject matter experts to develop, test, and implement assessment and engagement tools that will improve physical security at international nuclear facilities. Alan co-leads an effort to develop a new Nuclear Security academic program at the University of New Mexico (UNM) to provide the nuclear security workforce of tomorrow with both practical and theoretical experience. Alan also supports the NNSA Office of Nonproliferation and Arms Control (NPAC, NA-24) Bilateral Physical Protection Assessment Program (BPPAP).

In his current role, Alan uses his nuclear engineering and nuclear security expertise to conduct research and development for effective physical security systems for Advanced and Small Modular Reactors (ASMRs) for the Department of Energy's Office of Nuclear Energy Advanced Reactor Safeguards (ARS) program and the NA-211 Advanced Reactor Security Program (ARSP). Alan works to develop cost-effective security systems for ASMRs that will lead to effective deployment of ASMR technology domestically. Alan works with other national laboratories, and industry partners to ensure this work leads to successful security deployment of ASMR technologies. Alan works under the NA-211 office to develop security deployment strategies for nuclear power plants to ensure protection and mitigation against nuclear security incidents that may cause radiological consequences. Alan has also assisted in the development and execution of training activities in the Design and Operation of Physical Protection Systems, Integrated Performance Testing, Physical Protection Sustainability, Security Planning and Contingency Planning, for multiple national and international partner countries and agencies.

Prior to joining INSE, Alan was an undergraduate R&D intern in Sandia's Advanced Nuclear Concepts department, where he worked on novel cooling systems which would decrease water consumption at nuclear power plants.

Alan completed his B.S. in Nuclear Engineering in 2018 and earned an M.S. in Nuclear Engineering in 2019, both from the University of New Mexico.

Mr. Cliff Glantz is a chief scientist and project manager with the U.S. Department of Energy's Pacific Northwest National Laboratory (PNNL). His research focuses on critical infrastructure protection, cyber and physical security, risk assessment and management, consequence assessment modeling, and emergency response and preparedness. His work supports a variety of critical infrastructure sectors—including the nuclear, energy, dams, chemical, and commercial facilities sectors. His projects are sponsored by the U.S. government, industry, and international organizations. Mr. Glantz is the US nuclear cybersecurity team coordinator for US-India and US-UK bilateral engagements. He is the manager of PNNL's maturity modeling team and is the lead developer for their Cybersecurity Capability Maturity Model for nuclear facilities (C2M2-Nuclear). Mr. Glantz is one of the authors of U.S. NRC's cybersecurity rule (10CFR 73.54), U.S. NRC Regulatory Guide 5.71 (*Cyber Security Programs for Nuclear Facilities*), and several International Atomic Energy Agency guidance and training products. He has authored or co-authored well over 100 publications and 200 conference and meeting presentations since joining PNNL in 1982.

Dr. Sri Nikhil Gourisetti leads large teams in achieving corporate and project goals in support of multiple critical infrastructure sectors, including energy, dams, chemical, healthcare, and critical manufacturing. His current efforts focus on the biopharma subsector.

Prior to joining Resilience in 2023, he spent eight years as a senior cybersecurity researcher at Pacific Northwest National Laboratory. He also served as a visiting assistant professor at the University of Arkansas and Adjunct Facility at Washington State University. Dr. Gourisetti specializes in industrial control systems, operational technology, and internet of things, cybersecurity, software engineering, complex system modeling, and physics-informed machine learning. He is a strong proponent of leading and furthering the world of digital and security innovation to address evolving cyber-physical threats. He has over 10 patent applications and more than 50 publications with over a thousand citations. Dr. Gourisetti earned his Ph.D. in Engineering Sciences and Systems from the University of Arkansas at Little Rock.

Dr. Michael Hornish is a science advisor with the Office of Nuclear Incident Response at the Department of Energy National Nuclear Security Administration headquarters in Washington, DC. He is a radiological/nuclear emergency response subject matter expert supporting the Nuclear

Emergency Support Team (NEST) in Public Health and Safety. His background is gamma-ray spectroscopy, radiation detection, and experimental nuclear physics (Ph.D., Duke University), focusing on neutrino physics, rare decay processes, and nuclear astrophysics.

Michael previously supported NEST at the Remote Sensing Laboratory - Andrews (RSL/A), which is part of the Nevada National Security Site. As a scientist and group leader at RSL, he has conducted research and development with various sponsors in multi-laboratory collaborations, performed test and evaluation of cutting-edge technologies, managed technical projects and operational programs, oversaw NEST assets in domestic and overseas training, exercise, and response activities, and supervised and mentored scientific and technical staff.

Michael has supported numerous real-world responses and major exercises spanning preventive/crisis response (pre-release) and consequence management (post-release) events, including domestic and overseas events such as the response to the Fukushima Daiichi event in 2011. He has served as a team scientist and technical team leader on several NEST assets: Nuclear Search Program, Nuclear Radiological Advisory Team, Radiological Assistance Program, and Aerial Measuring System.

Dr. Narendra Kumar Joshi has done his M.Sc. (1970) and Ph.D. (1975) in physics from BITS, Pilani. He had worked as a postdoctoral fellow and a research associate at CEERI Pilani from 1975 to 1978. He had joined Bhabha Atomic Research Center in 1979 as a scientific officer (C) and retired as a senior scientist (G) after more than 30 years of service in Laser and Plasma Technology division. After his superannuation in 2009, he had worked as an adjunct professor at the Department of Applied Physics BIT, Mesra, Ranchi for two years. He has worked as a professor and head, Department of Nuclear Science and Technology at Mody University, Lakshmangarh (Sikar) from May 2011 to Dec. 2019.

He has around hundred research papers to his credit in reputed international/national journals and conference proceedings. He is the author/co-author of three technical books related to plasma technology. Two students have completed Ph.D. work under his guidance and he has also guided more than 20 students for M.Tech. dissertation work. He has successfully organized more than ten International and National Symposiums. He has delivered more than 18 invited technical talks and has chaired and moderated many scientific and technical sessions. His

current research interests include Nuclear Technology, Nuclear security, Nano-particle synthesis, Plasma simulations and diagnostics.

Ms. Karen Kaldenbach has been working in nuclear security for over 30 years. She began her career in material control and accountability (MC&A) at the Y-12 Nuclear Complex while working on her degrees in computer science and mathematics. After hiring into the Engineering Division in the Oak Ridge Complex, she obtained her masters in mechanical engineering and focused more on facility support and physical security systems. In 1997, Karen began supporting international efforts to enhance nuclear security, working primarily managing upgrade activities for sensitive facilities. These activities included design and installation of physical protection systems, establishment of regional training and technical centers, coordinating the infrastructure to support these installations, and implementation of all necessary elements to ensure long-term sustainability of sensitive facilities. This sustainable foundation includes establishment of a good security culture, training curriculum development, organization and development of maintenance programs, establishment of self-assessment programs and necessary regulatory basis, implementation of human reliability programs, and other performance assurance activities. Currently Karen serves as the Human Reliability Program (HRP) team lead for ORNL, assisting facilities both domestically and internationally to enhance nuclear safety and security.

Mr. Anil Kumar completed a Masters in Nuclear Physics from University of Delhi, India. He started his career as an Indian Police Service (IPS) officer in the year 1986. During 34 years of his distinguished service, he extensively dealt with issues relating to security of vital installations and important persons as well as issues relating to terrorism and anti-corruption. He superannuated from Government Service from the rank of Director General in 2020.

During his service, he also got an opportunity to work with Department of Atomic Energy as Inspector General (Security), Mumbai, from 2011 to 2016, where he supervised and advised on the physical security of installations of the Department of Atomic Energy across the country. He participated in various training courses on Nuclear Security conducted by IAEA and GCNEP. He went on to make significant contributions to the revision of the Physical Security Manual of DAE and various other SOPs. During his tenure, he coordinated meetings of various inter-ministerial committees on physical security matters of Atomic Energy

establishments in India. He also participated in various mock exercises on Nuclear Safety & Security related issues with the Government of India and Interpol.

Mr. Guy P. Landine is a National Security specialist within the National Security Directorate of the U.S. Department of Energy's Pacific Northwest National Laboratory (PNNL). He has extensive expertise in nuclear cybersecurity based on many years of cybersecurity research, including 17 years at PNNL and over 20 years of operational work within the nuclear power industry. Mr. Landine's cybersecurity work at PNNL has included the development of nuclear cybersecurity rules, regulations, and technical guidance; development and implementation of cybersecurity inspection programs; and the development and implementation of nuclear cybersecurity training programs. Mr. Landine is one of the authors of U.S. NRC's cybersecurity rule 10CFR 73.54 *Protection of Digital Computer and Communication Systems and Networks*. His current research focuses on secure network design, threat and vulnerability analysis, intrusion detection, penetration testing, forensic analysis, and malware analysis. Mr. Landine is a senior IAEA instructor and contributing developer of several IAEA advanced cybersecurity training programs. Mr. Landine's work supports the IAEA, the US Nuclear Regulatory Commission, the US Department of Energy, and other clients. Prior to joining PNNL, he led efforts to develop and implement the landmark nuclear cybersecurity program at the San Onofre Nuclear Generating Station and groundbreaking technical guidance issued by the Nuclear Energy Institute.

Ms. Alisa Laufer served as a Global Engagement lead in the U.S. Department of State's Office of WMD Terrorism within the Bureau of International Security and Nonproliferation (ISN). In that capacity, she coordinated multilateral exercises to facilitate smooth international cooperation in response to chemical, biological, radiological, and nuclear emergencies. She also has experience in the Department's Bureau of Political-Military Affairs and the U.S. Senate. She earned a Bachelor's in International Affairs, Security Policy, and Arabic Studies from the George Washington University. She recently departed her role in ISN to pursue of a Master of Public Affairs in International Relations at Princeton University. At Princeton, Alisa focuses her studies on the evolving dynamics, technologies, and geographies of armed conflict.

Ms. Cristina F. Lussier is currently a team lead within the Strategic Integration Directorate at the Defense Threat Reduction Agency. Experienced strategic systems analyst and change agent, Cristina brings over 25 years of experience working across the U.S. federal government supporting whole-of-government approaches against complex challenges within the national security arena, both domestically and abroad. Some of her past positions included working on the National Security Council, among the Intelligence Community, within Combatant Command staffs in the Indo-Pacific, European, and Middle East theaters, to shaping next generation workforce talent as the commander and professor of Aerospace Studies. She has studied abroad in London while earning her bachelor degree in Political Science from Pepperdine University and at Hong Kong's Robert Black College while earning an M.A. in Leadership Studies from the University of San Diego. Cristina also holds an M.A. degree in National Security Studies (Defense Decision Making & Planning) from the Naval Postgraduate School and an M.B.A. from Pepperdine's Graziadio Business School.

Mr. Patrick Lynch is the International Nuclear Engagement Portfolio manager for the Nonproliferation and Security Program (NSP) Office of Oak Ridge National Laboratory (ORNL). The NSP Office develops, coordinates, and assists in the implementation of domestic and international efforts aimed at the nonproliferation of weapons of mass destruction. Prior to joining ORNL, Patrick spent five years at the International Atomic Energy Agency and has also worked for the U.S. Department of State and was a fellow for the Senate Foreign Relations Committee. Most recently, Mr. Lynch has been supporting the U.S. Department of Energy National Nuclear Security Administration's Office of International Nuclear Security, assisting bilateral partners with Insider Threat Mitigation program development and assessments.

Since joining ORNL 2009, he has led global security engagements in over 30 countries related to CBRN threat mitigation. He also supports the University of Tennessee's Institute for Nuclear Security, supporting academic cooperative engagements focused on nuclear security curriculum development, joint research projects, and other cooperative arrangements promoting nuclear security. Patrick holds B.A. and M.Sc. degrees and is currently earning is Ph.D. He is also a 2010 World Nuclear University Summer Institute fellow and has a graduate certificate from the International School of Nuclear Law.

Lt. Col. James McCue currently works in the Global Integration Department of the Defense Threat Reduction Agency (DTRA). In this role he manages WMD experts who connect DTRA capabilities to each of the Geographic and Functional Combatant Commands. Lt. Col. McCue is a senior helicopter pilot with experience in all aspects of the Combat Rescue mission, including over 200 missions in Afghanistan and four deployments to East Africa in both operational and commander's staff roles. He began his career performing nuclear security in Montana, Wyoming, and North Dakota. He has been a detachment commander, instructor, and evaluator, built the aerial gunnery training program, ran response force certification, and managed Red Team vulnerability assessment and training operations. His academic background includes the Air Force Institute of Technology's Nuclear Weapons Effect, Policy, and Planning course, as well as a Master's Fellowship at the National Defense University (NDU) studying Defense and Security Studies with emphasis on emerging technology and nuclear deterrence. While at NDU, he co-authored a journal article on conventional-nuclear integration that was awarded the 2022 General Larry D. Welch Deterrence Writing Award by U.S. Strategic Command. He begins working as a visiting fellow with The Atlantic Council in 2024 where he will focus on researching national security strategy.

Ms. Pulkit Mohan is an associate fellow with the Centre for Security, Strategy and Technology (CSST) at the Observer Research Foundation, New Delhi. Her research focuses on the intersection of cybersecurity and nuclear security and nuclear deterrence, with a focus on South Asia. She also works extensively on India's nuclear programme and the utilisation of nuclear energy. She also helps curate ORF's Kalpana Chawla Annual Space Policy Dialogue. Pulkit is an active member of WINS and regularly contributes to CRDF Global and Stimson Center's South Asian Voices. Prior to joining ORF, Pulkit was an editorial assistant with a leading development journal. She graduated from the London School of Economics with a Masters in International Relations.

Dr. Radha Kishan Motkuri is a senior principal scientist/chemical engineer with the PNNL Energy and Environment Directorate. He serves as a principal investigator (PI), co-PI, and project manager in a diverse range of material chemistry, chemical engineering, and chemical, cyber, and nuclear security projects. Dr. Motkuri has over 26 years of experience in material chemistry and security. More specifically, his work on

security aspects includes chemical and supply-chain security, cybersecurity, cyber nuclear and cyber chemical security, vulnerability assessment, security training, physically enabled nuclear security, and assessment of energy security. His material research has focused on advanced materials for potential applications, including sorption/capture, separation, catalysis, detection, and sensing. Dr. Motkuri was the recipient of a 2017 R&D 100 Award for his work on developing thermal vapor-compression technology that runs off any low-grade heat source, called MARCool, and a 2021 R&D 100 Bronze award for the AirJoule Self-Regenerating Dehumidifier—a heating, ventilation, and air conditioner. Dr. Motkuri published more than ~103 publications, 15 journal covers, and >4900 citations with an H-index of 35 (Google Scholar). Also, Dr. Motkuri has 14 USA patents/patent applications (17 international patents) and more than 125 national/international presentations. Dr. Motkuri organized or co-organized several sessions at the American Chemical Society (ACS) and international chemical and nuclear security workshops. Dr. Motkuri has been an editorial board member for the prestigious inorganic and material journals: "Inorganic Chemistry (American Chemical Society)" from 2019 to 2021 and is currently serving on "Inorganic Chimica Acta" (Elsevier) and editorial advisory board member to "Scientific Reports" (Nature Publishing Group), responsible for handling the articles on nanoporous materials and their applications.

Dr. N. Ramamoorthy is an expert in the field of production and utilisation of radioisotopes and associated products and in the field of radiation technology applications, radiation safety, and security of radioactive materials. He has over 40 years of professional and managerial experience in development of products and techniques, as well as in fostering the effective, safe, and secure deployment of their applications, at national and international level.

Dr. Ramamoorthy served at the IAEA during 2003 to 2011 as director of the Division of Physical and Chemical Sciences, International Atomic Energy Agency (IAEA), Vienna and was the programme manager for "Nuclear Science," and "Radioisotope Production and Radiation Technology." Prior to that, he held senior managerial positions in India during 2000 to 2003 as a chief executive of Board of Radiation and Isotope Technology (BRIT) and concurrently as an associate director, Isotope Group, BARC.

Dr. Ramamoorthy has several academic and professional accomplishments to his credit—recipient of many awards and recognition in India and at IAEA; delivered invited talks at national and international events and published extensively.

Dr. Ramamoorthy is currently serving in AERB's Apex Advisory Committees: a chairman of SARCAR (Safety Review Committee for Applications of Radiation) and a member of ACNRS (Advisory Committee on Nuclear and Radiation Safety). He is also engaged in advisory and consultancy roles for the IAEA, including as editor of "Knowledge Management and HRD Applied to Radiation Technologies," an IAEA and Rosatom Technical Academy publication (2021); and as a member of Advisory Group for IAEA's ICARST-2022 (International Conference on Applications of Radiation Science and Technology).

Mr. R. S. Sundar a mechanical engineer from Coimbatore Institute of Technology (CIT), Madras University, joined Bhabha Atomic Research Centre (BARC) in 1980 in the 24th Batch of Training School and was absorbed as a scientific officer "C." He rose in the ranks to "Distinguished Scientist" in the Department of Atomic Energy. At the time of his retirement in June 2018, he held the post of Executive Director (Operation), Light Water Reactors, Nuclear Power Corporation of India Limited.

Under his leadership, Kudankulam Nuclear Power Project (KKNPP), Units #1 &2, built with the Russian collaboration, an advanced 3rd Generation plus 1000Mwe, VVER type of Reactors have been successfully commissioned and put into operation, adding 48 Million units per day to the National grid. This has paved way for additional Reactors 4x1000 Mwe at Kudankulam Nuclear Power Project (KKNPP), Tamil Nadu. KKNPP Units No. 3 and 4 civil construction activities have commenced and Units 5&6 agreements have been signed.

Shri Sundar proactively led the team during Public hearing of KKNPP Units 3 to 6, obtained statutory clearances well in advance for Consent to Establish (CTE) for KKNPP 3 to 6, and obtained "In Principle" approval from Tamil Nadu Maritime Board for construction of maritime structures and excavation works started from February 2016. He had fruitful interactions with MoEF related to Units 3 to 6 and also related to KKNPP 1&2 after Supreme Court directives.

Shri Sundar has served as a governor, Moscow Centre, World Association of Nuclear Operators (WANO), and participated in various Governing Board Meetings in China, Hungary, Czech Republic, Canada.

As a result of his team efforts and highest leadership qualities, Kudankulam Nuclear Power Project was awarded as "Project of the Year 2014" by *Power Engineering*, a U.S. magazine.

Major Anne L. Willey is a United States Air Force Munitions and Missile Maintenance officer. She has served in a variety of leadership positions in conventional and nuclear weapons munitions maintenance, intermediate-level aircraft maintenance, and program management, primarily at the squadron, depot, and Department of Defense levels. Most recently, she served as a branch chief for the Nuclear Weapons Accountability office for the Defense Threat Reduction Agency (DTRA) at Fort Belvoir, Virginia. She is currently a student at the Naval Postgraduate School (NPS) on a Foreign Area Officer (FAO) fellowship with a focus in National Security Strategy and Eurasian studies.

List of Figures

List of Tables

CHAPTER 1

Introduction

S. Paul Kapur, Rajeswari Pillai Rajagopalan, and Diana Wueger

Nuclear safety and security—the protection of nuclear facilities, weapons, technologies, and materials against accidents or attacks—is an understudied area of international security studies.[1] Periodically, the subject has received high levels of attention. Following the fall of the Soviet Union, for example, scholars and policymakers worried intensely about the fate

S. P. Kapur (✉) · D. Wueger
Naval Postgraduate School, Monterey, CA, USA
e-mail: spkapur@nps.edu; dbwueger@nps.edu

R. P. Rajagopalan
Observer Research Foundation, New Delhi, India
e-mail: rpr@orfonline.org

[1] Nuclear security refers to "the prevention and detection of, and response to, criminal or intentional unauthorized acts involving nuclear material, other radioactive material, associated facilities or associated activities," while nuclear safety refers to "the achievement of proper operating conditions, prevention of accidents and mitigation of accident consequences, resulting in protection of workers, the public and the environment from undue radiation risks." International Atomic Energy Agency, "IAEA Safety Glossary: 2018 Edition," Vienna (2019), https://www.iaea.org/publications/11098/iaea-safety-glossary-2018-edition.

S. P. Kapur et al. (eds.), *The Challenges of Nuclear Security*, Initiatives in Strategic Studies: Issues and Policies,
https://doi.org/10.1007/978-3-031-56814-5_1

of its nuclear arsenal and infrastructure.[2] The problem again came to the fore following the September 11, 2001 attacks, which raised the specter of terrorists gaining access to nuclear weapons or materials.[3] Much of this post-9/11 focus was directed at South Asia, where the Pakistani nuclear program's potential vulnerabilities to militants and other religious extremists were a major concern for the United States and the international community.[4]

Despite these periods of interest, however, the problem of nuclear safety and security has generally received only modest scholarly attention. Most scholars and analysts of nuclear-related matters have focused their attention elsewhere, such as the ways in which nuclear weapons can generate deterrence and how they might contribute to coercive success in the event of conflict.[5] A significant cohort studies nuclear proliferation, including the reasons why states acquire nuclear weapons, ways to prevent them from doing so, and proliferation's effects on the behavior of newly

[2] Daniel Ellsberg, Jerry Sanders, and Richard Caplan, "Nuclear Security and the Soviet Collapse," *World Policy Journal* 9, no. 1 (Winter/1992, 1991): 135–156; Joseph E. Kelley, "Soviet Nuclear Weapons: U.S. Efforts to Help Former Soviet Republics Secure and Destroy Weapons: Statement of Joseph E. Kelley, Director-in-Charge, International Affairs Issues, National Security and International Affairs Division," Testimony before the Committee on Governmental Affairs, U.S. Senate (U.S. General Accounting Office, March 9, 1993), https://www.gao.gov/assets/t-nsiad-93-5.pdf; David R. Marples, ed., *Nuclear Energy and Security in the Former Soviet Union* (Boulder, Colo.: Westview Press, 1999).

[3] Graham Allison, *Nuclear Terrorism: The Ultimate Preventable Catastrophe* (New York: Times Books, 2004); Charles D. Ferguson and William C. Potter, *The Four Faces of Nuclear Terrorism* (New York: Routledge, 2005); Jonathan Medalia, "Terrorist 'Dirty Bombs': A Brief Primer," CRS Report for Congress (Congressional Research Service, October 29, 2003), https://irp.fas.org/crs/RS21528.pdf.

[4] Douglas Frantz, "U.S. and Pakistan Discuss Nuclear Security," *The New York Times*, October 1, 2001, https://www.nytimes.com/2001/10/01/world/us-and-pakistan-discuss-nuclear-security.html; Scott D. Sagan, "The Perils of Proliferation in South Asia," *Asian Survey* 41, no. 6 (2001): 1064–1086; William Burr, "Pakistan's Nuclear Program Posed 'Acute Dilemma' for U.S. Policy" (George Washington University, August 30, 2021), https://nsarchive.gwu.edu/briefing-book/nuclear-vault/2021-08-30/pakistans-nuclear-program-posed-acute-dilemma-us-policy.

[5] For comprehensive reviews of the literature, see Paul K. Huth, "Deterrence and International Conflict: Empirical Findings and Theoretical Debates," *Annual Review of Political Science* 2, no. 1 (June 1999): 25–48; Erik Gartzke and Matthew Kroenig, "Nukes with Numbers: Empirical Research on the Consequences of Nuclear Weapons for International Conflict," *Annual Review of Political Science* 19, no. 1 (May 11, 2016): 397–412.

nuclear states.[6] Others study the normative aspects of nuclear weapons, debating whether their use can ever be justified, as well as the role of moral concerns in preventing their use in the past.[7]

To be sure, these are important areas of inquiry, helping us to assess the effects of nuclear weapons on the likelihood of war and peace, to limit their spread, and to grapple with the difficult moral questions that their possession and potential use inevitably raise. However, a nuclear-related disaster is more likely to result from a peacetime mishap or a terrorist operation at a power plant than from a nuclear war. Improving our understanding of ongoing, day-to-day means of protecting the entire nuclear enterprise, ranging from civilian power plants to military applications—in other words, the study of nuclear safety and security—is therefore essential.

Joint studies, in which experts work with colleagues from partner states to address key challenges in protecting the nuclear enterprise, can be a fruitful means of enhancing our knowledge in this area. Such projects create valuable learning opportunities, enabling partners to share experiences, identify best practices, and develop new ideas for jointly tackling common problems. They also build trust, as experts from the two countries share ideas and information in their efforts to address some of their most sensitive security concerns.

The United States and India are particularly promising candidates for these types of projects. Both countries are longstanding nuclear states

[6] Bradley A. Thayer, "The Causes of Nuclear Proliferation and the Utility of the Nuclear Non-proliferation Regime," *Security Studies* 4, no. 3 (March 1995): 463–519; Scott D. Sagan, "Why Do States Build Nuclear Weapons? Three Models in Search of a Bomb," *International Security* 21, no. 3 (1996): 54–86; Scott Douglas Sagan and Kenneth Neal Waltz, *The Spread of Nuclear Weapons: An Enduring Debate* (W.W. Norton & Company, 2013); Nuno P. Monteiro and Alexandre Debs, "The Strategic Logic of Nuclear Proliferation," *International Security* 39, no. 2 (October 2014): 7–51; Nicholas L. Miller, "The Secret Success of Nonproliferation Sanctions," *International Organization* 68, no. 4 (2014): 913–944; S. Paul Kapur, *Dangerous Deterrent: Nuclear Weapons Proliferation and Conflict in South Asia* (Stanford: Stanford University Press, 2007); and Vipin Narang, *Seeking the Bomb: Strategies of Nuclear Proliferation* (Princeton, NJ: Princeton University Press, 2022).

[7] Kishore Kuchibhotla and Matthew McKinzie, "Nuclear Terrorism and Nuclear Accidents in South Asia," in *Reducing Nuclear Dangers in South Asia*, ed. Michael Krepon and Ziad Haider, Report No. 50 (Washington, DC: Stimson Center, 2004), http://stimson.org/wp-content/files/file-attachments/Reducing%20Nuclear%20Dangers%20in%20South%20Asia%20-%20Krepon%20Haider%20-%202004.pdf; Scott D. Sagan, "The Perils of Proliferation in South Asia," *Asian Survey* 41, no. 6 (2001): 1064–1086.

with significant nuclear infrastructure. Both have suffered attacks on parts of their nuclear enterprise, revealing weaknesses that required further attention. And both countries are deeply concerned about threats to the safety and security of their nuclear enterprises, and determined to take concrete steps to mitigate them.

This is an opportune moment for such a joint U.S.-India project. A series of nuclear-security summits during the Obama Administration raised awareness of the issue, and led states to take steps to promote nuclear safety and security, including the issuance of joint communiques, repatriation of nuclear material, improved training of personnel, and efforts to combat the trafficking of nuclear and radiological materials.[8] Recent incidents like the Colonial Pipeline and Solar Winds attacks, though not nuclear-related, have highlighted the importance of threats to critical national infrastructure, as well as the centrality of supply-chain security.[9] At the same time, India and the United States' burgeoning bilateral strategic relationship has significantly increased the two countries' level of mutual trust, enabling them to work together in areas that would have been prohibitively sensitive just a few years ago.

This volume capitalizes on these opportunities by bringing together experts from the U.S. and India to address six nuclear safety and security issues that are of central and enduring interest to both countries. The project grew out of an annual dialogue on U.S.-India strategic relations, organized by the U.S. Naval Postgraduate School and the Observer Research Foundation and sponsored by the Defense Threat Reduction Agency (DTRA). The dialogue addresses a range of strategic issues critical to the U.S.-India partnership. Over time, across several meetings, nuclear safety and security emerged as a recurring topic. The quality of the exchanges between Indian and U.S. participants on this extremely sensitive topic convinced the dialogue organizers and their sponsors to take the project one step further. They subsequently commissioned a series of

[8] Sara Z. Kutchesfahani, Kelsey Davenport, and Erin Connolly, "The Nuclear Security Summits: An Overview of State Actions to Curb Nuclear Terrorism 2010–2016" (The Arms Control Association and the Fissile Materials Working Group, July 2018), https://armscontrolcenter.org/wp-content/uploads/2018/07/NSS_Report2018_final.pdf.

[9] Lily Hay Newman, "A Year After the SolarWinds Hack, Supply Chain Threats Still Loom," *Wired*, December 8, 2021, https://www.wired.com/story/solarwinds-hack-supply-chain-threats-improvements/; David E. Sanger and Nicole Perlroth, "Pipeline Attack Yields Urgent Lessons About U.S. Cybersecurity," *The New York Times*, June 8, 2021, https://www.nytimes.com/2021/05/14/us/politics/pipeline-hack.html.

papers from U.S. and Indian experts, many of whom had participated in the earlier dialogues, on a core set of nuclear security and safety-related challenges. Those papers became the chapters of this book.

The chapters address six substantive issues of relevance to all nuclear states: insider threats and personnel reliability; organizational culture within the nuclear enterprise; emergency response and crisis communications; physical protection of nuclear material; control of radioactive sources; and cyber security and nuclear infrastructure. Each chapter consists of two papers, one from an Indian perspective and one by a U.S. perspective. The contributors are established experts with deep experience in their fields, and include a mix of retired and active civil servants, military officers, and academics.

Few single-volume publications cover the breadth of topics that this project addresses, and none of them bring together Indian and U.S. authors to engage these issues from their national socio-political perspectives. Government agencies, including the U.S. Department of Energy and the U.S. Congressional Research Service, and international organizations, such as the International Atomic Energy Agency, have published technical white papers on specific aspects of nuclear security, such as ensuring the physical security of reactors or designing personnel reliability programs.[10] These studies tend to be narrowly focused, however, ignoring other important safety and security problems, as well as the socio-political context in which states' decision-making occurs. Governmental and non-governmental organizations have issued reports on specific crises, such as the Fukushima disaster, and analyses of particular states' safety and security regimes.[11] These reports lack a broader scholarly perspective, however, as well as inputs from national experts who could better explain their state's policy choices. Within the academic discipline of international relations, scholars have developed concepts like strategic culture to understand the differences between states' approaches to nuclear weapons.[12] As noted earlier, however, this research has focused

[10] See, for example, International Atomic Energy Agency, "Physical Protection of Nuclear Materials and Nuclear Facilities," IAEA Nuclear Security Series No. 27-G, 2018.

[11] See, for example, National Diet of Japan, "Official Report of the Fukushima Nuclear Accident Independent Investigation Commission," 2012.

[12] Jack Snyder, "The Soviet Strategic Culture: Implications for Limited Nuclear Operations" (Santa Monica, CA: RAND, September 1977), https://www.rand.org/content/dam/rand/pubs/reports/2005/R2154.pdf; Rajesh M. Basrur, "Nuclear Weapons and

primarily on deterrence, proliferation, and normative issues, with much less attention paid to the day-to-day challenges and tradeoffs of nuclear safety and security, or to the ways in which domestic politics conditions states' approaches to protecting nuclear technologies, materials, facilities, and weapons.

This project, by contrast, addresses nuclear safety and security as a unique problem, nested within national socio-political structures. In doing so, it helps to identify specific ways to protect the nuclear enterprise, while enhancing our broader understanding of variation in states' approaches to the challenges of nuclear safety and security. From a policy perspective, the volume highlights opportunities for India and the United States to learn from and cooperate with each other as they seek to mitigate the threats and risks posed by expanding nuclear infrastructure. For academics and students, it offers a useful primer on the ways states approach the myriad challenges associated with ensuring nuclear safety and security and the critical tradeoffs they must make.

Below, we outline each of the papers' main arguments. We then identify some broad themes that emerge from the papers, highlighting similarities between the challenges that the United States and India face, as well as similarities in the two countries' efforts to address them. Finally, we identify areas for collaboration between U.S. and Indian experts on nuclear safety and security at both the scholarly and the policy levels.

1.1 Mitigating Insider Threats

This chapter focuses on the human side of physical security, discussing the problem of insider threats and examining ways to protect against them, including personnel reliability programs, access controls, and defensive forces. What are the challenges and impediments in detecting and assessing insider threats? How can states ensure the reliability of the personnel who manage or use nuclear or radiological materials? What role does technology play in helping to ensure the reliability of personnel within the nuclear enterprise?

On the Indian side, Rajeswari Pillai Rajagopalan argues that insider threats are the most serious dangers to critical infrastructure, including

Indian Strategic Culture," *Journal of Peace Research* 38, no. 2 (2001): 181–198; Jeannie L Johnson, Kerry M Kartchner, and Jeffrey A Larsen, *Strategic Culture and Weapons of Mass Destruction* (Basingstoke: Palgrave Macmillan, 2009).

nuclear facilities. This is the case for several reasons. First, insiders are likely to know a facility's strengths and weaknesses and have a sense of what vulnerabilities can be exploited. Some may even have privileged access to multiple elements of the facility's security systems. Second, insiders may escape their colleagues' suspicion because they are known and trusted employees. Finally, insiders are able to plan their operations over a prolonged period, with opportunities to choose targets, times, and materials based on ongoing observations. Insiders' access levels and ability to avoid detection will vary based on their occupation and seniority. But any individual with legitimate reason to access the facility is more of a potential threat than a complete outsider.

Rajagopalan argues that cultures of complacency are a key problem that must be overcome if the risks of insider threats are to be mitigated. Among senior leaders in an organization, a culture of complacency can drive an inability or refusal to recognize the possible presence of insider threats. Rajagopalan identifies cognitive dissonance, perception bias, and overconfidence as serious challenges; if senior leaders believe their safety mechanisms are foolproof, they are likely to overlook or misinterpret any warning signs. Historically, she says, Indian officials were inclined to believe insider threat was primarily a problem for security guards, though this has evolved in last 10–15 years.

Insiders can threaten the facility itself, but they also pose a broader danger if they exfiltrate information or material that would facilitate nuclear or radiological attacks elsewhere. Insider threats to India can manifest themselves in many ways: passing information to adversaries about the transportation of nuclear materials, such as the agencies involved and the routes used; theft of small quantities of nuclear materials for sale in black markets; or the use of cyber technologies that could damage or destroy not only the installation's data but even the facility itself. Senior leaders must consider ways to layer defenses and to compartmentalize access in a way that allows for a greater likelihood of early detection of a potential insider attack.

Identifying and mitigating inside threats, Rajagopalan notes, requires an ever-evolving suite of tools and approaches. The factor that allows insiders to pose a threat—authorized, ongoing access to the facility—can also limit the effectiveness of simple material or kinetic security measures, such as gates and guards. Leaders must therefore develop alternative approaches. In this vein, stringent personnel reliability programs have been a primary area of effort for India, with positive results. Rajagopalan

identifies two potential areas of improvement for these programs: more thorough vetting of temporary migrant laborers and persistent monitoring of employees' online activities to detect radicalization.

In the U.S. paper, Todd Burbach and Patrick Lynch begin by noting that diverse United States agencies, as well as international nuclear bureaucracies, define "insiders" somewhat differently, given their divergent missions and foci of concern. Nonetheless all of these organizations agree that an insider is an individual with authorized access to sensitive materials, facilities, or information, who can use this position of trust to commit harmful acts. Echoing Rajagopalan, they note that while necessary to the operation of the nuclear enterprise, trusted status, and the access it affords, can pose significant threats to nuclear safety and security.

Burbach and Lynch point out that insiders' motivations to commit harmful acts can vary widely, ranging from ideology to greed, to ambition, to ego, to blackmail. Despite these multiple possibilities, insider attacks against the nuclear enterprise have not happened often; the historical record of such events is thin. Nonetheless, the insider danger is still serious, because one trusted malign actor with access to sensitive systems, facilities, or information could inflict enormous damage. Therefore, rigorous programs to mitigate insider risk are essential.

Burbach and Lynch explain that trustworthiness programs designed to determine employee reliability are an important means of risk mitigation. Such programs can identify personnel with disqualifying characteristics; help to select personnel with desirable traits; and imbue a workforce with pride in their positions and confidence in their colleagues. Program components include measures such as arrest checks, drug tests, and work verifications. As Burbach and Lynch point out, the process of ensuring trustworthiness is ongoing; personnel are reviewed periodically, and any concerning findings can be flagged and trigger a deeper investigative process.

In addition, trustworthiness programs must be combined with other tools, including technical measures such as large-volume data review and profiling, in the effort to mitigate insider threats. And such combinations of techniques, even if successful, cannot remain static. Managers must stay abreast of new capabilities and approaches, and evaluate existing policies periodically, even if these policies appear to be successful.

Finally, Burbach and Lynch argue that successful mitigation of insider threats depends on the cooperation of the workforce. One of its most important aspects of such cooperation is self-reporting. This enables the

enterprise to catch problems that it otherwise would miss and address them before it is too late. Often, this can save an employee's career. To encourage self-reporting, managers must maintain an environment where employees are comfortable admitting their problems and mistakes. Overly punitive policies will discourage such honesty, and ultimately be counterproductive.

1.2 The Role of Organizational Culture in Nuclear Security

Organizations within the nuclear enterprise must develop strong cultures of safety and security, where individuals feel empowered and responsible to do what is necessary to prevent emergencies or accidents. This chapter discusses what constitutes a strong culture of security and how cultural changes in organizations can best be implemented. How can the organizations charged with ensuring nuclear safety and security stave off complacency and stagnation? What can we learn about the role of culture, and how cultures can be changed, from the experiences and approaches of the agencies that comprise the nuclear enterprise in India and the United States?

From an Indian perspective, N.K. Joshi argues that organizational culture develops through organizational practices learned on the job and consists of observable and unobservable values, beliefs, attitudes, and behaviors. Joshi posits that a shared sense of vulnerability among all members of the organization is critical to establishing a strong nuclear security culture. Employees must be motivated to follow established procedures, comply with regulations, and take the initiative when they detect a potential breach or threat. Building a strong culture of nuclear security is a key responsibility of an organization's leaders, who must promote the beliefs and ideas necessary to create and maintain this culture.

Fostering an environment in which all personnel feel like part of a team is also critical to maintaining and expanding a culture of nuclear security. Scientists and engineers should support and contribute to security objectives rather than feeling like they are simply the passive victims of security rules and regulations. Similarly, security professionals should be treated as full partners with their peers in the nuclear safety community, not as subordinates or outsiders. Joshi suggests this may help mitigate the difficulties associated with national cultures and social norms that emphasize

obedience to authority, which can lead to a reluctance to raise alarms proactively.

Joshi also highlights how a culture of security, which relies on compliance and discretion, can be at odds with a culture of scientific enquiry, which prioritizes openness and change and requires sharing of knowledge and lessons learned. While compartmentalization and maintaining a need-to-know policy can be beneficial, Joshi argues, a need-to-share approach can build trust and goodwill, and sharing information can help avert crises. While there is a natural tendency toward secrecy about nuclear matters, too much secrecy, in the form of denying problems or failing to share lessons learned, can undermine nuclear security culture if the organization's members come to believe the risks are minimal or fully resolved. Security systems must be adaptable if they are to remain effective in the face of evolving threats, which requires leaders to prioritize continual learning and recursive feedback from all stakeholders.

On the U.S. side, Cristina F. Lussier and Karen Kaldenbach argue that the attitudes, values, and behaviors that together comprise culture are critical to the operational success of the nuclear enterprise, and to building trust between the enterprise and the public. Both operational success and trust are critical.

As a result, U.S. authorities take seriously the development of culture within the nuclear enterprise. For example, to help create a culture of openness and transparency, authorities have taken steps like declassifying the Nuclear Posture Review. They believe that an environment that promotes the free exchange of ideas in this manner can facilitate the solution of the complex, dynamic problems that the nuclear enterprise regularly faces. Similarly, the Nuclear Regulatory Commission tries to create a culture that promotes safety, preventing apathy and promoting agility in the workforce. To this end, it has promulgated a nine-part Safety Culture Policy Statement emphasizing the personal and organizational traits essential to the safe and secure operation of nuclear facilities.

These types of statements offer broad guidance, which departments and organizations use to impel cultural shifts that strengthen their establishments. They do this in a variety of ways. For example, the Department of Energy has created a Safety Culture Improvement Panel, to help outline DOE safety attributes and practices. And the Department of Defense Nuclear Weapon System Surety Policy has stressed the need to provide surety throughout the life cycle of a nuclear weapon.

Despite this diversity, the authors identify some common themes across organizations with healthy security cultures. They include the importance of surface indicators, such as proper execution of security protocols upon facility entry; personnel properly wearing credentials; and polite but alert security personnel; standardized expectations regarding the execution of plans and procedures, with leadership held responsible both for their own performance and that of their teams; hiring personnel with right qualifications for specific tasks; collective emphasis on the need for leadership to model good values and behavior; prompt problem identification, evaluation, and resolution; personal accountability; well-defined work processes; continuous learning across the organization; an environment conducive to questioning attitudes and open to raising concerns; effective safety communications; and a respectful work environment. Finally, healthy organizations recognize that creating a safety culture is not the responsibility just of security personnel; it is a top-to-bottom responsibility of all employees, with management communicating clearly and the workforce providing operational feedback from the ground up. Such measures and qualities cannot create a positive safety culture overnight. But with time, they can play a crucial role in creating an environment that promotes safety and security within an organization.

The authors show, through a detailed discussion of the Y-12 incident, that failure to cultivate a healthy safety and security culture in nuclear organizations can be catastrophic. In 2012, intruders were able to breach the Y-12 nuclear facility, defacing the building and remaining on the site for several hours. Subsequent investigation revealed a litany of failures, including poor maintenance, faulty communication, poor discipline, and weak adherence to security protocols. The investigation linked these failures directly to cultural shortcomings, with facility personnel focusing on a culture of compliance rather than one of performance.

The authors argue that the Y-12 incident should be a wakeup call for the United States nuclear enterprise. It demonstrates that attention to cultural health within nuclear organizations is crucial. This is the case not just because of the dangers inherent in nuclear operations, but also because of the challenge of rising Chinese and Russian nuclear capabilities. In today's strategic environment, the U.S. must be able to rely unquestioningly on its nuclear deterrent capabilities.

1.3 Emergency Response and Crisis Communications

As nuclear infrastructure grows, the risks of radiological or nuclear emergencies will increase as well. It is critical to be prepared to respond to potential crises in a timely and coordinated fashion. This chapter addresses best practices in emergency response and crisis communication, with an emphasis on holistically considering the need for procedures and policies, communications systems, networks of trained personnel, and emergency exercise execution and appraisal programs. How can organizations learn to work together effectively before crises? How does the nuclear enterprise approach the challenge of managing public opinion and preventing panic during a crisis?

On the Indian side, R.S. Sundar emphasizes the importance of building trust and familiarity among the local population to improve the acceptability of nuclear power plants. Establishing a positive, trusting relationship with the public begins even before the plant is constructed, and must remain a high priority during normal plant operations as well as during crises. Nuclear power projects must use print and electronic media and find ways to explain the project and answer questions in non-technical language. Sundar provides a detailed overview of how the Kudankulam Power Plant (KPP) approached the challenge of public relations. By using media appearances, reaching out to and through academics, and printing leaflets that answered common questions in an approachable way, KPP was able to assuage many of the fears and objections that had been raised by the local population in the wake of the Fukushima disaster.

Sundar then turns to emergency response and how nuclear site operators can approach communications during crises. Plants are required to have emergency preparedness plans and procedures in place before they achieve criticality. Part of the planning process involves exercises, of which there are three types: plant emergency exercises, which focus on the plant's response within the facility; site emergency exercises, which involve all facilities within a 16 km radius; and off-site emergency exercises, which involve district authorities as well as plant personnel to test and clarify crisis roles and responsibilities beyond the plant's boundaries. Because the characteristics of the radioactive material that could potentially be released from a nuclear power plant are known, response actions for mitigation of consequence can be planned in advance, though this does not obviate the need for exercises to practice the response.

The early phase of an emergency is the most important to get right. It is also, Sundar notes, the most challenging: there are high levels of uncertainty, particularly regarding plant conditions and field measurements, and sudden changes in assessments are frequent. There is often a lack of sufficient external technical support. As a result, decision-makers can under-react or overreact to the evolving situation.

Improving decision-making in the early phase of an emergency therefore requires nuclear power plants to establish criteria to classify emergencies in a timely manner. Classification requires a strong baseline understanding of plant conditions to determine when deviation from the norm is truly an emergency. By developing Emergency Action Levels in this way, plants are better prepared to take appropriate and necessary protective actions to reduce radiological consequences. These protective actions needed will depend on the amount, time, composition, and frequency of release.

Finally, Sundar notes that India has moved away from an exercise methodology that was based on known, rehearsed accident scenarios and coordinated field responses, toward more unpredictable scenarios and responses that emphasize early-phase decision-making. This methodology provides more realistic challenges to nuclear plant operators, district authorities, and federal agencies with responsibility for oversight and emergency response. It also provides an opportunity for iterative learning, as post-exercise reports can be analyzed for ways to improve.

On the U.S. side, Daniela Helfet Cooper, Michael Hornish, and Alisa Laufer show that although nuclear emergencies are especially dangerous events, many of the techniques that the United States employs to respond to them come from other, more ordinary types of crises. For example, a mainstay of nuclear crisis response is a tiered response structure that stretches across local and federal entities. This structure is not unique to the nuclear domain; it comes from the National Response Framework (NRF), which was developed in response to a series of storms, including Hurricane Katrina, which hit the southern United States in 2005. The NRF now governs U.S. responses to domestic emergencies that require federal support to augment state or local efforts. It specifies roles, terminology, and incident-management principles that enable multi-level coordination. The framework operates according to the principle that all responses should be handled first at the lowest possible

jurisdictional level, receiving higher-level support only as needed. A dedicated annex specifies how these principles and practices would apply to nuclear or radiological incidents.

The authors explain that a central challenge with crisis response is that, within organizations, it is often unclear who is authorized to make decisions regarding the authority to request and approve assistance. The problem is exacerbated as emergencies become more complex. This challenge was evident during the 1995 Aum Shinrikyo attacks in Tokyo, when paramedics had difficulty securing the necessary clearance from higher medical authorities to treat victims. One means of mitigating this problem, the authors note, is to delegate authority to request and approve assistance to the lowest possible level within an organization, and to identify the personnel with that authority in advance. Another solution is to identify circumstances under which restrictions will be waived and authorities delegated. The efficacy of this approach was seen in the U.S. response to the COVID-19 crisis, when some states provided waivers allowing out-of-state healthcare personnel to practice in them.

The authors explain that one of the most effective ways of ensuring a good emergency response is to prepare thoroughly for it. This involves devising a response plan and conducting exercises to practice its implementation. Realistic exercises enable responders to ensure that they can perform their missions in the event of a real crisis, without referring to written plans and procedures. They also can expose weaknesses in existing plans, pointing up areas requiring additional training and resources. And they help personnel to network across agencies and jurisdictions. The familiarity and trust that this networking builds can be invaluable in responding to a crisis.

In addition to responding directly to emergencies, government agencies must communicate with the public to explain the situation, combat misinformation, and prevent dangerous public reactions. Quickly providing clear, accurate information can help to ensure public safety. Some ways they can do this include pre-scripted communications plans and emergency guidance adaptable to the specifics of a crisis. It is important for government stakeholders to build consensus around them ahead of time. This will help to ensure timely and orderly dissemination of information.

One of the most difficult aspects of crisis communication is striking a balance between the accuracy of information and the speed of its dissemination. Appointing a lead authority for public messaging, whom the

public trusts, can help to ensure consistent communications across diverse government agencies. Also, government must be honest with the public, avoiding speculation, admitting when its understanding of a situation is incomplete, acknowledging that information can change, and explaining why any departures from earlier guidance have occurred.

The authors illustrate their arguments with discussions of two major nuclear disasters—Three Mile Island in 1979, and Fukushima Daiichi in 2011. These cases demonstrate the difficulty of coordinating multi-sectoral responses to fast-moving emergencies. They also show how a number of the principles that the authors identify emerged as best practices, to facilitate more effective crisis response.

The authors close by identifying opportunities for United States-India cooperation in the area of nuclear crisis response. These include expert exchanges, bilateral dialogues, and tabletop exercises. Such measures would enhance expertise on both sides, and build relationships necessary to advance collaboration in the future.

1.4 Physical Protection of Nuclear Facilities and Materials

Nuclear facilities and materials must be protected from a range of external threats, including attack, theft, and diversion. This chapter asks how the United States and India seek to do so, and how their approaches have evolved over time. In addition, the chapter seeks to identify new technologies or practices that can mitigate external threats in the future.

Anil Kumar offers an Indian perspective on this problem. He notes that physical protection regimes have four primary purposes: to guard against unauthorized removal, including theft and other unlawful taking of nuclear material; to locate and recover missing nuclear material rapidly and comprehensively; to protect nuclear material and facilities against sabotage; and to mitigate or minimize the radiological consequences of sabotage or accidents. The effectiveness of a physical protection system (PPS) for a nuclear facility depends on a combination of three factors: technology, procedures, and security personnel. Every physical protection system should be evaluated against a defined maximum threat level for which the facility owner will secure its facility and materials.

Kumar argues that for a PPS to serve its main functions—deterring, detecting, delaying, and defeating adversaries, as well as mitigating radiological consequences—it should employ defense in depth, with multiple

layers of increasingly robust protection. Detection should be as far as possible away from the targets, while delay mechanisms should be placed near the target. The levels of protection should follow a graded approach, increasing or decreasing with the potential threats and how attractive various materials and systems may be to adversaries. Kumar provides a model for the physical protection of nuclear facilities that details the multiple layers of security precautions. He argues that effective physical protection requires compartmentalization of physical spaces, with individuals granted access only to areas and information they need to perform their jobs. Nevertheless, security systems must not be allowed to inhibit the smooth functioning of the facility.

Security personnel must remain vigilant to changes in the threat environment. To avoid complacency, personnel should be kept alert through exercises, briefings on incidents elsewhere, and rotation between posts and responsibilities. As noted, emergency preparedness is a critical planning concern for physical security systems. As the personnel closest to the scene of an incident, security teams will be required to assist with triage and maintaining access control in a complex and fast-paced environment. This requires regular exercises of varying scopes.

Finally, Kumar addresses the specific challenges associated with transportation of nuclear and radiological material. Protection of materials in transit requires careful planning, with consideration given to such diverse issues as the packaging used to contain the materials; the legal and regulatory requirements of areas being transited; and how materials will be stored and guarded if there is an overnight halt. Kumar notes that in addition to the IAEA's categorizations, India's Atomic Energy Regulatory Board has developed its own system to identify the proper level of security needed. Because radiological materials differ in their hazard potential, degree of radioactivity, and attractiveness to adversaries, the AERB has identified three levels of increasingly stringent security arrangements. Kumar points out that transporting nuclear materials adds another layer of complexity. Materials may need to transit through areas with which the security contingent is not very familiar. The occasional need for temporary storage, the transition of guard forces, and the interaction with territorial authorities at jurisdictional borders further compounds the security risks.

In the U.S. paper, James McCue and Alan Evans offer a systems engineering approach to Physical Protection System (PPS) design. They discuss a methodology called Design Evaluation Process Outline

(DEPO), which has been widely used to design and evaluate both civil and military physical protection systems. Though they cannot directly discuss military applications, DEPO enables McCue and Evans to convey to the reader how physical protection challenges might be approached on the military side.

The authors describe in detail the dynamic process through which a physical protection system is constructed. Steps in this process include defining requirements based on the nature of the facility to be protected, regulatory standards, available resources, threats, and budgets; and designing physical protection elements based on a series of principles including detection, delay, and response. In addition, systems are evaluated through exercises, analysis, evaluations, and threat updates.

If a planned system fails this evaluation, it is redesigned, and the process starts again. If it passes, the system is built. But even in this scenario, the evaluation and design process does not stop; the system is continually evaluated against rigorous performance standards. This can lead to minor changes, or to the system's wholesale redesign, which starts the entire process over again.

The authors illustrate their points with applications of the DEPO method to physical security systems in U.S. ICBM launch facilities, and in nuclear warhead transportation. In addition to explaining how each step of the existing DEPO methodology applies to these examples, the authors make a number of suggestions for changes to the DEPO process. These include the addition of new analytic elements such as budgetary restraints, security system reputation, and threat capabilities defined in conjunction with the enemy's goals. The authors also recommend a move from compliance-based to more forward-looking, performance-based evaluation, which will help security managers to leverage the high quality of today's personnel, and stay abreast of emerging technologies. Changes such as these, they argue, can ensure the continued dynamism of the DEPO process, and help to make it even more effective in the future.

1.5 Controlling and Managing Radioactive Sources

Uncontrolled or orphaned radioactive sources pose serious dangers, yet effective regulation of the disparate types and users of radioactive material is a daunting task. How can states ensure that radioactive sources are appropriately regulated and adequately secured at all times? How have the

United States and India addressed the challenge of locating, recovering, securing, and recycling orphan sources?

On the Indian side, N. Ramamoorthy provides a panoramic view of the uses and importance of radioactive materials for a wide variety of industrial and medical purposes. He argues that different applications of radioisotopes come with different vulnerabilities, and it is therefore not possible to create a one-size-fits-all approach to security. Ramamoorthy provides an overview of the properties of radioisotopes that make them so useful for applications ranging from cancer treatments, to sterilization of medical products, to disinfestation of food products, to manufacturing of advanced materials, to mitigation of certain pollutants. Some of these uses inherently carry security risks, however; Ramamoorthy raises the example of industrial radiography, which requires transportation of devices with radioactive sources at short notice by companies operating in a fiercely competitive economic space. Effectively controlling and managing the use of radioactive sources requires ongoing attention to the multifarious threats and risks these sources may pose, from accidental loss of sources to intentional usage in an improvised radiological device.

Ramamoorthy notes that the production of radioisotope-based sources and equipment containing radioisotopes (RI) has been confined to a limited number of countries at national centers and in private industry. Their deployment, however, has been extensive, both geographically and across a wide variety of facilities, including at hospitals, industrial sites, academic centers, and research labs. Movements of packages containing these types of sources are routine throughout the year, with some occurring more frequently based on the half-life of RI involved and the need for source replacement or replenishment. The volume of sources and their regular movement can create opportunities for diversion or loss. To mitigate that likelihood, India has developed a web-based system, e-licensing of radiation applications (e-LORA), to facilitate registration, applications, approvals, accountability, and tracking by the Atomic Energy Regulatory Board. Ramamoorthy also highlights the problem of legacy and orphaned sources, which have resulted in high-profile accidents in several countries. In the 2010 Mayapuri incident, for example, eight people were injured and one died after a research irradiator owned by Delhi University was sold to and dismantled by a scrap-metal dealer who was unaware of the hazard.

Because there will always be some risks associated with the use of radioactive sources, Ramamoorthy argues, discouraging the use of

these sources where alternatives are available will be the logical first option. Technological, economic, and logistical issues create barriers to this approach, however, and its feasibility varies across issue areas. For applications where a non-radiological alternative does not exist, improving source security is likely to require better accountability and more proliferation-proof designs. Where alternatives do exist, government will need to partner with industry to make the use of these alternatives more attractive and achievable.

U.S. authors Christopher Boyd and Anne Wiley explain that sealed sources, radioactive materials intended to remain enclosed in a capsule or bonded in solid form, are widely used in life-saving medical treatments and infrastructure applications. But, in the wrong hands, they can be deployed as weapons, providing the radiological material needed to make "dirty bombs." This problem is particularly concerning because sealed sources are commonly used in relatively lax security environments, such as healthcare organizations and academic institutions. Sealed sources therefore require careful attention and management.

In the United States, dealing with the problem of sealed sources is difficult in part because of the complexity of the regulatory landscape, which features overlapping federal and state jurisdictions, and involves multiple entities. These entities include the Nuclear Regulatory Commission (NRC) and Agreement States, to which the NRC has relinquished portions of its regulatory authority. The Organization of Agreement States (OAS), in turn, facilitates interaction between Agreement States and the NRC, seeking to minimize conflicts between individual states and the NRC and create a role for states in national-security matters.

Beyond this jurisdictional complexity, a number of additional factors make federal-state regulatory cooperation particularly difficult. For example, state regulations must be compatible with, rather than identical to, federal standards. Nonetheless, in practice, the NRC may require a level of conformity that requires essentially identical rules. This can impede states' efforts to implement regulations that exceed federal standards, but are necessary because of their particularly high-risk profiles.

Performance-based approaches to determining state compliance with federal regulations give rise to additional challenges. For example, such approaches allow licensees flexibility in meeting regulatory intent. But their lack of specifics can create uncertainty about standards, and subjectivity in determining compliance.

Finally, both federal and state regulatory efforts focus on risk mitigation, rather than risk elimination. This approach suffers from a number of shortcomings. For instance, risk mitigation is costly, requiring large investments of human, economic, and political resources. And it relies on human factors such as norms and culture that can be difficult to influence.

Boyd and Wiley offer several solutions to these problems. They argue that while overregulation is bad, states must be able to exceed minimal regulatory standards. This may create some complexity, but also ensures that they are meeting the reality of their threat environment. The authors also maintain that while performance-based regulatory approaches promote flexibility, prescriptive approaches can be useful, reducing uncertainty and creating clear standards for compliance.

Finally, the authors offer a detailed argument in favor of risk elimination, arguing that, where viable options exist, governments should encourage the adoption of alternative technologies that do away with the risk of sealed sources entirely. As the U.S. experience replacing cesium blood irradiators demonstrates, such measures can be implemented even without a legislative mandate, through the voluntary replacement of dangerous technology. The authors argue that the U.S. experience can serve as a model for governments that wish to eliminate risky technologies in the absence of legal requirements to do so.

1.6 Cybersecurity and Nuclear Infrastructure

This chapter explores cyber threats to nuclear infrastructure, which have become more widespread and increasingly sophisticated with the digitization of the nuclear enterprise, even as states have sought to identify new ways to defend against them. What are the primary risks posed by cyber activities against nuclear facilities? How have the United States and India sought to prevent and prepare to recover from malicious cyber activities? What policy options exist to reduce the risk of a catastrophic cyberattack?

Pulkit Mohan describes the Indian context. She argues that serious Indian attention to cybersecurity is fairly recent, beginning roughly in 2013. Ironically, Indian concern was triggered by perceived dangers from the United States, as the Edward Snowden leaks revealed alleged U.S. spying on India. As Mohan explains, this led the Indian government to promulgate a National Cyber Security Policy, designed to create an ecosystem to defend against cyber threats and ensure the integrity of

information and information structures. She then describes the structure and functions of government agencies charged with building and maintaining cybersecurity mechanisms within the country's nuclear infrastructure. The importance of these agencies' efforts has grown, Mohan points out, as India's nuclear enterprise has that has become increasingly digitized.

Mohan then discusses the 2019 cyber breach at the Kudankulam Power Plant. She explains the nature of the attack, using malware known as Dtrack, which had previously been used to attack financial institutions, and the Indian government's response, which included a robust official investigation, and the implementation of measures such as hardening intranet and internet connectivity, restricting the use of removable media, and blocking malicious websites and IP addresses. Mohan argues that this incident could have been much worse, as it was limited to the plant's administrative network and did not affect its control systems. Still, it made clear the urgent need for improved security practices and structures in India's nuclear enterprise.

Although India significantly increased its attention to cybersecurity in a relatively short period of time, Mohan argues that more needs to be done, as Indian entities are frequently the target of cyberattack, and the country's nuclear infrastructure is increasingly digitized. At home, this will require increased attention to issues including the creation of a security culture, mitigating supply-chain vulnerability, increasing standards of personnel reliability, and enhancing industry-government cooperation. Internationally, India can benefit from strengthening agreements with likeminded countries, particularly in the areas of 5G technology, critical infrastructure, and supply-chain diversification.

In the U.S. article, the team of authors led by Clifford Glantz agrees with Pulkit Mohan that cybersecurity is becoming an increasingly important facet of nuclear safety and security, in large part because the nuclear enterprise relies more heavily on digital technology. In addition, they point out that an inconsistent regulatory environment, and the United States' and other countries' late recognition of the seriousness of the cyber threat, exacerbates cyber-related dangers. Not surprisingly, numerous attacks and breaches have occurred around the world, including in the U.S., Korea, Iran, and India.

Glantz's team shows that the sources of cyber threats to the nuclear enterprise, and the potential consequences of attacks, are extremely diverse. Threat sources include nation-states, cyber criminals, terrorists,

"hacktivists," and insiders. Their malign activity can result in harm to public health, economic losses, environmental damage, increased regulation, and a loss of public confidence in the nuclear facility, or in nuclear power generally.

The authors offer a detailed discussion of U.S. regulatory approaches, tracing their evolution as the Nuclear Regulatory Commission issued regulations and guidance, based on continual learning, since the early 2000s. The authors also explain that although a robust regulatory regime is necessary for cybersecurity, more regulation is not necessarily better. For example, not all compliance-based controls are applicable in all situations. Some controls can be costly to implement, or they may limit licensee flexibility and creativity. Furthermore, controls can feature digital components that are themselves vulnerable to exploitation. Performance-based regulatory approaches can help to mitigate these problems by encouraging innovation, improving cost–benefit ratios, saving time, reducing paperwork, and promoting communication between groups within a facility. These approaches are harder for regulators to inspect, however. To address these problems, and strike a balance between two types of approaches, the Nuclear Regulatory Commission is now incorporating risk-based components into its compliance-based program.

Glantz et al. also offer detailed discussions of U.S. approaches to risk assessment and cyber defense. Like cyber threats and consequences, these assessment and defensive approaches are diverse. The authors describe U.S. approaches to each of these measures in detail. Risk assessment include quantitative methods, focusing on such factors as asset values and risk of exploitation; qualitative processes, emphasizing discussions between subject-matter experts; and hybrid approaches, which combine elements of the previous two methodologies. The first two approaches are well established, while hybrid methods are still evolving.

Defensive measures include deterrence, detection, delay, and denial. Capabilities and techniques are extremely diverse, and include continuous monitoring programs; automated assessment of computer logs; honeypots, which lure attackers to attack decoy systems; and defense in depth, which employs multiple independent layers of security. As Glantz and his colleagues explain, all of these measures are essential components of an effective cybersecurity program.

The authors also discuss supply-chain security. They note that the integrity of supply chains is a longstanding concern of regulators and facility operators. Nonetheless, nuclear power plants have recently faced

serious supply-chain problems. The authors illustrate the nature of the challenge with a discussion of the 2020 SolarWinds incident, in which attackers inserted malware into a popular network management system, opening a back door into the computer networks of clients ranging from top private companies, to government entities including the National Nuclear Security Administration. The section closes with a discussion of tools being developed to enhance supply-chain security, including a bill of materials, which can help identify vulnerabilities in commercially available firmware or software used in nuclear facilities.

Finally, Glantz et al. addresses the challenge of assessing cybersecurity. Auditors conduct checklist-based inspections of nuclear facilities to evaluate regulatory compliance. Failure to meet standards can result in further monitoring, as well as other penalties. Facilities will therefore wish to conduct self-evaluations, which the authors argue should include risk-based assessments to ensure compliance while avoiding excessive operational and business disruptions.

1.7 Conclusion

This series of papers provides many important details regarding the United States and India's approach to nuclear safety and security. But a number of broad themes emerge from the papers as well. These themes can help us to identify similarities between the challenges that the U.S. and India face, and the two countries' efforts to surmount them. This can suggest opportunities for cooperation between India and the United States as well as areas for further research. These broad themes include the following:

Safety and security, though important, are not infinitely valuable. Marginal safety and security increases may not always justify the resultant financial burdens, legal conundrums, and stifled creativity. The pursuit of safety and security, then, must be balanced against other goods that the nuclear enterprise seeks to achieve.

Although formal rules and regulations governing the operation of nuclear facilities are important, they are ineffective without workforce buy-in. Personnel must be willing to follow the letter and spirit of the rules voluntarily, even in situations where they could get away with breaking them. Thus the safety and security of the nuclear enterprise depends, to a considerable degree, on normative and social factors, which can be difficult to understand and to manipulate.

New technology can create efficiencies while also generating new categories of risk. Recognizing these risks can take time, creating windows of vulnerability across the nuclear enterprise.

Although safety and security failures can be potentially catastrophic, they provide lessons that can help to avoid similar incidents over the long term. Failures should be discussed as openly as possible, and leveraged as learning opportunities.

The nuclear enterprise exists within a social and political context. Public beliefs about the dangers of nuclear facilities, even if unfounded, can severely hamper their operation. Effective communication between the nuclear enterprise and the public is essential.

The nuclear enterprise also exists in an economic context; nuclear security must be affordable. Failure to design a security system that is economically viable is failure to design an effective security system.

Efforts to secure the nuclear enterprise will be futile if the components on which it is constructed are compromised. Ensuring that component supply chains are secure is essential to avoiding unseen vulnerabilities.

Sophisticated designs may not yield the best security systems. Multiple rudimentary systems can sometimes generate security more effectively than one exquisite system.

The absence of catastrophe does not mean that the nuclear enterprise is sufficiently safe and secure; unidentified failures could be occurring at any time, making disaster imminent. Self-evaluation within the enterprise must be rigorous and continuous.

Although the notion of universal best safety and security practices is attractive, it is not always helpful. Approaches that work in one national or regional context may not work elsewhere. We must take care to differentiate between principles that apply universally and those that are region- or country-specific.

These themes suggest a number of opportunities for cooperation and further research. For example, Indian and the United States experts might collaborate on strategies to address shared problems such as cyber vulnerabilities, which have become increasingly important as nuclear facilities have become digitized; the need to ensure that sensitive materials are transported safely, which appeared in a number of chapters; and the need to develop healthy cultural environments within their workforces, which was a common theme in many issue areas. They also can conduct joint studies of safety and security failures, learning from each other's mistakes.

And the two countries can explore ways to pool their resources and capabilities, along with those of trusted partners, to create secure supply chains for their nuclear infrastructure.

Above all, expert communities in the United States and India must continue their dialogue on these sensitive issues, sharing wisdom and experience, and building trust. This will not only help to secure their respective nuclear enterprises, but will also enhance the two countries' broader strategic partnership. We hope that this volume constitutes a modest step in that direction.

References

Allison, G. *Nuclear Terrorism: The Ultimate Preventable Catastrophe*. New York: Times Books, 2004.

Basrur, R. "Nuclear Weapons and Indian Strategic Culture," *Journal of Peace Research* 38, no. 2: 181–198 (2001). https://www.jstor.org/stable/425494.

Burr, W. "Pakistan's Nuclear Program Posed 'Acute Dilemma' for U.S. Policy," George Washington University, August 30, 2021. https://nsarchive.gwu.edu/briefing-book/nuclear-vault/2021-08-30/pakistans-nuclear-program-posed-acute-dilemma-us-policy.

Ellsberg, D., Sanders, J., and Caplan, R. "Nuclear Security and the Soviet Collapse," *World Policy Journal* 9, no. 1 (1991): 135–156. http://www.jstor.org/stable/40209243.

Frantz, D. "U.S. and Pakistan Discuss Nuclear Security." *The New York Times*, October 1, 2001. https://www.nytimes.com/2001/10/01/world/us-and-pakistan-discuss-nuclear-security.html.

Ferguson, C., and Potter, W. *The Four Faces of Nuclear Terrorism*. New York: Routledge, 2005.

Gartzke, Erik and Kroenig, M. "Nukes with Numbers: Empirical Research on the Consequences of Nuclear Weapons for International Conflict," *Annual Review of Political Science* 19, no. 1 (May 11, 2016): 397–412. https://doi.org/10.1146/annurev-polisci-110113-122130.

Huth, P. "Deterrence and International Conflict: Empirical Findings and Theoretical Debates," *Annual Review of Political Science* 2, no. 1 (June 1999): 25–48. https://doi.org/10.1146/annurev.polisci.2.1.25.

International Atomic Energy Agency (IAEA). *IAEA Safety Glossary: 2018 Edition*. Non-serial Publications. Vienna: International Atomic Energy Agency, 2019. https://www-pub.iaea.org/MTCD/Publications/PDF/PUB1830_web.pdf.

International Atomic Energy Agency (IAEA). *Physical Protection of Nuclear Material and Nuclear Facilities*. IAEA Nuclear Security Series No. 27-G, 2018. https://www-pub.iaea.org/MTCD/Publications/PDF/PUB1760_web.pdf.

Johnson, J., Kartchner, K., and Larsen, J. *Strategic Culture and Weapons of Mass Destruction: Culturally Based Sights Into Comparative National Security Policymaking*. Basingstoke: Palgrave Macmillan, 2009.

Kapur, P. *Dangerous Deterrent: Nuclear Weapons Proliferation and Conflict in South Asia*. Stanford: Stanford University Press, 2007.

Kuchibhotla, K. and McKinzie, M., "Nuclear Terrorism and Nuclear Accidents in South Asia," in *Reducing Nuclear Dangers in South Asia*, ed. Michael Krepon and Ziad Haider, Stimson Center, Report No. 50 (2004). https://stimson.org/wp-content/files/file-attachments/Reducing%20Nuclear%20Dangers%20in%20South%20Asia%20-%20Krepon%20Haider%20-%202004.pdf.

Kutchesfahani, S., Davenport, K., and Connolly, E. *The Nuclear Security Summits: An Overview of State Actions to Curb Nuclear Terrorism 2010–2016*. Arms Control Association and Fissile Materials Working Group, July 2018. https://armscontrolcenter.org/wp-content/uploads/2018/07/NSS_Report2018_final.pdf.

Marples, D., and Young, M. *Nuclear Energy and Security in the Former Soviet Union*. Boulder, Colorado: Westview Press, 1997.

Medalia, J. "Terrorist 'Dirty Bombs': A Brief Primer," CRS Report for Congress (Congressional Research Service), 2003. https://irp.fas.org/crs/RS21528.pdf.

Miller, N. "The Secret Success of Nonproliferation Sanctions," *International Organization* 68, no. 4 (2014): 913–944. https://www.jstor.org/stable/43283283.

Monteiro, N. and Debs, A. "The Strategic Logic of Nuclear Proliferation," *International Security* 39, no. 2 (October 2014): 7–51. https://doi.org/10.1162/ISEC_a_00177.

Narang, V. *Seeking the Bomb: Strategies of Nuclear Proliferation*. Princeton, NJ: Princeton University Press, 2022.

National Diet of Japan Fukushima Nuclear Accident Independent Investigation Commission. *Official Report*. July 2012, https://warp.da.ndl.go.jp/info:ndljp/pid/3856371/naiic.go.jp/en/report/.

Newman, Lily. "A Year After the SolarWinds Hack, Supply Chain Threats Still Loom," *Wired*, December 8, 2021. https://www.wired.com/story/solarwinds-hack-supply-chain-threats-improvements/.

Sagan, S. "Why Do States Build Nuclear Weapons? Three Models in Search of a Bomb," *International Security* 21, no. 3 (1996): 54–86. https://doi.org/10.2307/2539273.

Sagan, S. "The Perils of Proliferation in South Asia." *Asian Survey* 41, no. 6 (2001): 1064–1086. https://doi.org/10.1525/as.2001.41.6.1064.

Sagan, S. and Waltz, K. *The Spread of Nuclear Weapons: An Enduring Debate*. W.W. Norton & Company, 2013.

Sanger, D. and Perlroth, N. "Pipeline Attack Yields Urgent Lessons About U.S. Cybersecurity," *The New York Times*, June 8, 2021, https://www.nytimes.com/2021/05/14/us/politics/pipeline-hack.html.

Snyder, J. *The Soviet Strategic Culture: Implications for Limited Nuclear Operations*. Santa Monica, CA: RAND, September 1977. https://www.rand.org/content/dam/rand/pubs/reports/2005/R2154.pdf.

Thayer, B. "The Causes of Nuclear Proliferation and the Utility of the Nuclear Non-Proliferation Regime," *Security Studies* 4, no. 3 (March 1995): 463–519. https://doi.org/10.1080/09636419509347592.

US General Accounting Office (GAO). "Soviet Nuclear Weapons: U.S. Efforts to Help Former Soviet Republics Secure and Destroy Weapons: Statement of Joseph E. Kelley, Director-in-Charge, International Affairs Issues, National Security and International Affairs Division," Testimony before the Committee on Governmental Affairs, U.S. Senate. 1993. https://www.gao.gov/assets/t-nsiad-93-5.pdf.

CHAPTER 2

Mitigating Insider Threats and Ensuring Personnel Reliability

Rajeswari Pillai Rajagopalan, Patrick Lynch, and Todd Burbach

2.1 An Indian Perspective

Rajeswari Pillai Rajagopalan

Nuclear security is a global challenge that gained great attention following the September 11 terrorist attacks in the United States. Since then, there has been a genuine fear that terrorists might get hold of nuclear and radiological materials and use it in attacks, with disastrous consequences. There have been some concerted efforts to secure global nuclear and radiological materials, but there are still impediments to developing an

R. P. Rajagopalan
Observer Research Foundation, New Delhi, India

P. Lynch (✉)
Oak Ridge National Laboratory, Oak Ridge, TN, USA
e-mail: lynchpd@ornl.gov

T. Burbach
Defense Threat Reduction Agency, Kirtland AFB, NM, USA

S. P. Kapur et al. (eds.), *The Challenges of Nuclear Security*, Initiatives in Strategic Studies: Issues and Policies,
https://doi.org/10.1007/978-3-031-56814-5_2

effective nuclear security regime. Nevertheless, this is an area that has seen reasonable progress despite some hesitations in the initial stages in certain quarters. There has been generally broad support for nuclear security because all states agree that it is a key challenge and an equal threat to every state. For instance, even states that have engaged in cross-border terrorism have agreed that this is a threat because terrorist groups could threaten the very states that have supported them, or these states could be blamed for sponsoring a nuclear or radiological attack, should there be an attack by their client groups. Therefore, this is an area that has seen large-scale consensus among states in working out institutional and legal mechanisms to address the threat effectively.

While there are several challenges to ensuring effective nuclear security, insider threats have emerged as one of the most significant challenges over the past decade.[1] It is particularly challenging in nuclear and other vital installations because it is almost impossible to imagine that one of your own could be a threat to the organization or the country, which leads to "blindness" in recognizing this threat. Nevertheless, even a cursory look at the numbers is evidence of the seriousness of the insider threat in these high security premises. Insider threat is a critical one also because even as these may be rare, they could impose serious costs in terms of economic, environmental, and human security. Almost all the recent cases of nuclear thefts or losses of highly enriched uranium (HEU) and plutonium (Pu) have had an insider committing the crime or helping someone else commit the crime and that should set the alarm bells ringing. Insider threats from disgruntled employees have been a well-known occurrence globally.[2]

This chapter looks at the challenge of insider threat from an Indian perspective, India's approach to addressing the threat, the challenges of ensuring trustworthiness among employees, and concludes with ways to strengthen measures that could be useful in addressing insider threats.

[1] Other threats include, but are not limited to, physical protection of nuclear and radiological facilities, and transportation security.

[2] Matthew Bunn and Scott D Sagan, *A Worst Practices Guide to Insider Threats: Lessons from Past Mistakes*, 2014, https://www.amacad.org/sites/default/files/publication/downloads/insiderThreats.pdf.

2.1.1 *Why and How Significant Is the Insider Threat?*

Attention to human factor in the context of nuclear security comes with the recognition that "the best equipment in the world is no better than its operator. Nor can the best written directives in the world compensate for apathy or technical incompetence in the workforce."[3] The human factor can be on a correct and secure path only with the right institutional culture of security. Therefore, insider threat containing the human element at its core goes hand in hand with security culture. The importance of security culture in the context of avoiding complacency cannot be ignored. Lack of incidents tends to otherwise provide a false sense of security and comfort that all is well in a facility and that there will be no insider threats. Prevalence of a positive security culture within a facility is critical in addressing complacency. Complacency and weak security culture can be a dangerous combination adding to the security vulnerability of a facility. The break-in at the Y-12 nuclear facility in the United States in July 2012 by an 82-year-old nun and two protesters is a reflection of such complacency and weak security culture.[4]

Insider threat is significant because the insider in question has knowledge of the facility, its strengths and weaknesses as well as the vulnerabilities that can be exploited. Insiders are authorised employees who enjoy access to the multiple layers of a security system. The fact that insiders are known colleagues, trusted and authorised employees make them immune to any suspicion from colleagues. The further fact that they have the complete knowledge of a facility's operations, their security systems, and nuclear material accounting practices provide enormous benefits compared to an adversary who as an adversary might not be privy to such knowledge normally. Therefore, insiders are considered possibly the most serious threat to critical infrastructure including nuclear facilities. An insider enjoys tremendous benefits as compared to an outsider because an insider knows how to circumvent and bypass certain processes that are put in place to mitigate the multiple threats. Insiders can also

[3] Igor Khripunov and James Holmes (Eds.), *Nuclear Security Culture: The Case of Russia* (Georgia: Center for International Trade and Security, University of Georgia, 2004), https://media.nti.org/pdfs/analysis_cits_111804.pdf.

[4] Geoffrey Chapman, Robert Downes, Christopher Eldridge, Christopher Hobbs, Luca Lentini, Matthew Moran, Alberto Muti and Daniel Salisbury, *Security Culture: An Educational Handbook of Nuclear & Non-nuclear Case Studies* (London: Centre for Science and Security Studies, King's College, August 2017, p. 14).

gain knowledge through training and experience. Therefore, for nuclear security purposes, the behaviour of individuals is as important or even more critical than the technologies and process that manage security at a nuclear facility.

Given this vast knowledge and access, an insider is also able to plan an operation over a prolonged period in order to remove all hindrances and ensure a successful outcome. They also enjoy the benefit of observing and studying the practices and approaches which gives an insider an advantage of choosing their target area or material, as well as the best time to engage in a malicious act with greater care. Insider threats become even more significant if an insider colludes with an outsider. It must also be added that an insider can be anyone within a nuclear facility. The threat can come from a senior scientist or a junior staff or a janitor at a nuclear facility. Designations and positions or the longevity of an employee within an organisation do not determine if a person can engage in a malicious act or not. Therefore, developing effective controls in addressing insider threat is that much more challenging because senior employees have access to every part of a facility to access to all the knowledge and sensitive data. It is also an extremely difficult challenge because human behaviour is complex and there could be many different motivations that influence an insider to commit such a malicious act.

There are other challenges as well in addressing an insider threat. Cognitive dissonance, perception bias, and a notion within the hierarchy of an organisation that they have everything under control and their facility has fail-proof mechanism can lead to ignoring any warning signs that may become evident.[5] Matthew Bunn and Scott Sagan note that assumptions like "Serious Insider Problems are NIMO (Not In My Organization)" are factors that can lead security officials to ignore the potential insider threat in a nuclear facility.[6] Organisational disfunction is also a factor that could impede the process of reporting in case of any abnormal behaviour and activities. Therefore, one also needs to look at ways to

[5] Matthew Bunn and Scott Sagan, "Insider Threats: A Worst Practices Guide to Preventing Leaks, Attacks, Theft, and Sabotage," 27th International Training Course, Sandia National Laboratories, May 17, 2018, https://scholar.harvard.edu/files/matthew_bunn/files/sandia_insider_threats_presentation_2018.pdf.

[6] Matthew Bunn and Scott Sagan, "Insider Threats: A Worst Practices Guide to Preventing Leaks, Attacks, Theft, and Sabotage," 27th International Training Course, Sandia National Laboratories, May 17, 2018, https://scholar.harvard.edu/files/matthew_bunn/files/sandia_insider_threats_presentation_2018.pdf.

create institutional incentives for employees, so they feel encouraged to report on any warning signs within a plant or notice any odd or suspicious behaviour outside work hours in their social lives. In the absence such incentives, even the most obvious signs can be misread and ignored, to the peril of the plant. There are a number of cases that reflect these systemic loopholes and vulnerabilities.[7] For instance, one of the earlier incidents occurred at the Koeberg nuclear power plant in South Africa when "an insider placed explosives directly on the steel pressure vessel head of a nuclear reactor and then detonated them" in 1982 (but before the plant went operational) to protest apartheid.[8] More recently, a French physicist employed at the European Organisation for Nuclear Research offered to assist an al-Qaeda associate to carry out terrorist attacks in France in 2012.[9] In yet another case in Europe, in 2014, a disgruntled employee at the Doel nuclear power plant imposed a shutdown of the reactor by intentionally draining out the lubricant of its turbine, resulting in a damage of hundreds of millions.[10] Insiders who are disgruntled employees are a real challenge but it is also something that could be rectified with a few remedial measures, which will be discussed in the later sections of this chapter.

2.1.2 India's Insider Threat Challenge

No country or no high security installation is immune from insider threats. Given the multilayer security system at nuclear power plants, the

[7] For a comprehensive list of nuclear and radiological incidents globally, see Noah G. Pope and Christopher Hobbs, "Insider Threat Case Studies at Radiological and Nuclear Facilities," LA-UR-15–22,642 (Los Alamos, N.M.: Los Alamos National Laboratory, 2015), http://permalink.lanl.gov/object/tr?what=info:lanl-repo/lareport/LA-UR-15-22642.

[8] David Beresford, "How We Blew Up Koeberg (… and Escaped on a Bicycle)," *Mail & Guardian* (South Africa), 15 December 1995, cited in Matthew Bunn and Scott D Sagan, *A Worst Practices Guide to Insider Threats: Lessons from Past Mistakes*, 2014, https://www.amacad.org/sites/default/files/publication/downloads/insiderThreats.pdf.

[9] "The Enduring Need to Protect Nuclear Material from Insider Threats," CRDF Global, 26 April 2017, https://www.crdfglobal.org/insights/enduring-need-protect-nuclear-material-insider-threats.

[10] Matthew Bunn, "Scenarios of Insider Threats to Japan's Nuclear Facilities and Materials—And Steps to Strengthen Protection," *NAPSNet Special Reports*, 2 November 2017, https://scholar.harvard.edu/files/matthew_bunn/files/bunn_scenarios-of-insider-threats-to-japans-nuclear-facilities-and-materials-and-steps-to-strengthen-protection.pdf.

propensity to cause significant damages using an insider could be the most attractive option from a perpetrator's perspective. The incidents across different regions mentioned above are a stark reminder of the magnitude of the problem. In a presentation at the IAEA, Jayarajan Kutuvan of the Bhabha Atomic Research Centre (BARC) near Mumbai, India, outlined the Indian awareness of the problem by acknowledging that insider threats are a serious issue also because they, depending on their level and rank, enjoy the "authority to acquire and ability to use tools, equipment, weapons or explosives."[11]

Explaining how the Indian approach to nuclear security culture has changed, Ranajit Kumar, formerly with the atomic energy establishment, said at a workshop held in Bangalore that even 10–15 years ago, if there was a question of sharing advice about nuclear security, most people would say that it is the responsibility of the security guards alone. Also, the response would have been that security incidents don't happen in my facility, but Kumar argued that this mindset has changed.[12]

India remains cognizant of the insider threat, and it has had to deal with one insider threat incident in Kaiga nuclear power plant in Karnataka, in southern India in 2009. According to the Minister for Science and Technology, Pritviraj Chavan, who spoke to the media, the incident involved a disgruntled employee who "mixed a small unit of tritium (radioactive isotope of hydrogen, D20), in a water cooler."[13] About 50 employers of the Kaiga nuclear power plant who drank the water were exposed to high level of radiation. There was no casualty from the incident. The minister confirmed that this was an "act of sabotage" possibly committed by an insider.

Commenting on the Kaiga water poisoning incident, KS Parthasarathy, former secretary of the Atomic Energy Regulatory Board (AERB) said

[11] Jayarajan Kutuvan, "Building Robust Nuclear Security Culture in Nuclear Research Centers," IAEA, n.d., https://www.iaea.org/sites/default/files/17/11/cn-254-kutuvan-presentation.pdf.

[12] Rita Guenther, Micah Lowenthal, Rajaram Nagappa and Nabeel Mancheri, *India-United States Cooperation on Global Security: Summary of a Workshop on Technical Aspects of Civilian Nuclear Materials Security* (Washington, DC: The National Academy Press, 2013), https://indianstrategicknowledgeonline.com/web/India-United%20States%20Cooperation%20on%20Global%20Security.pdf.

[13] "Sabotage in Kaiga: Tritium Added to Drinking Water," *The Economic Times*, November 30, 2009, https://economictimes.indiatimes.com/news/politics-and-nation/sabotage-in-kaiga-tritium-added-to-drinking-water/articleshow/5282881.cms?from=mdr.

that "Traditionally we have been thinking of securing nuclear plants from earthquakes and tsunami but the Kaiga incident has added another dimension to it."[14] The comment suggests that this was not considered a serious threat even a decade ago. Another former official of the atomic energy establishment, who did not want to be named, agreed with Parthasarathy's assessment and added that "Security today means checking handbags and inspecting vehicles and vigilance is all about who takes bribe. Our security at this level is good but is unprepared to deal with potential threats from scientific staff." He was worried that "Scrutiny of staff is totally missing in our power stations."[15]

The former official also pointed to a slightly different but related issue about the forces that protect the nuclear power plants. Currently, these plants are protected by the Central Industrial Security Force (CISF) who reportedly take their orders from their headquarters in Hyderabad or Delhi, but the station director has very little influence in directing the CISF who are posted at a particular facility. The former official suggested that "nuclear plants should have their own security staff with some training in reactor operation."[16] These comments have implications for a variety of threats in the context of nuclear security including insider threats and the ability to manage them. Since the incident at Kaiga nuclear power plant, the government agencies have organised mock drills and tabletop exercises at the plant site to assess the plant's emergency response preparedness to deal with a major natural disaster. In fact, the National Disaster Management Authority (NDMA) who was part of these

[14] "Kaiga Incident: Wake Up Call or Tempest in Teapot?" IANS, *The Hindu*, December 3, 2009, https://www.thehindu.com/sci-tech/energy-and-environment/Kaiga-incident-Wake-up-call-or-tempest-in-teapot/article16851321.ece.

[15] "Kaiga Incident: Wake Up Call or Tempest in Teapot?," IANS, *The Hindu*, December 3, 2009, https://www.thehindu.com/sci-tech/energy-and-environment/Kaiga-incident-Wake-up-call-or-tempest-in-teapot/article16851321.ece.

[16] "Kaiga Incident: Wake Up Call or Tempest in Teapot?" IANS, *The Hindu*, December 3, 2009, https://www.thehindu.com/sci-tech/energy-and-environment/Kaiga-incident-Wake-up-call-or-tempest-in-teapot/article16851321.ece; the Ministry of External Affairs in its publication, *Nuclear Security in India* too has noted that the CISF deployed at a nuclear facility is under the supervision of a senior Indian Police Service (IPS) officer. See Ministry of External Affairs, *Nuclear Security in India*, 2014, https://www.mea.gov.in/Images/pdf/Brochure.pdf.

exercises "ruled out the possibility of a Fukushima-type incident" at the Kaiga nuclear power plant.[17]

That there has been no reported insider threat incident (except the one at Kaiga) does not provide India with any comfort that it is not going to happen. Given the not-so-benign neighbourhood that India is located in, New Delhi remains mindful of the possibilities of an insider threat with an external element as the possible trigger. That an external agent could collude with an insider in committing an act of sabotage is real possibility. The Ministry of External Affairs, in its document released in 2014, *Nuclear Security in India* highlighted this as a possibility.[18] In fact, from the time of the design of a facility, key principles like Design Basis Threat (DBT) are taken into consideration. This involves a thorough examination of threats that the facility must be geared to protect against including terrorists, protestors, or saboteurs, which should further translate to designs that would mitigate those threats.[19]

While calculating the threat to a facility, India, like other countries, also takes into account who its adversary is, whether it is an insider or an outsider or are they working jointly, their motivations, whether it is economic, religious, and ideological or whether they use coercive methods like kidnapping a family member to force an employee to act. Other issues include the objective of the sabotage, whether is a limited operation because someone is a disgruntled employee and wants to send a message to the management, or a more serious crime of sabotage of the facility or theft of nuclear material to create panic and mass disruptions. The DBT also involves an examination of the style of attack and tactics and capabilities of the adversary. India maintains a national DBT, but a plant-specific DBT is also developed taking into account some of the plant location-specific local threats particular to a state or a region, and together the two DBTs detail each of these threats and their possible manifestation. Speaking at a nuclear security workshop co-organised by

[17] "No Threat to Goa from Kaiga Plant: S Goa Official," TNN, *Times of India*, August 6, 2011, https://timesofindia.indiatimes.com/city/goa/no-threat-to-goa-from-kaiga-plant-s-goa-official/articleshow/9499153.cms.

[18] Ministry of External Affairs, *Nuclear Security in India*, 2014, https://www.mea.gov.in/Images/pdf/Brochure.pdf.

[19] Jayarajan Kutuvan, "Building Robust Nuclear Security Culture in Nuclear Research Centers," IAEA, n.d., https://www.iaea.org/sites/default/files/17/11/cn-254-kutuvan-presentation.pdf.

the National Institute of Advanced Studies, Bangalore, Ranjit Kumar, a former official at the Indian atomic energy establishment stated that "an adversary with a colluding insider is very dangerous." He went on to add that such an adversary "can be internally motivated or externally coerced, passive or active, and nonviolent or violent."[20]

Insider threats for India can manifest itself in many ways. It could involve passing on to adversaries key information on transportation of nuclear materials, such as the agencies involved and the routes used for transportation of nuclear materials; theft of small quantities of nuclear materials for sale in black markets; or the use of cyber technologies (by an insider or in collusion with an outsider) that could inflict damage and destruction or sabotage at a facility. India has remained cognisant of the fact terrorist groups such as the Indian Mujahideen are seen to be recruiting people with IT skills and who are tech savvy. The arrest of Mansoor Peerbhoy, an IT professional who worked with Yahoo India, by the Mumbai Police in October 2008 was a stark reminder of how the face of terrorism had changed.[21] Indian Mujahideen has been known to recruit educated people with good IT skills and Mansoor Peerbhoy was not the first such recruit. While they are outsider threats currently, they could be looking at co-opting an insider to commit a range of malicious acts, mentioned above.

Given the substantial reliance of nuclear industries on computer-aided systems, insiders facilitating nuclear security threats in the form of bugs and viruses cannot be ignored. The Stuxnet cyberattack on Iranian nuclear facilities that damaged Tehran's nuclear facilities reflects the growing threats from cyber and cyber-related technologies. Insiders can become easy accomplices in carrying out these kinds of attacks. Similarly, the possibility of a disgruntled employee with access to sensitive information

[20] Rita Guenther, Micah Lowenthal, Rajaram Nagappa and Nabeel Mancheri, *India-United States Cooperation on Global Security: Summary of a Workshop on Technical Aspects of Civilian Nuclear Materials Security* (Washington, DC: The National Academy Press, 2013), https://indianstrategicknowledgeonline.com/web/India-United%20States%20Cooperation%20on%20Global%20Security.pdf.

[21] "Mansoor Peerbhoy: An Unlikely Jihadi, He Shows No Remorse," *Times of India*, October 7, 2008, https://timesofindia.indiatimes.com/india/mansoor-peerbhoy-an-unlikely-jihadi-he-shows-no-remorse/articleshow/3567756.cms; S. Hussain Zaidi and Brijesh Singh, "The Making of A Terrorist," *Rediff.com*, July 10, 2017, https://www.rediff.com/news/special/the-making-of-a-terrorist/20170710.htm.

selling the information to external adversaries for financial gains cannot be discounted.

India is cognisant of the cyber and network vulnerabilities, and such threats and vulnerabilities are addressed by a separate department within the Department of Atomic Energy (DAE) called the Computer Information and Security Advisory Group (CISAG). The CISAG is responsible for undertaking audits of computer and information systems on a periodic basis. The CISAG is also responsible for developing "plans and guidelines to counter cyber attacks and mitigate its adverse effects."[22] The guidelines have clear do's and don'ts about the use of internet, USBs, and smartphones in sensitive areas within a facility. The CISAG of the DAE issued new guidelines in May 2020 that outlined a number of precautionary steps for the work from home conditions. One of the points said that employees are "advised to keep official documents only in external storage such as Pen Drive, USB Hard Disk."[23] This is presumably done to protect the document from being stolen if computers are hacked, but this step has its risks as well. For instance, pen drives could be stolen or lost. A much worse scenario is if a disgruntled employee with all the information on a pen drive or USB decides to share this sensitive information with those who want to do harm. Under such circumstances, pen drives, or USBs with important sensitive information become easy tools for attackers. Nevertheless, there are no easy solutions to insider threat problems in an online or offline world. Therefore, the effort must be to inculcate a strong nuclear security culture including cybersecurity culture, whereby individuals are incentivised to be aware of the threats and to take proper precautions. It is important for India to focus on this aspect given that it has been one of the favourite targets

[22] Ministry of External Affairs, *Nuclear Security in India*, 2014, https://www.mea.gov.in/Images/pdf/Brochure.pdf.

[23] Computer and Information Security Advisory Group (CISAG), Department of Atomic Energy, "Guidelines for Work from Home," May 14, 2020, https://iopb.res.in/news/wp-content/uploads/2020/05/CISAG_Guidelines_for_Work_from_Home_14052020.pdf.

of cyberattacks in recent years.[24] Even though some of the recent cyber-attacks have targeted only administrative systems and had nothing to do with plant control and instrumentation system, this could be potentially dangerous too.[25] Gaining information on nuclear power plant staff and their personal details including their financial remuneration could be used by malign actors to extract benefits and could thus compromise India's nuclear security efforts.

2.1.3 Indian Approach to Addressing Insider Threat

The potential that an insider has to overcome normal security barriers and its consequences have prompted India to be ever vigilant to possible intrusions and collusions by external actors, especially those from across the border in Pakistan. This has driven India to give a particular focus to security culture. While technology has aided in new ways like automation within a nuclear power plant that could minimise the human element and thus reduce human errors in a facility, one has to recognise the limits of technology and the significance of the human element behind the technology. But when it comes to nuclear security, one can have the best technology and the best processes and procedures to minimise security gaps and vulnerabilities, but the individuals responsible for running the plant still have a big role to play in ensuring nuclear security. This brings

[24] There was a cyber-attack on the Kudankulam Nuclear Power Plant in 2019, although it was not an insider attack. Following the attack, the Indian Computer Emergency Response Team (CERT-In) and the Computer & Information Security Advisory Group (CISAG) carried out complete checks of the administrative network of the plant. In a question on the issue in the Rajya Sabha (Upper House of the Indian Parliament) in November 2019, Dr. Jitendra Singh, the Minister of State in the Prime Minister's Office, responded by saying that "Certain measures for immediate and short term implementation has been recommended. Several measures have been taken for further strengthening of Information Security in administrative networks viz. hardening of internet and administrative intranet connectivity, restriction on removable media, blocking of websites & IPs which have been identified with malicious activity etc." For details, see Lok Sabha, "Unstarred Question No. 1482 to be Answered on 27.11.2019—Cyber Security Audit KKNPP," November 27, 2019, https://pib.gov.in/PressReleasePage.aspx?PRID=1593768; there was a similar debate in India's Lower House of the Parliament, the Lok Sabha. For details, see Lok Sabha, "Unstarred Question No. 659, Answered on: 20.11.2019—Cyber Attack on KKNPP," November 20, 2019, http://loksabhaph.nic.in/Questions/QResult15.aspx?qref=6759&lsno=17.

[25] Department of Atomic Energy, "Cyber Attacks on Indian Nuclear Power Plants," November 28, 2019, https://pib.gov.in/PressReleasePage.aspx?PRID=1594020.

the focus towards security culture that prevails in a facility that could be helpful in mitigating some of these threats and challenges. According to the former US Department of Energy czar, Eugene Habinger, "good security is 20 percent equipment and 80 percent culture."[26]

A good security culture is one that prevails across all ranks and files, from scientists and managers to security guards and janitors, wherein each is conscious of the threats, challenges, gaps, and vulnerabilities and remains conscious of each one's responsibility to secure a nuclear facility and nuclear materials. A workshop report from the National Institute Advanced Studies that co-organised a workshop on nuclear security makes it clear that "every person, from a custodian to a technician to a scientist to a guard in the protective force, needs to believe in and support the nuclear security program for it to succeed."[27] According to Jayarajan Kutuvan of the BARC, nuclear security culture represents an "assembly of characteristics, attitudes and behavior of individuals, organizations and institutions, which serve to support and enhance nuclear security." He added that nuclear security "ensures that individuals stay vigilant and be aware of what is happening in their organization" by creating "a questioning attitude among individuals, which may help in detecting insider threat and outsider threat."[28]

According to the IAEA's 2017 report on security culture, security culture self-assessments with a focus on "perceptions, views and behaviour at all levels of the organization, regular self-assessment helps managers to understand the reasons for an organization's patterns of behaviour in certain circumstances and to devise more effective overall security arrangements". They are far more useful than typical audits, which highlights technical issues than intangible human elements. The document added that "The results of a security culture self-assessment will rarely point

[26] "Nuclear Security Culture: The Case of Russia," Center for International Trade and Security, University of Georgia, December 2004, https://media.nti.org/pdfs/analysis_cits_111804.pdf.

[27] Rita Guenther, Micah Lowenthal, Rajaram Nagappa and Nabeel Mancheri, *India-United States Cooperation on Global Security: Summary of a Workshop on Technical Aspects of Civilian Nuclear Materials Security* (Washington, DC: The National Academy Press, 2013), https://indianstrategicknowledgeonline.com/web/India-United%20States%20Cooperation%20on%20Global%20Security.pdf.

[28] Jayarajan Kutuvan, "Building Robust Nuclear Security Culture in Nuclear Research Centers," IAEA, n.d., https://www.iaea.org/sites/default/files/17/11/cn-254-kutuvan-presentation.pdf.

directly to specific technical actions, but will more typically shed light on why particular security related issues emerge, what the root causes of problems may be and how overall nuclear security can be enhanced."[29]

This brings into focus the importance of personnel reliability programmes (PRPs) or human reliability programmes (HRPs), as they are alternatively called. These programmes cannot offer any guarantee, but they go a long way in mitigating insider threats when implemented well. In fact, an earlier study by the author that involved extensive field visits and interactions with the security managers found that India has an extensive PRP, which have been quite effective in addressing potential gaps on this front. The Indian PRPs are done across the plant on all staff employed at various facilities and have included a series of rigorous background checks, vetting, and verification process before a person is inducted into a facility. The background screening and checks have included assessing a person's identity, family background, criminal and medical history, general reputation as well as out-of-office social interactions and any change in behavioural patterns. These are undertaken on a periodic basis and additionally, the PRP is done as and when an employee is to be assigned or transferred to a more sensitive facility or if the employee has been given a clearance to handle more secure and sensitive information. The PRPs are undertaken up to the level of contractors who are engaged with a particular nuclear facility. The Indian atomic energy agencies and security managers have maintained total and complete integrity with the PRPs, and the reliability of these programmes has not so far been compromised, as far as is known.

Nevertheless, as in any other sector, there is scope for improvement. One area that has continued to remain a challenge in this regard is the PRPs on temporary labourers who work with nuclear power plants. These labourers tend to work with a plant for a couple of weeks to a month at best and they work only at the peripherals of a facility and are nowhere near the core of a facility. These are migrant workers from rural India spread across different states and provinces and because they keep moving from place to place, police, and other security agencies have found it challenging to do effective vetting and background checks. Even as they work only for very short time and are at the periphery of a facility, it is still

[29] International Atomic Energy Agency, "Self-Assessment of Nuclear Security Culture in Facilities and Activities: Technical Guidance," IAEA Nuclear Security Series No. 28-T, 2017, https://www-pub.iaea.org/MTCD/Publications/PDF/PUB1761_web.pdf.

not a comfortable situation from a security and vulnerability perspective. Terrorists, criminals, or persons with malintent can exploit these labourers to commit a crime. Indian security agencies need to find a way to address this loophole.

While the Indian PRPs are fairly exhaustive, one area that needs to be included is a person's online activities. Cyber-space offers a menu of options if an insider wants to hurt the system.[30] Cyber means have been effective tools in pushing individuals towards religious radicalisation, which in turn have prompted employees to engage in activities that they would not have otherwise. Even as the security agencies around the world understand and acknowledge the importance of being alert to an individual's cyber interactions, it is a complex and sensitive issue, especially for democracies that value and seek to protect privacy and personal freedom. But given that online radicalisation has become a real threat, this is an inescapable area of vulnerability and security agencies have to find a way to monitor employees' cyber behavioural patterns. Keeping a watch for any abnormal behaviour as a fallout of their possible online radicalisation is one way to address it. For instance, if a person has become suddenly deeply religious, that is possibly a fallout of online radicalisation. So, PRPs must continue with periodic monitoring to keep a tab on a person's online and offline activities and behavioural patterns.

Therefore, an effective nuclear security policy and practice must evaluate the human factor as an important determining factor while assessing the efficacy of nuclear security. According to an International Atomic Energy Agency (IAEA) document on the self-assessment of nuclear security culture in nuclear facilities and activities, a robust nuclear security approach would input a series of elements including "proper planning, training, awareness, competence, knowledge, operations and maintenance, as well as on the thoughts and actions of all people in the organization."[31] The IAEA document further notes that "an organization may have appropriate technical systems in place but remain vulnerable if it

[30] Matthew Bunn, "Scenarios of Insider Nuclear Threats—And Steps to Strengthen Protection," Nautilus Institute Workshop on Reducing the Risk of Nuclear Terrorism and Spent Fuel Vulnerability in East Asia, January 21–22, 2017, https://scholar.harvard.edu/files/matthew_bunn/files/japan-insider-scenarios_2017.pdf.

[31] International Atomic Energy Agency, *Self-Assessment of Nuclear Security Culture in Facilities and Activities: Technical Guidance* (Vienna: IAEA, 2017), https://www-pub.iaea.org/MTCD/Publications/PDF/PUB1761_web.pdf.

underestimates the role of the human factor." It goes on to emphasise on the importance of human factor including the top layer of managers and leaders in maintaining effective nuclear security. A report co-authored by Matthew Bunn and his colleagues categorised insider threats as the most significant nuclear security threats.[32] So, even as the extensive vetting and background checks as part of PRPs are an important tool in addressing insider threats, they offer no guarantee that there will not be an occasional breach.

2.1.4 Challenges of Ensuring Trustworthiness

Ensuring trustworthiness of an employee at high security installations such as a nuclear power plant is not easy. Trustworthiness of employees is undertaken to validate a person's integrity, reliability, and suitability of them in offices that give them a wide range of access including to nuclear materials, facilities, technology, or sensitive security information.[33] Trustworthiness is done by different states differently but there are some similarities in terms of its application across all levels within an organisation, and the end goals of these programmes. Commenting on the trustworthiness issue, Jayarajan Kutuvan of the BARC said that the screening process that is undertaken as part of this effort will be in line with "the risks and threats related to specific role and responsibility."[34] To that extent, these are graded approaches. Graded approach will be dependent on the type of facility and materials within a facility. Similarly, there will be a graded approach depending on the level of personnel associated with a facility like janitors, lab researchers, technicians, security officers,

[32] Matthew Bunn, Martin Malin, Nickolas Roth, and William Tobey, "Key Steps for Continuing Nuclear Security Progress," at an "International Conference on Nuclear Security: Commitments and Actions," International Atomic Energy Agency, Vienna, Austria, September 12, 2016, https://scholar.harvard.edu/files/matthew_bunn/files/bunn_key_steps_for_continuing_nuclear_security_progress.pdf.

[33] "27. Introduction to Nuclear Security Trustworthiness Programs," 27th International Training Course, Sandia National Laboratories, Albuquerque, New Mexico, USA, April 30–May 18, 2018, https://share-ng.sandia.gov/itc/assets/27_introduction-to-nuclear-security-trustworthiness-programs.pdf.

[34] Jayarajan Kutuvan, "Building Robust Nuclear Security Culture in Nuclear Research Centers," IAEA, n.d., https://www.iaea.org/sites/default/files/17/11/cn-254-kutuvan-presentation.pdf.

and control room operators.[35] While handling radiological materials, for instance, the risk levels are accorded depending on the risks involved with each of the materials, trustworthiness is an issue that the Indian nuclear regulatory authority, Atomic Energy Regulatory Board (AERB) has flagged.[36]

Nevertheless, states need to consider trustworthiness programme that will continue monitoring mental well-being, substance abuse, unusual work hours, violent, criminal or any unusual behaviour inside and outside work premises, and political and ideological interests. Kutuvan also suggests that the screening process be applied to all temporary staff, contractors, and visitors, which is an ideal scenario. But the state's ability to vet temporary staff under PRP has shown some challenges. These challenges are not unique to India. At a conference on radioactive materials security organised by the IAEA in 2013, conference participants (officials from different atomic energy agencies) recognised that even the IAEA's Nuclear Security Series, while broadly useful in developing national regulations, has gaps in its guidance on insider threats and trustworthiness, gaps that require additional work.[37]

In the case of India, once individuals are employed by the atomic energy agency, the individual undergoes a one-year training programme at the Homi Bhabha National Institute located in Mumbai. Nuclear safety, nuclear security, and security culture are important components of the training programme. Further, nuclear facilities as well as atomic energy regulators run periodic seminar, workshops, and refresher courses on nuclear safety and nuclear security. The Global Centre for Nuclear Energy Partnership (GCNEP), one of India's centres of excellence has five schools including one focusing on nuclear security—the School of

[35] "27. Introduction to Nuclear Security Trustworthiness Programs," 27th International Training Course, Sandia National Laboratories, Albuquerque, New Mexico, USA, April 30–May 18, 2018, https://share-ng.sandia.gov/itc/assets/27_introduction-to-nuclear-security-trustworthiness-programs.pdf.

[36] See R. K. Singh, "Safety and Security Aspects of Radioactive Material During Transport," IAEA, 2011, https://inis.iaea.org/collection/NCLCollectionStore/_Public/43/014/43014475.pdf.

[37] International Atomic Energy Agency, "Safety and Security of Radioactive Sources: Maintaining Continuous Global Control of Sources throughout Their Life Cycle," Proceedings of an International Conference, Abu Dhabi, United Arab Emirates, October 27–31, 2013 (Vienna: International Atomic Energy Agency, 2015), https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1667_web.pdf.

Nuclear Security Studies (SNSS).[38] The training programmes undertaken at the GCNEP by the SNSS independently and in partnership with other countries and agencies involve a number of critical areas related to nuclear security including computer simulation exercises on possible nuclear security incidents and personnel reliability studies as well as systems for personnel and material access control and intrusion detection and vulnerability assessments.[39]

The effectiveness of trustworthiness programmes comes from continuing monitoring of an individual across a number of parametres including examination of different motivational factors like financial conditions, employee dissatisfaction possibly driving individuals to engage in unusual behaviour, and changed political or ideological orientations. Trustworthiness programmes and security culture training modules need to be evaluated on a periodic basis because of the changing nature of threats and challenges so that such programmes continue to be effective. In case there have been some personnel incidents and failures, these need to be studied both in terms of understanding the reason for the incident from a personnel's perspective but also to reveal and understand the gap in the trustworthiness programme that led to the failure. Hence, these programmes need to be dynamic, constantly evolving in relation to the changing threat environment.

2.1.5 Are There Solutions and Measures That Can Be Taken?

Addressing insider threats require a combination of strategies and measures because of the difficulties associated with continuous monitoring of human behaviour and impulses. A conference report found many participants agreeing that "the most cost effective measure is a strong security culture with an effective training program (letting employees know their role in security as well as the consequences of security failure) and employee concerns program (non-retaliation for

[38] School of Nuclear Security Studies, Global Centre for Nuclear Energy Partnership, http://gcnep.gov.in/schools/snss.html.

[39] Jayarajan Kutuvan, "Building Robust Nuclear Security Culture in Nuclear Research Centers," IAEA, n.d., https://www.iaea.org/sites/default/files/17/11/cn-254-kutuvan-presentation.pdf; for details, also see, School of Nuclear Security Studies, Global Centre for Nuclear Energy Partnership, http://gcnep.gov.in/schools/snss.html.

reporting aberrant behaviors and collusion)."[40] It is further suggested that there be "an appropriate 2-person or 3-person rule with robust surveillance and strict access and work authorizations systems so no single person is left alone to commit a malicious act."

Insider threats, especially those relating to a disgruntled employee can be addressed by taking simple steps such as by understanding the employee concerns and dissatisfaction, giving a sympathetic ear even if the problems are not entirely resolved to give the employee the satisfaction that he/she is being heard and if possible, rectify the issues that gave way to the disgruntlement. These steps are done at the level of reporting authority and the office management can address dissatisfaction-induced insider threat.

There are no easy fixes to addressing insider threats. Bunn offers a series of steps to incentivise good practices and nurturing security culture in nuclear facilities, both at individual and facility levels. Some of these include: the good citizen incentive, reviewing and rewarding security performance, rewarding reporting, making good security easy, "security watchdogs" award at the individual level, and including security performance in management reviews, and industry self-help and self-regulation, at the facility level.[41] Creating strong incentive structure for employees to report on unusual and odd behaviour can be a useful tool in mitigating the insider threat. Further, periodic refresher courses and training modules can get the entire facility staff to be on the same page on threat perceptions and ways to manage them. These modules and courses should try and build in real-life incidents that might give the staff a better sense of the magnitude of the problem. Extra vigilance and increased surveillance of areas that hold nuclear material could also be useful. An additional step, especially relevant during transportation of nuclear materials, is to have tamper indicating devices that would issue an alert if a vessel transporting nuclear materials has been tampered with.

[40] Galya Balatsky and Ruth Duggan, "Nonproliferation, Nuclear Security, and the Insider Threat," SAND2012-4855C, Office of Scientific and Technical Information, US Department of Energy, nd, https://www.osti.gov/servlets/purl/1294289.

[41] Matthew Bunn, "Incentives for Nuclear Security," In Proceedings of the Institute for Nuclear Materials Management 46th Annual Meeting, Phoenix, Arizona, July 14, 2005, https://scholar.harvard.edu/files/matthew_bunn/files/incentives_for_nuclear_security.pdf.

A related issue is to institute better material auditing process and strengthened inventory management. Material control and accounting of nuclear materials is not easy if an insider chips away materials in small quantities so that it does not catch the attention of the inventory managers. A useful step might be to institute random reviews and screenings by external agencies (other than the plant managers) to look for anomalies in material accounting and inventory management. As an additional step, it is useful to stop theft of materials if materials are kept in "difficult-to-steal forms" so that it is not easy for an individual to carry it out of a facility.[42]

Forged ID cards and documents are easy tools that perpetrators use to enter a facility. Change of ID cards on a periodic basis, with unique colours and holograms, could make it difficult to clear entry checkpoints. Additionally, vulnerability assessments need to be reviewed and updated on a periodic basis in coordination with threat assessments provided by national and local intelligence agencies. Vulnerability assessments need to look at three different facets while developing them which include characterisation of the threat through target identifications, followed by an analysis of the threat by looking at the vulnerabilities that a facility is exposed to and lastly ways to mitigate the threat and checking the effectiveness of the facility's security systems in place.[43]

Compartmentalising information can also be a useful step in delaying and deterring theft of data.[44] One must devise programmes and processes in way critical information goes through multiple folders, each with passcodes and encryption keys that would delay in case of a security breach. Even for physical protection, a security breach by insider can be mitigated to some extent if there are multiple layers of security in the form

[42] Matthew Bunn, "Scenarios of Insider Threats to Japan's Nuclear Facilities and Materials—And Steps to Strengthen Protection," *NAPSNet Special Reports*, November 2, 2017, https://nautilus.org/napsnet/napsnet-special-reports/scenarios-of-insider-threats-tojapans-nuclear-facilities-and-materials-and-steps-to-strengthen-protection/.

[43] Rita Guenther, Micah Lowenthal, Rajaram Nagappa and Nabeel Mancheri, *India-United States Cooperation on Global Security: Summary of a Workshop on Technical Aspects of Civilian Nuclear Materials Security* (Washington DC: The National Academy Press, 2013), https://indianstrategicknowledgeonline.com/web/India-United%20States%20Cooperation%20on%20Global%20Security.pdf.

[44] US Department of Energy, National Nuclear Security Administration, "Addressing the Insider Threat," n.d., https://www.internationaltransportsecurity.org/sartss-2021/wp-content/uploads/sites/6/2021/03/SARTT-Insider-Threat-GMS-3.4.21_skr.pdf.

of gates and other physical security barriers, including such as through RFID and retina screening measures, that would delay the intrusion into unauthorised areas and could alert the security managers of a possible security breach. Physical barriers and technology-aided delay measures have become fairly common in almost all nuclear material possessing countries. It might also be useful to conduct periodic audit of RFID and other screening measures to test the effectiveness of the barriers of a facility. Identification and maintenance of access levels of employees are useful. Similarly, access to areas within a facility needs to be clearly identified and reviewed periodically. Within the nuclear security context, the de facto format for access should be using "need-to-know" principle. Also, two-person rule needs to be enforced rigorously so that one individual is never alone with sensitive technology.

Addressing nuclear security threats can benefit also from international cooperation. Even as these threats are country-specific and cannot be generalised, sharing of critical information on incidents or a threat was averted can be useful. These can be done through bilateral routes or global conversations that could be hosted by, for instance, regional centres of excellence.

2.1.6 Conclusion

Nuclear security is constantly evolving with a number of threats including insider threats which can lead to havoc in the physical protection of nuclear facilities as well as cyber vulnerabilities in nuclear power plants. While India is yet to face any major nuclear incident, its geographical location and the internal security challenges are a continuous concern for New Delhi. India's personnel reliability programme is very stringent in addressing the insider threat, but it cannot afford the luxury of assuming that it has the perfect system that will not break down. This chapter has identified a series of steps that can be taken to further strengthen the measures to deal with insider threat. Security culture, better material accounting and audit processes, incentivising reporting of any unusual behaviour, including security performance as part of management reviews, training, and periodic refresher modules can be useful steps in mitigating the insider threat in the nuclear security arena. International cooperation remains another key step in this regard and sharing of information like lessons learnt from an incident or how a threat was dealt with can be useful in avoiding nuclear mishaps. India and the US can think of

such practices in the bilateral context first before taking it up in larger minilateral or multilateral formats.

2.2 A U.S. Perspective

Patrick Lynch and Todd Burbach

Insider threats to the nuclear community pose unique challenges. This paper will introduce insider threats by defining the insider threat from multiple perspectives and explaining the risk against these differences. It will further discuss mitigation measures while reinforcing the diverse nature driving differences between mission sets, including military and civilian processes. Introduction to measures within both the civilian and military approach including trustworthiness or reliability programs with challenges and opportunities will be provided along with a few technical measures. The importance of a reliability program as a tool to mitigate internal threats will be highlighted including approaches well suited to a graded approach, applying elements that are unique to an organization or country. The US approach to mitigating insider threats will be shown using tools and methodologies created to address the threats from the perspective of US nuclear operations culture. Lastly, the international community may seek to learn from best practices and consider applying relevant elements. Publications from the International Atomic Energy Agency (IAEA) and World Institute for Nuclear Security (WINS) will be provided to strengthen this endeavor.

2.2.1 Defining the Insider Threat

Since the various organizations manage different aspects or stages of nuclear or radiological material, their definition of what constitutes an insider threat and how to manage mitigation programs is different. For instance, the US Department of Energy's (DOE's) Human Reliability Program (HRP) and the US Department of Defense's (DoD's) Personnel Reliability Assurance Program (PRAP) are diverse by design because the mission(s) are dissimilar. The HRP mission is "involved in researching, testing, producing, disassembling, or transporting nuclear explosives, which, when combined with Department of Defense delivery

systems, become nuclear weapons systems."[45] One key mission difference then is the delivery system, which is reiterated in the DoD description of "nuclear weapons and nuclear weapon systems" but adds "nuclear command and control."[46] Mission does not define the totality of difference; magnitude plays a significant part. DoD designates two categories of certification, critical and controlled, to assist in management and provide cost savings for large numbers of personnel. The main difference between the categories is technical knowledge, but critical certification may also mean they "can either directly or indirectly cause the launch or use of a nuclear weapon."[47] Keeping these differences in mind, in broad terms, DoD identifies an insider as "a person who has been granted eligibility for access to classified information or eligibility to hold a sensitive position" and the threat insiders may pose "to DoD and US government installations, facilities, personnel, missions, or resources. This threat can include damage to the United States through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities."[48]

The DOE program is created with integration in mind, addressing threats to personnel, facilities, materials, information, equipment, and other DOE assets, establishing a central insider threat program for DOE.[49] In 2016, HRP experts from the US national laboratory complex, specifically Oak Ridge National Laboratory (ORNL), created an approach for the international community interested in developing an HRP, which leverages specific elements of the DOE HRP. In this case, the following definition was retained: "security and safety reliability program designed to ensure that individuals who occupy positions with access to certain nuclear materials, facilities, and programs meet the highest standards of

[45] Human Reliability Program, 10 CFR Parts 710, 711, and 712 (2002).

[46] US Department of Defense (DoD), *Department of Defense Directive 3150.02, DoD Nuclear Weapons Surety Program, Incorporating Change 4.*

[47] US Department of Defense (DoD). *Department of Defense Manual 5210.42, Nuclear Weapons Personnel Reliability Program, Incorporating Change 3*, 2018b.

[48] US Department of Defense (DoD). *Department of Defense Directive 5205.16, The DoD Insider Threat Program, Incorporating Change 2*, 2014.

[49] US Department of Energy. Department of Energy Insider Threat Program, DOE Order O 470.5 (DOE Order), 2014, https://www.directives.doe.gov/directives-documents/400-series/0470.5-BOrder/@@images/file.

- reliability (an individual's ability to adhere to security and safety rules and regulations),
- trustworthiness (confidence in an individual based on their character), and
- physical and mental suitability"[50]

International definitions of insider threats to the nuclear community are important to consider, as well as recommended programs to mitigate insider threats and ensure the trust and reliability of personnel with access and knowledge to nuclear materials and related information. The below definitions are from both the international nuclear community and the US nuclear community. The IAEA defines an insider threat as "an individual with authorized access to [nuclear material,] associated facilities or associated activities or to sensitive information or sensitive information assets, who could commit, or facilitate the commission of criminal or intentional unauthorized acts involving or directed at nuclear material, other radioactive material, associated facilities or associated activities or other acts determined by the State to have an adverse impact on nuclear security."[51] The World Institute for Nuclear Security (WINS), which is an international nongovernmental member organization that strives to be a leader in knowledge exchange, professional development, and certification for nuclear security management. WINS defines an insiders as "individuals who may take advantage of their authorised access to facilities, processes, materials, transport operations or sensitive computer and communications systems to perform a malicious act."[52]

To complement the US Department of Energy and Department of Defense definitions, the US Nuclear Regulatory Commission, which regulates government and civilian nuclear infrastructure, defines an insider as "a trusted person with protected or vital area access, or access to digital computer and communications systems and networks from outside the

[50] Oak Ridge National Laboratory (ORNL). *Roadmap to a Sustainable Human Reliability Program*.

[51] International Atomic Energy Agency (IAEA). *Preventive and Protective Measures against Insider Threats*, 2020, https://www-pub.iaea.org/MTCD/Publications/PDF/PUB1858_web.pdf.

[52] World Institute for Nuclear Security (WINS). *International Best Practice Guide, 3.4 Managing Internal Threats. V. 2.1.* 2021, https://www.wins.org/document/3-4-managing-insider-threats-in-the-nuclear-industry/.

protected area, can pose a significant threat to the safety and security of a nuclear power plant."[53]

2.2.2 *Introduction to Insider Threats*

Motivations between the controlled or critical groups may be similar but the reasons are numerous and can range from ideology, revenge, distorted ego, sabotage, financial need, to being threatened, or coerced by outside elements or even family members.[54] WINS identified two types of possibilities when it came to those who may be influenced by an ideological motivation: the plant and the convert.[55] The plant, as defined by WINS, is someone who specifically seeks employment with the intention of launching an attack or conducting a malicious act. This may be most successful if a poor security culture is present at a facility or the clearance process for granting access to information or material is weak. According to WINS, this raises the need for a layered approach to protection (defense-in-depth) while also raising awareness among staff that processes will be in place to verify trust and reliability.

Additionally, WINS defined the second type of ideologically motivated insider as a convert. In this case, a convert is an employee who becomes influenced or radicalized while already employed in the organization after successfully passing initial background investigations. Known measures should be considered to identify a convert's conversion: trauma, a lifestyle change, financial loss, or disgruntlement. An individual who exhibits behavior that deviates from their normal behavior may be identified by some processes deployed by the organization. These may include elements of a reliability or trustworthiness program that include an annual or random reevaluation, rescreening, or participation in an employee behavior observation program in which fellow employees are aware of a reporting process. Chelsea Manning and Edward Snowden represent

[53] US Nuclear Regulatory Commission. *Regulatory Guidance 5.77 Insider Threat Mitigation Program*, 2009, https://www.nrc.gov/docs/ML1521/ML15219A609.pdf.

[54] International Atomic Energy Agency (IAEA). *Preventive and Protective Measures against Insider Threats*, 2020, https://www-pub.iaea.org/MTCD/Publications/PDF/PUB1858_web.pdf.

[55] World Institute for Nuclear Security (WINS). *International Best Practice Guide, 3.4 Managing Internal Threats. V. 2.1.* 2021, https://www.wins.org/document/3-4-managing-insider-threats-in-the-nuclear-industry/.

multifaceted convert cases. Both believed they were whistleblowers and felt some responsibility to inform people of the actions of their government, even to the extent they mentally set themselves up as "protectors of the people." At the onset, this may seem motivation enough if given a disagreement or tendency to diverge from the beliefs of the organizations they support. In the former case, pacifism was an underlying motivational nuance, and in the latter case, surveillance and the technology involved including simple encryption and stirring the tech community appeared to be motivators.

Another motivating factor of an insider threat is ego. An insider may seek to prove their knowledge, intelligence, or abilities by performing an act of sabotage or the removal of material or information.[56] Identifying the traits of an individual who may be motivated by their ego may be difficult during the recruitment and hiring phase. Facilities are encouraged to deploy a graded approach when reviewing critical positions that may require additional measures to ensure trustworthiness and reliability. In 2020, the IAEA published a Nuclear Energy Series Technical Document, *Addressing Behavioural Competencies of Employees in Nuclear Facilities*, which provides the identification of critical roles, as well as information and recommendations for conducting a job task analysis to determine the key behavioral requirements for effective performance.[57]

An insider may also be motivated by disgruntlement, acting out against an organization or facility because they feel they are unfairly treated. This may take the form of a poor review or evaluation, not receiving a promotion, or other instances where an employee may feel slighted. The WINS International Best Practice Guide encourages employers to treat all employees fairly, which is an important preventive measure in the mitigation of disgruntlement. Similar to preemployment screening, identified as a mitigation effort for individuals motivated by their ego, incorporating preemployment assessments may identify individuals with

[56] World Institute for Nuclear Security (WINS). *International Best Practice Guide, 3.4 Managing Internal Threats. V. 2.1.* 2021, https://www.wins.org/document/3-4-managing-insider-threats-in-the-nuclear-industry/.

[57] International Atomic Energy Agency (IAEA). *Assessing Behavioural Competencies of Employees in Nuclear Facilities*, 2020, https://www-pub.iaea.org/MTCD/Publications/PDF/TE-1917_web.pdf.

higher-than-normal probabilities of perpetrating an attack to satisfy an emotional or psychological urge, but this is very difficult to confirm.[58]

The risk of the insider threat is uncertain at best, but it is likely quite small based on historical incidents. The issue is a single insider can inflict devastating consequences. So, how to balance such a low probability against an extremely disastrous outcome? The point is not to eliminate risk but to reduce or manage it in all aspects of the program. Even though "only those individuals who demonstrate the highest levels of integrity and dependability" are accepted, the risk is not zero.[59] Determining an acceptable level of risk is never an easy task but when applied to the program, it need be cost-effective and not overly burdensome, or it is destined to fail.

How we determine what is an acceptable level begins with determining what risks exist and an assessment of the level of the risk with the probability of occurrence. Many assessment examples exist and can be easily modified to suit each risk. An important note is the actual risk and/or likelihood may differ through another cultural lens. For instance, a cultural acceptance and therefore availability of drugs may increase the probability rating. Still, it becomes fairly easy to see where low severity coupled with low probability may be readily accepted whereas high severity and high probability may require mitigation. A bit harder perhaps are those with a high severity but with an extreme low probability. They may be readily acceptable but a determination must be made. Deciding by whom or at what level risk may be accepted or responsibility assigned is essential. Just as it is important to identify all risks and reassess after mitigation measures, the ultimate determination of acceptance must come from the right authority. Risks stemming from factors on individuals have considerations used by agencies which aid the authority in determining clearance or access determinations. Things such as circumstances, societal conditions, or rehabilitation efforts, to name a few, may be factored. It should be apparent that this is oversimplified and the actual criteria could fill volumes.

[58] World Institute for Nuclear Security (WINS). *International Best Practice Guide, 3.4 Managing Internal Threats. V. 2.1.* 2021, https://www.wins.org/document/3-4-managing-insider-threats-in-the-nuclear-industry/.

[59] US Department of Defense (DoD). *Department of Defense Manual 5210.42, Nuclear Weapons Personnel Reliability Program, Incorporating Change 3*, 2018.

In some instances trustworthy members may be coerced into perpetrating a malicious action, such as blackmail or the threat of violence. Often, individuals keep embarrassing problems to themselves, including an addiction to drugs, alcohol, or gambling. This type of information can be used to blackmail an individual, using the fear of retaliation if the information is presented to an employer. Behavioral changes observed by colleagues or management may be the first indication that a change has occurred. An important mitigation measure for this motivation is a commitment to an employee assistance program. If an individual is confident that the employer has the resources and interest in helping, rather than terminating, the individual may be more inclined to self-report challenges they are facing.

Although monetary incentives and others may appear to remain constant, the emerging threats imposed by new technology and what was once a seemingly cut and dry motivation bear close monitoring and adjustments to mitigation. For example, in financial gain, the development of various cryptocurrencies adds a new dimension possibly requiring changes to mitigation efforts. Because of the propensity of this new currency being used for illicit payments and the added difficulty in tracking transactions, this new technology changes the landscape of this incentivization tool. What about those who simply invest in this currency? Is this a statement of their character or another facet of their trustworthiness?

Closer to the enterprise was the 2014 US Air Force scandal involving missile workers who cheated on nuclear launch proficiency tests. On the surface, the behavior may be looked at from the perspective of having netted substandard workers or overarching character flaws and thoughts toward "what else would they be willing to shortcut." Opinions vary, but organizations must be careful what they incentivize because it influences behavior. Monetary incentivization may not always be external. If a member's promotion, career, and other job aspects are tied to the test and you add the press toward community and helping one another, then passing is no longer the standard and excelling is the norm, at all costs. This is reminiscent of some issues stemming from the inspection process (discussed briefly later). Units would often go to great lengths to do well on inspections, with competitions and ratings driving behavior (and nonmonetary incentives). Prepping the inspection became like polishing the car before your date. Zero faults and impressing the inspectors took the

importance. Would you really want a unit to "polish" assets or programs before an assessment or do you want them to do great every day?

As motivations evolve, so must the protective and preventive measures employed. Regarding the aforementioned discussion, simply inserting additional or modifying existing screening questions about cryptocurrencies could prevent an issue. Just as physical screening measures combined with authorization, a series of strict processes and procedures to gain access or establish requirements for teams of personnel are low cost, easily implemented measures. But adding technological advances such as readers, entrapment devices, or airport-style screenings can yield additional protection and defeat individuals attempting to enter inappropriately or enter or exit with restricted items. The measures employed can be tailored to the threat. Insider threat mitigation should never remain static. Times of prolonged stagnation can lead to complacency or worse. People change, situations change, and technology changes. Keeping abreast of these changes is imperative. A review comparing HRP to PRAP has occasionally occurred, which is important to refresh the program and see if there are other ways to mitigate insider threats or reduce costs without unacceptable risk. Even if other methods are not adopted, the review provides insight in the total accomplishment of safeguarding our nation.

Added risk through human error can work into any process, but when members become complacent or take shortcuts, the risk can rise to an unacceptable point. Not long after the 2007 incident involving accidental nuclear weapons transport from Minot Air Force Base to Barksdale Air Force Base, US Air Force leaders chartered a group to create processes to ensure no errors or missed indicators in Personnel Reliability Assurance Program (PRAP). The charter specified ignoring any preconceived ideas, past methods, costs, or difficulties. Such a system was developed but was prohibitive in human resource costs and unwieldy. In fact, it was described as unsustainable. In consideration to risk acceptance, a zero-error program is possible but unaffordable in terms of time, money, or management and maintenance. A decision to draw the line or make a tradeoff of acceptance to cost must be made. Less risk equals more cost. In the example, there were easy wins to be gleaned by such a drill. Many low to no cost process improvements could be implemented almost immediately, eliminating many error-prone steps and reducing the probability of shortcuts. The team's priority was to develop a training program for members charged with managing the program but who do not participate in the PRAP. Even with the many changes since, this remains

largely in place today. It establishes a minimum knowledge standard and eliminates a big portion of the learning curve.

Easy wins do not have to be expensive or revolutionary. Some small changes can yield significant benefits with minimal movement and costs. What is necessary is taking an in-depth look at processes, even if they do not appear broken or in need of corrections, without a precipitating significant event. Addressing challenges as they present can also provide opportunities to change for the better. A robust validation program (in DoD, inspections) can identify new issues or risks, determine changes needed, or evaluate changes made to fully understand their impact. This process includes capturing and evaluating data which is used to drive regulatory guidance and ensures it remains viable as the environment evolves.

The benefits of an HRP can be tremendous to an organization. The employees that are part of the program may experience a sense of satisfaction knowing they are part of a team that has been evaluated and assessed and determined to be reliable and trustworthy. The nuclear industry strives to employ the most reliable and trustworthy individuals. It is important that all employees within a nuclear facility clearly understand their role and their influence on coworkers, the environment, and the country. A clear security foundation is vital, and an HRP sets a standard for employees who occupy sensitive positions.

2.2.3 Trustworthiness/Reliability Programs

The first step toward certification is qualification. At the beginning of US military service, a prequalification is conducted to eliminate applicants who would not pass other pertinent requirements for entry in training for nuclear career fields. This is the equivalent to a preemployment screening in the civilian sector. It is important to understand some of the screening is done for entry into and continued military service, such as drug testing with random follow-on tests. What remains are the requirements for the duty position in the specific nuclear work or the security involved, which will be discussed further. From this pool of military inductees, potential workers who meet the initial requirements and test appropriately may enter training in a sensitive position. A more in-depth review of the service entrance requirements is conducted in the member's background, criminal history, financial verification, medical and psychological screening, and many other items. Security clearance review is initiated if

not already started because much of the technical training will involve material requiring certain clearance levels.

Qualifying criteria include a positive attitude toward nuclear weapons duty, dependability, personal integrity, emotional stability, and flexibility in a changing work environment to name a few.[60] Some of the items like allegiance to the United States may be a bit harder to judge initially, but consider the following definition of reliability: "a combination of the traits of integrity, trustworthiness, emotional stability, professional competence, and unquestioned loyalty and allegiance to the United States."[61] The importance of these characteristics requires much consideration to judge the member's suitability. Extremism has come to the forefront of recent news reports. According to a recent *Politico* article, Secretary of Defense Lloyd J. Austin empowered a new group to better screen recruits and those currently serving for extremist behaviors and affiliation.[62] Whether this bears fruit or not remains to be seen, but most agree that it requires a strict definition.

When the ORNL team described the international approach to implementing an HRP, it stressed the graded approach. Ensuring that the approach is designed to address the specific cultural elements of the country and organization, that it is closely aligned with the infrastructure available to operate, and the threats facing the nuclear stakeholders. Questions to consider when determining the stakeholders include the following:

1. What type of facility or information is to be protected?
2. How is access to sensitive information controlled?
3. How are personnel with access to sensitive information controlled?
4. What are the significant local threats to the organization?
5. What are all of the organizations responsible for safety and security of the facility?

[60] US Department of Defense (DoD). *Department of Defense Manual 5210.42, Nuclear Weapons Personnel Reliability Program, Incorporating Change 3.*

[61] US Department of Defense (DoD). *Department of Defense Instruction 5210.42, DoD Nuclear Weapons Personnel Reliability Assurance, Incorporating Change 3.*

[62] Bender, B. "Pentagon Orders New Screening Procedures to Weed Out Extremists." *Politico*, 2021, https://www.politico.com/news/2021/04/09/pentagon-extremism-screening-procedures-480615.

Once these, as well as other organization specific questions are answered, the initial steps within an HRP include an initial evaluation to establish whether an individual can be considered for admittance into an HRP. Research conducted at Oak Ridge National Laboratory (ORNL) on international programs supports using a type of security clearance as a precondition for an individual to be considered for a position that affords the individual access to information or materials. Both the qualifications for eligibility for a security clearance and for access to sensitive materials, information, and physical areas must be determined by the facility or country and should be defined in regulations.[63]

The initial evaluation of a potential employee is the first official check a facility uses to determine if the individual is qualified for employment and willing to be in a position. Negative or unresolvable issues such as arrests, employment concerns, substance use/abuse discovered during this initial evaluation will likely result in a decision not to hire an individual. This initial process is designed to determine if any information exists that shows a pattern of questionable judgment or emotionally unstable behavior. This initial evaluation will include the following components:

- Background check—The initial background check consists of gathering information and evaluating an individual's character, general reputation, personality traits, and lifestyle.
- Initial drug test—In many HRPs, before an individual can be considered for an HRP position, he must successfully pass a drug test. Because drugs can affect employee performance and safety, a positive drug test will eliminate the individual from employment consideration.
- Arrest record/criminal history check—A check with law enforcement will be conducted to determine if the individual has ever been arrested and for what charge. A criminal record may preclude an individual from consideration for a security clearance.
- Credit check—The credit check assesses an individual's financial situation, including loans, bill payments, and indebtedness. This is not just a credit check because the member is not being considered for a loan, but it involves an in-depth look at finances and if there are

[63] Oak Ridge National Laboratory (ORNL). *Roadmap to a Sustainable Human Reliability Program*.

flags of overextending or struggles that reveal a vulnerability. A poor credit history or excessive indebtedness are causes for concern and could prohibit an individual from being granted a security clearance.
- Education verification—This check validates the individual's attendance and graduation from educational institutions and their professional qualifications as indicated on their employment application and resume/curriculum vitae.
- Work history verification—Similar to the education verification, the work history verification validates employment history and reveals if any troubling work issues existed, such as disciplinary issues or termination for cause.[64]

Once employment has really begun in the nuclear enterprise, from training on, reviews and checks become more hidden to the member or behind the scenes. Autonomous checking or flags are set within systems to alert personnel to events or series of issues that may lead to questionable reliability. All this eventually leads to certification. A member is initially certified once, but they may need to be recertified under transfer to another unit or permanent change of station. Perhaps the largest benefit is arguably derived from the final point of certification when the certifying official sits with the member, given all the screening results, to ultimately rule on certification. This last step allows the certifying official the opportunity to discuss details of any findings, to hear any undisclosed information, and to review what used to be called the "spirit and intent" of the PRAP. This review is comprehensive, but it does not end at certification—the process is ongoing. Called "continuous evaluation," the requirements are set to "mitigate risks and protect the nuclear deterrent from insider threats."[65] The constant monitoring by an individual with direct knowledge of everything in the member's life, on and off duty, forms one of the backbone requirements of PRAP mitigation.

An employee may be subject to an annual and continuous evaluation process to ensure sustained eligibility for a sensitive position. As part of this annual and continuous process, any of the initial checks or tests may

[64] Oak Ridge National Laboratory (ORNL). *Roadmap to a Sustainable Human Reliability Program*.

[65] US Department of Defense (DoD). *Department of Defense Manual 5210.42, Nuclear Weapons Personnel Reliability Program, Incorporating Change 3*, 2018.

be reevaluated, and the HRP-certified employee will be monitored and evaluated based on the following criteria:

- **Unusual behavior:** Supervisors, workers, and managers should be trained on identification of unusual behavior, its possible causes, and ways to distinguish meaningful versus insignificant unusual behavior. All employees should be trained to make accurate observations and following appropriate reporting procedures. With this training in place, managers, supervisors, and workers will be able to effectively monitor behavior in the workplace and alert the proper authorities if unusual behavior is observed.
- **Supervisory review:** In most HRPs, supervisory reviews are required every 12 months regarding the suitability of employees to remain HRP-certified and continue performing HRP work. Supervisors are trained to evaluate the behaviors and performance of their employees to identify security or safety concerns.
- **Medical appraisal:** The HRP model requires employees to undergo an evaluation of their health status and health risk factors through a medical history review, physical examination, laboratory tests, and psychological and psychiatric evaluations. These screenings should be country-specific and take cultural aspects into consideration. If records are inadequate or questions arise, medical examinations may be scheduled to include psychological evaluation and testing (DoD 2018b). Health insurance claims may reveal and lead to reviews of care.
- **Management decision:** A designated senior manager evaluates the individual's supervisory review, medical appraisal, and personnel records related to any security or safety concerns and makes a recommendation to approve or disapprove the individual for continuation in the HRP. The senior manager makes this recommendation to the certifying official.
- **Certifying official review:** The certifying official acts as the final reviewer of all information gathered through the continuous evaluation process and makes the final determination on certification or decertification.
- **Training:** HRP-certified individuals must complete both initial and annual training, which include understanding the need for an HRP, insider risks, nuclear security awareness, and the employee's responsibilities.

- **Random drug and alcohol testing:** The HRP generally requires certified employees to undergo random drug and alcohol testing. The abuse of alcohol or use of illegal drugs can cause physical and mental impairment that impact the safety and security of the individual, coworkers, the institution/facility, and national security. Employees with drug and/or alcohol problems may be more susceptible to influence by outsiders and may compromise sensitive information.[66]

Figure 2.1 depicts the initial evaluation, continuous evaluation, and the annual evaluation elements, as well as the process in which the organization may determine the trustworthiness of a staff member. An important portion to remember is the self-reporting mentioned earlier.

This self-reporting forms the second backbone of PRAP/HRP mitigation. Self-reporting is indoctrinated from the very beginning, and its importance cannot be minimized. The member is taught to always address areas of concern about themselves with their supervisors and leadership. All personnel are required to report these factors to their certifying official or commander whether about themselves or their coworkers.

This information may be a lot to digest, so the DoD provided a guide for determinations and adjudication of this data to make a judgement about the trustworthiness of the individual. The guide is incorporated in *DoD Manual 5210.42, Nuclear Weapons Personnel Reliability Program, Incorporating Change 3* and gives considerations and mitigation for suitability factors to aid decisions to certify or continue member's certification. Contractors (if used) are no different other than if determinations are made of unsuitability, the contract agent need only be notified and they are removed.

2.2.4 Mitigating Insider Threats with Technical Measures

Technical measures are not limited to those mentioned earlier, and many others are geared directly to reliability programs. Most have knowledge of polygraph testing and the confines or fallibility inherent with it. Even with modern methods and equipment, there are limits to the accuracy of

[66] Oak Ridge National Laboratory (ORNL). *Roadmap to a Sustainable Human Reliability Program*.

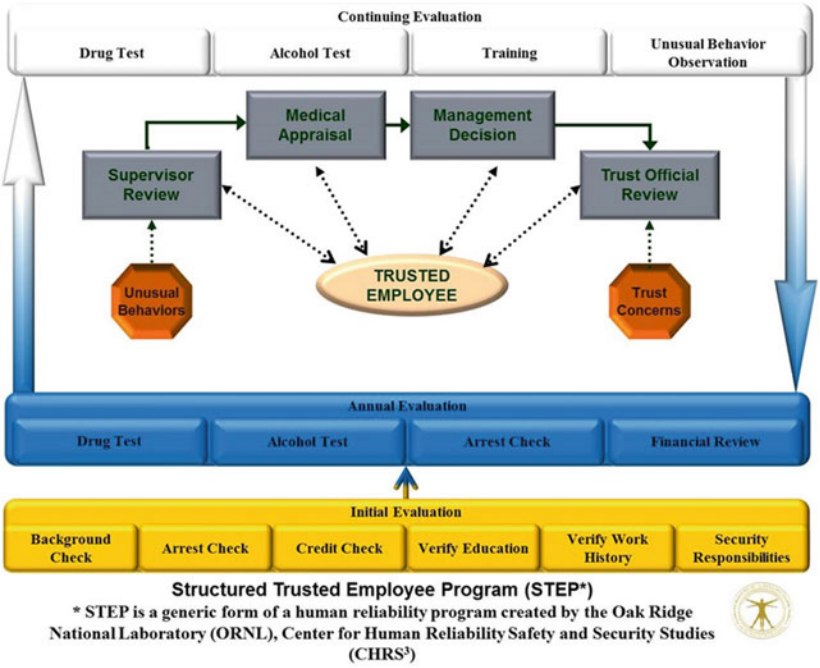

Fig. 2.1 STEP process[67] (*Note* STEP is a generic form of a human reliability program created by the Oak Ridge National Laboratory [ORNL], Center for Human Reliability Safety and Security Studies [CHRS]^3)

information obtained. One area has evolved significantly, and it is aimed directly at the technology which spurred it. Applying advanced cyber techniques allows for reviewing and screening large amounts of data including the potential to reflect on social media content. Although social media may provide a previously unknown look at the member, it also presents a vulnerability because of social media attacks and potential exploitation

[67] Coates, C. W., and G. R. Eisele. Roadmap to a Sustainable Structured Trusted Employee Program (STEP), 2013, https://info.ornl.gov/sites/publications/files/Pub45049.pdf.

of members.[68] This consideration should lead to policies on its use and restrictions. Although social media is a hard discussion point currently and not fully resolved at the time of this publication, the technical capabilities work for financial screening and ad hoc notifications for a myriad of reliability assurance measures.

One of the interesting innovations comes in the form of profiling. Highlighted by recent studies in radicalization and spurred by extremist concerns, University of Maryland's Study of Terrorism and Responses to Terrorism Research Brief from the Profiles of Individual Radicalization in the United States on QAnon offenders is a good example.[69] In the report, pre- and post-January 6, 2021, US Capitol attack activities are compared, showing a baseline related to data from the riot.[70] The same methods can be used across a multitude of groups to identify commonalities and further isolate specific indicators of negative behavior. Using this profile assessment provides an advantage over the standard insider threat indicators common across the enterprise (e.g., coworker performance decline, questions outside of scope, and requests for sensitive data).

Not everything needs this level of technical measure. One of the simplest measures and the final "backbone" piece is a basic mitigation called the "two-person" team, which pairs one fully certified member with others.[71] This effectively eliminates the lone insider and affords detection by others who are "always watching." Extensive, and often costly, measures are not always the best. Beginning with basic procedures and actions and then adding technological enhancements can net better results and at less cost.

[68] Cyware. Analyzing the Relationship between Social Media and Cyber Threats, 2021, https://cyware.com/news/analyzing-the-relationship-between-social-media-and-cyber-threats-47954e5b.

[69] Jensen, M., and S. Kane. "QAnon Offenders in the United States." University of Maryland, National Consortium for the Study of Terrorism and Responses to Terrorism, 2021, https://www.start.umd.edu/sites/default/files/publications/local_attachments/START%20QAnon%20Research%20Brief_3_23.pdf.

[70] Jensen, M., and S. Kane. "QAnon Offenders in the United States." University of Maryland, National Consortium for the Study of Terrorism and Responses to Terrorism, 2021, https://www.start.umd.edu/sites/default/files/publications/local_attachments/START%20QAnon%20Research%20Brief_3_23.pdf.

[71] US Department of Defense (DoD). *Department of Defense Manual 5210.42, Nuclear Weapons Personnel Reliability Program, Incorporating Change 3*, 2018.

2.2.5 Conclusion

In summary, mitigating insider threats to the nuclear community poses a unique and challenging problem, though a problem that is not insurmountable. It takes a community to recognize behaviors, changes in behaviors, and an awareness of what is required by staff with the privilege of working within the nuclear industry. Individuals with access to nuclear information and materials must appreciate the importance of self-declaration when they either commit an error or require notice to the organization based on a lifestyle change. Not all organizations will need to adopt all the measures identified in this paper. An organization will need to evaluate what may work best for it based on culture, infrastructure, and the level of threat. For example, a research institution that is introducing small amounts of nuclear material, may take a graded approach to this process and only apply elements that are appropriate to the country's laws and regulations. Also, it is imperative to recognize that being part of the community of practice is particularly important. This community can learn a great deal from one another, and the provided resources may allow for a platform to share lessons learned and experiences that may benefit organizations new to the nuclear community as well as organizations that have a history of operations.

References

Balatsky, G. and Duggan, R. *Nonproliferation, Nuclear Security, and the Insider Threat*. Office of Scientific and Technical Information, June 2012. https://www.osti.gov/servlets/purl/1294289.

Bender, B. 2021. "Pentagon Orders New Screening Procedures to Weed Out Extremists," *Politico*. Retrieved from https://www.politico.com/news/2021/04/09/pentagon-extremism-screening-procedures-480615.

Bunn, M. "Incentives for Nuclear Security," In Proceedings of the Institute for Nuclear Materials Management 46th Annual Meeting, Phoenix, Arizona, July 15, 2005. https://scholar.harvard.edu/files/matthew_bunn/files/incentives_for_nuclear_security.pdf.

Bunn, M. "Scenarios of Insider Nuclear Threats—And Steps to Strengthen Protection," Nautilus Institute Workshop on Reducing the Risk of Nuclear Terrorism and Spent Fuel Vulnerability in East Asia, January 21–22, 2017. https://scholar.harvard.edu/files/matthew_bunn/files/japan-insider-scenarios_2017.pdf.

Bunn, M. and Sagan, S. "A Worst Practices Guide to Preventing Leaks, Attacks, Theft, and Sabotage," 27th International Training Course, Sandia National

Laboratories, May 17, 2018. https://scholar.harvard.edu/files/matthew_bunn/files/sandia_insider_threats_presentation_2018.pdf.

Bunn, M. and Sagan, S. *A Worst Practices Guide to Insider Threats: Lessons from Past Mistakes*. Cambridge, MA: American Academy of Arts and Sciences, 2014. https://www.amacad.org/sites/default/files/publication/downloads/insiderThreats.pdf.

Bunn, M. Malin, M., Roth, N. and Tobey, W. "Key Steps for Continuing Nuclear Security Progress," at an "International Conference on Nuclear Security: Commitments and Actions," International Atomic Energy Agency, Vienna, Austria, September 12, 2016. https://scholar.harvard.edu/files/matthew_bunn/files/bunn_key_steps_for_continuing_nuclear_security_progress.pdf.

Bunn, M. *Scenarios of Insider Threats to Japan's Nuclear Facilities and Materials—And Steps to Strengthen Protection*. NAPSNet Special Reports, November 02, 2017. https://scholar.harvard.edu/files/matthew_bunn/files/bunn_scenarios-of-insider-threats-to-japans-nuclear-facilities-and-materials-and-steps-to-strengthen-protection.pdf.

CFR Parts 710, 711, and 712. 2002. "Human Reliability Program," *Code of Federal Regulations*. Vol. 67, No. 137, Washington, DC.

Chapman, G., Downes, R., Eldridge, C., Hobbs, C., Lentini, L., Moran, M., Muti, A., and Salisbury, D. *Security Culture: An Educational Handbook of Nuclear & Non-nuclear Case Studies*. Centre for Science & Security Studies, King's College London, August 2017. https://www.kcl.ac.uk/csss/assets/security-culture-handbook.pdf.

Coates, C. W., and G. R. Eisele. 2013. *Roadmap to a Sustainable Structured Trusted Employee Program (STEP)*. ORNL/TM-2013/303. Oak Ridge, TN: Oak Ridge National Laboratory. Retrieved from https://info.ornl.gov/sites/publications/files/Pub45049.pdf.

Computer and Information Security Advisory Group (CISAG). "Guidelines for Work from Home." Department of Atomic Energy, May 14, 2020. https://iopb.res.in/news/wp-content/uploads/2020/05/CISAG_Guidelines_for_Work_from_Home_14052020.pdf.

CRDF Global. "The Enduring Need to Protect Nuclear Material from Insider Threats," April 26, 2017. https://www.crdfglobal.org/insights/enduring-need-protect-nuclear-material-insider-threats/.

Cyware. 2021. *Analyzing the Relationship between Social Media and Cyber Threats*. Retrieved from https://cyware.com/news/analyzing-the-relationship-between-social-media-and-cyber-threats-47954e5b.

Global Centre for Nuclear Energy Partnership. "School of Nuclear Security Studies (SNSS)." Department of Atomic Energy. https://gcnep.gov.in/schools/snss.html.

Guenther, R., Lowenthal, M., Nagappa, R., and Mancheri N. *India-United States Cooperation on Global Security: Summary of a Workshop on Technical*

Aspects of Civilian Nuclear Materials Security. Washington, DC: The National Academies Press, 2013. https://indianstrategicknowledgeonline.com/web/India-United%20States%20Cooperation%20on%20Global%20Security.pdf.

Hobbs, C. and Pope, N. "Insider Threat Case Studies at Radiological and Nuclear Facilities," LA-UR-15-22642, Los Alamos National Laboratory, 2015. https://permalink.lanl.gov/object/tr?what=info:lanl-repo/lareport/LA-UR-15-22642.

INAS. "Kaiga Incident: Wake Up Call or Tempest in Teapot?" *The Hindu*, December 3, 2009. https://www.thehindu.com/sci-tech/energy-and-environment/Kaiga-incident-Wake-up-call-or-tempest-in-teapot/article16851321.ece.

International Atomic Energy Agency (IAEA). *Assessing Behavioural Competencies of Employees in Nuclear Facilities,* IAEA-TECDOC-1917, 2020a. Vienna: International Atomic Energy Agency.

International Atomic Energy Agency (IAEA). *Preventive and Protective Measures against Insider Threats*. IAEA Nuclear Security Series No. 8-G (Rev. 1), 2020b. Vienna: International Atomic Energy Agency.

International Atomic Energy Agency (IAEA). *Safety and Security of Radioactive Sources: Maintaining Continuous Global Control of Sources throughout Their Life Cycle*. Proceedings of an International Conference, Abu Dhabi, United Arab Emirates, October 27–31, 2013. International Atomic Energy Agency: Vienna, 2015. https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1667_web.pdf.

International Atomic Energy Agency (IAEA). *Self-Assessment of Nuclear Security Culture in Facilities and Activities*. IAEA Nuclear Security Series No. 28-T, 2017. https://www-pub.iaea.org/MTCD/Publications/PDF/PUB1761_web.pdf.

Jensen, M., and S. Kane. 2021. "QAnon Offenders in the United States." University of Maryland, National Consortium for the Study of Terrorism and Responses to Terrorism. Retrieved from https://www.start.umd.edu/sites/default/files/publications/local_attachments/START%20QAnon%20Research%20Brief_3_23.pdf.

Khripunov, I. and Holmes, J. *Nuclear Security Culture: The Case of Russia*. Center for International Trade and Security, University of Georgia, 2004. https://www.nti.org/wp-content/uploads/2021/09/analysis_cits_111804.pdf.

Kutuvan, J. "Building Robust Nuclear Security Culture in Nuclear Research Centers," IAEA, https://www.iaea.org/sites/default/files/17/11/cn-254-kutuvan-presentation.pdf.

Ministry of External Affairs. *Nuclear Security in India*. 2014. https://www.mea.gov.in/Images/pdf/Brochure.pdf.

National Nuclear Security Administration. *Addressing the Insider Threat*, U.S. Department of Energy. https://www.internationaltransportsecurity.org/sartss-2021/wp-content/uploads/sites/6/2021/03/SARTT-Insider-Threat-GMS-3.4.21_skr.pdf.

Oak Ridge National Laboratory (ORNL). *Roadmap to a Sustainable Human Reliability Program*. ORNL/TM-2016/, 2016. Oak Ridge: Oak Ridge National Laboratory.

PIB Delhi. "Cyber Attacks on Indian Nuclear Power Plants," Department of Atomic Energy, November 28, 2019. https://pib.gov.in/PressReleasePage.aspx?PRID=1594020.

PIB Delhi. "Cyber Security Audit KKNPP," Department of Atomic Energy, November 27, 2019. https://pib.gov.in/PressReleasePage.aspx?PRID=1593768.

Sandia National Laboratories. "27. Introduction to Nuclear Security Trustworthiness Programs," 27th International Training Course, Albuquerque, New Mexico, USA, April 30–May 18, 2018. https://share-ng.sandia.gov/itc/assets/27_introduction-to-nuclear-security-trustworthiness-programs.pdf.

Singh, R.K. "Safety and Security Aspects of Radioactive Material During Transport," International Atomic Energy Agency, 2011. https://inis.iaea.org/collection/NCLCollectionStore/_Public/43/014/43014475.pdf.

The Economic Times. "Sabotage in Kaiga: Tritium Added to Drinking Water." November 30, 2009. https://economictimes.indiatimes.com/news/politics-and-nation/sabotage-in-kaiga-tritium-added-to-drinking-water/articleshow/5282881.cms.

TNN. "Mansoor Peerbhoy: An Unlikely Jihadi, He Shows No Remorse," *The Times of India*, October 7, 2008. https://timesofindia.indiatimes.com/mansoor-peerbhoy-an-unlikely-jihadi-he-shows-no-remorse/articleshow/3568833.cms.

TNN. "No Threat to Goa from Kaiga Plant: S Goa Official," *The Times of India*, August 6, 2011. https://timesofindia.indiatimes.com/city/goa/no-threat-to-goa-from-kaiga-plant-s-goa-official/articleshow/9499153.cms.

US Department of Defense (DoD). *Department of Defense Directive 5205.16, The DoD Insider Threat Program, Incorporating Change 2*. No. 5205.16 USD(I), 2017. Retrieved from http://www.esd.whs.mil/.

US Department of Defense (DoD). *Department of Defense Directive 3150.02, DoD Nuclear Weapons Surety Program, Incorporating Change 4*. No. 3150.02 USD(A&S), 2018a. Retrieved from http://www.esd.whs.mil/.

US Department of Defense (DoD). *Department of Defense Manual 5210.42, Nuclear Weapons Personnel Reliability Program, Incorporating Change 3*. No. 5210.42 USD(A&S), 2018b. Retrieved from http://www.esd.whs.mil/.

US Department of Defense (DoD). *Department of Defense Instruction 5210.42, DoD Nuclear Weapons Personnel Reliability Assurance, Incorporating Change 3*. No. 5210.42 USD(A&S), 2019. Retrieved from http://www.esd.whs.mil/.

US Department of Energy. *Department of Energy Insider Threat Program*, *DOE Order O 470.5* (DOE Order), 2014. Retrieved from: https://www.directives.doe.gov/directives-documents/400-series/0470.5-BOrder/@@images/file.

US Nuclear Regulatory Commission. *Regulatory Guidance 5.77 Insider Threat Mitigation Program*, 2009. Retrieved from https://www.nrc.gov/docs/ML1521/ML15219A609.pdf.

World Institute for Nuclear Security (WINS). International Best Practice Guide, 3.4 Managing Internal Threats. V. 2.1, 2015.

World Nuclear News. "ENEN Launches Master's Course on Nuclear Safeguards," *World Nuclear News*, 2021. Retrieved from https://www.world-nuclear-news.org/Articles/ENEN-launches-Masters-course-on-nuclear-safeguards.

Zaidi, S. and Singh, B. "The Making of A Terrorist," *Rediff.com*, July 10, 2017. https://www.rediff.com/news/special/the-making-of-a-terrorist/20170710.htm.

CHAPTER 3

The Role of Organizational Culture in Nuclear Security

Narendra Kumar Joshi, Cristina F. Lussier, and Karen Kaldenbach

3.1 An Indian Perspective

Narendra Kumar Joshi

In India, various facilities and organizations such as educational institutions, hospitals, industries, nuclear power reactors, nuclear fuel complexes and nuclear waste treatment facilities use radioactive materials and radiation sources. Each organization has its own culture and governing structure. Effective nuclear security culture is characterized by compliance

N. K. Joshi
Mody University, Laxmangarh, India

C. F. Lussier (✉)
Defense Threat Reduction Agency, Fort Belvoir, VA, USA
e-mail: cristina.f.lussier.civ@mail.mil

K. Kaldenbach
Oak Ridge National Laboratory, Oak Ridge, TN, USA

S. P. Kapur et al. (eds.), *The Challenges of Nuclear Security*, Initiatives in Strategic Studies: Issues and Policies,
https://doi.org/10.1007/978-3-031-56814-5_3

with rules, regulations, procedures, and constant vigilance and a proactive questioning attitude on the part of personnel. The Indian nuclear security architecture is mainly based on five pillars: National legal provisions (Atomic Energy Acts and Rules-DAE) in consonance with IAEA guidelines; the regulator; the Atomic Energy Regulatory Board, which stipulates standard operating procedures; the security and intelligence agencies in charge of threat assessment and physical protection; and the personnel with the responsibility of oversight or observance, surveillance and technology for the detection, delay, and response approach. Radioactive material is much more likely to go out of regulatory control than nuclear material, particularly when it is used in educational institutions, and in industrial and medical applications. Depending on the organization, physical, and cyber security arrangements vary and security risk and vulnerabilities change. This chapter provides details of Indian physical security, cybersecurity, and emergency response system in an effort to apprise the security culture prevalent in the Indian civil nuclear facilities. The chapter then concludes with a few weaknesses in India's nuclear security programmes, which become particularly important as adversaries refine and evolve their capabilities and tactics, and new threat scenarios emerge. These threats require India to keep pace with evolving security systems and adapt to changing threat environments.

All stakeholders in the field of nuclear science and technology need a good understanding of relationships and interfaces among safety, security, and safeguards (3S). It will benefit all: designers and operators, shippers and carriers of nuclear material, national and international authorities, researchers and academicians, and the world population at large. Nuclear employees, the public and the environment are all subject to threats arising from hazards related to both safety and security. Nuclear safety can be defined as the means to protect people or the environment from accidents and human error. Similarly, nuclear security refers to the means to protect nuclear and high hazard radioactive material from unauthorized access, theft, diversion, sabotage, or other malicious acts. Therefore, safety threats entail accidents due to system failure, human error, or natural disaster whereas security threats may include terrorism due to sabotage, external attack, or malicious actions by insiders. In 2008, the International Atomic Energy Agency (IAEA) published the NSS Implementing

Guide on Nuclear Security Culture.[1] The guide defines the concept and characteristics of nuclear security culture while describing the roles and responsibilities of institutions and individuals entrusted with a function in the security regime. The IAEA Technical Guidance Self-Assessment of Nuclear Security Culture in Facilities and Activities was finalized and released by the agency in November 2017.[2]

This chapter focuses on India's approach to security culture in the nuclear security realm. Following an introduction of basic tenets of culture, the second section details the nuclear security management structure within nuclear facilities by identifying the roles, responsibilities, and accountability within Indian facilities. The section also assesses the security culture as prevalent in the organisation, the reporting of security incidents, and personnel reliability programmes that aid an effective security culture. The third section examines the Indian approach by studying the key legislations, physical and cyber security measures, and emergency response mechanisms.

3.1.1 Basics Aspects of Culture

Many scholars use the word "culture" to explain a variety of phenomena, but there is no unanimously accepted definition. From a sociological perspective, the four basic aspects of culture are beliefs, values, attitudes, and behaviour.[3] National culture is a set of shared beliefs, assumptions, and modes of behaviour derived from common experiences and accepted narratives that shape collective identity and determine appropriate ends and means for achieving specific objectives.[4] **Beliefs** consist of ideas that

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

[2] International Atomic Energy Agency. *Self-Assessment of Nuclear Security Culture in Facilities and Activities: Technical Guidance*. IAEA Nuclear Security Series No. 28-T (Vienna: IAEA, 2017).

[3] Kerry M. Kartchner, "Strategic Culture and WMD Decision Making," in Jeannie L Johnson, Kerry M. Kartchner, and Jeffrey A. Larsen, ed., *Strategic Culture and Weapons of Mass Destruction* (New York: Palgrave Macmillan, 2009), p. 57; E. H. Schein, *Organizational Culture and Leadership*, 5th Edition (Hoboken, NJ: Wiley, 2017).

[4] Marc Schabracq, *Changing Organizational Culture: The Change Agent's Guidebook* (Chichester, UK: Wiley, 2007); John Kotter, *Leading Change* (Boston, MA: Harvard Business School Press, 1996); Igor Khripunov, *Nuclear Security Culture: The State of Play*, INSEN text book, June 2018.

each of us accept as true. We have beliefs about all areas of our lives, from religion and morality to economics and society. We are not born with beliefs; rather, they are our deep-seated, personal responses to life experiences and the backgrounds in which we are raised. **Values** are global abstract principles that serve as guiding principles for our lives. Examples include freedom, community, honesty, equality, learning, and perseverance. **Attitudes** arise from an inner framework built upon our values and beliefs; they also have an element of emotion. Developed over time, attitudes form the basis of our likes, dislikes, and judgements. Our attitudes trigger an emotional, verbal, behavioural, and/or mental response to a task or person based on our internal belief system.

Behaviour is the ultimate, tangible demonstration of our values, beliefs, and attitudes. For example, if an employee of nuclear organization **believes** that nuclear security plays a fundamental role in protecting the safety of their organization, they might hold such **values** as: Security is the responsibility of every person in the organization including me. Strong security is essential to an organization's overall success, not an impediment to it. They might have such **attitudes** as: the work performed by security professionals in the organization is important. Teamwork is critically important when resolving both safety and security matters. And they might exhibit such behaviours as: proactively seeking to learn more about the threats an organization faces and conscientiously adhering to all security procedures and requirements. These are all indicators of a positive nuclear security culture. Identifying those attitudes and beliefs, determining how they manifest themselves in the behaviour of security personnel, and transcribing them into formal working methods is the key to a culture that yields good outcomes.

3.1.2 Organizational Culture

Numerous constituent factors contribute to national culture and make it distinctly different from one country to another. National cultural values are learned early, held deeply, and change slowly over the course of generations. Organizational culture, on the other hand, is comprised of broad guidelines that are rooted in organizational practices learned on the job. An organization is a social system where its members are involved in it only during working hours and when quitting the job, they leave it behind. Organizational culture has more common international traits due to globalized trade and communication. IAEA methodologies for

nuclear safety and nuclear security culture are based on Edgar Schein's widely recognized principles of organizational culture.[5] The word culture here may be defined as "a pattern of shared basic assumptions that the group learned as it solved its problems of external adaptation and internal integration that has worked well enough to be considered valid and, therefore, to be taught to new members as the correct way to perceive, think, and feel in relation to those problems."[6] Security, in a general sense, refers to the degree of protection against danger, damage, loss, and criminal activity. The IAEA defines nuclear security culture as: "The assembly of characteristics, attitudes and behaviours of individuals, organizations, and institutions which serves as a means to support and enhance **nuclear security**."[7] The role of organizational culture plays a significant role in contributing to higher standards of performance, productivity, safety, security, compliance, and personnel discipline.

Effectiveness is the rationale behind efforts to bolster organizational culture and subsequently, security culture. Organizational effectiveness demands the agility and determination to reorient security standards when new risks emerge in internal and external environments. The effectiveness can be quantified by two major parameters which give rise to four main organizational cultural clusters: clan, adhocracy, market, and hierarchy.[8] The four clusters of organizational culture are helpful in determining a management mechanism to promote nuclear security culture in specific organizations. The first parameter measures an organization's flexibility, discretion, and dynamism. Some organizations are viewed as effective if they change and adapt readily. A measure of disorder characterizes their operations. Others are considered effective if they are stable, orderly, and mechanistic. Most government agencies and business conglomerates fall into this category. The second parameter measures an organization's orientation. Organizations at one end of the continuum are

[5] Schein, Edgar, *The Corporate Culture and Leadership*, 3rd ed. (San Francisco, CA: Jossey-Bass, 2004).

[6] Igor Khripunov, "Nuclear Security: Attitude Check," Bulletin of the Atomic Scientists, January 2005, 10.2968/061001013.

[7] K. Bachner, *Overview of Nuclear Security Culture*. BNL-212323–2019-IN, November 2019. Non-proliferation and National Security Department, Brookhaven National Laboratory, USA.

[8] Kim S. Cameron and Robert E. Quinn, *Diagnosing and Changing Organizational Culture*, rev. ed. (San Francisco, CA: Jossey-Bass, 2006).

internally oriented, highly integrated, and unified. At the other end are organizations characterized by external orientation, differentiation, and rivalry.

Below are brief characterizations of each of the four cultural clusters with an emphasis on security-relevant traits:

- **Clan Culture**: The organization is held together by loyalty or tradition and commitment levels are high. The organization emphasizes long-term benefits of human resource development and attaches great importance to cohesion and morale. It may be seen as a friendly place to work where people share a lot about themselves. The organization also places a premium on teamwork, participation, and consensus—educational and training institutions fall in this category.
- **Hierarchy Culture:** Formal rules and policies hold the organization together. The long-term concerns are stability and performance, viewed as the product of efficient and smooth operations. Management practices emphasize predictability. The leaders pride themselves on being good, efficiency-minded coordinators and organizers. It is considered as a very formal structured place to work. Procedures govern what people do and how to do it. Security awareness has a better chance to make inroads in a hierarchical culture. Regulatory authorities represent a good example of this type of organizational culture.
- **Adhocracy Culture:** The glue that holds the organization together is commitment to experimentation and innovation. It is viewed as a dynamic, entrepreneurial, and creative place to work, a place where people consistently stick their necks out and take risks. The leaders are considered to be innovators and risk-takers. The organization encourages individual initiative and freedom. However, diversity and individualism of members may pose obstacles in the way of security culture promotion.
- **Market Culture**: The glue that holds the organization together is an emphasis on winning. Reputation and success are common concerns. The organizational style is hard-driving competitiveness. It is a result-oriented organization. The major objective is to get the job done. People are competitive and goal oriented. Often, the vision of success may outweigh security considerations.

Natural radioactive elements are a part of our environment and radioactivity is a natural phenomenon. There are numerous beneficial applications of radioactive elements (radioisotopes) and radiation, starting from power generation to usages in medical, industrial, and agriculture applications. Various facilities and organization are using radioactive sources such as educational institutions, hospitals, industries, nuclear power reactors, nuclear fuel complexes, and nuclear waste treatment facilities. Each organization has its own culture and governing structure. For example, a regulatory authority predominately belongs to the hierarchy cluster, a nuclear physics university to clan, an advanced research institution to adhocracy and finally, a manufacturer and supplier of nuclear technology to market. Any optimal cluster combination would depend on the organization's missions, profiles, workforce, and other additional factors. Most organizations with nuclear infrastructure can benefit from the proposed methodology by developing an optimal and balanced combination of all four clusters.

3.1.3 Nuclear Security Culture

Nuclear security culture is a subset of organizational culture and draws on its experience. It is designed to improve the performance of the human component and makes its interface with security technologies and regulations smoother and more effective. Security culture is applicable to the entire workforce and can be an effective tool to address both unintentional and intentional breaches. Security culture connotes not only the technical proficiency of the people, but also their awareness of security risks and motivation to follow established procedures, comply with regulations, and take the initiative when unforeseen circumstances arise. The organization must allocate sufficient financial, technical, and human resources to implement the assigned security responsibilities. It must ensure that all security personnel have the necessary qualifications and that the qualifications are maintained by an appropriate training and human-capacity development program. Personnel must have the necessary equipment, adequate work areas, up-to-date information, and other forms of support to carry out their security responsibilities.

Nuclear Security Culture has five distinct components that are both unobservable and observable: beliefs and attitudes, principles for guiding decisions and behaviour, management systems, leadership behaviour, and personnel behaviour. The most important assumption for the nuclear

security culture of an organization is that there is a credible insider and outsider threat and that nuclear security is important. In other words, there must be an underlying assumption of vulnerability that permeates the whole workforce, not the organization's security specialists alone.

3.1.4 Bridging the Gap Between Nuclear Safety and Security Culture

Safety and security responsibilities involve individuals from diverse backgrounds and experiences. Thus, bridging the gap between safety and security may be a challenging process. Scientists and engineers who are engaged in nuclear safety place a high value on creativity, skepticism, problem-solving, and analysis. Security personnel, by contrast, have military or police backgrounds and place high value on discipline, duty, courage, and commitment. One group, then, naturally seeks compliance with the rules, whereas the other group naturally seeks to change, question, and modify them. And one group places a high value on secrecy and discretion—need to know—whereas the other places a high value on openness and sharing of mistakes and lessons learned—need to share.

A need-to-share approach to security is better than the need-to-know approach. Such an approach achieves a much better balance between the risk of malicious or unintended disclosure and the risk of failing to share information that could help avert a threat or event. Need to share doesn't necessarily mean that an organization divulges classified information on the measures it is taking to counter threats. It does, however, mean that the Security Department shares more information, more openly, with their cross-functional counterparts within the organization. This not only encourages a strong security culture and growing levels of trust and goodwill, but also increases overall security.

Although guns, guards, and gates remain an important feature of nuclear security implementation, the growing complexity of security threats has required a radical reappraisal of the traditional approach toward security. The threat of knowledgeable insiders and cyberattacks requires high levels of technical knowledge about nuclear facilities that are not generally present in security departments. Real symbiotic relationships have to be created between security and safety teams to address a real challenge that cannot be solved by the partners acting alone. Teamwork is the only way to make security more effective. In fact, safety and security professionals should conduct joint vulnerability assessments. Scientists

and engineers should support and contribute to security objectives rather than feeling like they are simply the passive *victims* of security rules and regulations. Similarly, security professionals should be seen as full partners with their peers in the safety community, not subordinate to it (or vice versa). Due to the threat and regulatory environment, the competency framework for safety and security professionals needs to be modified to ensure that both have the necessary knowledge, skills, and attributes to work together as a unified team.

3.2 Nuclear Security Management Structure of the Organization

The organizational level has three dimensions—a facility, its management, and personnel—each with distinct roles and responsibilities to build and sustain a robust nuclear security culture. The belief that managing a complex nuclear security program simply involves the management of guns, guards, and gates is both simplistic and outdated. An operating facility has full responsibility for nuclear security in all activities under its jurisdiction. **The organization must define roles, responsibilities, and accountability for each level**, including security and other interfaces. **Management systems must be put in place for each security function** to define expectations, implement and maintain processes, measure progress, assess compliance, improve performance based on experience, and manage change.

3.2.1 Roles, Responsibilities, and Accountability at Each Level of the Organization

Organisations should have in place a nuclear security policy statement that declares a sound commitment to quality of performance in all nuclear security activities. As part of this process, they should have an effective security risk assessment process and accept threat as a baseline for site security and ensure that the organisation and its employees understand the security threat and risks. Organisations should set security competence standards and build them into the human recruitment processes. They should also ensure competence on company boards with regards to security and have ownership control of security resources. Organisations should identify areas of performance for improvement (or to sustain excellent performance) and develop key point indicators for the smooth

functioning of business. They must benchmark performance periodically and work collaboratively with other organisations in supporting the development of good industry practice. All the above factors are to ensure that appropriate information and advice is available for all levels with the breadth of competence to interpret it and take actions accordingly.

Organisational management systems should ensure that correct information is fed into the governance processes. Organisations should have systems, processes, and competence to deliver threat information to all employees tailored to their security clearance and their role. They should also have an effective security risk register and a system for communicating the risks. These risks should feed into training and development. Organisations should have a system of self-assessment in place to maintain motivation, leadership, and security culture in general. As part of this process, they should also promote security responsibility from the executive level. It should integrate security expectations into normal business and translate objectives and good practice into local policy and procedures. Management should be provided resources to enable communication of expectations to the workforce and to check understanding of rules. Management should have proactive and reactive ability to ensure individual accountability and use internal and external resources to review success of initiatives and challenges. Management should take action against individuals when appropriate (rehabilitation as well as punishment) and communicate to show that transgressors have been dealt with. The company board should monitor and oversee the performance of managers and executives. They must also benchmark performance periodically and work collaboratively with other organisations in supporting the development of good industry practice.

All personnel should understand their part in ensuring that security threats are controlled and managed and all board members, senior executives, and managers should take leadership roles with regard to security. All personnel should understand security performance and expectations, participate in improvement activities, and report events and matters in accordance with security regulations. Individuals should be confident about how a 'whistle blowing' process operates and be able to access evidence that shows a fair reporting culture. All personnel should use security information responsibly to manage/mitigate and improve performance and understand the consequence of misuse. All personnel should

understand security expectations and strive to achieve associated standards. They should also participate in improvement activities, encourage others, and report security events in accordance with regulations.

Role-model managers influence culture throughout their organization with their leadership style, management practices, and personal behaviour. By employing incentives and disincentives at their disposal, managers establish patterns of behaviour, alter the physical environment, and foster an effective nuclear security culture by ensuring that people understand that a credible threat exists and that nuclear security is important. Managers need to encourage personnel to report any event that could affect nuclear security. Though security is a concern for everyone in a nuclear facility, the personnel specifically responsible (e.g., protective forces and security guards) have to be well-trained, rewarded, and kept motivated. These individuals must be allowed career opportunities as well as redeployment possibilities in order to maintain the workforce and competence.

3.2.2 Security Culture Assessment

Security culture assessment plays a key role in developing and maintaining an awareness of the strengths and weaknesses of organizational culture and nuclear security culture as its subset. Security culture assessments have distinct features compared to a traditional audit or performance evaluation: it is a learning curve rather than a checklist of expectations. Threat assessment lies at the heart of performance-based security. It involves complex risk and vulnerability analysis, as well as analysis of possible consequences. Both nuclear safety and security need to be integrated to assist with coordination to effectively protect people and the environment. It can be helpful to use the ARCI Technique, which is based on the premise that in any decision-making process, one person is ultimately **A**ccountable and one or more people may be **R**esponsible, **C**onsulted, and **I**nformed. The ARCI process may help to identify functional areas, key activities, and decision points. Risk management hierarchy may be based on **E**liminate, **R**educe, **I**solate, **C**ontrol-**P**rotect, and **D**iscipline. Organizations invest considerable sums of money to purchase nuclear security equipment; their investments are wasted if lack of maintenance leads to breakdowns and total system failures. There are two key types of equipment failure. The first is *functional* failure, which is usually reported

by an operating crew; the second is *potential* failure, which is usually discovered by a maintenance crew.

3.2.3 System of Self-Assessment

There must be a **system of self-assessment** that includes a wide range of assessment programs, root-cause analyses, culture indicators, lessons learned, and corrective tracking programs for nuclear security. Self-assessment needs conscious efforts to think in terms of how individuals and teams interact with one another, with the physical surroundings within the site, and with the external environment. Nuclear security at an organization has several important off-site stakeholders and understanding their priorities, perceptions, beliefs, and attitudes is central to effective on-site security and teamwork among all players. These stakeholders include organizations that provide intelligence, security skills training, medical assistance, mitigation, and other services. Organisations should identify areas of security learning and development performance for improvement in order to meet objectives/goals. They should also set targets for security learning and development improvement and provide an environment where personnel feel empowered to challenge security behaviours in others. Companies and organisations should explain the importance of security to staff in the context of its own organisational activities and identify training needs. Organizations should involve their staff in developing improvements, conduct surveys periodically, and consult internally on necessary changes.

3.2.4 Reporting of Security Incidents

A reporting policy is a commitment to the highest standards of ethical, moral, and legal business conduct. It protects those who report wrongdoing, as well as those who may be wrongly or falsely accused, from undue negative repercussions. If we see a problem and do not communicate that problem to the right people who can address it, then we have failed as an organization. The organization should have a security liaison officer, who has the primary role to foster communication between different departments by being fully knowledgeable about security policies, procedures, responsibilities, and requirements, as well as skilled in interpreting and promoting them to the people in their department.

3.2.5 Personnel Reliability Programmes

Personnel reliability programmes (PRPs) should be developed for careful screening and vetting of potential employees from the 'pre-employment' stage to the 'post-employment' stage. It is generally applied on a graded basis. These programs include the security clearances through comprehensive background checks and vetting process, continuous evaluations of employees, behavioural observations, management reviews, promotions or financial benefits, personal file evaluations, medical and psychological evaluations, and random drug and alcohol tests. It requires a focus on recognising behaviour that is concerning or deviant and raises serious concern.

3.2.6 Effective Security Culture:

In an **effective security culture**, all personnel are accountable for their behaviour and are motivated to ensure nuclear security. Effective nuclear security culture is characterized by compliance with rules, regulations, procedures, and constant vigilance and a proactive questioning attitude on the part of personnel. Drills and exercises should be used to reinforce the understanding of response procedures and any deficiencies should be identified and eliminated before an actual emergency occurs. Personnel need to recognize the importance of information protection for effective nuclear security. An effective nuclear security culture depends upon teamwork and cooperation of all personnel involved in security. Personnel must understand how their particular roles and interfaces contribute to maintaining security. An effective nuclear security culture is dependent on proper planning, training, awareness, operation, and maintenance, as well as on people who plan, operate, and maintain nuclear security systems. The human factor is a primary contributor to most nuclear security-related incidents as well as malfunctions related to activities involving nuclear and other radioactive material. A significant part of establishing an effective nuclear security management structure is having clearly defined roles and responsibilities. Members of all organizations need a clear understanding of 'who is responsible for what' in order to achieve the desired results. It is particularly important to review and update the responsibility system when organizational change is being planned or executed.

3.3 India's Approach to Nuclear Security

A brief brochure released by the Indian Ministry of External Affairs (MEA) provides an insight into India's nuclear security architecture.[9] The first report on this subject was published by Observer Research Foundation and presented a detailed analysis of the strengths and weaknesses of India's nuclear security policies.[10] This included an overview of the legal and institutional architecture and also a critical review of the policies in practice by some of the established nuclear powers. Another important publication on this subject focuses on the country's nuclear security institutions, instruments, practices, and culture and has also put forward a number of policy recommendations.[11]

The **Indian nuclear security architecture** is based mainly on five pillars:

1. National legal provisions (Atomic Energy Acts and Rules-DAE) in consonance with IAEA guidelines;
2. Regulator AERB that stipulates the SOPs;
3. The security (and intelligence) agencies in charge of threat assessment and physical protection;
4. The human element (personnel) with the responsibility of oversight or observance; and
5. Surveillance and detection technology for detection, delay, and response approach.

Nuclear security here takes care of physical protection, cyberattacks, and radioactive material transport. A workforce made up of individuals who are vigilant, question irregularities, execute their work diligently, and exhibit high standards of personal accountability is able to contribute to a more effective nuclear security architecture.

[9] Government of India, Ministry of External Affairs, "Nuclear Security in India", March 2014. https://www.mea.gov.in/in-focus-article.htm.

[10] Rajeswari Pillai Rajagopalan, *Nuclear Security in India*, Observer Research Foundation, January 2015; Rajeswari Pillai Rajagopalan, Rahul Krishna, Kritika Singh, Arka Biswas, *Nuclear Security in India*, Second Edition (Observer Research Foundation, October 2016).

[11] Sitakanta Mishra, and Happymon Jacob, *Nuclear Security Governance in India: Institutions, Instruments, and Culture* (2019), SANDIA REPORT, SAND2020-10916.

3.3.1 Key Legislations

The country's legislative framework for nuclear matters flows from the Atomic Energy Act 1962 passed by the Indian Parliament. As per the Act, the Atomic Energy Commission (AEC) is the sole authority in the country that deals with nuclear energy matters. Various rules have been established under the 1962 Atomic Energy Act, such as:

1. Atomic Energy (Working of Mines, Minerals and Handling of Prescribed Substance) Rules, 1984;
2. Atomic Energy (Safe Disposal of Radioactive Wastes) Rules, 1987;
3. Atomic Energy (Factories) Rules, 1996;
4. Atomic Energy (Control of Irradiation of Food) Rules, 1996; and
5. Atomic Energy (Radiation Protection Rules, 1971(which were further revised in 2004).

The Atomic Energy (Radiation Protection) Rules sanction activities for nuclear fuel cycle facilities as well as radiation use in the arena of industry, medicine, and research. The regulatory body for civil nuclear installations in India is the Atomic Energy Regulatory Board (**AERB**), which was established in 1983.[12] The primary authority of the institution comes from the Atomic Energy Act of 1962. It reviews the safety and security of the country's operating nuclear power plants, nuclear power projects, fuel cycle facilities, and other nuclear/radiation facilities and radiation facilities. The AERB periodically issues and updates safety and security-related documents such as the "Nuclear Security Requirements for Nuclear Power Plants," the "Security of Radioactive Sources in Radiation Facilities," (AERB/RF-RS/RG1), and the "Security of Radioactive Material During Transport" (AERB/NRF-TS/SG-1, AERB/NRF-TS/SC-1 (Rev.1), 2016).[13]

The Mayapuri incident in 2010, where radiological material was accidentally sold as scrap metal, brought to the fore the violation of protocols by an educational institution and significant deficiencies in legislation,

[12] Government of India, Atomic Energy Regulatory Board, Acts & Regulations, Rules. https://aerb.gov.in/english/acts-regulations/rules.

[13] Government of India, Atomic Energy Regulatory Board, "Regulatory Inspections of Operating NPPs," July 2019. https://www.aerb.gov.in/images/PDF/NPP-RI-July-2019.pdf.

surveillance, and regulations for radiation protection in India.[14] The AERB's new directive (UGC D.O. No. F 10-1/2010 (CPP-II). 7th Jan. 2011) requires educational institutions to get a no-objection certificate for all radioactive materials and related equipment, including X-ray machines. The guidelines also require that these institutions have a proper disposal mechanism for radioactive materials and have trained manpower such as radiation safety officers RSOs. The AERB has developed a comprehensive database of radiation sources utilized in the country and instituted a very successful e-LORA (e-licensing of Radiation Application) platform for complete automation and to facilitate end-to-end licensing of facilities using radiation sources. The components of e-LORA are chosen to achieve Business Solution with Security, Performance, Availability, Scalability, Manageability, and Maintainability.

3.3.2 Physical Security

The **provision of physical security** for nuclear and other radioactive material is built upon several basic concepts. These include taking a graded approach to security, providing defence in depth, and applying four basic security objectives: deter, detect, delay, and respond. This approach incorporates a variety of technologies and mechanisms, electronic and mechanical access control systems, intrusion detection systems, video surveillance systems, and alarm systems as well as physical barriers that help to delay adversaries until a response can arrive. Typically, the physical protection system (PPS) around Indian nuclear facilities is designed on the basis of their threat assessment, taking into account the Design Basis Threat (DBT) and beyond DBT to create a layered protective envelope consisting of inbuilt reactor security, perimeter security, personnel reliability, material protection and accounting, transportation security, air and water front defence, emergency preparedness, legal provisions, and, in extreme situations, military protection.[15]

[14] S.R. Singh, et al., "Fatal Radiation Exposure due to Careless Disposal of Cobalt-60 from a University Lab," *Journal of Indian Academic Forensic Medicine* 35, no. 3 (July–September 2013): 283.

[15] Ranajit Kumar, "Technologies and Physical Security of Nuclear Materials: An Indian Perspective," in the National Academy of Sciences compiled *India-United States Cooperation on Global Security: Summary of a Workshop on Technical Aspects of Civilian Nuclear Materials Security* (2013), Washington, DC: The National Academies Press, 2013.

In 2008, the AERB issued a safety guide on security levels of radioactive material during transport (AERB/NRF-TS/SG-10) that prescribes the requirements for ensuring safety in the movement of radioactive material through the public domain. In compliance with IAEA stipulations, the AERB revised its code on the Safe Transport of Radioactive Material—AERB/NRF-TS/SC-1 (Rev.1)—in 2016, which "prescribes the classification, design, and test requirements for radioactive material for packaging… transport and administrative requirements for transportation of radioactive material in the country."

The CISF, a paramilitary force, oversees the security provided to civilian nuclear facilities across the country. CISF officials trained to safeguard nuclear installations are rotated among the nuclear installations and are not kept in one place for more than a certain number of years as a standard operating procedure for security forces. However, some nuclear institutes (such as IPR) and heavy water plants have their own security arrangements. The physical security of nuclear installations is provided by a mix of multiple organizations such as the CISF, local police, and sometimes even private security organizations. Material accounting is handled by the DAE, and the review of security practices is the responsibility of AERB. It would be better to have a strategy of a unified or centralized security arrangement in all nuclear-related installations for better coordination, security planning, and implementation.

3.3.3 Cybersecurity

Cyber threats can be perpetrated by lone individuals, loosely organised groups, active terrorist organisations or nation-states. Attacks can occur remotely, from anywhere in the world, and be very difficult to track to their source. Nuclear facilities have become increasingly dependent on digital technology to maintain reliable operations, increase efficiency, and reduce costs. Consequently, computer-based systems are generally designed to facilitate these operational objectives rather than to maximise security. An unintended consequence of the widespread introduction of digital systems is that they have potentially increased vulnerability to malicious cyberattacks, as well as the likelihood that critical digital assets and

industrial controls systems can be compromised. Many reports have identified human error as the main cause of computer security breaches in nuclear facilities.[16]

The IAEA recently (2021) issued its first implementing guide, Nuclear Security Series (NSS) No. 42-G *Computer Security for Nuclear Security*, to support experts worldwide in implementing computer security measures to strengthen their national nuclear security regimes. This guide will support Member States in strengthening computer security in their national nuclear security regimes, ensuring the benefits of digital technology can be embraced without weakening the regime and the capacity to protect, detect, and respond to cyber threats. Other publications in the NSS that touch upon computer security for nuclear security are NSS No. 17-T (Rev. 1) *Technical Guidance on Computer Security at Nuclear Facilities*, published in September 2021, and NSS No. 33-T *Technical Guidance on Computer Security of Instrumentation and Control Systems at Nuclear Facilities.*

The Computer Information and Security Advisory Group (CISAG), formed in 2001 in the DAE, is in charge of periodic oversight of information systems. It has put in place plans and guidelines to counter cyber-attacks and mitigate any adverse effects.[17] Specific guidelines are under preparation to deal with network-related risks to control and instrumentation systems used in various installations. In addition, regulations require computer-based critical safety systems to have a parallel system. For information security, India has developed a secure messaging and voice communication device placed within a mobile device to communicate in a secure manner. Specifically for nuclear facilities, the Secure Network Access System (SNAS), developed at BARC, is designed with several modules for real-time detection, identification, and authentication of the end-system in a network (SNAS-Network Admission Control).[18]

[16] Computer Security at Nuclear Facilities, IAEA. Nuclear Security Series Publications. Asp No. 17 (2011), https://www.iaea.org/publications/8691/computer-security-at-nuclear-facilities.

[17] R.M. Suresh Babu, "An Indian Perspective on Cybersecurity," in the National Academy of Sciences compiled India-United States Cooperation on Global Security: Summary of a Workshop on Technical Aspects of Civilian Nuclear Materials Security (Washington, DC: The National Academies Press, 2013).

[18] Gigi Joseph, "Secure Network Access System (SNAS)," BARC Newsletter, Special Issue, October 2014.

3.3.4 Emergency Response System

Emergency response preparedness is an essential aspect of nuclear safety and security. India's national emergency response system architecture is a combination of the Indian Environmental Radiation Monitoring Network (IERMON), ERC network, meteorological data network, emergency communication rooms, Crises Management Group (CMG), National Technical Research Organisation (NTRO), and NDMA. In the Indian atomic energy sector, Integrated Command Control & Response (ICCR) exercises focus on testing command and control functions, response mechanisms, and communication. Additionally, given the proximity of population centres to nuclear facilities, field exercises, and public interactions are an important requirement of emergency management in India. The objective of emergency preparedness is to prevent and minimise the impact of any nuclear or radiological incident on both workers and the larger public. The response plan for a nuclear emergency entails notification, activation, request for assistance, and protective action. First responders to such emergencies are required to prevent spread of contamination and restrict entry to the accident area. The key is recognising the existence of an emergency situation, identifying and characterising the source and origin, monitoring the magnitude, and providing reliable communication to personnel from medical, civil, police, and transport agencies.

Responding to emergency situations requires continuous assessment of emergency levels, determining the area for countermeasures, decision-making on protective measures for public and the surrounding environment, as well as prediction of contamination levels. For example, the DAE's Emergency Control Room (ECR) is responsible for the dissemination of authentic information regarding emergencies to the control rooms and response teams across agencies such as the AERB. The nearest ECRs are alerted for response deployment and briefings for further information dissemination. Based on the information provided through timely briefings, the level of emergency and conclusion of the emergency is determined by the AERB. Effective and procedural communication between all actors and institutions involved in emergency response is a crucial aspect in averting crises as a result of an emergency. Successful inter-agency coordination and provision and dissemination of accurate information are key to handling an emergency efficiently.

3.3.5 *Establishment of Global Centre for Nuclear Energy Partnership*

In fulfilling the promise made by India at the inaugural Nuclear Security Summit, it has established the Global Centre for Nuclear Energy Partnership (GCNEP) with a view to "help in capacity building, in association with the interested countries and the IAEA, involving technology, human resource development, education & training and giving a momentum to R&D in enlisted areas."[19] The centre currently has five schools, including one School on Nuclear Security Studies (SNSS) with the mission "to impart training to security agencies on application of physical protection system and response procedure, to enhance physical security of nuclear facilities by developing and deploying most modern technological tools including information security and to provide facilities for test and evaluation of sensors and systems used for physical security."[20] In addition, computer security methodologies will be developed for protection of information related to the entire nuclear fuel cycle activities including that of nuclear security.

3.3.6 *Holes in the Security Wall*

In India, nuclear power plants under Nuclear Power Corporation of India (NPCIL) and big government research centres have adequate nuclear security machinery. Ionizing radiation applications have been accruing huge societal benefits, in terms of cancer treatment, diagnosis, and industrial uses such as non-destructive testing, gauging and in food processing applications, etc. However, the ionising radiation has certain radiological hazards associated with handling of radiation sources. Radioactive sources and radiation generators used are required to be handled safely throughout their life cycle to prevent any undue risk to health and environment. Physical protection at the sites where radiological sources, materials, devices, and instruments are used in India (e.g., hospitals, research facilities, oil and gas exploration industry, road construction industry, and steel manufacture) is lacking and physical security is rather

[19] Global Centre for Nuclear Energy Partnership, http://www.gcnep.gov.in.

[20] GCNEP NEWSLETTER, SNSS Special Volume-1, Issue 3, May 2015.

lax, at best comparable to the protection provided at ATM.[21] Loss of radioisotope sources occurs as a result of the violation of safe work practices and non-compliance with rules and guidelines.[22] The main causes are human error and negligence in source handling and storage, as well as mismanagement and lack of supervision.

Most alarming are reports of radioactive material smuggling in and around India. Recently, in May 2021, over 7 kg of uranium was seized. India has established an inter-ministerial Counter Nuclear Smuggling Team to devise a coordinated multi-agency institutional mechanism to strengthen the national detection architecture for nuclear and radioactive material and deal with the threat of individuals or groups of individuals acquiring nuclear or radiological material for malicious purposes. Little open-source information is available on the steps India takes to prioritize security of its strategic assets, including nuclear weapons, components, or strategic facilities. The Nuclear Command Authority is responsible for all matters relating to the safety and security of India's nuclear and delivery assets at all locations. It is believed that the physical security of warheads and components is provided by a specialized force drawn from the Indian Army.

3.3.7 Conclusion

Nuclear security is important for India for a number of reasons. India has a large nuclear programme and its atomic energy facilities are spread across the country. There are also significant vulnerabilities of nuclear terrorism and other threats from country's immediate neighbourhood. The leaders of an organization have a particularly strong influence over the assumptions and ideas that need to be promoted to achieve and maintain a successful security culture. Principles ensuring nuclear security are based on multi-tier protection systems, and involving technological aspects, security framework, and SOPs, all firmly instituted and scrupulously enforced. Even a well-designed system can be degraded if the

[21] Rajesh M Basrur and Friedrich Steinhäusler, "Nuclear and Radiological Terrorism Threats for India: Risk Potential and Countermeasures," *The Journal of Physical Security* 1, no. 1 (2004): 5.

[22] U.C. Mishra, A.S. Pradhan, Loss and recovery of radiation sources in India, 1998, XA9949014. https://inis.iaea.org.

procedures necessary to operate and maintain it are poor, or if the operators fail to follow procedures. The biggest threat to nuclear security lies in complacency. Threats may arise because of the absence of security-related crises, low priority of security in operational activity, human nature for denial and scepticism, failure of senior management to act as role models, scarcity of resources, outdated procedures, and poor attitude towards those that report faults and flaws. Therefore, there is always scope for improvement. Security-related information needs to be communicated effectively, both inside and outside the organisation. Excessive and unwarranted secrecy is counterproductive. Although India has evolved and nurtured a coherent nuclear security culture, complacency is always a threat. Obedience to authority and reluctance to question authorities, which are ingrained aspects of Indian culture, may prove to be the cause of poor security performance.

No amount of security can be security enough, and as threats evolve, security has to be dynamic. The security system has to be adaptable to deal with a complex world. Adaptability controls the space between reaction and prediction, providing an inherent ability to respond efficiently to a wide range of potential challenges—not just those that are known or anticipated—as they arise in their environment. No adaptation is truly helpful if it's considered a one-time event. Adaptation is a continual learning process that needs to be replicated and improved upon repeatedly. The best process for fostering this kind of recursive feedback in human systems is an intense focus on learning from success and failures.

3.4 A U.S. Perspective

Cristina F. Lussier and Karen Kaldenbach

The U.S. nuclear enterprise has focused on earning the trust of the American public in both safety and security since the end of World War II. While the U.S. Department of Energy continues to find unique opportunities to integrate the use of nuclear power as an alternative sustainable energy source for millions of Americans and their communities, the U.S. Department of Defense maintains its strong, credible nuclear arsenal to serve as a strategic deterrent against adversaries threatening America's homeland and its allies.

While both nuclear energy and nuclear weapons involve the release of power from atomic reactions, "neither the physics nor the technologies are the same, nor are the institutions that manage the two."[23] Yet throughout the years, these different organizations have collectively worked together to build a stronger bond of trust amongst the American public in accepting the use of nuclear power to both protect their national interests and support their daily livelihood. This chapter will explore events and characteristics that have defined the culture within these two entities of the nuclear enterprise. It also will analyze how Americans have come to accept the risk of nuclear power in order to maintain their prosperity and their independence.

3.4.1 Incorporating Lessons Learned

Since the end of World War II, the U.S. nuclear enterprise has worked hard to both maintain the Department of Defense's nuclear arsenal and to share nuclear technology across the globe. After the U.S. dropped the first atomic bomb on Hiroshima, Japan in 1945, the world was put on notice: Americans will go to great lengths to protect their independence and national security.

Following the war, the world entered a new era, in which nuclear weapons emerged as the bedrock of strategic deterrence. As the nuclear arms race unfolded, so did the use of nuclear power for civilian use. Nuclear energy became not just a reason for fear, but also source of hope for clean, reliable, renewable energy.

3.4.1.1 Communicating Concerns Builds Understanding

Today, millions of Americans are dependent on nuclear-generated power. Almost one-fourth of all civil nuclear power plants in the world are in the U.S. This accounts for approximately one-third of the world's global nuclear power generation.[24]

[23] T. Nordhaus, "Time to Stop Confusing Nuclear Weapons with Nuclear Power," *The Hill*, May 14, 2017. https://thehill.com/blogs/pundits-blog/energy-environment/333329-time-to-stop-confusing-nuclear-weapons-with-nuclear/.

[24] United States Civil Nuclear Energy Framework, Atoms for Prosperity. Source: https://legacy.trade.gov/mas/ian/build/groups/public/@tg_ian/@nuclear/documents/webcontent/tg_ian_005298.pdf.

Today's nuclear strategic deterrence and the increase of civilian nuclear infrastructure projects over the years have relied on an effective national strategy driven by a committed workforce. Workforce culture can be an organization's best asset or its worst liability. As Peter Drucker famously stated, "Culture eats strategy for breakfast."[25] To understand how the nuclear enterprise has achieved its national security strategy objectives is to examine the attitudes, values, and behavior that together have comprised the organization's culture. The ability to achieve operational success, as laid out by strategy, is driven by this culture, which ultimately wins or loses in both operations and in gaining the trust of the public that it serves.

After the Cold War ended and the Soviet Union collapsed, there was a need for the United States to better understand what role nuclear weapons would play in national security. In 1994, the U.S. government legislatively mandated the Department of Defense to perform a Nuclear Posture Review (NPR). Through the NPR, U.S. nuclear policy, strategy, capabilities, and force posture were to be outlined for the next five to ten years.[26] The first few NPRs were classified, making the document unavailable to the public. In 2010, the NPR was published as an unclassified document, making it publicly available. The administration did this because it "did not want to leave big open questions about what might be left unsaid because it's in the classified domain."[27]

The 2010 transition from a classified to an unclassified NPR is noteworthy. It continues to impact the organizational culture of the Department of Defense and nuclear enterprise today. Whereas much of the emerging civilian technology involving nuclear energy falls into the open, unclassified programming space, the opposite was the case for much of U.S. defense organizations and support agencies. To seek solutions

[25] S. Hyken, "Drucker said Culture Eats Strategy for Breakfast," *Forbes*, December 5, 2015. https://www.forbes.com/sites/shephyken/2015/12/05/drucker-said-culture-eats-strategy-for-breakfast-and-enterprise-rent-a-car-proves-it/#7a7572822749.

[26] U.S. Department of Defense. Nuclear Posture Review. https://dod.defense.gov/News/Special-Reports/NPR/.

[27] E. MacDonald, "Five things Everyone Should Know About the Nuclear Posture Review," October 4, 2021. Retrieved October 25, 2021, from All Things Nuclear. https://allthingsnuclear.org/emacdonald/five-things-everyone-should-know-about-the-nuclear-posture-review/.

to the complex security issues facing the United States and its allies and partners required a shift in how these threats are seen and communicated.

Changing the NPR to an unclassified document allowed for transparency regarding the security challenges ahead. This facilitated collaboration amongst organizations and agencies in which they could discuss fighting domains and the impact of emerging threats—"including nuclear, conventional, cyber and space."[28] As the speed of advancing technology in the twenty-first century diminishes latency between the decision to act and the execution of operation, the potential for devastating error is compounded. It is within this scope that senior political and defense leaders have stressed the importance of confidence in its workforce. Admiral Charles Richard, commander of U.S. Strategic Command, highlighted the need for nuclear modernization and considering the intricacies of command-and-control structures. He stated, "it has to be very clear to the military who has the authority and who has the responsibility to give that order."[29]

The United States nuclear enterprise seeks to empower individuals and organizations to do what is necessary to prevent and address existential threats that weaken collective strategic deterrence, creating an environment that promotes individual and organizational safety.

Whether discussing the concerns of conventional nuclear integration or nuclear power as clean energy, the United States' focus on safety has enabled national organizations, industries, and workforces better to understand, engage, and respond to strategies to keep the nuclear enterprise safe, secure, and effective.

3.4.1.2 Taking Steps for Action

The U.S. Nuclear Regulatory Commission (NRC) has long recognized the importance of a positive nuclear safety culture. With a collective commitment from individuals and organizations, the practice of maintaining a positive safety culture tackles apathy in its earliest stages, before it grows into security atrophy resulting in a nuclear mishap. It also helps

[28] A. C. Richard, *The Future of Strategic Deterrence and Nuclear Modernization*, May 5, 2021. Brookings Institute. https://www.brookings.edu/events/the-future-of-strategic-deterrence-and-nuclear-modernization-a-conversation-with-adm-charles-richard/.

[29] A. C. Richard, "The Future of Strategic Deterrence and Nuclear Modernization," May 5, 2021. Brookings Institute. https://www.brookings.edu/events/the-future-of-strategic-deterrence-and-nuclear-modernization-a-conversation-with-adm-charles-richard/.

to build a more agile workforce. The NRC encourages nuclear organizations to cultivate a persistent focus on implementation of sound practices, where complacency is virtually absent. To support this goal, the NRC created a Safety Culture Policy Statement that includes nine key traits for individuals and organizations.[30] Figure 3.1 lists the nine traits and provides a brief description of each.

Research shows that certain personal and organizational traits exist in positive safety and security cultures. These traits are patterns of thinking, feeling, and behaving that continually emphasize safety and security. They are especially important when conflicts arise, such as disagreement between operations and security components about implementation of security measures that delay operational schedules.

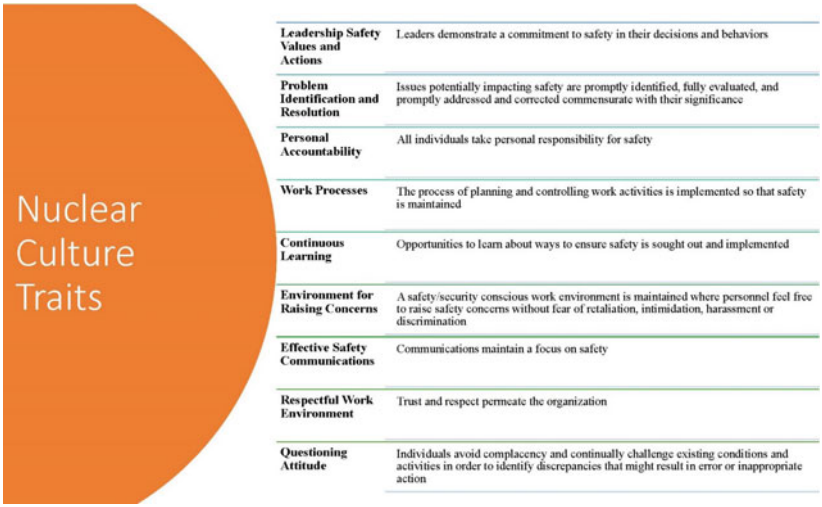

Fig. 3.1 NRC safety culture traits[31]

[30] The US Nuclear Regulatory Commission's Safety Culture Policy Statement (76 FR 34773; June 14, 2011) can be further explored at https://www.nrc.gov/about-nrc/safety-culture/sc-policy-statement.html.

[31] Reproduced courtesy of the United States Nuclear Regulatory Commission.

Although these traits were first identified as safety culture traits, they equally apply to the collective security of an organization. There are significant differences between safety and security. Safety is primarily focused on protecting people and the environment from things, whereas security is focused on protecting things from people. For example, a security perspective aims to keep nuclear and radioactive materials secure within locked areas with no breach possible. A safety perspective, by contrast, would seek to protect the workforce in a nuclear facility from radioactive material that could present a health or safety concern.

Despite these differences, a synergistic relationship between safety and security is essential. For individuals working in and around the nuclear arena, the stakes are high. Adequately considering both safety and security helps propagate a positive overall culture. Staffs realize the importance of safety protocols designed to keep themselves, as well as those around them, from harm. However, for years many security requirements were viewed as the exclusive responsibility of the security staff. For example, if a site breach was attempted, the safety of those within the complex was viewed as a security issue, not a safety concern. The notion that security is everyone's responsibility, just as maintaining safety protocols within a facility keeps everyone safe, had not been cultivated as common understanding until recently.

Over the last decade, the NRC made a concerted effort to correct this view within the workforce, with the publication of its Safety Culture Policy Statement. Efforts such as this, where leadership invested in its workforce by actively communicating implementation solutions and providing proactive follow through, have been essential to success within the nuclear enterprise. Despite its importance, however, the NRC Safety Culture Policy Statement was just a guiding document. How departments and organizations used the document is what ultimately created a cultural shift within the enterprise. The following examples highlight how organizations have communicated the NRC guidance.

The U.S. Department of Energy (DOE) stood up a Safety Culture Improvement Panel, which helped to outline practicing safety attributes in DOE's Integrated Safety Management System Guide.[32] In a publicly

[32] United States Department of Energy, "Safety Culture Improvement Panel," Department of Energy, 2018, August. https://www.energy.gov/sites/default/files/2018/08/f54/Safety%20Culture%20Improvement%20Panel%20Overview%20Trifold%20-%20508v2.pdf.

available trifold, the work done by the department's panel helped to explain roles and responsibilities that have now become internalized by its workforce. The intuitive nature of the guidance has enabled it to become part of the workforce's "DNA" at all echelons of the department.[33]

Aligned with the DOE, and with a long history of helping to safeguard the nuclear enterprise for the U.S. Department of Defense, is the Defense Threat Reduction Agency (DTRA). DTRA is the U.S. Department of Defense agency that confronts challenges related to weapons of mass destruction and emerging threats.[34] The agency proudly emphasizes that its people are its most precious resource. In addition to people, integration of programs is very important. As Commander of the U.S. Strategic Command, Navy Adm. Charles A. Richard, recently commented, "it's also important to understand how our modernization programs support and integrate with our efforts to rethink how we do strategic deterrence."[35] A well supported, agile workforce is best prepared to meet this challenge.

The Atomic Energy Commission (AEC) led the safety of production, transportation, and storage of nuclear material at the beginning of the nuclear era. Today, U.S. Department of Defense Nuclear Weapon System Surety Policy provides maximum safety consistent with operational requirements. A key tenet of this program states, "to achieve nuclear weapon system safety, and to maintain the public trust by protecting public health, safety, and environment, it is critical that surety be considered throughout the life-cycle of the weapon."[36]

[33] United States Department of Energy, "Safety Culture Improvement Panel," Department of Energy, 2018, August. https://www.energy.gov/sites/default/files/2018/08/f54/Safety%20Culture%20Improvement%20Panel%20Overview%20Trifold%20-%20508v2.pdf.

[34] Defense Threat Reduction Agency. About DTRA. Retrieved April 26, 2021 from https://www.dtra.mil/WhoWeAre/.

[35] T. M. Cronk. "DoD Must Rethink, Prioritize Strategic Deterrence," *DoD News*, October 21, 2020. https://www.defense.gov/Explore/News/Article/Article/2389931/dod-must-rethink-prioritize-strategic-deterrence/.

[36] U.S. Department of Defense. "DoD Nuclear Weapon System Safety Program Manual," 2021. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/315002m.pdf?ver=x45aWEVjJWieQw0euniZYw%3D%3D.

3.4.2 Nuclear Security from the Workforce to the Community

Workforce culture is often apparent upon entering a facility. Are all staff members executing safety protocols intuitively and in an organized fashion? Are security officers following procedures, being polite yet cognizant of unusual behaviors that may require further inquiry? Are staff members wearing credentials in the appropriate manner and following safety and security procedures, such as not allowing piggybacking of known coworkers into facilities, showing respect to others, and executing all protocols? The answers to these questions demonstrate the strength of an organization's culture. Although an assessment may be required to determine the long-term viability of a positive culture, a leadership team that fosters an environment of continuous learning with positive enforcement can often achieve internalized systemic change.

For example, within the Department of Defense, standards, plans, procedures, and other positive measures are established to help the department accomplish its nuclear mission in a safe, secure, and reliable manner. Uniformity in expectation allows the workforce to achieve this successfully. Leadership throughout the ranks of the organization is held accountable not just for its actions, but for those of the team as well. These "standardized expectations" are part of an effective cultural foundation.

Hiring the right talent with specific skills needed for the task, right-sizing teams, and mandating initial and recurring periodic training are additional factors that keep the U.S. nuclear enterprise at its best. This is all part of the overall strategy. The plan is written down, approved, and funded for execution in maintaining nuclear security.

Toxic culture can put this strategy in jeopardy. Even the most engaged leaders and supervisors may fall victim to a toxic culture if another part of the internal process is broken or there is lack of communication across business lines of effort within an organization. For example, rushed hires, poor trainers, and substandard working conditions can all contribute to poor performance, which weighs heavily on organizations.

Consider, for example, how U.S. nuclear power plants, which are operated by contractors across the country, execute site protocols. While the workforce is trained with a focus on "safety first," there is also a concerted effort to adapt to the diverse regions in which the plants are located. The ability to execute safety protocols differently while maintaining the strict security standards and expectations set forth by the NRC allows the

contract teams to be effective and efficient in the regions in which they operate.

Job requirements and deeply held social expectations can sometimes conflict. For example, overt friendliness is generally considered an important trait in the southeastern United States. However, in some of the southern nuclear facilities, this friendliness prevented staff from challenging personnel who entered parts of the facility without authorization. These facilities adapted their training to incorporate polite inquiry regarding someone's authorization to be in an area. This enabled them to maintain security but adapt to the local culture. Training and awareness of all expectations and skill sets to perform jobs, fostering of personal accountability, encouraging a questioning attitude, nurturing an environment for raising concerns, leadership support and encouragement, and implementation of sanctions are all important cultural traits needed to help ensure a safe and secure nuclear environment.

Working with and alongside local communities across the country means that leadership teams must deal with differing public opinions toward nuclear power. The Tennessee Valley Authority (TVA) has long sought to educate the public on the benefits of nuclear energy, to foster acceptance of nuclear power within the community. TVA actively shares employment opportunities and maintains an updated, publicly available website. It is willing to discuss issues and concerns surrounding nuclear power, to maintain trust and transparency of safety operations with the workforce and community, and to raise awareness of planned security operations. Before COVID-19, TVA hosted community days that included activities and food for the local community. During these events, TVA capitalized on the opportunity to build strong community relations. It distributed free calendars noting when drills would impact traffic and when it would sound warning sirens or make announcements to raise awareness about what the power plant does and how it maintains safety and security.[37]

3.4.3 Defining Common Language, Values, and Standards

Publishing new policy statements does not uniformly alter organizational norms and behavior. Transformations that build strong organizational

[37] To learn more on how TVA communicates with its communities about nuclear security, visit TVA at https://www.tva.com/energy/our-power-system/nuclear.

cultures occur from repeated processes that the workforce comes to believe in over time. The traits outlined by the NRC highlight key values that complement an already well-trained and highly educated workforce. The first step is to be able to communicate a vision that is easily understood, relevant, and viewed as collectively beneficial. The NRC Safety Culture Policy Statement clearly addresses the requirement that organizations ensure personnel in the safety and security sectors have an appreciation for the importance of both safety and security in their activities. U.S. nuclear power plants must demonstrate that a cognizant link between nuclear safety and nuclear security exists by NRC regulation. The IAEA Technical Report Series No. 1000 *The Nuclear Safety and Nuclear Security Interface*: *Approaches and National Experiences* addresses the management of this relationship.[38] As the Report makes clear, a safety issue has the potential to become a security issue just as a security issue has the potential to become a safety issue. We must protect against both.

Below, we discuss the traits that the NRC identifies as contributing to a robust safety and security culture. The nine traits are not meant to be all inclusive. The NRC's expectation, however, is that both individuals and organizations foster those characteristics that actively embrace a strong safety and security culture within the nuclear enterprise.

Leadership safety values and actions are the first cultural trait. Organizational leaders not only implement the criteria to ensure security and safety are priorities within any facility; they also set the example for staff to emulate their behaviors. When leaders demonstrate a commitment to safety and security, staff recognize the importance of doing so themselves. It is important for leaders to ensure that necessary resources are allocated to constantly self-assess and ensure proper implementation of safety and security functions. Having a field presence to interact with safety and security personnel, and to recognize their achievements, can motivate staff. Often personal recognition is more meaningful than any financial incentive. Conversely, implementing sanctions for those who do not follow procedures and show the appropriate support for safety and security may help to prevent violations.

[38] IAEA Technical Report Series No. 1000 *The Nuclear Safety and Nuclear Security Interface: Approaches and National Experiences* can be found at. https://www.iaea.org/publications/13654/the-nuclear-safety-and-nuclear-security-interface-approaches-and-national-experiences.

Problem identification helps ensure that when safety or security-related issues arise, they are promptly identified, evaluated, addressed, and resolved based upon their significance. The promptness with which organization do these things reflects upon how safety and security are prioritized. Those with a strong safety and security culture typically raise awareness with the staff about the importance of their participation in the process of identifying and addressing problems. Organizations can implement a corrective actions program with simple input capabilities, while also addressing progression and resolution of the issue. Implementing training programs to ensure that staff understand proper procedures allows them to report issues as they arise, before they become problematic.

In the realm of nuclear security, the objective for the U.S. is to maintain a safe, reliable, and credible nuclear deterrence posture. Any event, gap in capability, or issue that prevents even one of these objectives can have a negative impact on the role nuclear forces plays in properly executing strategy, plans, and programming. Thus, corrective action to address concerns of unwanted subcultures and attitudes is given high priority. Corrective action also entails prompt release of information to the public in the event of incidents involving nuclear weapons or nuclear components, radioactive material, nuclear weapon launch or transport vehicles, or nuclear reactors under Department of Defense control, as outlined in the Nuclear-Radiological Incident Public Affairs Guidance.[39]

The duty of every staff member to identify and report problems leads to **personal accountability**. Employees must understand their specific job assignment and the importance of standards in performing their assigned tasks. Every staff member, from cleaner to CEO, plays a role in ensuring the safety and the security of the facility. Individuals must work well within teams in pursuit of this goal. Leadership can be essential in cultivating teamwork among staff and propagating a positive workplace environment.

Ensuring **work processes** are well defined and implemented to nurture good safety and security is also extremely important. This involves planning and controlling work activities via measures such as defining policies, implementing strong operating procedures, ensuring staff are properly trained on these procedures, and ensuring that work is managed in a way

[39] U.S. Department of Defense. "DoD Instruction 5230.16 Nuclear-Radiological Incident Public Affairs (PA) Guidance," 2015. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/523016p.pdf.

that safety and security are the overriding priorities. The design margins within which work should be performed must be well defined, and all staff should be trained on how to react when approaching these margins. All work processes should be adequately documented, with staff trained on the processes and knowing where to find necessary reference documentation. Last, staff must understand the importance of their rigorous adherence to procedures—knowing these were put into place to ensure a safe and secure work environment for all. If steps are deemed unnecessary and are often skipped by staff, this should be reported. If staff identifies potential improvements to standard operating procedures, the old procedure should be followed until replaced by a new one. Staff should discuss concerns with leadership to determine if a procedural review is necessary. Staff training should include learning opportunities to help them understand why certain steps may be necessary in light of specific safety or security concerns.

Successful organizations provide staff robust initial training and then enable them to engage in **continuous learning** regarding both safety and security. Such learning enhances the ability and willingness of individuals to apply their knowledge in the workplace. As this knowledge and experience are shared, it spreads throughout the organization, strengthening the culture in the process. Staff who feel that an organization is investing in their personal and professional success are motivated to perform better. Organizations can aid this process by conducting self-assessments and benchmarking to define areas of needed improvement. Also, lessons learned should be collected and made available to staff to avoid repeating mistakes.

When security staff are hired by TVA's Watts Bar Nuclear Power Plant, they go through four weeks of rigorous training before beginning their official assignment. This training focuses not just on their security duties, but also on the operation of a nuclear power plant. This investment in staff has paid dividends on multiple occasions. One such case involved a security officer who, while performing his normal patrols, noticed an unusual steam pattern emanating from a valve. He took the initiative to report this to his supervisor, who immediately contacted operations staff. A pressure issue that could have led to progressive degeneration was identified early and corrected without damage to the plant. The security officer applied his existing knowledge and observations of normal plant processes with his personal accountability to raise awareness and report a potential

issue. His management listed him as security officer of the month for his dedication to ensure safety and security at the site.

This example speaks to both the security officer and to the organization for promoting an environment for raising concerns. In a positive workplace, personnel feel free to raise concerns without fear of retaliation, intimidation, harassment, or discrimination. Leadership ensures that when staff do so, the issue is promptly and transparently reviewed. The appropriate level of management should be engaged in resolution of the issue, fostering an environment that promotes open communication where there is never retribution for reporting (Fig. 3.2).

An incident at Exelon's Dresden Nuclear Power Station illustrates the dangers of staff's failure to report concerns. Two senior reactor operators were found to have been plotting an armored car heist, even soliciting support within the power station. Although staff members had become aware of the plot, and understood its potential seriousness, no one reported any concerns to management. The plot ultimately unraveled, but "the case sent ripples through the nuclear power industry, prompting the Exelon Corp.—which owns the Dresden plant and is the largest U.S. operator of nuclear reactors—to change how it trains its employees to spot and report behavior that might pose a security threat."[40]

Fig. 3.2 TVA's Sequoyah nuclear plant

[40] G. Aegerter, "Nuclear Plant Workers in Hot Water After Alleged Plot to Rob Armored Car Goes Awry," *NBC News*, November 18, 2013. https://www.nbcnews.com/news/world/nuclear-plant-workers-hot-water-after-alleged-plot-rob-armored-flna2d11612598.

Effective safety communications, which are facilitated by a pro-reporting environment, constitute one of the most important characteristics of a strong safety and security culture. Leadership works to ensure that information flows effectively from the top down and encourages open dialogue among staff at all levels. Safety and security communications must be incorporated into all work activities as a normal part of operations. If this has not occurred at a facility, then procedures must be revised and staff must be retrained on the revised procedures.

This process was implemented recently at one national laboratory in the United States. After careless errors were repeatedly reported, the lab director conducted a shutdown of all activities for one week to retrain and refocus staff on effectively implementing procedures and communicating concerns through the appropriate channels. This was a very costly exercise, but the lab director recognized that safety and security issues could have caused far worse problems. It also successfully communicated leadership's expectations and prioritization of safety and security.

A critical element in helping staff feel empowered to communicate well is a respectful work environment. Leaders can greatly assist in creating a workplace where everyone is treated with dignity and respect. However, all staff members impact this effort through their daily treatment of one another. Ensuring trustworthiness and implementing necessary security protocols to verify reliability is necessary, and everyone can show that opinions are valued and demonstrate respect. This is a circular process, which recognizes that each position within the facility can contribute to the safety and security of everyone at that site. This happens when all accept personal accountability in carrying out the work processes, identifying problems and seeking resolution, and communicating with the appropriate staff to raise concerns. Employees must demonstrate a high level of trust in resolving all conflicts using fair and objective methods, seeking to aid learning for all involved parties to achieve a reasonable outcome.

The final cultural trait fits seamlessly with the previous eight. All individuals within a facility should have a questioning attitude. A questioning attitude does not mean disrespect for the opinions of others; instead, it means that individuals do not become complacent in the workplace. In their individual positions, they should continually evaluate conditions and activities to identify abnormalities that could result in errors or inappropriate action. Knowing that nuclear facilities are unique, it is important

that work is continuously assessed to identify inconsistencies and abnormalities. It is possible to become blind to minor changes over time. Sometimes those with "fresh eyes" can more easily notice a problem than those exposed to it every day. Staff must be encouraged to challenge assumptions and ask questions about things they do not fully understand. Explaining the process helps reinforce learning for newer staff and may bring an opportunity for exchange of fresh ideas from which all can learn. Staff should always have a respectful attitude and be open to such opportunities.

A review of the facility breach incident at the Y-12 National Security Complex (Y-12) facility in Oak Ridge, Tennessee, as a case study showcases the importance of the nine traits discussed above, and the danger of failing to maintain a culture that promotes safety and security.

3.4.4 Y-12 Case Study

Perhaps one of the best examples of the interconnectedness of security and safety and how the failure of one impacts the other in the nuclear community is the July 2012 incident at the Y-12 facility. Y-12 is a US Department of Energy National Nuclear Security Administration (NNSA) facility that was originally established as a uranium enrichment site as part of the Manhattan Project and currently serves as one of the central repositories for highly enriched uranium in the United States. This is one of the United States' most sensitive facilities, spending approximately $150 million annually to ensure security is maintained. It is not uncommon for antinuclear protests to occur at this facility; however, protests are usually registered with local city ordinances and typically remain peaceful (Fig. 3.3).

In the early morning on July 28, 2012, three protestors (the most well-known being an 82-year-old Catholic nun) crossed multiple fences and security systems, activating numerous alarms and sensors between fences. The trespassers gained access to the most protected area of the site around the highly enriched uranium materials facility, banged on the building, defaced it with paint, and remained in the protected area for several hours before security officers intervened. The protestors did not gain entry to the building and were removed for later prosecution.[41] But how could

[41] United States Department of Energy, Office of the Inspector General, Office of Audits and Inspections, "Special Report: Inquiry into the Security Breach at the National

Fig. 3.3 Delay barriers at Y-12[42]

unauthorized personnel gain access to one of the nation's most highly secured areas?

The contractor operating Y-12 had recently changed, resulting in new management of the facility. The contract for maintenance and operation of the facility was split from that for the physical protection of the site. Multiple problems had emerged relating to the performance of maintenance, budgeting for new equipment, classification of failures, communications, and reporting of concerns. Staff were reported to be embittered with the new contractor's dismissive attitude regarding equipment failures and lack of attentiveness to employee concerns. Leadership did not allow staff to follow procedures in all cases. With the obvious lack of attention and mindfulness of staff to the previously mentioned cultural traits, a spiraling effect degraded the facility's safety and security culture.

The subsequent DOE inquiry highlighted "multiple system failures on several levels," identifying "troubling displays of ineptitude in

Nuclear Security Administration's Y-12 National Security Complex," US Department of Energy, 2012. https://www.energy.gov/sites/prod/files/IG-0868_0.pdf.

[42] Reproduced courtesy of Department of Energy.

responding to alarms, failures to maintain critical security equipment, overreliance on compensatory measures, misunderstanding of security protocols, poor communications, and weaknesses in contract and resource management."[43] These issues, combined with "contractor governance and federal oversight failure to identify and correct early indicators of these multiple system breakdowns," allowed potentially catastrophic failures. Weak adherence to security protocols was clearly cited as a key dimension of the breach with failures "contributing to an atmosphere in which the trespassers could gain access to the protected security area." NNSA staff determined that "contributing and direct causes of the security event included an inappropriate Y-12 cultural mindset, as well as a severe lapse of discipline and performance." An additional problem was "a culture of compliance, as opposed to a culture of performance."[44]

The Y-12 security breach resulted in much criticism of how DOE safeguards nuclear materials and damaged the reputation of the DOE and supporting contractors. The protective force contractor lost its contract as a direct result of the breach. Y-12 and NNSA took actions to improve security at the site with an active focus on improving both safety and security cultures of the organization. "Ironically, the Y-12 breach may have been an important 'wake-up' call regarding the need to correct security issues at the site," as well as the importance of security and safety culture generally.[45]

3.4.5 Conclusion

This chapter demonstrated the importance of a robust safety and security culture within the nuclear enterprise and identified key building blocks necessary to create it. An important theme throughout the chapter was the importance of leadership, which plays a critical role in fostering

[43] G. H. Friedman, "Inquiry into the Security Breach at National Nuclear Security Administration's Y-12 National Security Complex," Department of Energy, August 2012. https://www.energy.gov/sites/default/files/IG-0868_0.pdf.

[44] Dan Zak, "The Prophets of Oak Ridge," *The Washington Post*, 2013. https://www.washingtonpost.com/sf/wp-style/2013/09/13/the-prophets-of-oak-ridge/.

[45] United States Department of Energy, Office of the Inspector General, Office of Audits and Inspections. "Special Report: Inquiry into the Security Breach at the National Nuclear Security Administration's Y-12 National Security Complex," US Department of Energy, 2012. https://www.energy.gov/sites/prod/files/IG-0868_0.pdf.

healthy cultures, which in turn sustain a strong, agile workforce able to meet the demands of a changing security environment. Such a workforce is inclusive, not afraid to identify and admit to failures, and able to limit the spread of toxic subcultures within an organization. Leaders who can articulate the immense value of safety and security and promote healthy cultures are therefore force multipliers, strengthening the nation's nuclear security posture. The leadership necessary to foster strong safety and security cultures within the U.S. nuclear enterprise did not appear overnight, but evolved over decades of dedicated political and financial commitment. Continued long-term investment of intellectual, financial, and political resources will be necessary to ensure that such leadership continues into the future.

References

Aegerter, G. "Nuclear Plant Workers in Hot Water After Alleged Plot to Rob Armored Car Goes Awry," *NBC News*, November 18, 2013. https://www.nbcnews.com/news/world/nuclear-plant-workers-hot-water-after-alleged-plot-rob-armored-flna2d11612598.

Bachner, K. *Overview of Nuclear Security Culture*. BNL-212323–2019-IN, Non-proliferation and National Security Department, Brookhaven National Laboratory, USA, November 2019. https://www.osti.gov/servlets/purl/1574910.

Babu, R.M. "An Indian Perspective on Cybersecurity," in *India-United States Cooperation on Global Security: Summary of a Workshop on Technical Aspects of Civilian Nuclear Materials Security*, ed. Rita Guenther, Micah Lowenthal, Rajaram Nagappa, and Nabeel Mancheri. Washington, DC: The National Academies Press, 2013. https://indianstrategicknowledgeonline.com/web/India-United%20States%20Cooperation%20on%20Global%20Security.pdf.

Basrur, R. and Steinhäusler, F. "Nuclear and Radiological Terrorism Threats for India: Risk Potential and Countermeasures," *The Journal of Physical Security* 1, no. 1 (2004).

Cameron, K. and Quinn, R. *Diagnosing and Changing Organizational Culture*. San Francisco, CA: Jossey-Bass, 2006.

Cronk, T.M. "DoD Must Rethink, Prioritize Strategic Deterrence," *DoD News*, October 21, 2020. https://www.defense.gov/Explore/News/Article/Article/2389931/dod-must-rethink-prioritize-strategic-deterrence/.

Defense Threat Reduction Agency. *About DTRA*. Retrieved April 26, 2021 from https://www.dtra.mil/WhoWeAre/.

Friedman, G.H. *Inquiry into the Security Breach at National Nuclear Security Administration's Y-12 National Security Complex*. Department of Energy, August 2012. https://www.energy.gov/sites/default/files/IG-0868_0.pdf.

Global Centre for Nuclear Energy Partnership. "About GCNEP." https://www.gcnep.gov.in/about/about.html.

Global Centre for Nuclear Energy Partnership. *GCNEP Newsletter, SNSS Special* 1, no. 3, May 2015. https://www.gcnep.gov.in/downloads/newsletter/GCNEP%20Newsletter%20Vol-1%20Issue-3%20May%202015.pdf.

Government of India, Atomic Energy Regulatory Board. "Acts & Regulations, Rules," https://aerb.gov.in/english/acts-regulations/rules.

Government of India, Atomic Energy Regulatory Board. "Regulatory Inspections of Operating NPPs," July 2019. https://www.aerb.gov.in/images/PDF/NPP-RI-July-2019.pdf.

Government of India, Ministry of External Affairs. "Nuclear Security in India," March 2014. https://www.mea.gov.in/in-focus-article.htm

Gray, A. U.S. "Air Force Officers Fired Over Nuclear Mix-Up," *Reuters*, October 20, 2007. https://www.reuters.com/article/us-usa-military-nuclear/air-force-fires-commanders-over-nuclear-mix-up-idUSN1930047820071019.

Hyken, S. "Drucker Said Culture Eats Strategy for Breakfast,' *Forbes*, December 5, 2015. https://www.forbes.com/sites/shephyken/2015/12/05/drucker-said-culture-eats-strategy-for-breakfast-and-enterprise-rent-a-car-proves-it/#7a7572822749.

International Atomic Energy Agency (IAEA). *Nuclear Security Culture: Implementing Guide*. International Atomic Energy Agency, 2008. https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1347_web.pdf.

International Atomic Energy Agency (IAEA). *Computer Security at Nuclear Facilities*. IAEA Nuclear Security Series No. 17 Technical Guidance. International Atomic Energy Agency, 2011. https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1527_web.pdf.

International Atomic Energy Agency (IAEA). *Self-Assessment of Nuclear Security Culture in Facilities and Activities: Technical Guidance*. IAEA Nuclear Security Series No. 28-T, International Atomic Energy Agency, 2017. https://www-pub.iaea.org/MTCD/Publications/PDF/PUB1761_web.pdf.

International Atomic Energy Agency. *The Nuclear Safety and Nuclear Security Interface: Approaches and National Experiences*. IAEA Technical Reports Series No.1000, 2021. https://www-pub.iaea.org/MTCD/Publications/PDF/PUBDOC_1000_web.pdf.

Johnson, J., Kartchner, K., and Larsen, J. *Strategic Culture and Weapons of Mass Destruction: Culturally Based Sights into Comparative National Security Policymaking*. Basingstoke: Palgrave Macmillan, 2009.

Joseph, G. "Secure Network Access System (SNAS)," in *BARC Newsletter Founder's Day Special Issue*, Government of India, Bhabha Atomic Research Centre, October 2014. https://www.barc.gov.in/barc_nl/2014/spl2014.pdf.

Kotter, J. *Leading Change*. Boston, MA: Harvard Business School Press, 1996.

Kotter, J. P. "Implications for the Twenty-First Century," in *The Organization of the Future*, ed. J. Kotter (pp. 174–175). Boston, MA: Harvard Business Review Press, 2012.

Khripunov, I. "Nuclear Security: Attitude Check," *Bulletin of the Atomic Scientists*, 61, no. 1 (January 2005). https://doi.org/10.2968/061001013.

Khripunov, I. *Nuclear Security Culture: The State of Play*. International Nuclear Security Education Network, June 2018.

Kumar, R. "Technologies and Physical Security of Nuclear Materials: An Indian Perspective," in *India-United States Cooperation on Global Security: Summary of a Workshop on Technical Aspects of Civilian Nuclear Materials Security*, ed. Rita Guenther, Micah Lowenthal, Rajaram Nagappa, and Nabeel Mancheri. Washington, DC: The National Academies Press, 2013. https://indianstrategicknowledgeonline.com/web/India-United%20States%20Cooperation%20on%20Global%20Security.pdf.

MacDonald, E. "Five Things Everyone Should Know About the Nuclear Posture Review," Union of Concerned Scientists, October 4, 2021. https://allthingsnuclear.org/emacdonald/five-things-everyone-should-know-about-the-nuclear-posture-review/.

Mishra, S. and Jacob, H. *Nuclear Security Governance in India: Institutions, Instruments, and Culture (2019)*. SANDIA REPORT SAND2020–10916. Sandia National Laboratories. https://www.osti.gov/servlets/purl/1678824.

Mishra, U.C. and Pradhan, A.S. *Loss and Recovery of Radiation Sources in India*. XA9949014, International Atomic Energy Agency, 1998. https://inis.iaea.org/collection/NCLCollectionStore/_Public/30/008/30008061.pdf.

Nordhaus, T. "Time to Stop Confusing Nuclear Weapons with Nuclear Power," *The Hill*, May 14, 2017. https://thehill.com/blogs/pundits-blog/energy-environment/333329-time-to-stop-confusing-nuclear-weapons-with-nuclear/.

O'Hanlon, M. E. *The Other 4+1: Biological, Nuclear, Climate, Digital, and Internal Dangers*. Brookings Institute, January 25, 2021. https://www.brookings.edu/research/the-other-41-biological-nuclear-climatic-digital-and-internal-dangers/.

Parthemore, C. *The Climate-Nuclear-Security Nexus: A Collision Course or a Road to new Opportunities?* The Center for Climate and Security, May 2, 2016. https://climateandsecurity.org/2016/05/briefer-the-climate-nuclear-security-nexus-a-collision-course-or-a-road-to-new-opportunities/#_edn1.

Rajagopalan, R., *Nuclear Security in India*. Observer Research Foundation, January 2015. https://www.orfonline.org/wp-content/uploads/2015/02/NUCLEAR_SECURITY_IN_INDIA.pdf.

Rajagopalan, R. *Nuclear Security in India*. Second Edition, Observer Research Foundation, October 2016. https://www.orfonline.org/wp-content/uploads/2016/10/ORF_Monograph_Nuclear_Security.pdf.

Richard, A. C. *The Future of Strategic Deterrence and Nuclear Modernization*. Brookings Institute, May 5, 2021. https://www.brookings.edu/events/the-future-of-strategic-deterrence-and-nuclear-modernization-a-conversation-with-adm-charles-richard/.

Schabracq, M. *Changing Organizational Culture: The Change Agent's Guidebook*. Chichester, UK: Wiley, 2007.

Schein, E. *The Corporate Culture and Leadership*. San Francisco, CA: Jossey-Bass, 2004.

Schein, E. *Organizational Culture and Leadership*. Hoboken, NJ: Wiley, 2017.

Singh, S.R., Karthik, K., Behera, C., Tabin, M., Bhadwaj D.N., and Swain, R. "Fatal Radiation Exposure due to Careless Disposal of Cobalt-60 from a University Lab," *Journal of Indian Academy of Forensic Medicine* 35, no. 3 (2013): 281–284. https://www.indianjournals.com/ijor.aspx?target=ijor:jiafm&volume=35&issue=3&article=024.

Tennessee Valley Authority. *Nuclear*. Retrieved November 21, 2023 from https://www.tva.com/energy/our-power-system/nuclear.

United States Department of Energy. "Safety Culture Improvement Panel," Department of Energy, August 2018. https://www.energy.gov/sites/default/files/2018/08/f54/Safety%20Culture%20Improvement%20Panel%20Overview%20Trifold%20-%20508v2.pdf.

United States Department of Energy, Office of the Inspector General, Office of Audits and Inspections. *Special Report: Inquiry into the Security Breach at the National Nuclear Security Administration's Y-12 National Security Complex*. US Department of Energy, 2012. https://www.energy.gov/sites/prod/files/IG-0868_0.pdf.

United States Nuclear Regulatory Commission. *Safety Culture*, 2021. https://www.nrc.gov/about-nrc/safety-culture.html.

U.S. Department of Defense. *DoD Nuclear Weapon System Safety Program Manual*, 2021. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/315002m.pdf?ver=x45aWEVjJWieQw0euniZYw%3D%3D.

U.S. Department of Defense. *DoD Instruction 5230.16 Nuclear-Radiological Incident Public Affairs (PA) Guidance*, 2015. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/523016p.pdf.

U.S. Department of Defense. *Nuclear Posture Review*. Retrieved November 21, 2023, from U.S. Department of Defense. https://dod.defense.gov/News/Special-Reports/NPR/.

Zak, Dan. "The Prophets of Oak Ridge," *The Washington Post*, 2013. https://www.washingtonpost.com/sf/wp-style/2013/09/13/the-prophets-of-oak-ridge/.

CHAPTER 4

Emergency Response and Crisis Communications

R. S. Sundar, Daniela Helfet Cooper, Michael Hornish, and Alisa Laufer

4.1 An Indian Perspective

R. S. Sundar

The world continues to aim to produce clean energy with no carbon, and the energy sector strives to attain near zero greenhouse gas emissions. In order to combat the threat of a global warming, producing dependable, cleaner power is a global priority. As the most dependable source of carbon-free power generation providing around-the-clock energy supply

R. S. Sundar
Nuclear Power Corporation of India Limited (retired), New Delhi, India

D. H. Cooper
Department of State, Washington, DC, USA

M. Hornish (✉)
National Nuclear Security Administration, Department of Energy, Washington, DC, USA
e-mail: michael.hornish@nnsa.doe.gov

S. P. Kapur et al. (eds.), *The Challenges of Nuclear Security*, Initiatives in Strategic Studies: Issues and Policies,
https://doi.org/10.1007/978-3-031-56814-5_4

without interruption, nuclear energy is an important part of the power generation landscape. It is a critical pillar in the move towards to a carbon-free future. Many developing countries are setting their focus on carbon-free nuclear power generation as part of their energy mix to ensure a dependable source of cleaner power with the highest level of reliability and safety, thus ensuring energy security. Given the urgency of the climate challenge, decision-makers should ensure that nuclear energy is included in the discussion.

The COVID-19 outbreak is likely to leave a lasting impact on the future of energy production, distribution, and usage. Reduced global power consumption due to the worldwide lockdown has been one of the short-term effects of the pandemic. However, in the long-term, the demand for electricity is unlikely to diminish and governments (and their electorates) will be no less keen to ensure that their energy systems are reliable and more resilient than ever to future disruptions. So, what is the future for nuclear power? (Fig. 4.1).

According to the IEA, the largest low-carbon source of electricity in Europe, North America and, soon to be, Japan is nuclear power. Nuclear technology undoubtedly plays a major role in ensuring secure supplies of energy in many economies. Therefore, nuclear power should be seen as part of any country's energy mix, along with other sources of low-carbon energy generation. While wind and solar have lower capital costs and shorter construction and commissioning lead times, they are less consistent and constant than nuclear energy generation. Nuclear can provide a steady baseload of supply to complement other renewable energy generation technologies.

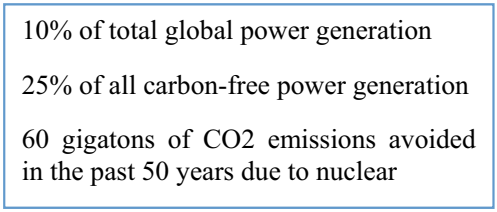

Fig. 4.1 International Energy Agency (*Source* International Energy Agency)

A. Laufer
RAND Corporation, Washington, DC, USA

Third and fourth generation technologies have taken into account decommissioning designed into the construction, commissioning, and operation of the nuclear facilities so that the decommissioning challenges we face from earlier generation technologies have been significantly mitigated.

Before the pandemic, there were challenges in finding suitable funding solutions for nuclear energy compared to the investment made in its greener alternatives. The low-carbon nature of nuclear power still goes unrecognized in most countries' policies on clean electricity and frameworks for clean energy financing. Even in countries where there is general support for nuclear, there is a possibility that the role of nuclear power in their energy systems will be undermined.

4.1.1 Public Relations

Nuclear power's reputation is among its biggest hurdles. In the public imagination, nuclear power presages disaster. On one side are purists who believe nuclear power is not worth the risk and that the exclusive solution to the climate crisis is renewable energy. The opposing side agrees that renewables are crucial but adds that the society needs a baseload of power to provide electricity when the sun is not shining and the wind is not blowing. Nuclear energy, being far cleaner than oil, gas, and coal, is a natural option, especially where hydroelectric capacity is limited.

Though the word "nuclear" evokes images of landscapes pulverized by atomic calamity—Hiroshima, Chernobyl, Fukushima—nuclear power plants are relatively safe. Proponents point out that nuclear power produces huge amounts of electricity while emitting low or no carbon. This separates it from fossil fuels, which are consistent but contribute heavily towards global warming as well as renewables, which are clean but weather dependent. Further, as Eric Dawson, a grassroots campaigner at Nuclear New York argued, "Any energy policy has pros and cons, and we feel, after putting a lot of scrutiny on it, that the pros outweigh the cons of nuclear energy."[1] Many scientists and experts believe nuclear power is necessary to achieve carbon neutrality by 2050. In order to prevent the dangers of climate change, it is crucial to advocate for nuclear power.

[1] Daniel Van Boom, "How Nuclear Power Plants Could Help Solve the Climate Crisis," CNet, November 16, 2021, https://www.cnet.com/news/how-nuclear-power-plants-could-help-solve-climate-crisis/.

Reactor core meltdowns, while rarer than once-in-a-generation, have severe consequences. And the question of how to best store nuclear waste is contentious: The US storage site at Yucca Mountain was initiated but it abandoned the project, though Finland, France, and Canada seem to have found potential solutions.

4.1.1.1 Communications

Public relations depend on building trust and a long-term relationship with the public through platforms such as print and electronic media, which play a vital role in disseminating positive news to people. Additionally, social media has become a common communication medium amongst Indians. However, there is the issue of misinformation. Misinformation can be spread across communication mediums unintentionally or as a result of malicious intent. There are lessons to be learnt during the COVID-19 pandemic about the impact of social media and its ability to spread information—accurate and false—at a much faster rate than traditional modes of communication.

It is essential to communicate true and accurate information to the public during a crisis that will help develop a more efficient and effective response. Below are a few real-life experiences to illustrate this.

4.1.1.2 Three Phases of Communication

During Construction of a Nuclear Power Project (NPP)

Communication is important from the time when a nuclear power plant is being constructed in order to address the concerns of local people. Communication with journalists, educational institutions, and opinion-makers must be open and transparent in order to avoid rumours and increase trust amongst the locals. Providing employment opportunities to local and affected people also can help to establish trust in the early stages.

The critical link is the process of communication. How the plant communicates with temporary workers, for instance, illustrates this. Security or plant personnel may, at times, treat temporary workers poorly, which may exacerbate the negative connotations attached to nuclear power. Furthermore, India is a multilingual society and a language barrier may act as an irritant during interaction between the locals and security agencies. Communication in local languages is, therefore, necessary. It is also important to conduct workshops for journalists to help them appreciate nuclear power projects and share relevant safety and security

information as a confidence-building measure. Interactions need to be a continuous process, rather than one time action.

Communication During Normal Plant Operating Conditions
It is important for senior management officials and public relations officers to interact with journalists and media personnel regularly and provide honest and technically competent responses. This is to build a long-term engagement, treating media as an important stakeholder in the area of nuclear safety and security. Creating a local narrative involving different aspects of nuclear power, the operations of the power plant, and the response mechanisms and processes in case of contingency situations, can help build a positive and responsive relationship with the public.

Communication During Crisis
Crisis communication is different from communication that is executed during normal operating conditions. It is important to provide as much information as possible, with immediate responses as well as subsequent clarifications, to the media and locals on the workings of the nuclear power plant and the situation at hand. This is particularly important in order to avoid misinformation. Depending on the stakeholder, communication could focus on technical aspects of the crisis as well as the mitigation measures that are being undertaken, which could be a source of assurance to the larger population.

Clear, Precise Communication
Along with timeliness, what is conveyed and how it is conveyed are important. When handling emergencies during the construction phase or plant operation phase, it is important to: increase people's confidence in the plant and its operations; build trust between the organisation and the locals through appropriate communications and the broader approach; provide information on the project and share details on how the project will benefit the region, such as economic growth; provide assurances related to basic livelihood; and provide also an outline of the crisis management and mitigation plans should there be a disaster.

4.1.1.3 A Case Study: Kudankulam NPP
For the first time in a nuclear power project at Kudankulam NPP in India, there has been marketing and communication about the positive

and safety aspects of nuclear power. Previously, the lack of proper information had led to fear and panic. The methods used to do so were carried out via commercials in various media outlets, handouts, interactions with educational institutions, and other outreach programmes.

Commercials on Media Platforms

Officials put out short videos and audio advertisements on TV channels as well as the radio to disseminate accurate information about nuclear power and also about the nuclear power plant operations to the public. Although expensive, these commercials were able to reach the right audience in a short time span. They provided clear information on the safety of the nuclear power project and addressed the concerns of the local population.

Site personnel also actively participated in TV programs to increase awareness. For example, questions raised on the transfer of heat from the reactor primary circuit to the secondary water circuit were explained verbally by the site personnel in a simplified manner. Some of these explanations were done in a public debate, as well as through videos and other means of communication. It was found that simplicity in communication helped reach a wider audience and strengthened the support base among the local population. For instance, the classic example of cooling down hot milk using water as a medium was used to explain why radioactivity will not spill over to the environment from the reactor circuit. This was a serious concern among the local community of fishermen, and providing such simple examples assuaged their fears.

Handouts

The public outreach team made small handouts and pamphlets to distribute directly to local people. In order to have a wider reach, the handout information was disseminated in local languages such as Tamil, Malayalam, and English. Copies were distributed at railway stations and bus terminals, and were also widely circulated during government festivals. These handouts were helpful in alleviating the fears and doubts raised by local people and protestors.

Interaction with Educational Institutions

Public outreach through educational institutions played a vital role. By providing detailed presentations as well as engaging in Q&A sessions with local audiences, students and academics were essential in expanding local understanding about nuclear power plant safety and design features, such

as ability to withstand extreme weather conditions like cyclones, tsunamis, or earthquakes. In the case of earthquakes, for example, project and plant officials used simple examples such as the structural integrity of 1000-year temples in local areas and their ability to withstand extreme conditions as a result of stable conditions of the land in the area as well as the safety aspects of the site.

Outreach Programs

Arranging site visits for students, local people, and other individuals also proved useful in raising awareness, building trust, and reducing apprehensions about nuclear power. These site visits included safety presentations, plant site visits—including construction sites such as the reactor hall—as well as familiarization with safety protocols and procedures at the site. Senior management personnel also participated at times, adding creditability to the outreach programmes.

4.1.2 Crisis Communication

Nuclear power plants are generally built with highest safety standards to meet internal and external challenges. All NPPs are designed to withstand conditions beyond the general design-basis threats in order to protect plant personnel, maintenance teams, and local populations in case of an incident or accident. In order to face any event occurring at a nuclear power plant, emergency preparedness is made mandatory. It is a regulatory requirement and must be fulfilled by all nuclear power plants in India even before attaining the first chain reaction.

Exercises are designed and conducted in each of the nuclear power stations in India.[2] The first type of exercise is called plant emergency exercise which involves the plant management under plant personnel. This

[2] Much of this is based on personal experience but these can be found in various reports produced by the atomic energy agencies in India. See, "Chapter 7: Emergency preparedness for nuclear and radiation facilities," in Department of Atomic Energy, *Report of the Comptroller and Auditor General of India on Activities of Atomic Energy Regulatory Board for the year ended March 2012*, Report No. 9 of 2012-13 (Performance Audit), https://saiindia.gov.in/uploads/download_audit_report/2012/Union_Performance_Atomic_Energy_Regulatory_Board_Union_Government_Atomic_Energy_Department_9_2012.pdf; "Emergency Preparedness," in Atomic Energy Regulatory Board, Annual Report 2019, https://www.aerb.gov.in/images/PDF/Annual_report/ar2019/chap5aerbannualreport2019.pdf.

exercise is conducted every 3 months to ensure that all operating crews are well trained to face any emergency situation.

The second type of exercise is called site emergency exercise, which involves all facilities that exist within a 1.6 km radius of the nuclear power plant. This exercise is conducted annually and requires the participation of all site management personnel and the staff including contract manpower.

The third type of exercise is called off-site emergency exercise. This exercise is held once in two years to familiarize all plant personnel as well as district authorities who are in charge of the areas beyond the plant boundary.

An AERB-approved document by the district and/or state authorities must be available to conduct these exercises. The document specifies the diverse roles of the various agencies involved. The nuclear power plant assumes the lead and ensures all personnel and district authorities are clear about their responsibilities. Various training programs are conducted to emphasize these aspects. For example, off-site emergency exercises are conducted on the basis of a pre-decided scenario and involve observers from regulatory bodies and other organizations in the exercise. Further, feedback sessions are held right after the exercise to evaluate performance and identify areas for improvement. As a result, new safety, security, protection, and mitigation measures are conceptualized and implemented at sites for use in an actual emergency. Crisis communication can succeed only when personnel are well versed with the various mitigation measures to be adopted during an emergency.

Nuclear emergencies in future are unlikely to happen from any known scenarios and conditions that are understood and incorporated in the risk design. The Fukushima accident was a reminder that severe nuclear accidents beyond those postulated in the design can never be completely ruled out. Therefore, emergency planning and preparedness are crucial to prepare for unlikely events. During a nuclear emergency, intervention must be carried out in a manner that ensures that the actions taken result in more good than harm. The Fukushima accident demonstrated that responses can cause more harm than good, if not properly justified and optimised.

Nuclear and associated hazards allow a certain amount of time to respond, as the immediate impact of an accident may not be high. The actual consequence also depends on the cumulative dose of radiation over a period of time. In addition, the design of PHWRs, which are the main stay of the Indian program, has inherent strength against the propagation

of an accident sequence, and has been further enhanced through features that offer additional resistance against the release of radio nuclides.

Since the characteristics of the radioactive material that can be released from a nuclear power plant are known, response actions for mitigation of consequence can be well-planned. Typical response actions include: taking potassium iodide tablets, sheltering in place, restrictions on food and water consumption, and in some cases, evacuation. Simple protective measures like taking iodine tablets in a timely fashion, wearing protective gear when outdoors and avoiding drinking water from open source are very effective. The COVID-19 response protocols have made it easier for the public to understand various protective methods, such as the use of masks and protective coveralls, and preemptive measures, such as the administration of potassium iodate tablets as a prophylactic similar to a vaccine.

4.1.2.1 Early Phase Decision-making

The response to the Fukushima accident showed that early phase decision-making is the most critical part of overall emergency management. The early phase is characterized by high levels of uncertainty particularly regarding plant conditions and measurements from field. In this phase, sudden changes are frequent and coupled with a lack of external technical support. As a result, decision-makers may under or overreact to the evolving situation (Table 4.1).

The core of emergency management, especially during the early phase, is decision-making that emphasizes the criteria and basis for a response. Early phase decision-making is predicated upon the ability to identify

Table 4.1 Emergency management timeline

Preparedness	*Response*		*Recovery*
	Early (Hours-days)	*Intermediate (Weeks-months)*	*Late phase (Months-years)*
Planning stage	Immediate decisions based primarily on the status of the plant and the prognosis for worsening conditions	Releases are under control and no longer increasing and reliable environmental measurements are available for decisions on protective actions	Recovery actions to reduce radiation levels in the environment to acceptable levels

and execute a course of action promptly and adequately in order to protect the public and emergency workers. A host of actions are critical in managing the outcome of an emergency situation, including:

- Meeting to evaluate early phase decision-making during emergencies at NPPs and during the conduct of emergency exercises.
- Discussing and emphasizing the importance of managing the early phase of an emergency.
- Placing an emphasis on response actions that do more good than harm.
- Improving understanding and knowledge of plant conditions/ parameters.
- Emphasizing the importance of linkages between plant conditions and the emergency response actions.
- Presenting consolidated feedback regularly from the stations, NPCIL headquarters, and BARC experts on current emergency management efforts, including emergency exercises being carried out.
- Providing emphasis on Emergency Action Level (EAL)-based decision-making during emergency exercises, which strengthens the preparedness for the early phase of an emergency.

There is also a four-point strategy that can help prepare NPPs to deal with emergency situations:

- Develop criteria for early phase decision-making in advance of an emergency (EALs, OILs, etc.);
- Determine the basis and principles for public protection during different phases of emergency (doing more good than harm);
- Establish an emergency plan with an effective and coordinated operational framework;
- Revise emergency exercise methodology as needed.

4.1.2.2 Emergency Action Levels

One of the most important aspects of emergency preparedness is to establish mechanisms for timely classification of nuclear and radiation emergencies and their declaration to the larger public. Such a mechanism provides assurance to the emergency director and justifications for the declaration. The International Atomic Energy Agency (IAEA) mandates

that "the emergency classification system shall be established with the aim of allowing for the prompt initiation of an effective response in recognition of the uncertainty of the available information."[3]

In order to address this, nuclear power units should use a deterministic approach to pre-analyse all industrial control systems (ICs) for their consequences. They should also determine the imminence of release through a PSA Level 2 study. The utility needs to identify plant-specific threshold values for instrumentation readings and status indications, which if exceeded would determine if specific ICs are met. This will help in timely identification of the emergency classification and declaration. These plant-specific instrument readings, status reports, and threshold values are a part of the Emergency Action Levels. There are three fundamentally different types of EALs:

- Symptom-based EALs, which are site-specific instrument readings or other observable or quantifiable thresholds
- Event-based EALs, which are more subjective criteria requiring the judgment of the operating staff; and
- Fission barrier-based EALs, which are developed through the analysis of the full range of postulated conditions that can result in radiological consequences, including very unlikely scenarios such as reactor core melt.

Analysis of results and understanding of the attributes and purpose of each emergency class (alert, plant, on-site, and off-site) are used to align each EAL appropriately (Fig. 4.2).

Information from other measurements like those provided by Decision Support Systems (DSS) instruments could aid in making the decision-making process more effective. For example, a DSS directly linked with real-time data from the weather bureau can be simultaneously monitored by the headquarters-based design and operation teams. Reasonable assurance of the correct approach for precautionary or urgent protective actions comes through in such processes. A Wind Profile Radar system is being planned at Kalpakkam site as part of DSS (Fig. 4.3).

[3] IAEA Safety Standards, "Preparedness and Response for a Nuclear or Radiological Emergency," 2015, https://www-pub.iaea.org/MTCD/Publications/PDF/P_1708_web.pdf.

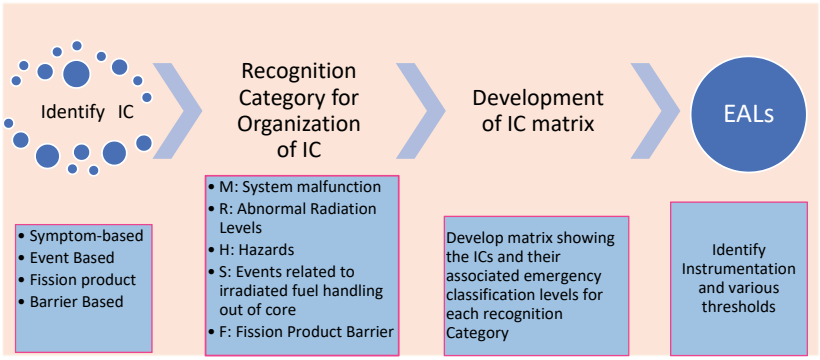

Fig. 4.2 EAL development scheme

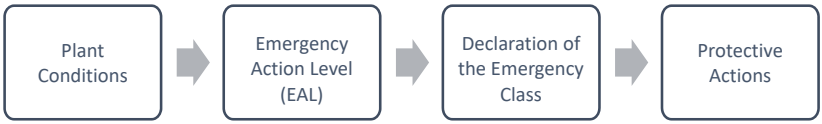

Fig. 4.3 Improved framework for taking protective actions

Protective measures to mitigate the consequences of a nuclear or radiological accident can be divided into precautionary (preventive), urgent (early), and late (recovery) measures. The initial protective actions are implemented on a precautionary basis following a set of accident sequences. The precautionary (preventive) and urgent (early) measures, which may be required to be decided as part of the initial phase of a developing emergency with possible off-site consequences, need special care. If overdone, these actions may result in more damage than benefits. The "early" phase response comprises of:

i. "Event/response initiation," including recognition of an emergency situation and initiation of response.
ii. "Crisis management," including efforts to characterize and gain control over the accident scenario and implementation of protective measures that must be taken promptly in order to be effective.

During this phase, decision-making needs to be done with little or no input from outside technical support or analysis by persons beyond the plant authorities.

Protective action to reduce radiological consequences will depend on amount, time, composition, and frequency of release. For example, for certain types of release, sheltering along with food control is enough. For another type of release, however, temporary evacuation may be required. EALs were developed such that they can differentiate between these different release situations. EALs provide a graded approach to protective action commensurate with the consequences.

4.1.3 Improved Emergency Exercise Methodology

Previous radiological emergency exercises did not adequately challenge the skills of operating and maintenance staff and did not result in appropriate use of emergency operating procedures. As a result of discussions between plant unit heads, the decision to move to desktop exercises was made. Observations from peer-review reports and meetings with regulators help evolve and implement desktop exercises at nuclear power plants (Table 4.2 and Fig. 4.4).

4.1.3.1 Features of New Exercise Methodology

The exercise is designed to challenge all organizations playing a role in responding to a nuclear emergency. It spans a wide spectrum of response

Table 4.2 Improvements to exercise approach

Previous approach	*New approach*
Predetermined Scenario	Exercise Scenario not known
Well-Rehearsed	Observables in the form of inject (by controller)
Emergency classification based on event	Emergency Classification based on EALs
Protective action based on field data	Protective actions during early phase of emergency based on pre-calculated Source Term and projected dose, and later by real-time analysis
Focus on coordinated field actions	Focus on decision-making in early phase and necessary capabilities to enhance preparedness in early phase

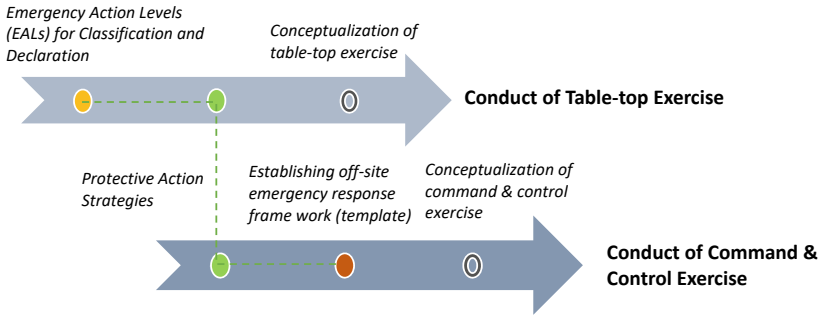

Fig. 4.4 Integrated approach for finalization of emergency exercise policy

functions that would normally take place. The exercise evolved from the initial indications of a problem at the plant to the subsequent notification of response organizations. The accident scenario is not pre-briefed to respond, but is revealed gradually, as the accident scenario unfolds. Response organizations are asked to analyze the impact on actual environmental and metrological conditions. Emergency operations centres were then activated as the scenario demanded. The DSS are used to determine the affected area according to prevailing meteorological conditions, followed by recommendation of actions to protect the public to district authorities (Table 4.3 and Fig. 4.5).

Finally, acceptance by the Operation and Maintenance team and other supporting elements, such as the radiological protection team and the environment survey laboratory team, is also crucial.

The teams that participate in the desktop exercises understand the scope of work and importance of decision-making in the early phase. Prior exercises were based on site-field measurements data; this slowed the process. Also, online weather-based and source term-based online digital platforms were previously not available. The dynamic wind pattern data along with readings from field radiation level instruments were extremely beneficial in the decision-making process. Post-Fukushima, engineering upgrade measures, including emergency operating procedures, have been incorporated in all sites. Their appropriate use during desktop exercises proved to be crucial in handling emergencies.

Moreover, the headquarters team and regulators visit the site in advance to brief relevant personnel about the surprise element in the desktop exercise. The response of the operation team and site teams is

Table 4.3 Scope for participating organizations

NPP site	*District administration*	*DAE-RERD*	*AERB*
Identification, declaration & notification of Emergency Class	Activation of Emergency Operation Centre	Protective action recommendation in the intermediate phase	Activation of NREMC (Nuclear and Radiological Emergency Monitoring Centre)
Activation of PECC, SECC and off-site emergency support center	Field exercise to reach identified villages for warning and early response actions under unknown realistic scenario	Check for Residual dose and its approach towards lower bond of reference level and other criteria for termination	Observation of conduct of exercise
Protective action recommendation for early phase	Preparation of write-up for media briefing (focus on crisis communication)	Recommendation for termination of emergency	Corrective action and improvement in the exercise methodology (policy)

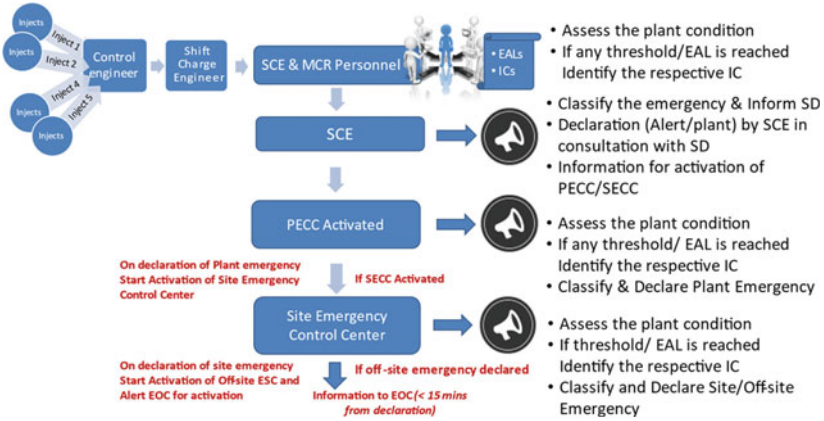

Fig. 4.5 Improved exercise planning process

based on the situation, which evolve as time progresses. For the NPP personnel, it is ideal to combine source term with meteorological data, predict the scenario under worst- and best-case scenarios, and adopt corrective measures in advance.

Weather patterns have been very tricky, but with more monitoring of locations within the first 16 km Emergency Planning Zone (EPZ), the exact number of villages or localities likely to be impacted by a radioactive plume can be predicted more easily. Also, at times ground level release can occur due to prevailing weather situations; in those cases, the personnel within the site premises need to be protected. On sites where operating and construction sites co-exist, a large number of people have to be protected including construction teams, security and other defence personnel, in addition to the teams executing the rescue mission. With the advent of faster computers and critical modeling of individual reactors, the validation of modeling is quite reassuring.

4.1.4 Conclusions

Following good practices, especially in communication and outreach in emergency situations is critical to keeping the crisis under control. Some of the key points for consideration in this regard are to work on building trust from the initial stages of an NPP in order to buy in the support from the local population that will ensure greater support and compliance with measures during emergency situations. Localized issues need to be addressed to gain confidence. The general population needs to be taken into confidence including plant visits and explaining the beneficial and safety aspects of Nuclear Power. Inclusiveness of the local nearby population is beneficial in trust and confidence-building measure in a long way. This is to sustain trust and communication over time, and ensuring that there is clear and direct information to the people, in partnership with the District and State machinery. Ensuring spread of accurate information through social and traditional media and providing clarification at the earliest in case of misinformation are critical in the area of nuclear security. This can be done by 24 $\times$ 7 emergency response centres that remain functional and coordinate across relevant agencies.

In order to achieve long-term acceptability of nuclear power in India, some measures that may be undertaken include skilling of local populations with the prime goal of employability in NPP construction or in general fields of specialization; periodic distribution of Potassium Iodate

tablets (including replacement based on shelf life) to individual residents in the Emergency Planning Zone of 16 km. At present, these prophylactics are stored in Primary Health Centers and need to be distributed by the local health authorities. This would reduce burden on state teams that would have to distribute it in a situation where the administering time is essential to prevent radioactive Iodine intake. Thyroid gets saturated with Potassium iodate and prevents absorption of radioactive iodine. Infrastructure developments in the area adjacent to NPPs like educational institutions, healthcare centers, skill centers, communication network, etc. including reliable electric power supply are consequential in managing nuclear security. Synchronized communication by nuclear power units, regulators and agencies such as the NDMA to ensure public confidence is also important. Building a robust weather monitoring system with dual sensors for identifying wind direction, velocity, local radiation monitors within the Emergency Planning Zone of 16 Km/10 miles as well integrating these with the prediction models being used presently while investing in advanced technologies like the use of drones for air sampling, air samples collection to measure radioactive particles, wind velocity can be enormously useful. The information required during any conditions can be gathered quickly and are accurate. Additionally, drones can be used to survey plant areas in conditions similar to Fukushima, where the accessibility was an issue due to debris. Establishment of reliable weather and radiation levels monitoring stations and transmission of data to Emergency control centre remotely within 32 Km radius of power plants are also required.

4.2 A U.S. Perspective

Daniela Helfet Cooper, Michael Hornish and Alisa Laufer

Emergencies, crises, and catastrophes riddle the world daily and yet no two events are exactly alike. While most of the elements that comprise a response remain consistent across events, the unique nature, scope, timing, and location of an event invariably ensure that some key differences exist. Whether this is a result of the material associated with a crisis, or its geostrategic location, or even something as seemingly simple as the time of day, the fact stands that there will always be something novel—some friction that forces responders to adapt. And while some may consider this fact daunting, there is room for optimism: This means

that there is *always* something to learn and improve upon. This is especially true of radiological and nuclear emergencies, which carry uniquely complex considerations. From Fukushima to Three Mile Island to Chernobyl, each crisis has posed a unique set of challenges. This increased layer of complexity understandably causes many to pause or even shy away from the high-stakes world of emergency response. However, it is that same dynamic—and the corresponding commitment of the response community to do everything possible to proactively anticipate and mitigate this inevitable friction—that has shaped the modus operandi for emergency response as we know it.

This chapter summarizes several best practices in emergency response and crisis communications for use in radiological and nuclear emergencies. The best practices herein encapsulate many years of lessons learned from our country's greatest successes and failures—some of which have neither radiological nor nuclear components, but directly shaped United States response doctrine for emergencies, crises, and disasters writ large. The United States nuclear security community has largely agreed upon these strategies based on its experiences, resources, capabilities, and systems of governance. But these practices are not the "best" choice for everyone—each comes with tradeoffs. For example, the United States chooses to prioritize lifesaving in response operations—even when funneling resources to lifesaving can compromise other elements of the response. The United States also takes an "incident until proven accident" approach to minimize risk, even when the resulting need to preserve potential evidence slows the decontamination process. The United States' approach is neither the only nor the best way to address these crises. As different countries balance different threats, resources, and constraints, they naturally emerge with different priorities and strategies for responding to emergencies.

Reflecting on the United States' experiences and priorities, this chapter begins by discussing U.S. best practices for response operations broadly, focusing on several elements that the United States has found critical to success including: (1) building a tiered response structure, (2) identifying and delegating necessary response authorities, (3) establishing predetermined standards and thresholds for action, (4) developing detection, monitoring, and modeling capabilities, (5) integrating pre- and post-event response communities, and (6) building robust exercise programs and after-action processes. We then take an in-depth look at best practices for communications, which is a key part of crisis response.

There is no better way to explain the emergence of these best practices than through real-world examples of crises that necessitated them. The chapter therefore offers two in-depth case studies that demonstrate the need for these practices: the Three Mile Island accident and the Fukushima Daiichi nuclear disaster.

We close the chapter with a discussion of how emerging threats may impact the future of radiological and nuclear crisis response and provide recommendations for ways through which bilateral partnership can meet these challenges. We do so not because we know the solution, but because we know tomorrow's challenges will require us to once again grapple with our plans and adapt our approach. Our best practices today may not be the best practices of tomorrow and indeed, there is always more we can do to increase our prospects for success.

4.2.1 Tiered Response Structure

An emergency is, by definition, "a serious, unexpected, and often dangerous situation requiring *immediate action*."[4] If immediate action is required, one must quickly identify the appropriate steps and determine whether those on the scene are *equipped* and *empowered* to handle the situation. If not, an individual on-scene must have the wherewithal and training to identify what additional support is required and determine who can provide it. These are, at their core, the key initial decision points at nearly every level of a crisis. *Do I have what I need or do I need to request more support?*

A fundamental element of an effective response is the implementation of a *tiered* response structure. A tiered response structure starts at the lowest jurisdictional level and allows local officials to request and integrate more expertise as needs are identified. A tiered response structure can be established in a number of ways—both formally and informally—depending on the nature and scope of an emergency. However, for complex crises like nuclear or radiological events, formal, detailed, and *practiced* tiered response structures—also referred to as response frameworks—are imperative. While this chapter focuses on nuclear and radiological events, many best practices utilized today are born out of

[4] Emergency. In *Oxford Online Dictionary*, 2019. Retrieved from https://en.oxforddictionaries.com/definition/emergency.

other more typical types of crises, ranging from natural disasters to deliberate chemical attacks.

One of the most pivotal and complex crises to impact the contiguous United States occurred in 2005 when Hurricanes Katrina, Rita, and Wilma rocked the U.S. Gulf Coast region in quick succession. This marked the first time in modern history that such a large swath of the country was impacted near-simultaneously, stressing the general capacity—and, specifically, the coordinating mechanisms—that were established to enable a tiered response across local, state, and federal entities. The insufficient capacity and integration across various levels during the response—among other shortfalls—led Congress to enact the Post-Katrina Management Reform Act (PKMRA). The legislation that followed PKMRA directed the Department of Homeland Security to develop and issue the National Response Framework, or NRF, that is still utilized today.

The NRF establishes how the United States responds to domestic emergencies of any scale or type and applies to emergencies where the nature and scope require a federal response to supplement the state, tribal, or local incident response. Taking an all-hazards approach, the framework defines key roles, coordinating structures, consistent nomenclature, and incident management principles that enable a coordinated response across communities, tribes, states, the federal government, private sector partners, and non-governmental organizations. It also includes several support and incident annexes that provide further guidance for certain complex disasters. Among those incident annexes is the Nuclear/Radiological Incident Annex (NRIA) which provides guidance to all levels of government for planning, response to, and recovery from nuclear and radiological emergencies.[5] The NRF's guidelines enable responders at the tactical, operational, and strategic levels to conduct a unified response wherein roles, responsibilities, and authorities are clearly defined.

An underlying tenet of the NRF is its tiered response structure, meaning that all incidents will be managed first at the lowest jurisdictional level and supported by higher-level authorities or resources only when needed. This delegation of responsibilities allows local authorities

[5] U.S. Department of Homeland Security, *Nuclear/Radiological Incident Annex to the Response and Recovery Federal Interagency Operational Plans*, October 2016, https://remm.hhs.gov/NRIA_FINAL_110216.pdf.

to guide the response based on their knowledge of their community's unique needs and challenges. The principle of a tiered response structure was born out of multiple lessons learned and the United States continues to refine its supporting frameworks and authorities at every level, across nearly every field, to further reduce friction.

Since establishing the NRF in 2008, the United States has faced countless emergencies that have demonstrated a need for additional solutions to empower and more effectively support lower jurisdictional levels in a crisis. This reinforced another best practice: identifying and delegating necessary authorities to the lowest possible level.

4.2.2 Identifying and Delegating Necessary Authorities

In a crisis, people tend to look "up the chain" for approvals. This causes unnecessary delays and can temporarily paralyze a response. There are two concrete steps that all entities at all levels can take to expedite decision-making and the provision of assistance. First, these entities can proactively identify those within their organization with the authority to request and approve assistance. Second, they can delegate those authorities down to the lowest possible level. Doing so will dramatically streamline decision-making, increase access to critical resources, improve information sharing between responders and decision-makers, enable the provision of care, and reduce friction, confusion, and bureaucracy.

While this concept seems intuitive, few organizations know with certainty who is authorized to make a final decision. The more complex an incident or accident, the more likely individuals are to experience discomfort with unilaterally shouldering the burden of decision-making. This is especially true at the operational and strategic levels, but there are tactical-level examples of this challenge from real-world responses as well.

In 1995, five members of the religious cult Aum Shinrikyo released packages of sarin on five separate Tokyo subway lines. Overall, the Japanese local and national response to this unprecedented event was remarkable, but even the best real-world responses carry lessons learned—especially those involving chemical, biological, radiological, or nuclear (CBRN) materials. In the case of the Aum Shinrikyo attack, one of the more notable lessons pertains to the capabilities of Emergency Management Technicians (EMTs) on site and the actions they were—and were not—authorized to take.

Japanese law prohibits EMTs from performing certain procedures without the express consent of a doctor. Normally, EMTs obtain approval by calling the Tokyo Metropolitan Ambulance Control Center (TMACC). However, the TMACC became overwhelmed during the incident and EMTs failed to make contact, impeding the EMTs' ability to triage patients on-scene. Moreover, given the scale of the situation, the coordinating entity (Tokyo Metropolitan Fire Department) also became overwhelmed and requested medical assistance from nearby hospitals to assist the EMTs. St. Luke's Hospital dispatched personnel to various stations. When they arrived, however, most casualties had already been processed or transferred to higher echelons of care, in many cases back to St. Luke's Hospital. The reduced staff remaining at St. Luke's was not adequate to handle the large numbers of incoming patients.

While local, provincial, state, regional, and/or national authorities and assets may not wish to waive certain restrictions during normal circumstances, a solution may be to identify circumstances wherein those restrictions are waived and authorities are delegated. The United States has learned this time and again and can still do more to anticipate friction that may arise during unprecedented events. Unfortunately, the United States, along with every other country in the world, has recently experienced aspects of this challenge first-hand during the ongoing COVID-19 pandemic.

The COVID-19 pandemic reinforced the need for governing entities to be able to rapidly activate and enable an agile, flexible response across jurisdictions to facilitate the flow of emergency responders, healthcare practitioners, and other relief. For example, while some states had pre-existing legislation that permitted them to recognize out-of-state licenses for healthcare workers during a declared emergency, many did not. Further, many states could not authorize *volunteer* health practitioners to assist due to licensure restrictions and an inability to quickly assess qualifications in the absence of reciprocity or "compact" legislation across jurisdictions. During the pandemic, more states began enacting legislation and providing waivers to address this reciprocity gap.[6] Once enacted, such legislation empowered frontline healthcare workers to more swiftly address personnel shortages.

[6] Federation of State Medical Boards, "U.S. States and Territories Modifying Licensure Requirements for Physicians in Response to COVID-19," March 31, 2021.

4.2.3 Predetermined Standards and Thresholds

A primary objective in an emergency response to a radiological incident is to prevent acute and chronic health effects, by limiting unnecessary exposure to radiological dose. A common principle used to achieve this objective is the establishment of predetermined standards and thresholds of radiological hazards, and methods used to model or estimate them, above which protective actions or intervention may be warranted or required. Through organizations like the International Commission on Radiation Protection (ICRP) and the International Atomic Energy Agency (IAEA), widely accepted methodologies, risk thresholds, and best practices are used to establish a set of standards and procedures for radiological/nuclear emergency preparedness and response. This approach ensures that, during an emergency, debate on acceptable exposure levels will not impede organizations responsible for responding based on these standards.

This compilation of standards is commonly referred to as a protective action guide, which is designed to protect the health and safety of emergency responders and the public. Manuals that summarize protective action guides assist emergency response team leaders, public officials, and others in planning for emergency response by providing radiological protection criteria for a wide range of incidents.[7]

Protective action guides allow emergency responders to perform critical response functions while reducing exposure to radiation or risks of radiological contamination. Examples of protective actions applied to emergency responders include establishment of a cordon or exclusion zone at a specified dose rate; enforcement of limits associated with individuals' radiological exposure (e.g., cumulative dose, dose rates, stay times); use of personal protective equipment (PPE); respiratory protection; and decontamination procedures when thresholds are reached. These types of protective actions may utilize tiered thresholds that depend on the severity

[7] PAG Manual: Protective Action Guides and Planning Guidance for Radiological Incidents, EPA-400/R-17/001 (PDF—1.48 MB) (EPA, January 2017), https://www.epa.gov/sites/production/files/2017-01/documents/epa_pag_manual_final_revisions_01-11-2017_cover_disclaimer_8.pdf; 2020 Emergency Response Guidebook (PDF—3.97 MB) (DOT, July 2020), https://www.phmsa.dot.gov/sites/phmsa.dot.gov/files/2020-08/ERG2020-WEB.pdf; Planning Guidance for Response to a Nuclear Detonation (PDF—2.69 MB) (National Security Staff, June 2010), https://remm.hhs.gov/PlanningGuidanceNuclearDetonation.pdf.

of the emergency. For example, a general emergency dose limit may allow even higher limits for activities needed to protect critical infrastructure and valuable property, or to save lives.

Emergency actions designed to protect the public from unnecessary radiation exposure emergencies will likely disrupt normal living conditions. Public protective actions may include evacuation, sheltering-in-place, relocation, interdiction of food supply, and using alternative drinking water supplies. Guides help officials select applicable protective actions under emergency conditions involving relatively short-term exposures. Generally, these guides are not intended to be reflexively enforced; rather, they serve as guidelines to be considered in the broader context of incident-specific conditions and hazards. Furthermore, they do not apply to non-emergency conditions and do not delineate safe and unsafe zones. Finally, the benefits of an action should be balanced against any potential harm that may be introduced in the context of other factors or conditions.

4.2.4 Detection, Monitoring, and Modeling Capabilities for Prevention and Response

Incident prevention is a core function of emergency response organizations across all levels of government in the United States. Prevention requires careful planning and coordination between national, regional, and local assets, and ensuring that those entities have received proper training and understand how they can most effectively work together.

Preventing radiological incidents often involves enhanced security and law enforcement, augmented by technical capabilities that can detect, identify, locate, and help interdict hazardous, uncontrolled radiological material. The scale and complexity of a radiological incident response reaches beyond law enforcement to include protection of public health and safety. In this context, it is important to quickly understand the scale and the severity of the incident through a combination of data collection using radiological instrumentation, and dispersion models that predict effects in areas where actual data are unavailable. These functions occur simultaneously, while first responders work to mitigate any residual or secondary hazards that could affect public health and safety.

The detection capability needed to address both prevention of and response to radiological incidents is available in handheld, portable, or vehicle-mounted form factors. An important element of this detection capability is the identification of specific radioisotopes, which helps

distinguish hazardous materials from innocuous radiation. In most cases, isotope identification is achieved through gamma-ray spectroscopy. To understand the extent of the hazard, it is also important to estimate the quantity of material dispersed, and to identify its location—on the ground, in the water, or in the air. This provides insights as to possible dose pathways and locations where radiation may exceed thresholds for protective action. Lastly, telemetry or reporting of data from the field enables remote subject matter experts to quickly analyze and assess data.

Once a radiological incident has occurred, dose projections can determine whether protective actions should be taken. However, in the immediate aftermath of an incident, reliable field data may not be readily available for accurate estimates of the source term, in which case experts make projections and estimates using modeled or historical atmospheric dispersion and transport data. A dispersion modeling capability can play a critical role in helping predict which areas may be most affected by the incident and where protective actions may be warranted. Because models are based on a set of assumptions or initial conditions such as source term, dispersion characteristics, and meteorological conditions, experts must refine and update modeled results to ensure they are consistent with actual measurements collected in the field. This iterative process is important for characterizing the scale of the incident and ensuring protective actions are considered in a timely process in the affected areas. It is also important to communicate to responders and the public that safety guidance will be updated as predictions are refined with actual measurements. This type of transparency and expectation setting is critical to maintaining trust throughout the response.

4.2.5 Integrating Pre- and Post-Event Response Communities

Despite the United States Government's efforts to ensure an integrated inter-agency response, the communities responsible for various stages of a response do not always cooperate as well as they should. As noted previously, Hurricane Katrina revealed many areas for improvement across the local, state, and federal response—including the need for better integration between preparedness and response communities. As a result, the United States has since strived to better integrate response elements across the spectrum of a crisis to ensure that any entity involved in a response receives necessary information as soon as possible. Integrating consequence management entities into early planning has proven important to

initial response actions, as there are medium- and long-term considerations that can be deliberated before initial actions are taken. For example, understanding how evacuating a community, as opposed to sheltering them, will affect traffic and can hinder the ability of response assets to reach their destination. Another example could be considering how the use of water to decontaminate infrastructure could cause issues at water treatment plants.

In intelligence and defense applications, early notification is often referred to as "indications and warnings" (I&W). Despite the term's origin, it is often used more broadly to refer to the sharing of any information that could indicate a budding crisis, enabling emergency personnel and other supporting response assets to prepare. For example, consequence management elements—responsible for taking action to restore essential services and functions and mitigating negative impacts from disasters—are now notified as early as possible of any unusual events that may develop into crises. Doing so ensures that response assets can proactively plan and stage, mitigating delays resulting from the "tyranny of time and distance." While these delays can be planned for and shortened, they cannot be completely avoided during the initial phase of an emergency, especially if the situation was unanticipated.

4.2.6 Robust Exercise Programs and After-Action Processes

A successful response plan rests on the preparedness of those who execute it. When disaster strikes, time is of the essence and responders must execute their responsibilities efficiently without having to refer to their plans and procedures. Responders perform optimally when they have practiced their responses ahead of time and have played their role in a realistic, simulated emergency scenario.

Exercises allow responders at all levels to gain familiarity with their respective roles and responsibilities, their tactics, techniques, and procedures (TTPs), and their organization's concepts of operations (CONOPs), which often allows them to act in a more confident, decisive, and coordinated manner during a real-world event. Exercises also provide an opportunity for responders and policymakers to validate capabilities in a controlled setting and to reflect on where they should invest additional training and resources. At the same time, through controlled and simulated scenario designs that are objective-driven, organizations

can validate established plans and procedures and expose potential shortfalls therein. When scrutinizing a response plan by exercising it, we learn whether doctrine aligns with the evolving threats we face and the priorities of our government.

In addition to building confidence in response plans, exercises help create networks across agencies and various jurisdictions prior to a crisis. This allows counterparts to establish or reinforce relationships and build rapport in a relaxed environment. In doing so, exercises facilitate greater understanding of cross-agency or cross-jurisdictional roles and responsibilities, and initiate conversations about how organizations can leverage one another for reach-back and force multiplication during a crisis. These collaborations often lead to greater trust and understanding when disaster strikes. Exercises can also facilitate communications pathways, data flow, information sharing, and reporting procedures within and across agencies—all of which can increase coordination, ensure efficient use of resources, and build situational awareness during a response.

The exercise planning process involves work within individual organizations and across different agencies to ensure exercise plans touch all levels. An exercise plan should address the breadth of the emergency landscape, incorporating scenarios of varying magnitude and locations to stress the response community across different timescales and jurisdictions. To make effective use of limited time and resources, exercises can range in scope and complexity from basic proficiency drills and field training exercises (FTX), which are limited and focus on specific field-level functions or technical disciplines, to integrated full-field drills that are designed to explore most or all field-level functions in a simulated response scenario. An exercise plan may also include other types of activities, such as tabletop exercises (TTX), command post exercises (CPX) and senior leaders seminars (SLS). These events focus on higher-level decision-makers presented with scenarios and questions that elicit dialog and responses about what actions or decisions to take. They can often be accomplished with simulated or no field-level play. It is also important to have a long-term exercise plan to continue validating new capabilities or procedures, to account for new circumstances, and to mitigate personnel turnover and reorganizations that impact the distribution of roles and responsibilities. An emergency response plan loses value sitting on the shelf. Good plans are living, breathing documents that are updated with lessons learned from exercises and real-world events. This is especially true

in an information age in which technology develops faster than we can adapt.

An essential element of effective exercise programs is the control and evaluation cell, from which controllers provide scenario scripts and injects, control the flow of the exercise, and enforce boundaries to keep exercise play on track. Concurrently, exercise evaluators observe the performance of responders and assets at all levels (in the field, in command-and-control centers, in reach-back centers and watch offices, and elsewhere). They capture observations on successes and areas for improvement. There are several ways to ensure these observations are recorded and shared, including through formal After-Action Review (AAR) processes and reports. AARs summarize lessons learned, enumerate best practices and areas for improvement, and provide recommendations on how to address gaps and shortfalls. Because the AAR process is often delayed relative to the exercise execution, critical information is occasionally lost or not sufficiently documented. In response, exercise controllers often hold "hotwash" meetings with key players and planners daily during the exercise. Hotwash meetings provide a forum where participants can share and capture lessons learned while they are still fresh in mind.

These hotwash and AAR processes are also critical components of real-world responses, but documenting AAR findings and lessons learned is just the first step. Good planning for future events requires making time to facilitate improvements and take corrective actions to address the shortfalls in the various components of a response framework including equipment, training, and procedures. In other words, response organizations need to fix the things that are not working properly in response to "learning" the lesson. Otherwise, a lesson has not been truly learned if it is at risk of being exposed again in a different response or exercise. An archive of best practices, lessons learned, and areas for improvement is only as good as those actions that are taken to address gaps and improve the overall response capability.

4.2.7 Crisis Communications[8]

From the moment a radiological disaster strikes, members of the public may experience a variety of emotions including panic, fear, and alarm.[9] On top of fear, public reactions are often fueled by uncertainty and speculation; a lack of prompt information can lead the public to unwittingly take steps that threaten their safety. However, by providing rapid and clear communications during radiation crises, governments can preempt such counterproductive steps by providing the public with the information they need to respond safely.

The public will look towards officials in their community for guidance in the immediate aftermath of an emergency. Especially in the case of a radiation emergency—a disaster for which few are prepared—the public will be eager to know which steps they can take to mitigate health risks. The United States has found that the best way to keep pace with these demands is to plan ahead. A key component of this planning includes developing pre-scripted communication plans and emergency guidance that are adaptable to the scale and nature of the emergency. U.S. experts have found that this approach allows stakeholders to build consensus and familiarity with the message prior to an emergency, saving critical time if and when the event occurs. Understanding that many people will want access to pre-scripted messages during a radiological emergency, the U.S. created a word-searchable clearinghouse of publicly available, pre-scripted radiological and nuclear emergency response messages.[10]

In addition to building consensus around the message itself, it is equally important to build consensus around primary and alternate channels for delivering the message. Because a consistent message is critical to maintaining public trust, officials should be mindful of the order in

[8] The insights shared in this section are largely informed by personal communications between the authors and Jessica Weider of the U.S. Environmental Protection Agency (EPA).

[9] S. Becker, "Emergency Communication and Information Issues in Terrorist Events Involving Radioactive Materials," *Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science* 2, no. 3 (2004): 195–207.

[10] Understanding that many people will want access to pre-scripted messages during a radiological emergency, the U.S. created a word-searchable clearinghouse of publicly available, pre-scripted radiological, and nuclear emergency response messages. These can be located at: https://www.radresponder.net/#resources/library?rltf=104. Individual documents can also be located at https://www.epa.gov/radiation/pag-public-communication-resources.

which they deliver recommendations so the public is not confused about what action they should take first. For example, offering shelter-in-place recommendations concurrently with recommendations for procuring safe food and drinking water may create confusion.

The U.S. Environmental Protection Agency (EPA) maintains and updates a document, "Communicating Radiation Risks," which provides organizations with guidance on how to communicate during a radiation emergency. EPA's "Protective Action Questions & Answers for Radiological and Nuclear Emergencies" provides pre-scripted messages approved for use in any type of radiological emergency.[11] The guides are publicly available so that local, state, and federal officials can reference them at any time. By building consensus around scripts and dissemination plans ahead of time, officials can deliver clear and actionable information to the public without delay. Rapid information flow is important for multiple of reasons. Mainly, it provides communities with immediate steps they can take to minimize damage to their health and safety. Additionally, by providing rapid and accurate information, officials can build public confidence in—and compliance with—the response.[12]

Striking an appropriate balance between speed and accuracy is perhaps the most challenging element of crisis communications, and one with which any responders would struggle. However, the importance of providing accurate and consistent information throughout the response cannot be overstated. Those who have been involved with any kind of CBRN disaster response know that at the onset of the emergency, even the experts have more questions than answers. So, one might reasonably wonder how to provide accurate information at the onset of a radiological emergency when so many unknowns remain. In thinking through this challenge ahead of time, U.S. experts have identified several universal steps that we can encourage the public to take immediately in the case of

[11] United States Environmental Protection Agency, *Protective Action Questions & Answers for Radiological and Nuclear Emergencies: A Companion Document to the U.S. Environmental Protection Agency Protective Action Guide (PAG) Manual*. EPA-402/K-17/002, 2017.

[12] H. Carter, J. Drury, G. J. Rubin, R. Williams, and R. Amlôt, "The Effect of Communication During Mass Decontamination," *Disaster Prevention and Management: An International Journal* 22, no. 2 (2013): 132–147. https://doi.org/10.1108/09653561311325280.

a radiological emergency. The federal pre-scripted messages include information on how to safely shelter in place, how to self-decontaminate, and where to look for further information.

Information officers should be clear with the public that such steps are recommended based on initial information about the emergency, but the recommendations could be updated as officials learn more. If and when those recommendations do change, information officers should provide the public with rationale for why this has occurred.

After the initial stages of the response, when responders are learning more about exposure levels and risks, officials must continue to provide clear, coordinated, and honest messaging. Identifying a lead authority for public information and messaging ensures that communications remain consistent across the various entities involved in the response. In the U.S., that authority will pass down new messaging and information—including clarification on what information remains unknown—to other information officers as it becomes available. Instead of providing potentially inaccurate information, all spokespeople should be honest about what information remains unconfirmed or unknown. If just one entity goes off-message to speculate on unconfirmed information, the public may grow skeptical of the validity of that source as well as others. Even worse, if speculative information is later found to be false, it can lead to a significant breakdown in trust between the public and the authorities, creating additional complications for effective response.

U.S. crisis communications experts recommend that subject matter experts and information officers' work together to translate data and technical language on radiation risks into accessible and actionable language for the public. For example, we try not to make the public do math in a crisis. Also, maintaining unit consistency throughout the response allows for easy comparison; do not mix rem with millirem or sievert with millisievert. In addition, radiation data should be juxtaposed with information on health and safety implications, as well as next steps for those who have been exposed.

By providing accurate, clear, and consistent messaging across various responding entities, officials build trust and confidence among the public. This approach can also help authorities thwart the spread of disinformation. A splintered message is more easily scrutinized and exploited by bad actors. This challenge was evidenced by the U.S. government's response

to COVID-19, where inconsistent messaging from state and federal officials led to skepticism, creating an environment more susceptible to misinformation and disinformation.[13]

The means through which officials convey a message can also impact levels of public trust in the message itself. One way the U.S. strives to build credibility through public communications is by selecting a trusted spokesperson to deliver the message. The spokesperson should be capable of conveying empathy and respect for the public's concerns. Validating public feelings without amplifying fears strengthens messaging in any crisis, but is especially important in a radiation emergency, where people are more likely to comply with recommendations if they feel heard.

In addition to selecting a trusted government spokesperson, U.S. experts have found it useful to cooperate with "seconders." "Seconders" are allies from local communities and the private sector who endorse and amplify the official message. Their endorsement provides additional reassurance to those who may be initially skeptical of government messaging.

Lastly, when delivering the message, the U.S. prioritizes the underserved, including non-English speaking communities, and those that lack internet access. Reaching these communities often requires planning for effective outreach. By working with them before an emergency, we can provide more equitable and accessible communications during a response.

4.2.8 Case Studies[14]

The best practices described above emerged as lessons learned from real-world responses to various crises. To demonstrate the challenges of incorporating all of these best practices into a response, we discuss two case studies: the 1979 accident at Three Mile Island and the 2011 Fukushima Daiichi disaster. The U.S. response to these incidents revealed major gaps in our plans and capabilities. Both case studies illustrate the complexity of coordinating multi-sectoral responses to rapidly evolving crises. By describing shortcomings in past U.S. responses, we hope to

[13] Disinformation is false or misleading information, communicated with intent to deceive. Misinformation is false or misleading information that may or may not be communicated with an intent to deceive.

[14] This section draws upon two comprehensive official reports and publications on the Three Mile Island and Fukushima accidents (see individual references).

illustrate how some of the best practices above emerged to ensure more streamlined and efficient responses.

4.2.9 Three Mile Island (1979)

Shortly after 4 pm on Wednesday, March 28, 1979, several water pumps began malfunctioning in Unit 2 of the Three Mile Island power plant (TMI-2) in Dauphin County, Pennsylvania. The events that followed, initiated by equipment failures and compounded by human error, spiraled into the U.S.'s worst nuclear power crisis to date.

Investigations into the accident have concluded that the radiation was largely contained and any releases would have a negligible impact on public health. However, the stress and anxiety caused by the event—compounded by a lackluster response—led to long-lasting negative effects on mental health. Some of those feelings are to be expected in any emergency, regardless of how it is handled. However, we can mitigate stress significantly by providing transparent, clear, consistent, and actionable public information through a well-coordinated response.

The failures in the response to Three Mile Island illuminate the importance of four best practices previously highlighted in this chapter: planning and exercising, tiered response structures, predetermined thresholds for notification and action, and robust crisis communication plans.

Prior to the accident, the U.S. Nuclear Regulatory Commission (NRC), the plant operators, and local authorities did minimal planning for a nuclear crisis. In fact, the local communities surrounding the plant had no response plans for a radiation emergency.[15] The plant itself maintained some plans and procedures for emergencies; however, these plans were not only found to be inadequate, but unfamiliar to the staff and therefore ineffective during the event.[16]

The accident presented problems that could have been easily discovered and resolved in an exercise. For example, the accident revealed that the configuration of the control room was not conducive to a

[15] United States. President's Commission on the Accident at Three Mile Island, *Report of the President's Commission on the Accident at Three Mile Island: The Need for Change: The Legacy of TMI* (Washington: President's Commission on the Accident at Three Mile Island, 1979), p. 15.

[16] President's Commission on the Accident at Three Mile Island, p. 28.

successful response. Key emergency indicators were hidden in counter-intuitive places—such as on the back of the control board. Further, the accident set off over 100 alarms in its early stages. With no way of suppressing the unimportant alarms, control room operators struggled to identify the important ones.[17]

The disordered response at TMI-2 also revealed that the various entities responding—including local authorities, federal authorities, and the utility—had not prepared to respond collaboratively. Although some of the existing federal plans prescribed a tiered response structure, due to the lack of exercising, the response did not reflect that system.

Like the working-level staff, senior officials were unfamiliar with procedures for an emergency at Three Mile Island. Unaware of their own responsibilities and authorities, local and federal officials often took delayed or duplicative actions. Further, the NRC, the utility, and local responders did not collaborate on writing, exercising, or revising their plans and thus the accident required them to test the plans' interoperability in real-time. As the accident unfolded, it revealed gaps in the plans and in officials' awareness of their responsibilities. For example, local hospital administrators could not identify who at the state level had the authority to recommend evacuating patients and when to resume regular admitting procedures.[18] The Pennsylvania Secretary of Health viewed his role as informational—not advisory—with respect to the local hospitals. Lacking awareness of who had responsibility—and how they should hand off that responsibility—officials slowed critical steps in the response.

This lack of streamlined coordination between various levels of governance at Three Mile Island illuminates the need for a clear delineation of authorities for local, state, and federal entities. A tiered response structure, as discussed previously, can help local officials escalate incidents to higher authorities as needed. Instead of acting in a mutually reinforcing manner, those responding to the accident took some actions that were duplicative, while other critical needs were left unmet. Overall, the entities involved failed to support one another due to a lack of awareness of responsibilities and ability to support a tiered response.

The slow and jumbled Three Mile Island response also demonstrates the need to predetermine thresholds for notification and action

[17] President's Commission on the Accident at Three Mile Island, p. 29.

[18] President's Commission on the Accident at Three Mile Island, p. 37.

in response plans. The Three Mile Island emergency plan did not require the plant operators to notify state or local health authorities in the event of a radiological accident.[19] Had the accident caused greater radiation exposure to the public, such inaction could have been catastrophic. Early notification is critical to developing support options and resources.

Finally, one of the greatest flaws in the response to Three Mile Island was the officials' inability to communicate clearly and effectively with the public. Officials made numerous and severe communications errors throughout the response, leading to a significant breach in trust between authorities and the public.

Different organizations gathered information from their own sources, with each organization providing its own story to the public. In the initial hours of the accident, the utility attempted to downplay its severity when speaking with the press. However, days later, the NRC began providing inaccurate information to the public.[20] The NRC's assessments, however, were based on scientific errors. For example, NRC officials concluded incorrectly that a hydrogen bubble inside the reactor vessel would soon contain enough oxygen to burn or explode.[21] Despite other sources providing the NRC with calculations to counter this theory, the NRC continued to warn the public of the hydrogen bubble. Based on incorrect information, the Governor recommended evacuation for pregnant women and preschool-aged children within 5 miles of the accident.[22]

Eventually, the NRC designated a lead for communications—Harold Denton. Coordinating between the NRC, the Governor's Office, and the White House, Denton would be the sole source of information to the public. Although this decision brought some order to the public messaging strategy, it also created an additional challenge. Once the NRC appointed Denton, it prohibited any other organizations from speaking publicly about the accident. Instead of working collaboratively with other organizations to provide them with talking points to mirror the NRC's message, the NRC silenced its partners. The media was therefore unable

[19] President's Commission on the Accident at Three Mile Island, p. 41.

[20] President's Commission on the Accident at Three Mile Island, p. 18.

[21] President's Commission on the Accident at Three Mile Island, p. 40.

[22] President's Commission on the Accident at Three Mile Island, p. 41.

to confirm information they received from the NRC with other sources—a standard practice reporters undertake to corroborate a story.[23] This likely bred further skepticism from the media and the public.

In addition to providing inconsistent messaging, officials provided information in a way that was difficult for the public to decipher. Officials fed information to the press in technical jargon but failed to provide briefings to familiarize the press with the terms. The messaging related to radiation releases was particularly difficult for the press to understand. Given the press's inability to comprehend information on the releases—and the implications of those releases for public health and safety—the press also struggled to present the facts in a clear and accessible manner to the public.

Many of the severe communication challenges that followed the accident at TMI-2 could have been avoided with pre-arranged communication plans. Exercising and building consensus around those plans ahead of a crisis would likely have facilitated the flow of more consistent and actionable information to the public. Although the communications failures led to undue stress and panic, they also provided valuable lessons that shaped best practices in the field for years to come.

4.2.10 Fukushima Daiichi (2011)[24]

The 2011 Fukushima Daiichi Nuclear Power Plant crisis represents the most complex and wide-ranging radiological emergency response case study of our generation. Japan bore the brunt of responding to the event on its home soil, and, given that it occurred during the aftermath of the offshore earthquake and devastating tsunami, it stressed the country and its citizens in immeasurable ways. At the same time, given the extent of the event and the fact that the incident remained in a dynamic phase for several weeks, it represented a global crisis that also stressed response organizations worldwide.

The United States Government (USG) response was multi-faceted and ultimately centered around (1) assisting U.S. interests in Japan—specifically, American citizens in-country as well as U.S. military operations and

[23] President's Commission on the Accident at Three Mile Island, p. 58.

[24] D. Blumenthal, "Introduction to the Special Issue on the U.S. Response to the Fukushima Accident," *Health Physics* 102 (2012): 482–484, and subsequent articles from the same issue, *Health Physics* 102: 482–588 (2012).

personnel operating out of U.S. Department of Defense (DoD) installations in Japan; and (2) partnering with the Government of Japan (GOJ) to provide assistance. Efforts by U.S. response organizations focused on many elements, including the radiological monitoring and assessment for DoD bases and public locations impacted by releases of radiological material into water and airborne pathways and the associated downrange fallout. However, there were delays in gathering information early on since many of the applicable resources had to mobilize and deploy overseas.

Furthermore, due to the extent of the releases into the environment, there were concerns that radiological material could reach the U.S. Ultimately the amount of radiation measurable in the U.S. was very small—barely above background in the worst of cases and orders of magnitude below any actionable levels. Thus, the actual stresses on the home front, such as dealing with public messaging and perceived versus actual risk, were quite different from those in Japan, where the radiation levels were much greater and warranted careful planning and coordination. As we will see, decisions related to conditions in Japan were compared and scrutinized against conditions and planning assumptions in the U.S.

Although there is a multitude of important factors and considerations that warrant review, the remainder of this section will center on the importance of and challenges for three focus areas: (1) predetermined thresholds, (2) crisis communications, and (3) the AAR process.

First, utilizing predetermined thresholds proved complex for an international response. The Fukushima response involved other governments with different standards and the application of U.S. standards for its own citizens in Japan that departed from those used on U.S. soil. The NRC decided early on to recommend evacuation of U.S. citizens within 50 miles of the Daiichi power plant, which is a significantly larger area than NRC's established emergency protection zones that only stretch 10 miles from domestic U.S. power plants. As a result, citizens surrounding those U.S. plants were concerned and confused about an apparent double standard; more effective messaging about the difference between default assumptions and departures from them could have allayed fears and concerns.

The technical experts providing analysis for these efforts had to apply one set of standards (and units of measure) for products generated for U.S. parties and apply a different set of standards and assumptions (and

units) for those generated for GOJ consumption. The double tasking taxed the experts in ways that had not been fully considered before. Special scrutiny and quality assurance measures were enforced to mitigate mistakes, but they delayed product delivery. Other, more subtle assumptions common to U.S. plans proved invalid overseas, where cultural differences (such as diet and shelter types) and technical differences on risk acceptance (e.g., how sheltering protection from radiation is accounted for) can lead to varied assumptions needed to make representative dose projections. Many of these issues remain today, where the U.S. applies one set of standards and methods and other parts of the world use a different set.

Second, many lessons were learned about the most clear and effective methods of crisis communication. Although the release of radioactive material posed virtually no risks on U.S. soil, it nevertheless presented a challenge to those organizations responsible for communicating this fact. The U.S. public paid substantial attention to the event. Organizations had to be responsive to the demand for information. For example, the EPA rapidly stood up a public-facing website shortly after the event began to provide context for data that were being collected and presented. It also made iterative improvements to the content in response to feedback and requests for information from the public and media.

The difference in Japanese and U.S. guidance, including topics such as evacuation and exclusion zones, caused confusion and concern for Japanese and U.S. citizens. Call centers in the U.S. were flooded with queries from members of the public near domestic nuclear power plants, who wondered if evacuation and exclusion zone guidance applied in Japan would in turn be applied in the U.S. An array of resources and channels, including internet, social media, public meetings, and other forums, were used in new ways to communicate frequently with responders and the public.

Finally, the AAR process played a critical role in the aftermath of the response, and the ripple effects continue to be felt more than a decade later. The response exposed numerous capability gaps and shortfalls for dealing with a long-duration, overseas, multi-hazard response for which no exercise could have hoped to simulate. There were countless lessons learned from this event—some procedural, some technical, and others focused on public messaging and communications. Some of those lessons are provided in the following paragraphs.

It was absolutely essential for the response organizations to document observations, not just for archival purposes, but more importantly to use as justification for a massive effort to enact improvements, refine plans, and take other corrective actions to ensure better USG preparedness for future events of this magnitude. For example, technological capabilities built on assumptions for a U.S. domestic response were, in some cases, not well suited for an overseas response. For example, at the time, many response plans for radiological scenarios assumed single releases, shorter durations, and more predictable source terms. The Daiichi release was significantly more complex and variable than that. Additionally, the risk of airborne contamination from the extended unstable state of the reactors precluded collecting data in some areas that existing plans highlighted as most critical. As a result, typical mission planning assumptions for aerial surveys proved invalid and resulted in survey planning modifications to account for changing conditions and crew safety considerations that had not been accounted for previously.

Other technical issues stemmed from the magnitude of the survey area, the overwhelming amount of measured data, and the massive number of collected samples (air, soil, and water). The tools needed to aggregate and analyze these sets had to be modified in the midst of the response. There were also significant procedural gaps in how to appropriately share data collected for another government to other U.S. federal, state, local, and tribal entities. As a result of tremendous effort and expertise, subject matter experts were able to adapt during the response to make the most of the situation at the time. However, the gaps and shortfalls exposed in this event laid the groundwork for a significant technology development effort that refined how equipment is configured, how measurements are conducted, how data are aggregated and assessed, and how resulting data products and assessments are interpreted and shared.

4.2.11 Future Threats and Challenges

This chapter has articulated the importance of learning and adapting based on previous successes and failures. However, we recognize that it is insufficient to simply strive to emulate past successes or seek to prevent recurrent failures in such a rapidly evolving world. Emergency response and crisis communications communities must also effectively anticipate future threats and challenges and remain agile enough to prevent, detect, deter, and respond to them. In particular, global warming

and corresponding climate change, cyber incidents and accidents, and the malign use of unmanned aerial systems (UAS), all pose significant future challenges for nuclear and radiological communities.

Climate change has increased the frequency and severity of extreme weather events such as hurricanes, heatwaves, wildfires, droughts, floods, and precipitation, which in turn pose threats to critical facilities. In particular, unpredictable, and severe weather patterns and accelerated sea-level rise threaten nuclear and radiological facilities in various ways. Nuclear reactors rely on water supplies as coolant, which places a majority of reactors around the world in littoral areas; in fact, many are built just meters above sea level. Rising sea levels and volatile weather patterns can lead to serious flooding and more frequent storm surges that leave reactors along coastlines especially vulnerable. Without adequate protection and backup, as happened in the Fukushima incident, these factors can impact critical plant infrastructure, including electrical systems that power the cooling mechanisms and water pumps needed to prevent overheating or meltdown.

Cyber incidents and accidents, including both malicious direct and indirect attacks, are another concern for nuclear and radiological facilities. Chapter 7 of this publication delves into this topic in much greater detail, but it is worth emphasizing here as well. Malicious, direct attacks are deliberate attempts to disrupt, deny, degrade, destroy, or otherwise compromise nuclear or radiological facilities. Although major attacks of this nature are not known to have targeted U.S. nuclear or radiological facilities, examples such as the Stuxnet attack on the Iranian nuclear program—allegedly intentionally destroying critical infrastructure—demonstrate the damage that can be inflicted. Further, a non-nuclear example of novel cyber TTP involves the 2021 Colonial Pipeline attack for ransom. In other scenarios, malicious, indirect cyber incidents, or attacks—which do not intentionally target nuclear or radiological facilities but could affect them by the spread of malware from other targets—could inflict collateral damage that negatively impacts those facilities' operations and security.

Cyberattacks can not only instigate nuclear security incidents, but they can further complicate an ongoing response to an otherwise accidental event. During an ongoing response, adversaries can attack the devices of first responders and officials managing the incident as a second wave. This threat requires that we train more regularly to leverage secondary

and tertiary methods of communication and information storage during a response.

The threat of disinformation also poses a great challenge that will increasingly complicate emergency response operations. Disinformation is false or misleading information that is communicated with intent to deceive. By proliferating disinformation after a radiological event, malicious actors can stir fear among the public, in addition to sowing distrust in government. Disinformation operations prevent widespread compliance with a government's recommendations on protective measures, which can adversely affect public health and strain healthcare systems.

Finally, the proliferation of UAS capabilities has significantly out-paced the ability of organizations to adequately identify, track, intercept, and counter these systems in the event they are used for unauthorized activities, flown in restricted air space, or used as a weapon. This situation raises serious concerns as drone incursions are on the rise, and nuclear facilities are vulnerable, as is other critical infrastructure. Freedom of Information Act (FOIA) documents note 24 different U.S. nuclear sites experienced at least 57 drone incursions between 2015 and 2019, and again in 2020 despite new security measures. The 2020 incident specifically involved drone "swarm" incursions over a restricted area at the Palo Verde Nuclear Power Plant on two consecutive nights.[25] Furthermore, attacks conducted with UAS or drone systems on critical infrastructure facilities have already been undertaken, including the 2019 armed drone attack by Yemeni Houthi rebels against Saudi Arabian energy giant Aramco's facilities.

4.2.12 Advancing the Bilateral Partnership

Recognizing the significant challenges that emergency response and crisis communications communities will continue to face worldwide, the United States and India—and in fact a wide range of partners—would benefit from enhanced cooperation in a number of areas. For example, expert exchanges to discuss local, provincial, and national response plans and frameworks can provide fresh perspectives on shared challenges related to cross-jurisdictional response coordination. This is especially true for the United States and India, both of which have federal systems of

[25] The documents were obtained from the U.S. Nuclear Regulatory Commission by Douglas D. Johnson on behalf of the Scientific Coalition for UAP Studies (SCU).

governance. Further, given the shared challenges we anticipate due to global warming and corresponding climate change, the United States would benefit from a bilateral dialogue discussing the unique threats and challenges facing the nuclear and radiological communities. In addition, bilateral tabletop exercises (TTXs) can provide a venue for open conversation to work through the scenarios most likely to impact both countries. This could be done as a series of TTXs that would enable participants to build relationships and capacity, starting with simpler scenarios and moving together towards more complex crises.

4.2.13 Conclusion

The breadth and depth of best practices in emergency response and crisis communications signify both the existence of and potential for superior response capabilities worldwide. While the best practices discussed above were born of historical lessons, the emergency response and crisis communications communities remain committed to anticipating and combatting future threats and challenges. Through these efforts, which will focus particularly on *partnership*, the practitioners and institutions of the response and communications communities will undoubtedly forge an even brighter, more proficient, and safer future.

References

Atomic Energy Regulatory Board. "Emergency Preparedness." *AERB Annual Report 2019*. https://www.aerb.gov.in/images/PDF/Annual_report/ar2019/chap5aerbannualreport2019.pdf.

Becker, S. "Emergency Communication and Information Issues in Terrorist Events Involving Radioactive Materials," *Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science* 2, no. 3 (2004): 195–207. https://doi.org/10.1089/bsp.2004.2.195.

Blumenthal, D. "Introduction to the Special Issue on the U.S. Response to the Fukushima Accident. Introduction," *Health Physics* 102, no. 5 (May 2012): 482–484. https://pubmed.ncbi.nlm.nih.gov/22469927/.

Carter, H., Drury, J., Rubin, G. J., Williams, R. and Amlôt, R. "The Effect of Communication During Mass Decontamination," *Disaster Prevention and Management* 22, no. 2 (2013): 132–147. https://doi.org/10.1108/09653561311325280.

Federation of State Medical Boards, "U.S. States and Territories Modifying Licensure Requirements for Physicians in Response to Covid-19," March, 31, 2021.

International Atomic Energy Agency. *Preparedness and Response for a Nuclear or Radiological Emergency*. General Safety Requirement No. GSR Part 7, 2015. https://www-pub.iaea.org/MTCD/Publications/PDF/P_1708_web.pdf.

National Security Staff. *Planning Guidance for Response to a Nuclear Detonation*. Second Edition. Interagency Policy Coordination Subcommittee for Preparedness & Response to Radiological and Nuclear Threats, June 2010. https://remm.hhs.gov/PlanningGuidanceNuclearDetonation.pdf.

The President's Commission on the Accident at TMI. *Report of the President's Commission on the Accident at Three Mile Island: The Need for Change: The Legacy of TMI*. United States, October 30, 1979. http://large.stanford.edu/courses/2012/ph241/tran1/docs/188.pdf.

Union Government Department of Atomic Energy. *Report of the Comptroller and Auditor General of India on Activities of Atomic Energy Regulatory Board for the Year Ended March 2012*. Report No. 9 of 2012–13 (Performance Audit). https://cag.gov.in/webroot/uploads/download_audit_report/2012/Union_Performance_Atomic_Energy_Regulatory_Board_Union_Government_Atomic_Energy_Department_9_2012.pdf.

United States Environmental Protection Agency. *PAG Manual: Protective Action Guides and Planning Guidance for Radiological Incidents*. EPA-400/R-17/001, January 2017. epa.gov/sites/default/files/2017-01/documents/epa_pag_manual_final_revisions_01-11-2017_cover_disclaimer_8.pdf.

United States Environmental Protection Agency. *Protective Action Questions & Answers for Radiological and Nuclear Emergencies: A Companion Document to the U.S. Environmental Protection Agency Protective Action Guide (PAG) Manual*. EPA-402/K-17/002, 2017.

U.S. Department of Homeland Security. *Nuclear/Radiological Incident Annex to the Response and Recovery Federal Interagency Operational Plans*, October 2016—Final. https://remm.hhs.gov/NRIA_FINAL_110216.pdf.

U.S. Department of Transportation. *2020 Emergency Response Guidebook*, July 2020. https://www.phmsa.dot.gov/sites/phmsa.dot.gov/files/2020-08/ERG2020-WEB.pdf.

Van Boom, D. "Nuclear Power Is Clean and Safe. Why Aren't We Using More of It?" CNET, November 16, 2021. https://www.cnet.com/science/how-nuclear-power-plants-could-help-solve-climate-crisis/.

CHAPTER 5

Physical Protection of Nuclear Facilities and Materials

Anil Kumar, James McCue, and Alan Evans

5.1 An Indian Perspective

Anil Kumar

In the current global scenario with emerging international security challenges, it is a distinct possibility that nuclear or other radioactive materials could be maliciously employed. Nuclear security is fundamental in the management of nuclear technologies and in applications where nuclear or other radioactive material is used or transported. An effective national nuclear security regime consists of the implementation of relevant international legal instruments; information protection; physical protection;

A. Kumar
Department of Atomic Energy (retired), Mumbai, India

J. McCue (✉)
Defense Threat Reduction Agency, Fort Belvoir, VA, USA
e-mail: jamesmccue81@gmail.com

A. Evans
Sandia National Laboratories, Albuquerque, NM, USA

S. P. Kapur et al. (eds.), *The Challenges of Nuclear Security*, Initiatives in Strategic Studies: Issues and Policies,
https://doi.org/10.1007/978-3-031-56814-5_5

material accounting and control; detection of and response to trafficking in such material; national response plans; and contingency measures.[1] Each state carries full responsibility for nuclear security; specifically, to provide for the security of nuclear and other radioactive material and associated facilities and activities; to ensure the security of such material in use, storage, or transport; to combat illicit trafficking and the inadvertent movement of such material; and to be prepared to respond to a nuclear security event.[2] Physical protection against unauthorized removal of nuclear material and against the sabotage of nuclear facilities or transports has long been a matter of national and international concern as well as an area of cooperation.[3]

5.1.1 Components of Physical Protection Regime and Indian Commitments

The overall objective of a state's nuclear security regime is to protect persons, property, society, and the environment from malicious acts involving nuclear and other radioactive material. The objectives of the state's physical protection regime, which is an essential component of the state's nuclear security regime, are[4]:

- To protect against unauthorized removal, including theft and other unlawful taking of nuclear material
- To locate and recover missing nuclear material rapidly and comprehensively
- To protect nuclear material and facilities against sabotage
- To mitigate or minimize the radiological consequences of sabotage.

[1] IAEA, "Objective and Essential Elements of a State's Nuclear Security Regime: Nuclear Security Fundamentals," *IAEA Nuclear Security Series*, no. 20 (2013).

[2] IAEA.

[3] IAEA, "IAEA Nuclear Security Series No. 27-G Implementing Guide," 2018.

[4] IAEA, "IAEA Nuclear Security Series No. 13 Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5)," n.d.

The state's physical protection regime is intended for all nuclear material in use, in storage and during transport, and for all nuclear facilities.[5] The regime should be reviewed and updated regularly to reflect changes in the threat and advances made in the physical protection approaches, systems, and technology, and also the introduction of new types of nuclear material and nuclear facilities.

During international transport of nuclear material, particularly Category 1 material, the responsibility for physical protection measures should be the subject of written arrangements accepted by the states concerned. The relevant competent authority of the shipping, receiving, and transit states, and the flag state of the conveyance should establish specific measures to ensure the continued integrity of the shipment, and to ensure that responsibility for response planning and capabilities is defined and fulfilled. Additionally, any sensitive information shared by the states concerned should be protected and the overall arrangements for the shipment should be in accordance with the relevant states' national laws. The point at which responsibility for physical protection is transferred from one state to another should be determined in advance, to enable the relevant state to make adequate physical protection arrangements.

India is committed to provide for the security of nuclear and other radioactive materials, and associated facilities and activities, either in use, storage, or transport. It is also fully prepared to respond to any nuclear security event arising due to illicit trafficking or inadvertent movement of such materials. India follows INFCIRC/225/Rev.5, which contains recommendations issued by the International Atomic Energy Agency (IAEA) for the information of all member states.[6] For an effective physical protection system, every state needs to determine its requirements. The overall Physical Protection System (PPS) requirement should be evaluated for protection performance against a particular threat level. This threat level should be well defined by the country, as mentioned in INFCIRC/225/Rev.5.[7] The threat of unauthorised removal of nuclear materials or

[5] IAEA, "IAEA Nuclear Security Series No. 27-G Implementing Guide."

[6] IAEA, "Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5): Recommendations, Vienna, International Atomic Energy Agency," 2010.

[7] Ibid.

sabotage of nuclear facilities, against which the facility owner is responsible for designing and providing protection, is known as Design Basis Threat (DBT).

India has developed DBT in a very meticulous manner, and it was reviewed in 2009 after the terrorist attack on Mumbai in November 2008. On the basis of the national Design Basis Threat, every facility prepares its own DBT for which it designs a Physical Protection System and gets concurrence from the nuclear regulator. The DBT is reviewed when a very prominent and probable change in the threat scenario occurs.

Adversaries posing a threat to nuclear materials and facilities can be separated into three classes—outsider, insider, and outsider in collusion with insider. These threats could manifest using the tactics of deceit, force, or stealth while infiltrating into facilities. The national DBT recognizes these categories of adversaries and their capabilities as a comprehensive aspect of nuclear threat analysis.

5.1.2 Considerations for Designing a PPS

The physical protection system (PPS) of any facility depends on a proper combination of three factors: technology, procedures, and security personnel. Every physical protection system should be evaluated against a defined maximum threat level for which the facility owner will secure its facility and materials.

The potential targets in each facility should be identified according to the attractiveness of unauthorised removal or sabotage for an adversary. In a reactor complex, a vital area is defined as a set of equipment, systems, devices, or materials whose failure, destruction or misuse could result in radiological release endangering the public. An inner area is defined as a set of targets attractive for unauthorised removal.

The regulator specifies the physical protection system's requirements after obtaining full information regarding facility characterisation, threat definition, and target identification. Optimal solutions come from synergizing all three requirements for a viable physical protection system

through a combination of fences, vaults, sensors, procedures, communication devices, and response force personnel. Every PPS should have the primary functions of[8]:

- Deterrence of an adversary
- Detection of an adversary
- Delaying an adversary in reaching the target
- Defeating the adversary by Response Force
- Mitigation of radiological consequences

The following general guidelines and principles should be adhered to while designing a PPS:

- Detection should be as far as possible away from the targets
- Delay mechanisms should be placed near the target
- Alarms must be reliably communicated to the response force
- Levels of protection should follow a graded approach, increasing or decreasing with the potential hazards, and attractiveness to adversaries, of materials and systems
- The PPS should employ defence in depth, with multiple layers of increasingly robust protection
- Each layer of a physical protection system should have same level of strength against adversary penetration at all points

5.1.3 Nuclear Security and Physical Protection in India: An Overview

5.1.3.1 Historical Perspective

The Department of Atomic Energy in India was established in 1954. It was mandated to develop nuclear-power technology, with an aim to develop and research applications of radiation technology in the fields of Agriculture, Industry, Medicine, and Basic Sciences. The Atomic Energy Regulatory Board was constituted in 1983 to carry out regulatory and

[8] IAEA, "IAEA Nuclear Security Series No. 13 Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5)."

safety work. Later, in 2009, it was also empowered to regulate and supervise the security of the nuclear facilities. India's first nuclear research reactor became critical in 1956 and its first nuclear power reactor achieved criticality in 1969. Presently, 22 nuclear power reactors in India are operational. India has an accumulated experience of operating of nuclear power reactors of more than 500 reactor-years without any major security, safety, or safeguard breach. Many of its reactors have achieved record days of continuous operation. Recently, a 700 MW Nuclear Power Reactor achieved criticality without any issues. In light of the above experience, it can be well presumed that India's Nuclear operators and regulators have shown their capabilities and established their credentials in this field.

India has been facing threats from a hostile external neighbourhood, as well as from home-grown extremist groups. In the 1980s, the country suffered from Sikh terrorism, which included the assassination of Prime Minister Indira Gandhi. There was also a constant threat in the southern part of the country from various groups that supported another terrorist group, the Liberation Tigers of Tamil Elam (LTTE). Eastern India has also faced various separatist/extremist movements, which have orchestrated a long-drawn Maoist insurgency against the Government. Finally, the 2008 Mumbai terrorist attack, executed by highly trained militants who were receiving clear directions from Pakistan, resulted in significant loss of life and property.

5.1.3.2 Security Architecture in India: General Considerations

With the above backdrop in mind, let us visit the security architecture in nuclear facilities in India. Nuclear installations in India are under well-guarded multilevel security systems right from the border of the country to the site of the facility. Security of nuclear assets has long been of paramount importance to India, as is evident from provisions relating to security of facilities and materials included in the Atomic Energy Act of 1948.

Nuclear facilities are declared "Prohibited Areas" under the Atomic Energy Act, which allows regulation of movement in and around them. The Indian Official Secrets Act also restricts photographing or drawing nuclear facilities. In addition, the Government of India has declared "No Fly Zones" and "No Fishing Zones" around nuclear facilities. The security environment is continuously reviewed by inter-ministerial committees. These committees meet at regular intervals to share and

review security information and ensure smooth inter-agency coordination with each other.

Specific components of physical protection systems in India include:

- Strict access control measures for personnel, vehicles, and materials
- Robust perimeter defence with watchtower and patrolling track
- Early detection capabilities
- Continuous monitoring and intrusion detection in operating island, as well as vital/inner areas
- Securely located, continuously manned Central Alarm Station
- Well-trained and equipped, round-the-clock federal response force

A model layout of the physical protection system of a power reactor, clearly depicting its multilayer security structure, is shown in Fig. 5.1. The Exclusion Zone Boundary is the first layer of defense, where entry is restricted through a manned gate. The area between the Main Plant Boundary and Exclusion Zone Boundary is a no man's land. The Main Plant Boundary (MPB) has access control portals for personnel, vehicles, and material. Watchtowers are also located along the MPB, and a continuous patrol is kept up. The Operating Island, including the Vital/Inner Area, is double-fenced, with intrusion detection devices between the two fences.

The following security practices are essential to an effective physical protection system:

- ***Need-to-Know and Need-to-Go***: Every stakeholder in a facility should be given only the information that he needs to know at that moment, including information regarding security systems. Similarly, areas within nuclear facilities should be compartmentalised according to their security significance. Personnel should be allowed entry only into specifically permitted areas of movement.
- Security systems should facilitate smooth functioning of the facility; they should not inhibit it. There should be ***perfect synergy*** between facility operation, safety requirements, and security requirements.
- Security personnel should understand that the security environment is ***dynamic***, and they should act according to its changing requirements.

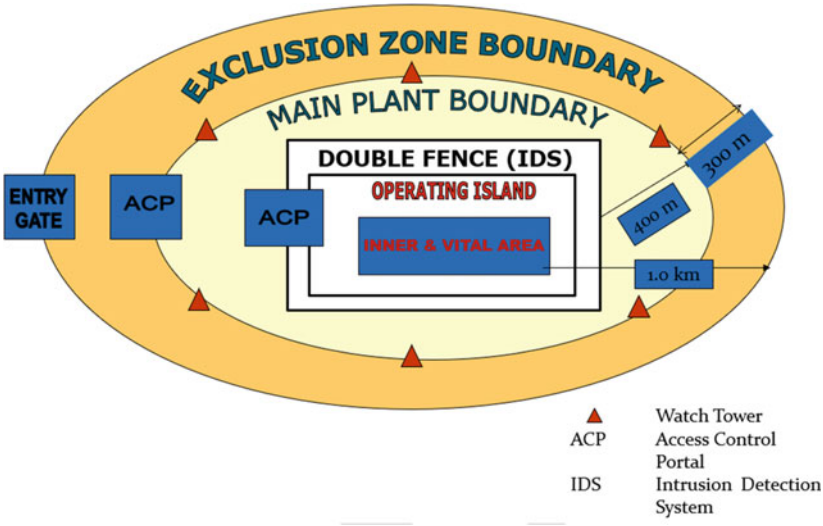

Fig. 5.1 Layout of model physical protection system

- Security personnel should continuously ***monitor vulnerabilities*** and should enhance security measures accordingly.
- Security personnel must remain ***alert***. Uneventful periods can create a sense of complacency. Remedial measures include rotating posts, briefing and debriefing, discussing security incidents elsewhere, and making preemptive arrangements to thwart emerging security threats. The arrangement of very light refreshment at the duty-post in dull hours can help keep the security forces alert in addition to boosting their morale.
- All safety incidents should be considered ***potential security incidents***.
- ***Root-cause analysis*** of all incidents, accidents, and near-miss situations should be meticulously done and should be shared with other facilities and the regulator.
- There should be a continuous schedule of training and ***mock drills*** for the response force.
- There should be ***self-auditing*** of PPS equipment and infrastructure. The gadgets should be in an operational condition and if found otherwise, then appropriate measures should be taken to rectify

or compensate for the situation. There should be a strict timeline for replacement of a faulty equipment and accountability should be ensured.
- Security guards should be alert to possible ***cyber-hacking*** of PPS gadgets and control panels.

Stakeholders should make a conscious effort to improve nuclear safety and *nuclear safety and security culture*. They can do so by:

- encouraging employees and security personnel to strictly adhere to SOPs
- encouraging employees to communicate any suspicious incident, behaviour, or conduct
- supporting activities that enhance stakeholders' pride in the organisation
- keeping a transparent grievance redressal mechanism
- improving the Personnel Reliability Programme (PRP)

These procedures and principles are codified in a manual and SOPs. They are used to sensitize appropriate stakeholders to their role in nuclear security on a strict need-to-know basis.

5.1.3.3 Emergency Preparedness and Response

Physical protection systems should be able to mitigate the consequences of radiation release for workers, the public and the environment. They should also be able to locate lost or stolen material. India has a complete system for dealing with nuclear or radiological emergencies. This system is an integral part of the national disaster mitigation architecture.

In nuclear power plants, the plan for off-site emergency mitigation is part of the documents for regulatory approvals. This plan is also shared with local administrative authorities and with the Government of India. The area around a nuclear power plant is divided into an Emergency Planning Zone, a Sterilized Zone, and an Exclusion Zone. The Exclusion Zone is an area around the plant with a radius of 1 km. In this area, no habitation is allowed. The Sterilized Zone is an area with a radius of 5 km from the plant. In this area, any new industrial or commercial

activity which attracts new population is forbidden. The emergency planning zone is an area around the facility with a radius of 16 km. Emergency exercises are held periodically, as per the regulator's requirements.

Mitigation plans for emergencies arising out of other nuclear or radiological accidents are planned according to the guidelines of the National Disaster Management Authority. In any such incident, technical guidance is given to the local law enforcement authority or to the National Disaster Response Force by Crisis Management Group (CMG) of Department of Atomic Energy, which consists of experts of various disciplines. If local law enforcement authority requires on-site assistance of technical experts, it is provided from the nearest Emergency Response Centre. These Emergency Response Centres (ERCs) are located at 30 different locations across India. The Department of Atomic Energy has also established a 24 × 7 Emergency Communication Room (ECR) and alternate ECRs with multiple redundant modes of communication.

A model layout for planning an emergency response system is provided in Fig. 5.2. Following a radiological emergency, the premises are triaged into the inner cordoned area, decontamination area, outer cordoned area, and staging area. Access control between these areas is of paramount importance. The response is coordinated by an incident commander, who is assisted by the response force and local authorities. He also helps in setting up the medical response base, radiological monitoring and assessment centre and evacuee monitoring and registration area, while also interfacing with the public information centre.

India has already shown its expertise in Goiania, Brazil, and Afghanistan in locating lost radioactive sources. India has been a signatory of IAEA's Convention on Early Notification of a Nuclear Accident[9] and Convention on Assistance in the case of a Nuclear Accident or Radiological Emergencies.[10]

[9] International Atomic Energy Agency IAEA, "Information Circular Convention on Early Notification of a Nuclear Accident," 1986.

[10] International Atomic Energy Agency IAEA, "INFCIRC/336—Convention on Assistance in the Case of a Nuclear Accident or Radiological Emergency," 1986.

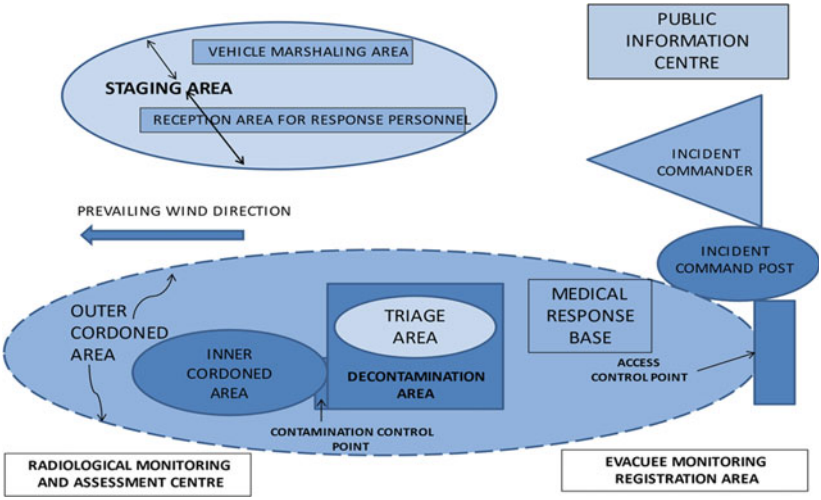

Fig. 5.2 Conceptual plan for emergency operations

5.1.3.4 The Role of Technology in Nuclear Security in India

Technology enhances nuclear security in India.[11] In addition to RF-based identity cards, secure communication systems, radiation detection portals, networked systems of cameras with video analytic software, sensors, and barriers and access control measures, India has adopted policies of "Closed Fuel Cycle" and "Reprocess to Reuse for Plutonium," with strict no-stockpiling rules. India is also working on proliferation-resistant technology such as vitrification of high-level nuclear waste, and vitrified cesium pencils. These proliferation-resistant technologies add an additional layer of security apart from existing physical protection systems. In reactor technology, India is working on a Design-Basis-Security concept, where reactor design itself will provide a required level of security. India's forthcoming indigenous Prototype 300 MW Advanced Heavy water Reactor will have many such advanced features designed and inbuilt to enhance security of the reactor and its systems.

[11] Government of India Ministry of External Affairs, "Nuclear Security in India," 2014, https://mea.gov.in/Images/pdf/Brochure.pdf.

5.1.4 *Security of Radioactive Materials in Nuclear Facilities*[12]

Radioactive materials are provided "cradle to grave" security. It improved tremendously after the regulator deployed an **e-LORA** (e-Licensing of Radiation Applications) portal. This portal not only keeps a registry of radioactive sources but also provides authorisation for procurements and movement of sources, self-audit reports regarding accounting of sources, and return of disused sources either to a government depository or to its manufacturer.

The security of radioactive materials in nuclear facilities depends on the same principles as that of nuclear materials. The threats associated with radioactive materials are less concerning than those posed by nuclear materials because radiological materials cannot be used to fashion an Improvised Nuclear Device. Radiological materials can be used to construct either a Radiological Dispersal Device (RDD) or Radiological Explosive Device (RED), however.

The Physical Protection System for radiological materials takes a graded approach. Radioactive materials are characterised in five categories of descending danger, from the most-dangerous Category I to the least-dangerous Category V.[13] Category V material is managed through measures such as a security plan, safe storage area, proper accounting, access control, continuous monitoring, and periodic regulator audits. The graded approach builds on this foundation to provide enhanced levels of security as the danger of radiological material increases.

5.1.5 *Transport Security of Nuclear and Radioactive Materials*

5.1.5.1 *Security of Radioactive Materials in Transit*

Radioactive sources find widespread application in industry, medicine, and agriculture. As such, there is a significant need for safe transport of these materials because of the potential hazards of mishandling. The United Nations has issued a model regulation for security during transport of

[12] "Guide No. AERB/RF-RS/SG-1 Government of India Security of Radioactive Sources in Radiation Facilities AERB Safety Guide Atomic Energy Regulatory Board," n.d.

[13] IAEA NSS9, "Security in the Transport of Radioactive Material | IAEA," accessed May 10, 2021, https://www.iaea.org/publications/7987/security-in-the-transport-of-radioactive-material.

dangerous goods.[14] India's Atomic Energy Regulatory Board (AERB) has adopted the UN guidelines.[15]

Radioactive materials must be packaged to ensure that no significant radiological emissions occur during a transit accident. Types of packaging depend on the hazard value of the radioactive materials as defined in the IAEA's document NSS 9.[16] Certain Low Specific Activity (LSA) materials that involve low risk of radiological exposure, like uranium ore or its concentrate, are transported in industrial packages. These strong, light containers will protect LSA materials during normal shipping activities. Radiopharmaceuticals are packed for transport in type A packages, which have demonstrated, through a series of tests, the ability to protect their contents under normal transportation conditions. Materials with high radioactive content, which pose a significant danger if released, are shipped in type B packages, which will maintain their integrity even under severe accident conditions.

The IAEA has grouped all sealed sources into five categories. Sources in Category I are highly radioactive and considered to be the most "dangerous"; they can pose a very high risk to human health if not managed safely and securely. At the lower end of this spectrum is Category 5, the least-dangerous materials. A second method of categorisation, employed by the Atomic Energy Regulatory Board (AERB)[17] in India, is based on ease of operation for repeated transportations and covers all types of radioactive materials including sealed sources, unsealed sources, and irradiated nuclear fuels. This categorisation of radioactive materials aims to aid the consignor or consignee in determining the security arrangements

[14] UN, "Recommendations on the Transport of Dangerous Goods," 2017, 1–8, https://doi.org/10.18356/a122d749-en.

[15] India Atomic Energy Regulatory Board, "Guide No. AERB/NRF-TS/SG-10 Government of India Security of Radioactive Material During Transport AERB Safety Guide Atomic Energy Regulatory Board," 2008th ed., n.d.

[16] IAEA NSS9, "Security in the Transport of Radioactive Material | IAEA."

[17] "AERB Safety Code No. AERB/NRF-TS/SC-1 (Rev.1) Safe Transport of Radioactive Material," 2016.

necessary for safe transportation. A list of commonly transported radioactive materials is given below in increasing order of radioactivity and hazard potential[18]:

i. Reference sources
ii. Consumer products (like smoke detectors, luminous painted dials, tritium light sources)
iii. Uranium/thorium ores or ore concentrates, depleted uranium, unirradiated natural uranium fuel assemblies and other RAM defined as
iv. LSA I/II/III in AERB's safety code AERB/SC/TR-1, Safety Code for the Transport of Radioactive Materials
v. Surface contaminated objects defined as SCO I / II in AERB's safety code document AERB/SC/TR-1, Safety Code for the Transport of Radioactive Materials
vi. Radiopharmaceuticals
vii. Nucleonic gauges
viii. Neutron sources used in oil-well logging
ix. Manually handled brachytherapy sources
x. Industrial Radiography Sources
xi. Remotely handled brachytherapy sources
xii. Teletherapy sources
xiii. Gamma irradiator sources
xiv. Decayed sealed sources for disposal
xv. Uranium hexafluoride (enriched)
xvi. Wastes arising from the nuclear fuel cycle
xvii. Unirradiated enriched nuclear fuel
xviii. Special nuclear material in different types of packages
xix. Irradiated nuclear fuel

The radioactive and nuclear materials being transported differ in their attractiveness for IED and RED, radiological dispersal devices depending on their hazard potential or radioactivity content. Hence, on the principles of the graded approach, the AERB identifies three levels of appropriate security arrangements:

[18] Atomic Energy Regulatory Board, "Guide No. AERB/NRF-TS/SG-10 Government of India Security OF Radioactive Material During Transport AERB Safety Guide Atomic Energy Regulatory Board."

- *Level 1: Prudent Management Practices*—This is applicable to materials of type (i) to (iv). Level 1 requires that consignor or consignee should adhere to security practices like maintenance of a minimum level of security; maintenance of a formal system of accounting of material; using a formal system of selection of transport; ensuring prompt notification to consignee regarding the dispatch and receipt of the material, and any untoward incident enroute; keeping track of consignment while in the public domain; and avoiding movement of consignment at night.
- *Level 2: Basic Security Measures*—This applies to the transportation of materials v to viii and xiii. The recommended security measures for Level 2 supplement the previously described prudent management practices. This level requires appropriate background checks to establish the trustworthiness of the transporter.
  - Operators should be alert to any unanticipated threats that may emerge during the transport. There should be a robust mechanism for tracking and recovery of lost consignments, which should be put into motion as soon as an incident occurs. If materials are at any point kept in temporary storage, the security measures employed should match those employed during transport or in their permanent facility. The consignment should be carried in a closed vehicle or in an otherwise sealed and secured manner. The integrity of locks and seals should be verified by the security contingent enroute as well as by the consignee on receipt of the material.
  - All personnel involved in the transport of radioactive materials should be trained and retrained regarding security procedures and responsibilities. Each crew member of the conveyance carrying radioactive materials should have positive identification and transport vehicle should also be checked thoroughly for its fitness and road worthiness. The vehicle should be searched to ensure that there has been no tampering of any sort with the packages or the vehicle. The personnel operating the transport should be briefed in their own language regarding emergency procedures. A Transport Emergency Card (TREM CARD), containing basic precautions and emergency contact numbers, should be kept in the vehicle.

- *Level 3: Enhanced Security Measures*—Level 3 measures, which are to be implemented in addition to measures under Levels 2 and 3, apply to materials ix to xv. These measures include proper carrier identification; preparation of a formal security plan, which should be commensurate with the current threat scenario; and measures for continuous tracking and communications link with the transport convoy.
  - The security plan identifies the responsibilities of security personnel and establishes a chain of command. It specifies the number of security guards, the quantity and type of weapons they carry, their training, briefing and debriefing procedures, arrangements for continuous watch even during halts and temporary storage, well-defined routes with predetermined overnight stops, and other operating practices, equipment and resources required to mitigate the security risks. The security plan should also establish clear procedures to report threats and security incidents. During transportation, the consignment should be subject to continuous monitoring, to ensure that it has not deviated from its assigned route. The security plan should also have a provision for periodic review and audit.

5.1.5.2 Security of Nuclear Materials in Transit

Physical protection of nuclear materials during transit/transport is one of the most difficult and challenging tasks. Materials must transit through areas with which the security contingent is not very familiar. The occasional need for temporary storage and the transition of guard forces and territorial authorities at jurisdictional borders further compound the security risks.

NSS 26[19] and NSS 9[20] along with NSS 13[21] are IAEA guides for Physical Protection of Nuclear and radioactive materials during transport. Atomic Energy Regulatory Board (AERB) has also issued a guideline

[19] International Atomic Energy Agency, "Security of Nuclear Material in Transport," *IAEA Nuclear Security Series No. 26-G*, no. 26 (2015): 5–43.

[20] IAEA NSS9, "Security in the Transport of Radioactive Material | IAEA."

[21] IAEA, "IAEA Nuclear Security Series No. 13 Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5)."

titled TS/SG-10[22] for security of radioactive materials during transport, which augments the provisions of the IAEA guide. Physical protection of nuclear materials during transport should be capable of preventing unauthorised removal of material and locating and recovering missing material. In addition, it should prevent sabotage and mitigate the radiological consequences of any sabotage on individuals, the public, and the environment.

A comprehensive security plan for the domestic or international transport of nuclear materials requires meticulous planning and inter-agency coordination. It is devised by the consignor on the orders of competent authority for nuclear material transport. This plan clearly defines route and alternate routes, places of temporary stoppages and night-halts if required, routine and emergency communication procedure, handing over arrangement at the destination and defines the responsibility of each person involved in the transport. It should be reviewed when threat perception or the technical environment changes. The international transport of nuclear materials additionally requires extensive coordination between the consignor's country, the consignee's country, the flag country of the conveyance, and other countries with territorial jurisdiction for either temporary storage or passage. The countries must also agree regarding the use of firearms by security personnel, and arrangements for locating and recovering lost material, as well as mitigating the consequences of any radiation exposure.

5.1.5.3 Special Security Measures

Consignment of materials xvi to xviii should be provided special measures of security during transport. This level of security is over and above Level 3 "enhanced security measures" listed above. The consignor must submit a shipment plan along with a detailed security plan to the competent authority for prior approval. The security plan should consist of details of route, carrier, security, and escort, tracking mechanism and communication equipment. The plan should also include procedures and places for hand-over of material between security agencies and proper vetting of all the personnel involved in transportation.

[22] Atomic Energy Regulatory Board, "Guide No. AERB/NRF-TS/SG-10 Government of India Security of Radioactive Material During Transport AERB Safety Guide Atomic Energy Regulatory Board."

Packages and vehicles should be specially designed to counter the threat of sabotage and associated radiological consequences. Consignor should give advance notice to the consignee and the competent authority before starting the shipment regarding the mode of transport and a detailed timeline of the transport with an expected date of arrival to the consignee. Consignor should start the shipment after receipt of confirmation regarding readiness to receive the consignment. Consignor should also contact local law enforcement, through whose jurisdiction the consignment will pass, to assist smooth passage of shipment, and agree on contingency plans in case of a security incident.

All personnel should receive written instructions specifying their role and responsibilities and be thoroughly briefed on them prior to commencement of the operation. There should be an arrangement for automated tracking of the shipment during transport, which should be monitored at the transport control centre. Vehicles must be inspected to ensure roadworthiness and to detect any evidence of tampering, and then placed under armed guard. Finally, after handing over the consignment to the consignee, personnel should be de-briefed, for the purpose of making future operational improvements.

5.1.6 Conclusion and Future Initiatives

Physical protection systems consist of equipment and infrastructure, procedures, and security personnel. A short-coming or vulnerability in any of these three areas renders the whole system vulnerable. PPS is a dynamic and ever-changing system, which needs to adapt and evolve constantly in the light of emerging threat scenarios and ongoing technical advancements.

There are many new technologies that make physical protection more cost effective and robust. We must try to include these in our system based on the experience of our American partners. A system of continuous bilateral dialogue and organisation of bilateral symposiums to showcase these technologies could provide an excellent platform for cross pollination of ideas among like-minded international partners.

DAE installations in India employ a force of personnel who are primarily trained for general industrial security. The generalist training that is currently imparted to this cadre may be insufficient to address the

unique and highly specialized security challenges that arise in the nuclear sector. There is a growing need for specific training in this critical sector, where every countermeasure has to be deployed discretely and judiciously, keeping in mind the possibility of serious radiological emergencies. Close engagement and cooperation with our security counterparts in the U.S. can help these efforts; both sides can benefit through sharing of mutual experiences. Threat simulations on the lines of joint military exercises could go a long way in training of security personnel and improving their efficiency.

Despite having multiple Emergency Response Centres across the country, in a real-world emergency scenario on the scale of Fukushima or Chernobyl, emergency response equipment would need to be decontaminated before it could be employed again. As such, a large redundancy of emergency response equipment is needed for tackling a large-scale contamination. The existing emergency response system of one nation may be overwhelmed in this type of situation. Anticipation of such a scenario requires states to foster close cooperation with international partners and start formalizing plans for a regional emergency response centre, so that any emergency requirement of one nation may be supplemented. Expressions of political support in international forums may help to advance this effort.

The infrastructure of the Indian road transport sector was not designed meet the requirements for transportation of dangerous goods, and the personnel involved often lack the literacy and knowledge base to understand the requirements of this sector. Thus, there is a need to develop a specialised road transport sector for transporting nuclear and radiological materials. Staff must be trained about the requirements of transport and sensitized to the relevant security threats, and conveyances appropriately modified to enhance their security. Indian stakeholders may benefit hugely from the experience of their U.S. counterparts in this field.

The Indian system of physical protection of nuclear and radiological materials has come a long way since its inception and has displayed a commendable track record. International cooperation will ensure that the Indian best practices can be emulated by others and the Indian system can be refined continuously by drawing upon others' experience as we all move towards the collective goal of a safe and secure nuclear world.

5.2 A U.S. Perspective

James McCue and Alan Evans

Nuclear weapons programs require credible safety and security systems—especially when the programs include nuclear warheads. In this chapter, we apply a systems engineering approach to explain Physical Protection System (PPS) design. We also provide two examples of U.S. nuclear security conditions to highlight key elements for systemic improvement. In this chapter, we discuss a methodology from the civil nuclear sector with the Sandia National Laboratories' (SNL) Design Evaluation Process Outline (DEPO). This design concept has been used extensively across the world for civil nuclear security programs, and military programs, and relies heavily on the work of Mary Lynn Garcia.[23] This methodology was specifically developed for securing nuclear assets, including nuclear weapons, nuclear power plants and other high-consequence facilities (HCFs). While civilian nuclear material protection is an important topic, this paper focuses on nuclear weapons. These assets represent the ultimate high-consequence risk, justifying the highest protection effort and so offer the most depth for discussion.

This chapter explains the DEPO methodology and offers some suggested changes. These proposed amendments include new elements for added analysis such as budgetary restraints, security system reputation, and threat capabilities defined in conjunction with enemy mission goals. We then apply this method to analyze Inter-Continental Ballistic Missile (ICBM) security performed under two different configurations and security situations. We consider warhead security while "on alert" in underground silos and look at how effective security concepts operate during transport for maintenance. We identify several system design challenges such as vulnerability of static doctrine, planning factors for conscripted personnel, and risk from outdated threat concepts. We show how vestigial Cold War security goals can deny theft yet result in programmatic failure through political or financial loss. This paper's modified DEPO method is designed to account for these problems and create enduring security success through performance-based evaluation to defeat current and future threats.

[23] Garcia, M. L. *Design and Evaluation of Physical Protection Systems*, 2nd ed. (Sandia National Laboratories, 2008).

5.2.1 *DEPO Method Overview*

The Design Evaluation Process Outline (DEPO) methodology has been used for many years to design and evaluate physical protection systems. This methodology employs a system engineering approach to provide a framework that captures guiding regulations, facility characteristics, and stakeholder needs. The second PPS design phase is integration of people, procedures, and equipment to maximize security effects of the overall system.[24] This methodology does not then end. Rather, it continues through evaluation to complete the process, making a continual cycle that keeps the security system perpetually updated. This continuous evaluation approached creates a forward-looking, threat-anticipating system, rather than a backwards-justified, regulation-focused security enterprise. DEPO-type evaluation uses a variety of analysis techniques such as path analysis, probability of interruption and neutralization analysis, scenario analysis, tabletop exercises, and force-on-force exercises to ensure effectiveness and provide regular feedback from both human and computer-originated analysis. Figure 5.3 is adapted from the National Security Training Center's curriculum and illustrates these phases, the elements within each phase, and the components of each element.

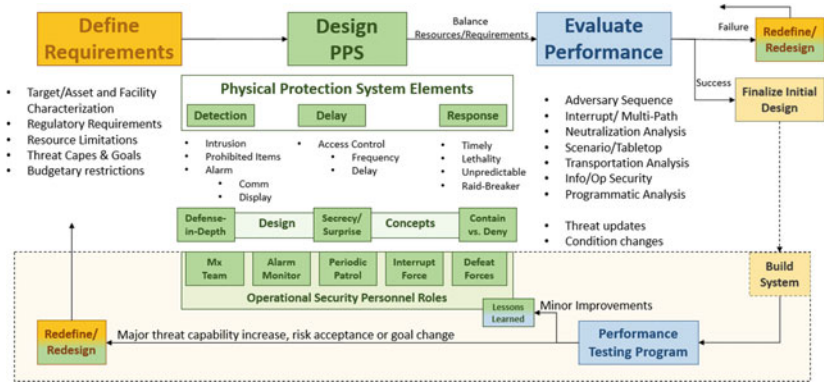

Fig. 5.3 Adaptation of DEPO methodology

[24] Garcia (2008, p. 57), the opening sentence to the section on PPS design.

The Define Requirements phase identifies the physical and environmental conditions of the site as well as the asset(s) under protection. A properly designed physical protection systems avoids impeding mission operations as much as possible, though some trade-offs between security and operational efficiency can be expected. This phase also identifies the litany of regulatory requirements that establish the minimum capabilities required at the international, national, and local levels. For the United States this means considering IAEA, U.S. Nuclear Regulatory Commission rules, DOD, and DOE instructions as well as having to comply with the EPA/OSHA, state, and county rules for hazard prevention, and even traffic laws. Whether civil or military, each nuclear possessor state's risk tolerance will set the relationship between ease of operations security stricture.

The U.S. began building its nuclear triad soon after WWII in a relatively risk-accepting time, with safety technology and security concepts for these weapons in their infant stages. It would take half a century, and be almost a decade after the 9/11 attacks, before a major investment in U.S. nuclear "modernization" brought remote video surveillance to ICBM launch facilities.[25] The attacks on 9/11 made clear that there was now a capable, dedicated threat to nuclear security systems. Yet this environment, and the desire to "do something," caused designers to rush. This led to costly measures such as an upgrade for the brand new Remote Visual Assessment system.[26] This restraining effect is why we add budgetary planning for the entire system life cycle as a stand-alone element within the first phase of DEPO analysis. Additionally, significant changes in threats or other restraints such as risk tolerance should trigger programmatic redesign, rather than just patching. Comprehensive requirement assessment ensures capturing interactive effects as well as second-order impacts.

The Design phase is based on three components at the heart of the PPS: Detection, Delay and Response. For a security system to succeed, the combined effects of the first two elements must result in a protection time longer than time the adversary needs to gain access to the facility, so

[25] Defense Industry Daily Staff. Also funded at this time was additional concrete head works for security effects as opposed to hardening against a nuclear strike.

[26] The RVA was funded for upgrades that added "new capabilities" in 2011, and this re-design right after initial install cost nearly double the initial system cost.

that security personnel can interdict it. In other words, the facility must take longer to break into than it takes a responding team to arrive.

It is important to understand that detection is not an action; it is the compilation of efforts among the many sensors and trusted communications that bring about a declared security situation. Detection is the realization of the adversary's action, not just the effort of looking.[27] Designers need to also consider that delay can be created in two ways: through passive delay barriers (i.e., doors, windows, walls, fences, etc.) and through active delay barriers (i.e., pop-up vehicle barriers, dispensable barriers, etc.). Delay barriers increase the adversary task time and increase the complexity of the attack for the adversary force. The final element, response forces, consists of a variety of security teams with differing capabilities and purposes such as periodic patrols, initial interruption forces and the neutralizing team that defeats the adversary.

Design is both art and science requiring the balancing of conflicting requirements as well as competing strategies. One such oppositional set of security concepts are containment and denial. Containment focuses on the asset and keeping it within a specific boundary, while denial centers on the adversary and preventing it from gaining access to a restricted area. Denial further breaks down into access denial and task denial. Access denial often imposes a cost in operational efficiency. This reduces risk from a few potential threat actors, but imposes operational costs for even valid users with lost work time satisfying entry procedures. Alternatively, task denial creates delay by forcing an adversary to complete a series of difficult tasks or changing the task conditions after an unauthorized access attempt is detected. Containment strategies are often the least expensive to design, build, and maintain. Access denial is usually the costliest both financially and operationally. Containment and denial can be complimentary design concepts, but each consumes budgetary resources and addresses different threat types and goals and creates different delay effects.

Another double-edged security strategy is secrecy and surprise. Secrecy can be either an alternative or supplement to delay. A secrecy-based design relies on hiding an asset rather than locking it away in a safe.[28] Secret

[27] Garcia (2008, p. 59).

[28] This is not an option in many cases but can be very effective where technology and conditions permit. Even art museums gain security value out of adding uncertainty to how and when they will ship special exhibits or by sending 3 replicas of the Mona Lisa on 3 different routes.

routing, a lock's combination, and randomly leaving missile silos or transporters empty are security concepts that all rely on varying degrees of secret information to create security effects. Surprise is another supplement to PPS's that can provide cost-efficient security effects. Secrecy ensures surprise. But this inherently creates a problem, since the goal of security is deterrence and an unknown threat cannot deter. Nonetheless, secrecy and surprise deter by eroding a would-be attacker's confidence.

The Evaluate phase of the DEPO methodology tests the effectiveness of PPS's during design and throughout its life cycle. Evaluation of the physical protection system ensures that the system behaves as designed (or gets rejected for redesign) and gives feedback over time. This enables growth and relevance in the face of evolving threats, resource availability, and risk tolerance. Performance-based approaches to PPS's ensures asset defense at a level effective against the postulated threat.

5.2.2 Applying the DEPO Method

Using the DEPO method to analyze two operational nuclear security challenges helps draw out important nuances and operational considerations difficult to see with only theoretical examination. Reflecting on the security conditions of U.S. ICBM launch facilities and warhead transportation shows how physical protection works in practice and reveals ways to leverage new technologies.

Designing for physical-security system effectiveness requires clearly defining the program's strategic purpose. The nuclear weapon PPS objective is to negate unauthorized warhead access obtained by breaching physical barriers and/or neutralizing security personnel. This definition clarifies what is, and what is not, a physical security concern. Personnel reliability programs, cyber defense, and other security related considerations are vital for the success of the overall nuclear security enterprise. However, those considerations are beyond the scope of physical security. Precisely defining the nuclear physical security task and purpose also enables performance evaluation and analysis techniques such as analogy and comparison. Security industries with similar challenges provide useful points of departure and the have a longer history of both successes and failure to draw from.

It is important to note that each security situation has an ideal attack outcome as well as a limited series of bad ones. Bad outcomes may have different paths, and each must be understood so that all can be defended

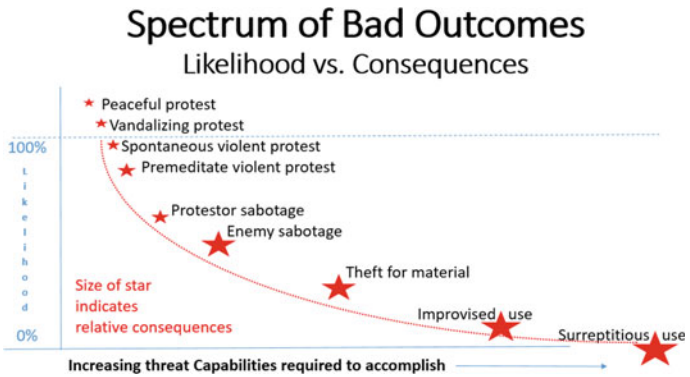

Fig. 5.4 Potential undesirable results of an attack

without risking bad assumptions regarding lesser-included threats. This spectrum of bad outcomes must be understood to avoid creating an exquisite system immune to total failure but fragile in its propensity to fail partially (Fig. 5.4).

5.2.3 Defining System Requirements

5.2.3.1 Asset(s) Under Protection

The International Atomic Energy Agency (IAEA) regulates security of civilian nuclear material and nuclear facilities worldwide. The IAEA employs three tiers of security requirements based on the quantity and type of nuclear materials in storage. The IAEA standards are tiered to allow for a graded approach to physical protection measures in civilian security design. However, military responsibility begins at a tier well above even the highest IAEA consequence scenarios based on the presence of weapons-grade nuclear material. The adversary must be prevented from accessing this material. If that fails, then the plutonium, uranium, and other key nuclear materials must not be stolen. Partial success in preventing access or theft, though suboptimal, is more survivable for the enterprise than total failure regardless of whether the adversary seeks physical or political objectives.

Extreme weather is not itself a security threat, but it is a part of defining the conditions within which a security system must operate. Weather events can decrease the effectiveness of the security system and may slow

responders. Extreme weather events can lead to damage or disruption of critical security components such as intrusion detection systems, barriers, or assessment capabilities. U.S. nuclear silos were initially designed and evaluated without regard to this challenge and instead were placed to maximize survivability for use in a second strike against the Soviet Union. Including weather-related contingency and compensatory measures in system design minimizes costs and reduces second-order effects. Tabletop exercises and simulations are helpful design tools for exploring this problem set.

Across the U.S. nuclear triad, the assets under protection are quite similar. However, the security conditions vary considerably. The storage and maintenance facilities all create a similar degree of protection, but there are significant differences among the distances security personnel must travel during response. Long transit is the largest factor in the time required to respond, and thus drives delay requirements. In this respect the nuclear ICBM poses a unique and extremely difficult security challenge; distances between warheads and security personnel are much greater than in other weapon security conditions.

Most modern nuclear warheads rely on limited-life components requiring regular maintenance.[29] U.S. warheads must be moved between silos and the main base or, less frequently, be transferred to the Department of Energy for laboratory work. Both the Defense Department and Energy Department must perform this transport on public roads. They perform this mission with nearly inverse security strategies, each employing tactics optimized for their very different security conditions.

5.2.3.2 Defining System Constraints and Restraints

The process of defining both what the security system can't do (constraints), and what it must do (restraints) typically starts with review of the applicable high-level international regulations alongside national and provincial mandates. The U.S. appetite for risk has decreased over the past half century. Much of this change occurred as a result of the 9/11 attacks and the accident at the Fukushima nuclear power plant in 2011. Over the lifetime of the U.S. nuclear enterprise, and with each

[29] With a half-life of 12.3 years and the ability to drastically increase weight-to-yield ratios, tritium is an essential component of some thermonuclear designs. This short half-life forces regular replacement of this material, driving up maintenance costs and increasing security burdens.

new generation of nuclear weapons over the decades, a plethora of new safety and operational requirements have emerged. Risk reduction is now so difficult, yet so desirable, that the generation of weapons currently under development are likely to cost five times more than the original Manhattan project, in large part because of the emphasis on and difficulty of risk reduction.

Military security regulations and doctrine for each of the nuclear weapon possessor states are understandably classified. However, a series of recently concluded nuclear security summits provides some public information regarding international protection standards and design concepts for securing nuclear material from "terrorist groups and smugglers."[30] From international down to local security expectations and limits, the totality of physical, financial, and political constraints and restraints establishes the security conditions within which the system must operate. Therefore, the system designers must be well acquainted with these rules.

Transitioning from designing on paper to concrete reality means overcoming restraints such as budgetary limits. Successful budget planning includes many components such as initial facility design and security system design, but also incorporates operational budgeting. Some initial budgetary considerations for physical protection systems include initial system design, technology research, installation construction, and performance testing. Likewise, recurring costs such as personnel, facility maintenance, and operational costs must also be included to ensure long-term financial viability. Budgeting should be for the entire engineering lifecycle of the nuclear program. This timeline is typically 50 years for a nuclear power plant, but the US's ICBM and B-52 planning horizon have expanded out to around a century.[31] Domestic privacy rules can limit detection options and up-front investment for delay features can be difficult to squeeze between regulatory restraints and budgetary constraints. But designers should approach this difficulty conservatively as high redesign costs or budgetary overrun can lead to program failure. These

[30] For an overview of these events, see: https://www.armscontrol.org/factsheets/NuclearSecuritySummit.

[31] The B-52 began flying in May 1961 and the USAF recently contracted to upgrade the 60-year-old engines with a new design, adding as much as 40% more range and another 40 years of life to the airframe. Likewise, the 1970's Minuteman III ICBM, with an originally planned ten-year lifespan, is housed in the original MMI silos that came online in June 1961. While the GBSD is meant to replace these in 2040, some analysts and lawmakers are pushing instead to extend the MMIII.

security conditions bound the PPS design space and require extensive research alongside iterative planning to mitigate risk.

The security industry has reduced costs significantly by replacing people with technology; it has long been known that people make bad sensors.[32] Active delay systems, new sensor concepts, increased security-force lethality, new less-than-lethal options, digital communications, and automation all work together to reduce the number of personnel needed for an effective PPS.[33] U.S. military training costs have also been lowered in various fields through modeling and simulation tools that reduce training needs.[34] Combining modern remote sensing with computerized training and threat analysis tools reveals new compensatory options. This narrows the scope and frequency of expensive field testing and operational training. Simulation tools may not provide the same experience that field exercises offer, but they can greatly reduce the costs, time, and risk. In the near future, this concept could be expanded to include reducing costs by using smaller numbers of staff in more roles, such as site maintenance, through use of augmented reality.

5.2.3.3 Defining the Threat

The final component of requirements analysis is determining plausible threat capabilities and goals. The U.S. nuclear security enterprise traditionally approached this problem from a capabilities perspective. This method requires planning against an adversary's potential means of carrying out an attack. This focuses on factors like equipment and skills but ignores intent. Consequently, this policy may discount scenarios in the middle of the risk spectrum and thereby create niche vulnerabilities.

[32] Starting in 1973, Tickner and Poulton found a range of 50–85% for probability of detection in their article for the journal *Ergonomics* titled "Monitoring up to 16 Television Pictures Showing a Great Deal of Movement." A large number of studies have been conducted to follow up this effort, confirming Garcia's conclusion that "humans are generally not good detectors."

[33] Anduril Technologies is just one of several security technology firms providing turn-key solutions for detection/surveillance systems, with myriad options unavailable to Cold-War era security designers, such as mobile virtual fences, fully autonomous UAVs, and artificial intelligence that allows a single person to surveil hundreds of miles of terrain."

[34] The USAF recently experimented with using VR systems for initial helicopter flight training and saw immediate success, with a 35% reduction in flight time. This concept is also being used to reduce training needed for maintenance, ground combat, and remote project collaboration, and even surgery.

Defending against a wider range of risk demands analysis of adversary goals as well as capabilities by the system designer and response force trainer.

Characterizing threat actors by capability identifies key features such as the number of attacking personnel, their sophistication in thwarting detection, likely vehicles or weapons used, and familiarity with tools for breaching applicable delay features. Mission objectives and strategic purpose are then knowable through normal intelligence analysis. These mission goals do not readily change. If a nation is willing to "eat grass" in order to secure a nuclear capability, it is unlikely to give up due to technical setbacks.[35] Highly risk averse states that are less interested in nuclear weapons, by contrast, are more susceptible to compellence.[36] Characterizing adversaries by capability and motivation provides a clearer understanding of potential threats and allows the system to mount a successful defense on either level.

An adversary must be capable of defeating the physical delay systems and challenging the response force to be considered a credible threat for theft or sabotage. Protestors and non-credible attackers can threaten the enterprise, but do not present a plausible chance of succeeding at theft. To gain this higher-level credibility, would-be thieves must operate with basic military organization and discipline. Such a plausible threat group would be operating with the benefits, as well as the limitations, of a raiding party. In this vein, several recent terror attacks have displayed the tactics and equipment normally reserved for professional militaries.[37] More concerning is the increasing ease of target surveillance and growing adversary lethality, as well as the difficulty of determining state sponsorship.[38]

[35] Singh (1979).

[36] Edited by Kelly M. Greenhill and Peter Krause (2018). See Chapters 6, 7, and 8, which deal with non-state actors. This book provides a detailed accounting of how "weak" actors have coerced stronger states in recent history.

[37] The 2015 Paris terror attack, the 2019 DusitD2 attack in Nairobi, and the March 2021 Palma Mozambique attacks, are all recent complex attacks where military-style command, control, and communications were employed.

[38] The Westgate Mall in Kenya was attacked by an unknown number of men in 2013, killing 67 over a 4-day siege. A handful of terrorists held all of Mumbai hostage during their 2008 attack that killed more than 160.

Likening potential attackers to a raiding party highlights potential countermeasures. The small size, minimal depth, and light footprint of a raiding party give it mobility and a low signature, but also render it vulnerable to well-trained and equipped security patrols or immediate response forces. Viewing the adversary as a capable yet limited enemy with specific mission goals—in other words seeing the enemy as a raiding party—is therefore a helpful heuristic for improving threat analysis.[39] Regardless of the threat type and security conditions, the more comprehensively that all requirements are defined, the better the security system can and will be designed and operate.

5.2.4 Design: Delay, Detection, and Response

This section discusses the three main design elements of physical security and shows how U.S. ICBM security balances each to maximize synergy and resiliency.

5.2.4.1 Detection

Given enough time, every castle wall can be breached by hammer, shovel, or ladder. Therefore, PPS's must have mobile, capable response forces. Yet without a timely alert, these forces will be ineffective. Moreover, if an alarm sounds and no one hears it, then it is ineffective. That is why detection is graded for both sensing and communication.

The best detection systems are built with a variety of complimentary sensors installed to achieve overlapping fields of regard. Successful adversaries will have to defeat the combined effects of multiple sensor types covering the same physical space. Complimentary sensing means fields of regard overlap such that defeating one type of sensor makes the target more vulnerable to the other kind of sensing. For example, a motion sensor might be defeated by exceptionally slow movement. Camera surveillance of the same area compliments motion detection because the slow movement to defeat motion sensors ensures that an attacker will spend an exceptionally long time on the video screen. Linear layering of zones then enables defenders to monitoring attack progress to support decision-making. Ideally, each layer or zone employs these complimentary

[39] Samuel A. Southworth provides a great outline of key functions and characteristics of a raiding party in the introduction to his book. (Southworth, 1997).

sensors on independent secure communication links, feeding redundant monitoring stations.

Sensor outputs are now rarely binary because of advances in technology. This provides a higher volume and quality of detection information. Observable sensors may be intimidating but are likely to be destroyed once the adversary abandons its efforts at stealth.[40] Designers should plan for a number of covert sensors to ensure continuous monitoring across layered zones throughout the attack sequence. This affords vital intelligence for the response force, such as which layers of delay have been breached. When combined with timing information and video images, it reveals what special equipment the adversary may have, or may still require in order to gain access. Independent lines of communication add to this information, and if one is compromised this provides information regarding the attacker's sophistication and likely goals.

The nature of nuclear material transportation does not lend itself stationary physical barriers such as multi-ton concrete doors. The need for mobility forces defenders to adopt active measures. The Department of Defense responds by convoying several escort vehicles with heavy firepower. By contrast, the Department of Energy chooses more clandestine movement. This low-signature approach is facilitated by DOE's relatively small number of missions along a large variety of routes.[41] Maintaining secrecy is becoming harder, however, in the age of social-media connected plane spotter groups.[42] Secrecy is a beneficial security add-on but should not be the primary means for creating security effects in a world of cell phones and AI-supported search algorithms.

5.2.4.2 Delay

The delaying element ensures that adversary task time is long enough for the defender's response component to defeat an attack. An intruder

[40] See Garcia, Chapter 13, for an explanation of the concept of the Critical Detection Point (CDP) and a deeper treatment of the relationship of adversary stealth vs. speed as strategies for beating the delay system and avoiding interruption by the responding force.

[41] https://www.energy.gov/nnsa/office-secure-transportation.

[42] The practice of "plane spotting" can be detrimental to operational security, and is taking off in many unrelated fields of niche interest such as boats and bird watching. This technology is far more sophisticated than that used by the groups that successfully ended the U.S. nuclear train-based system for transporting warheads to and from the Pantex facility.

is slowed by having to penetrate multiple layers of delay infrastructure. Ideally, security design avoids creating multiple entry routes, as the adversary will then be able to choose the most advantageous path. In practical terms, however, three-dimensional objects can hardly avoid offering multiple routes, as we show below. Instead, proper design balances each path so that all options provide similar task complexity and delay. In a well-designed facility, all paths of entry should be equally difficult and time consuming (Fig. 5.5).

Delay features are graded in terms of the time it takes an uninterrupted and knowledgeable attacker to defeat them.[43] A key-card locked door is a simple example of a delay system with inherent filtering of unauthorized users. The more frequently credentials must be checked the more difficult it is to delay an adversary without degrading operations. One tactic for harmonizing these competing access/security interests is through situationally dependent time delay, such as time locks. Such a system opens only during pre-set times, such as when security personnel are expected to be present. Alternatively, it might be set to open only 30 minutes after

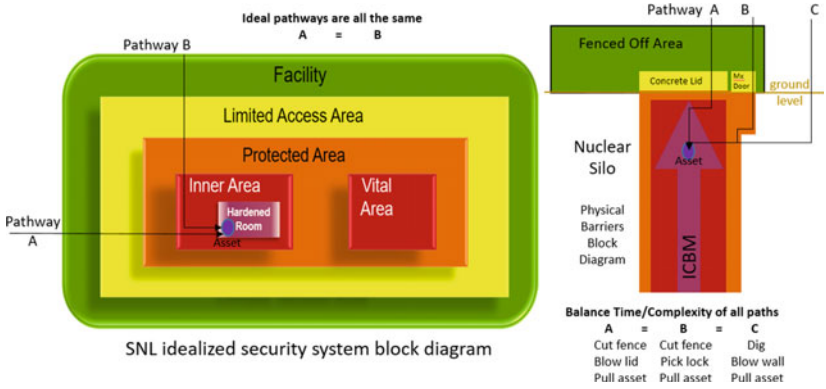

Fig. 5.5 Adapted from physical security areas (SAND2021-0176 TR)

[43] Garcia (2008, p. 219).

a correct code is entered.[44] Layered defenses best increase security effects when they require a variety of breaching methods and equipment. Additionally, surprise delay features can add outsized effects. For example, using non-standard or even random locations for security door locking pins makes it harder to guess where on the door to drill.

Though initially intended to defend against nuclear strikes, the hardening of ICBM silos can delay intruders and enable security forces to respond.[45] The "lid" on a Minuteman silo is more than 12 feet across, several feet thick and made up of concrete and rebar meant to withstand a near miss nuclear strike.[46] Cutting through this massive obstacle requires special equipment and skills and cannot be done with simple hand tools. Alternatively, active delay systems, such as sticky foam, can be effective in mobile scenarios, slowing an attack on a nuclear weapon transport vehicle.[47] It is important to note that delay features can only slow—not stop—a credible attacker. Therefore, the suite of sensors that underpin a detection system also demands extensive consideration by PPS designers.

5.2.4.3 Response

A competent response force will respond to an intrusion before the adversary can access a protected asset(s). Credibility in this role is the foundation of this element's deterrence effect. Spoiling enemy objectives requires more than simply preserving mobility and lethal overmatch, however. The response element must be adaptable, unpredictable, and able to tackle unexpected problems that computer algorithms and battle checklists cannot solve. No matter how competent they may be, defenders face motivated adversaries. Terror groups regularly reaffirm their willingness to sacrifice their lives in pursuit of their political objectives. And

[44] Because this technology is based on simple digital systems, home use models cost less than $500, while early spring-watch type designs from the early 1900s, which are impervious to electronic interference or hacking, can be obtained from antique dealers for a few thousand dollars.

[45] According to the Air Force's Global Strike Command, the Launcher Closure Door—the official name for the "lid"—weighs in at 110 tons.

[46] https://www.nps.gov/mimi/index.htm.

[47] https://www.osti.gov/servlets/purl/442050.

attribution of state sponsorship of attacks on nuclear facilities is becoming harder, making it more tempting.[48]

Even if defenders achieve deterrence, there is no guarantee that it will last. The human element of the PPS design must consider the possibility of being attacked and then having to reestablish credible deterrence. At the strategic level, nuclear security requires a tactical force capable of more than just fending off attack. The degree of an attack's failure would largely shape the aftermath, the likelihood of follow-on attempts, political fallout, compensatory measures, and new regulations. PPS success, in this sense, can only be measured from the adversary's perspective. Tactical success followed by strategic failure could also result from design that ignores sensitivities regarding disproportionate friendly force, inept responders, or high levels of civilian collateral damage. A resilient security design includes risk to reputation to account for the implications of partial success.[49]

The security mission is by nature a defensive action and is unavoidably reactive, ceding initiative to the adversary. Internal predictability is mandatory for organized action, but deadly if allowed from the adversary's perspective. Standard procedures, communications plans, and unit tactics are examples of internal predictability that ensure cohesive action and, when built and executed properly, increase the appearance of randomness. Increasing security force precision and range helps reduce predictability. Staging security teams in a variety of places ensures their arrival from multiple directions at different times. Random patrolling adds an irregular presence and creates outward randomness. Modernized command and control systems ensure this force can be quickly re-assigned to interrupt the adversary early in the attack.[50]

[48] The potential state actors, or state sponsors of such an attack, all have recent experience operating in the grey zone with hard-to-attribute, or deniable activities including use of WMD. These risky activities among potential adversaries from the nuclear club include; Russia's Novichok attack, Russian support for Syria's Assad regime despite Syrian use of chemical weapons, North Korean cyber-attacks, and China's use of its fishing militia. The nearly nuclear-weapons capable Iran should also be considered, given that they employed UAVs used against Saudi Arabia and supplied Iraqi insurgents with marginally deniable shaped charge components for IEDs, which killed many U.S. service members in Iraq.

[49] Taleb, Antifragile, 2012. Taleb's book "the Black Swan" is cited more often by security professionals based on its treatment of high-consequence low-likelihood situations. However, his concept of anti-fragility is just as important to consider when designing a security system to survive being attacked.

[50] Blue force tracker is a digital, map-based location monitoring system that incorporates voice or text-based communications including key data such as threat location warnings

Flexibility is what makes security personnel so valuable to creating security effects. Security forces trained in dynamic tactical decision-making are able to shift priorities and seize new opportunities; they can outthink as well as outgun the adversary. For example, a response force dispatched to perform initial disruption can become a neutralizing force, should the adversary be less capable than expected.[51] The inverse condition must also be trained for, so that a neutralizing force can fall back to performing disruption and self-preservation actions when appropriate.

Effective mobility of personnel is another security requirement, and therefore creates a potential vulnerability. The most effective responding vehicles are those least constrained by terrain, such as ATVs, snowmobiles, and planes or helicopter—both manned and unmanned. Commercially available unmanned aerial surveillance systems are nearing maturity and small military systems add lethal options to vastly increase the speed and security effects of response assets.[52] Incorporation of these systems could cheaply and quickly add reliable, all-weather options for countering an attack.

Response forces require training to stay sharp and evolve with adversaries' improving capabilities and changing mission goals. Viewing attackers as a raiding party offers defenders unique ways of defeating a threat. For example, defenders can leverage layered and redundant detection systems to learn about their enemy in real-time and adjust tactics or priorities as the attack unfolds. In this way, a properly trained security team becomes harder to defeat over the course of an attack.

5.2.4.4 Evaluate

Evaluation is an essential aspect of a training program and design process. It facilitates success over time by making growth an appendage of the system. Initial design evaluation can prevent cost overruns for major

or routing suggestions. A credible adversary will be using command and control systems, given that most middle-class U.S. families employ essentially the same functions to manage their Disney vacation via smartphones, or line-of-sight radios if cell reception is uncertain.

[51] In 2006, a protest group wearing clown suits forcibly gained entry to the top side of an ICBM launch facility. Though some news sources claimed these clowns accomplished "sabotage," they did not possess the equipment necessary to penetrate beyond a simple padlock on the perimeter fence.

[52] Today's technology offers lethal and even less-than-lethal UAS to simultaneously deploy upon security incident declaration and increase options against everything from peaceful protestors up to a state-sponsored raid.

redesign as well as the much worse outcome of getting out-paced by the changing threat.

Evaluation standards must continually evolve alongside the larger institution the security system serves, to ensure security standards match the changing nature of the threat. Nuclear security is a national enterprise requiring whole-of-government treatment to stay aligned with shifting risk tolerance, fiscal priorities and changes to acceptable police or military tactics. Moreover, pre-attack threat detection comes from sources outside the U.S. military. Many intelligence and law enforcement elements of the US government authorized and equipped to interrupt this point of the attack cycle have limited interaction with the DOE or DOD elements responsible for security. Even a failed attack poses a major risk to national reputation, so deciding the right balance between intelligence sharing and privacy rightly falls to the highest level of state leadership. Effects-based evaluation ensures that detection standards are aligned to national trends.

Improving US nuclear security requires moving beyond rote security doctrine. Training for dynamic tactics and performance-based evaluations naturally incorporates the benefits of new technologies and the higher quality of an all-volunteer security force. Compliance-based assessment focuses on sets of rules and engenders a backwards view of individual actions during response, raising the question "what was I told to do?" In contrast, performance-based evaluation encourages predictive thinking centered on defeating the enemy with the resulting effect as the key grading consideration. It raises the question "how do I successfully defend?" The quality of response personnel is a major factor in which approach is feasible since high order thinking and judgement under fire may not be a reasonable expectation for the troops available. In the past, the U.S. was forced to employ a conscript army, or draft, and at that time the compliance-based approach was most appropriate. Increasing performance-based evaluation and emphasizing effects is one way to address the glacial speed of nuclear doctrine and equipment upgrades.

Performance-based evaluation, then, is the best means for judging security effectiveness. Taking a performance-based approach to assessment processes and device certification would help to keep pace with emerging lethal and supporting civilian technologies. Burdensome nuclear certification rules slow the adoption of new non-nuclear weapon-related equipment such as detection sensors, munitions, or communications systems, while centralized control of security personnel equipment has similarly deleterious effects. Recent advances in commercial imaging,

processing, and automated target identification and tracking offer the adversary major improvements in surveillance capability.[53] Change detection algorithms can help to cue security personnel and even dispatch them in their most effective response roles during facility-protection, convoy, or urban operations.[54] Building an evaluation system that grades security effects from technology or dynamic tactics is the most cost-efficient means to design for optimal security effects across all possible threats and their objectives.

5.2.5 Conclusion

The modified DEPO method that we discussed in this chapter offers simple yet robust optimization tools for iteratively designing a maximally effective security system. We showed, through application of our modified DEPO method to the U.S. nuclear security enterprise, several options for improving security in both static and mobile ICBM security scenarios.

This chapter also demonstrated the importance of properly characterizing the assets being protected at the tactical and strategic level, and of guarding both the warheads and the reputation of the security system. These assets must be protected within resource restraints and constraints, while balancing acceptable levels of risk outlined in a variety of regulatory sources. We also showed that viewing the threat as a raiding party helps the defender to identify key capabilities and dissect nested mission objectives. And we explained why designing security for effect is preferable to design for compliance. While the effectiveness of U.S. nuclear weapon security is currently without question, our modified DEPO methodology thus offers several opportunities for gaining cost efficiencies and improving security effects.

[53] Recent attacks against Russian bases in Syria employed a "swarm" of ten drones using "improvised air-dropped munitions." These systems used commercial, off-the-shelf remote control aircraft—equipment that is readily available within the U.S.—and turned them into fully autonomous bombers.

[54] Software-enhanced security cameras are transforming how video surveillance is performed, taking the simple camera far beyond just threat detection into new areas such as behavior analysis for early situation declaration.

References

Arms Control Association. "Nuclear Security Summit at a Glance," 2018. https://www.armscontrol.org/factsheets/NuclearSecuritySummit.

Atomic Energy Regulatory Board. "AERB Safety Code No. AERB/NRF-TS/SC-1 (Rev.1) Safe Transport of Radioactive Material," Mumbai, India, March 2016. https://www.aerb.gov.in/images/PDF/CodesGuides/RadiationFacility/Transport/1.pdf

Atomic Energy Regulatory Board. "Guide No. AERB/NRF-TS/SG-10 Government of India Security of Radioactive Material During Transport AERB Safety Guide," Mumbai, India, January 2008. https://aerb.gov.in/images/PDF/CodesGuides/RadiationFacility/Transport/2.pdf.

Atomic Energy Regulatory Board. "Guide No. AERB/RF-RS/SG-1 Government of India Security of Radioactive Sources in Radiation Facilities," Mumbai, India, March 2011. https://www.aerb.gov.in/images/PDF/CodesGuides/RadiationFacility/RadioactiveSources/1.pdf.

Bennett, M. "Projected Costs of U.S. Nuclear Forces, 2019 to 2028," Congressional Budget Office, 2019. https://www.cbo.gov/system/files/2019-01/54914-NuclearForces.pdf.

Caesar, E. "The Incredible Rise of North Korea's Hacking Army," *The New Yorker*, April 19, 2021. https://www.newyorker.com/magazine/2021/04/26/the-incredible-rise-of-north-koreas-hacking-army.

Carafano, J. "The Draft Should be Left Out in the Cold," The Heritage Foundation, May 18, 2017. https://www.heritage.org/defense/commentary/the-draft-should-be-left-out-the-cold.

Copp, T. "U.S. Nuclear Weapons Are Aging Quickly. With Few Spare Parts, How Long Can They Last?," McClatchy DC, March 29, 2021. https://amp.mcclatchydc.com/news/nation-world/national/national-security/article250187880.html.

Doyle, J. "AeroVironment Unveils Improved Version of Switchblade One-Way Attack Drone," *Seapower*, October 1, 2020. https://seapowermagazine.org/aerovironment-unveils-improved-version-of-switchblade-one-way-attack-drone/.

Dudley, Ian. "583rd MMXS: Opening the Door, One Missile at a Time," Air Force Global Strike Command AFSTRAT-AIR, June 20, 2017. https://www.afgsc.af.mil/News/Features/Display/Article/1226716/583rd-mmxs-opening-the-door-one-missile-at-a-time/.

Garcia, M. L. *Design and Evaluation of Physical Protection Systems*, 2nd ed. Sandia National Laboratories, 2008.

Garmin. "Rino 750 2-Way Radio/GPS Navigator with Touchscreen." https://www.garmin.com/en-US/p/533999.

Goldstein, P. "Air Force Turns to VR, AR for Training and Maintenance." *FedTech Magazine*, April 13, 2020. https://fedtechmagazine.com/article/2020/04/air-force-turns-vr-ar-training-and-maintenance.

Gould, J. "Lawmakers Set for Battle Over Next-Gen Nuclear Missile," *DefenseNews*, September 9, 2021. https://www.defensenews.com/congress/budget/2021/09/09/lawmakers-set-for-battle-over-next-gen-nuclear-missile/.

Greenhill, K. and Krause, P. *Coercion: The Power to Hurt in International Politics*. Oxford University Press, 2018.

Gregory, A. "Salisbury Poisoning: How a Lethal Substance Sparked an International Incident in a Quiet English City," *Independent*, November 11, 2022. https://www.independent.co.uk/news/uk/crime/salisbury-poisoning-sergei-skripal-russia-b2223018.html.

Grossman, D. and Ma, L. "A Short History of China's Fishing Milita and What It May Tell Us," RAND Corporation, April 6, 2020. https://www.rand.org/pubs/commentary/2020/04/a-short-history-of-chinas-fishing-militia-and-what.html.

Heikkinen, K. "New START: 564th MS Siles Being Eliminated," 20th Air Force, March 14, 2014. https://www.20af.af.mil/News/Article-Display/Article/825777/new-start-564th-ms-silos-being-eliminated/.

Horton, A. "Soleimani's Legacy: The Gruesome, Advanced IEDs That Haunted U.S. Troops in Iraq," *The Washington Post*, January 3, 2020. https://www.washingtonpost.com/national-security/2020/01/03/soleimanis-legacy-gruesome-high-tech-ieds-that-haunted-us-troops-iraq/.

Hubbard, B., Karasz, P., and Reed, S. "Two Major Saudi Oil Installations Hit by Drone Strike, and U.S. Blames Iran," *The New York Times*, September 15. 2019. https://www.nytimes.com/2019/09/14/world/middleeast/saudi-arabia-refineries-drone-attack.html.

Huber, M. "USAF Slashes Helo Training Time with Virtual Reality," *Aviation International News*, October 16, 2019. https://www.ainonline.com/aviation-news/defense/2019-10-16/usaf-slashes-helo-training-time-virtual-reality.

International Atomic Energy Agency. "Security in the Transport of Radioactive Material," Nuclear Security Series No. 9, 2008. https://www.iaea.org/publications/7987/security-in-the-transport-of-radioactive-material.

International Atomic Energy Agency. "INFCIRC/335—Convention on Early Notification of a Nuclear Accident," November 18, 1986. https://www.iaea.org/sites/default/files/infcirc335.pdf.

International Atomic Energy Agency. "INFCIRC/336—Convention on Assistance in the Case of a Nuclear Accident or Radiological Emergency," November 18, 1986. https://www.iaea.org/sites/default/files/infcirc336.pdf.

International Atomic Energy Agency. "Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5)," Nuclear Security Series No. 13, 2011. https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1481_web.pdf.

International Atomic Energy Agency. "Objective and Essential Elements of a State's Nuclear Security Regime," Nuclear Security Series No. 20, 2013. https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1590_web.pdf.

International Atomic Energy Agency. "Security of Nuclear Material in Transport," Nuclear Security Series No. 26-G, 2015. https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1686_web.pdf.

International Atomic Energy Agency. "Physical Protection of Nuclear Material and Nuclear Facilities (Implementation of INFCIRC/225/Revision 5)," Nuclear Security Series No. 27-G, 2018. https://www-pub.iaea.org/MTCD/Publications/PDF/PUB1760_web.pdf.

Kay, G. "These Tech Startups Enable Surgeons to Train and Supervise Operations Remotely During the Pandemic," Business Insider, February 13, 2021. https://www.businessinsider.com/hospitals-surgeons-startups-operate-from-home-2021-2.

Kelley, R. "Starve Nuclear Weapons to Death with a Tritium Freeze," Stockholm International Peace Research Institute, 2020. https://www.sipri.org/commentary/topical-backgrounder/2020/starve-nuclear-weapons-death-tritium-freeze.

Korb, L. "Vietnam Showed the Need for a More Highly Trained Military," April 29, 2015. https://www.nytimes.com/roomfordebate/2015/04/29/lessons-40-years-after-the-fall-of-saigon/vietnam-showed-the-need-for-a-more-highly-trained-military.

Lafontaine, D. "Army Set to Modernize Blue Force Tracking Network," U.S. Army, July 13, 2018. https://www.army.mil/article/199916/army_set_to_modernize_blue_force_tracking_network.

Lasserre, S. "4 Use Cases for Virtual Reality in the Military and Defense Industry," TechViz, November 2, 2022. https://blog.techviz.net/4-use-cases-for-virtual-reality-in-the-military-and-defense-industry.

Lindsey, S. and Woolf, B. "The New Rules of Security: How AI Will Transform Video Surveillance," *Security*, April 6, 2021. https://www.securitymagazine.com/articles/94961-the-new-rules-of-security-how-ai-will-transform-video-surveillance.

Lister, T. "The March 2021 Palma Attack and the Evolving Jihadi Terror Threat to Mozambique," *CTC Sentinel* 14, no. 4 (2021). https://ctc.usma.edu/the-march-2021-palma-attack-and-the-evolving-jihadi-terror-threat-to-mozambique/.

Military.com. "Clowns Sabotage Nuke Missile," June 23, 2006. https://www.military.com/defensetech/2006/06/23/clowns-sabotage-nuke-missile.

Miller, N. "The Secret Success of Nonproliferation Sanctions," *International Organization* 68, no. 4 (2014): 913–944. https://doi.org/10.1017/S0020818314000216.

Ministry of External Affairs, Government of India. "Nuclear Security in India," 2014. https://mea.gov.in/Images/pdf/Brochure.pdf.

Mizokami, K. "New Engines Will Keep the B-52 Bomber Flying for 100 Years," *Popular Mechanics*, April 30, 2020. https://www.popularmechanics.com/military/aviation/a32320801/b-52-new-engines/.

Monteiro, N. and Debs, A. "The Strategic Logic of Nuclear Proliferation," *International Security* 39, no. 2 (October 2014): 7–51. https://doi.org/10.1162/ISEC_a_00177.

Moore, L. "10 Best Family Tracking Apps for Android and iOS [Both Free & Paid]," Family Orbit. https://www.familyorbit.com/blog/best-family-tracking-apps/.

Narang, V. *Seeking the Bomb: Strategies of Nuclear Proliferation*. Princeton, NJ: Princeton University Press, 2022.

National Museum of the US Air Force. "ICBM 50th Golden Legacy Enduring Deterrence." https://www.nationalmuseum.af.mil/Portals/7/documents/other/af_space_command_icbm50th.pdf.

National Nuclear Security Administration. "Office of Secure Transportation." https://www.energy.gov/nnsa/office-secure-transportation.

National Park Service. "Minuteman Missile National Historic Site South Dakota." https://www.nps.gov/mimi/index.htm.

Nelson, M. "Northrop Books $73M USAF Contract to Update Missile Remote Visual Assessment Tech," ExecutiveBiz, 2020. https://executivebiz.com/2020/12/northrop-books-73m-usaf-contract-to-update-missile-remote-visual-assessment-tech/.

Organisation for the Prohibition of Chemical Weapons. "Fact-Finding Mission." https://www.opcw.org/fact-finding-mission.

"Pakistan Arrests Militant Leader on Terror Financing Charges," Deutsche Welle (DW), February 01, 2021. https://www.dw.com/en/pakistan-arrests-alleged-mumbai-attacks-leader-on-terror-financing-charges/a-56115881.

"Paris Attacks: What Happened on the Night," BBC, 2015. https://www.bbc.com/news/world-europe-34818994.

Peck, M. "The Pentagon Wants to Arm Drones With Non-Lethal Lasers and Microwave Cannon," *Forbes*, March 8, 2021. https://www.forbes.com/sites/michaelpeck/2021/03/08/the-pentagon-wants-to-arm-drones-with-non-lethal-lasers-and-microwave-cannon/?sh=48d7be961727.

"Pratt & Whitney Outlines Vision for Renewing the B-52," *Air & Space Forces Magazine*, August 5, 2021. https://www.airandspaceforces.com/pratt-whitney-outlines-vision-for-renewing-the-b-52/#:~:text=The%20Air%20Force%20has%20set,years%20after%20its%20first%20flight.

Robitzski, D. "The U.S. Army Is Using Virtual Reality Combat to Train Soldiers," Futurism, March 22, 2019. https://futurism.com/army-soldiers-vr-combat-training.

Sagan, S. "Why Do States Build Nuclear Weapons?: Three Models in Search of a Bomb," *International Security* 21, no. 3 (1996): 54–86. https://doi.org/10.2307/2539273.

Sagan, S. and Waltz, K. *The Spread of Nuclear Weapons: An Enduring Debate*. W. W. Norton & Company, 2013.

Schelling, T. *Arms and Influence: With a New Preface and Afterword*. Yale University Press, 2008.

Schelling, T. *The Strategy of Conflict*. Audible Studios, 2018.

Scott, S. "Sticky Foam as a Less-Than-Lethal Technology," Sandia National Laboratory, 1996. https://www.osti.gov/servlets/purl/442050.

Sengupta, Kim. "Nairobi Attack: Who Was the SAS Solider with Pirate Badge Pictured at Scene of Deadly Assault?," *Independent*, January 16, 2019. https://www.independent.co.uk/news/world/africa/nairobi-attack-sas-soldier-terror-pirate-badge-hotel-dusitd2-kenya-al-shabaab-a8730561.html.

Singh, K. "FOREIGN AFFAIRS Pakistan, India, and the Bomb," *The New York* Times, 1979. https://www.nytimes.com/1979/07/01/archives/foreign-affairs-pakistan-india-and-the-bomb.html.

Southworth, S. 1997. *Great Raids in History, Drake to Desert One*. Da Capo Press.

Stars and Stripes. "Spies? Saboteurs? Or Just Tailwatchers?," June 9, 2013. https://www.stripes.com/theaters/asia_pacific/spies-saboteurs-or-just-tailwatchers-1.223835.

Stilwell, B. "How Effective Draftees in the Vietnam War Actually Were," We Are THE MIGHTY, April 29, 2020. https://www.wearethemighty.com/mighty-history/draftees-vietnam-war/.

Taleb, N. 2008. *The Black Swan: The Impact of the Highly Improbable*. Penguin.

Taleb, N. 2012. *Antifragile: How to Live in a World We Don't Understand*. Allen Lane.

Thayer, B. "The Causes of Nuclear Proliferation and the Utility of the Nuclear Non-Proliferation Regime," *Security Studies* 4, no. 3 (March 1995): 463–519. https://doi.org/10.1080/09636419509347592.

The Brookings Institution. 2002. "The Costs of the Manhattan Project." https://www.brookings.edu/the-costs-of-the-manhattan-project/.

The Cornell Lab. "Project FeederWatch." https://feederwatch.org/.

Tickner, A. H. and Poulton, E. C. "Monitoring up to 16 Synthetic Television Pictures Showing a Great Deal of Movement," *Ergonomics* 16, no. 4 (1973): 381–401. https://doi.org/10.1080/00140137308924529

TRIPwire. "Syria: Drown Swarm Attacks Russian Military Bases," January 12, 2018. https://tripwire.dhs.gov/news/209478.

United Nations. "Recommendations on the Transport of Dangerous Goods," June 2017. https://doi.org/10.18356/a122d749-en.

United States Army Special Operations Command. ""Little Green Men": A Primer on Modern Russian Unconventional Warfare, Ukraine 2013–2014," 2022. https://www.jhuapl.edu/sites/default/files/2022-12/ARIS_LittleGreenMen.pdf.

Ward, J. and Sottile, C. "Inside Anduril, the Startup That Is Building AI-Powered Military Technology," NBCNews, October 3, 2019. https://www.nbcnews.com/tech/security/inside-anduril-startup-building-ai-powered-military-technology-n1061771.

"Westgate Attack: Two Jailed Over Kenyan Shopping Mall Attack," BBC, October 20, 2020. https://www.bbc.com/news/world-africa-54748341.

CHAPTER 6

Controlling and Managing Radioactive Sources

N. Ramamoorthy, Christopher Boyd, and Anne L. Willey

6.1 An Indian Perspective[1]

N. Ramamoorthy

This chapter deals with the Indian policy, practices, and experiences in managing and controlling radioactive sources. The second section details the processes in place to control and secure radioactive sources in major areas of their applications. The section also examines the human element and legacy issues and related incidents and lessons. The third section

[1] This article is based on the career experience of the author as the Head of the radioisotope and radiation technology programme concurrently at both BARC (as Associate Director) and BRIT (as Chief Executive), India during August 2000–September 2003,

N. Ramamoorthy
National Institute of Advanced Studies (NIAS), Bangalore, India

C. Boyd (✉)
MARC Strategic Solutions, Ann Arbor, MI, USA
e-mail: chris.boyd@marcstrategics.com

A. L. Willey
United States Air Force, Washington, DC, USA

S. P. Kapur et al. (eds.), *The Challenges of Nuclear Security*, Initiatives in Strategic Studies: Issues and Policies,
https://doi.org/10.1007/978-3-031-56814-5_6

outlines the production of RI-based sources and operation of radiation technology facilities and services. The fourth section looks at the IAEA support and contributions with regard to safety and security of radioactive sources. The fifth section looks at the interface between safety and security of these sources while the sixth section suggests measures to strengthen the control of the use of radioactive sources and ways to foster alternative technologies. The final section looks at the continuing challenges and the way forward with a few recommendations.

6.1.1 Introduction

The field of ionising radiation, in terms of technologies and their multiple applications, has continuously evolved over time and is well-recognised worldwide for delivering numerous societal benefits. In particular, the benefits accruing to industries and healthcare are invaluable. As a result, radiation technology and its utilisation are now spread across the world, including in developing countries and in small and large nations. The IAEA, as the global forum for all matters nuclear, has an extremely important role in supporting the interested Member States (MS) in the adoption of radiation technologies, capacity building, and fostering safety and security in all practices involving the use of ionising radiation, along with appropriate regulations. The IAEA's Ministerial Conference on "Nuclear Science and Technology: Addressing Current and Emerging Development Challenges" held in November 2018, was a large event, with over 160 Member States of IAEA, 54 Ministers, and about 1100 national delegates in attendance. The Ministerial Declaration succinctly portrays the status and trends in the field.[2] Among the various practices in vogue, the use of high-intensity, high-risk radioactive sources—made of radioisotopes (RI) such as ^{60}Co, ^{137}Cs, among others—has been attracting increasing global attention for the past 20 years—especially after the 9/11 terrorist attack in USA in 2001. Consequently, several

and subsequently at the IAEA (as Director of NAPC) during October 2003–March 2011, as well as his current role as the Chairman of the Apex Advisory Committee called SARCAR (Safety Review Committee for Applications of Radiation) of AERB, India, from June 2016 onwards. All the views expressed in the article are personal, professional ones of the author and not necessarily those of the organisations shown above as author's past and current affiliation.

[2] https://www.iaea.org/sites/default/files/18/11/ministerial-declaration-281118.pdf and https://www.iaea.org/sites/default/files/18/11/cn-262-conference-summary.pdf.

national leaders have repeatedly called for strengthened nuclear security measures and cooperation, most notably in the Nuclear Security Summit biennial events held from 2010 to 2016. The appeal includes efforts concerning high-intensity radioactive sources cited above. It is against this backdrop that the current article on "Controlling and managing radioactive sources" is presented describing the status of the field, the Indian experience, and the global scenario based on IAEA documents and events, as well as the challenges to be addressed and certain options and recommendations for the path forward.

There has been consistent interest in exploring and deploying the beneficial uses of radioactive materials. The use was initially confined to natural sources and has subsequently been based on the vast range of radioisotopes (RI), which could be produced in nuclear reactors and charged-particle accelerators. The ensuing applications based on ionising radiation are well established in industry, healthcare, food and agriculture and research (Ramamoorthy WNU 2019; Gopinath and Ramamoorthy 2020). They are not only harnessed by industrialised countries, but in almost all parts of the world, be it small or large nations, developing countries or low- and middle-income countries (LMICs).

The source of radiation in most of these cases has been radioisotopes (Table 6.1), e.g., ^{60}Co, ^{137}Cs, ^{192}Ir, coming under the class of radioactive (sealed) sources. The production of the RI-based sources and equipment containing RI has been confined to a limited number of countries at national centres and in private industry. Their deployment, however, has been very extensive, across the world and to a large extent in the public domain at hospitals, industrial sites, academic centres, and research labs. For example, RI-based sources of ^{192}Ir and ^{60}Co (high-intensity, sealed sources, and devices) are used for industrial applications such as radiography cameras and gamma radiation processing plants as well as for healthcare applications like radiotherapy for cancer patients (Ramamoorthy 2019, 1–12). Thus, movements of RI-containing packages/cargo are routine exercises throughout the year, with some being more frequent than others based on the half-life of RI involved and the need for source replacement or replenishment.

In order to leverage alternative sources of radiation in certain types of applications, such as those requiring very high or very low dose rates, electron accelerators and X-ray systems have been developed. Many such systems are in regular use apart from the use of RI-based sources (Chmielewski and Haji-Saeid 2019, 37–44, Fidarova and Erbas 2019,

Table 6.1 Major types of RI source-based equipment and volume of use

RI source and activity	*Equipment*	*Main uses*	*Indian scenario*	*Global scenario*
^{192}Ir, 74d, 0.7–3.7 TBq (20–100 Ci)	Radiography exposure device	Gamma radiography as part of NDT/NDE	>2000 units	Tens of thousands
^{60}Co, 5.27 y, up to 11.1 TBq (300 Ci)	Radiography exposure device	Gamma radiography as part of NDT/NDE	50+ units	Several hundreds
^{60}Co, 5.27 y, 3.7–185 PBq (0.1–5 MCi)	Source racks of gamma radiation plants	Sterilisation of medical products; disinfestation of spices; hygienisation/preservation of food/agro products	20+ plants	About 250 plants
^{60}Co, 5.27 y, 444 TBq (12 kCi)	Tele-cobalt therapy units	Radiation therapy for cancer patients	<200 units	Several hundreds
^{192}Ir, 74d, 370–555 GBq (10–15 Ci)	Brachytherapy system HDR	Radiation therapy for cancer patients (mostly female patients)	>300 systems	Several hundreds
^{60}Co, 5.27 y, 74 GBq (2 Ci)			Very few	Limited numbers
^{60}Co, 5.27 y, 30 TBq (0.8 kCi)	Blood irradiator	For safe blood transfusion to immuno-compromised patients	About 40	Limited numbers
^{137}Cs, 30y, 111 TBq (3 kCi)			About 20	A few hundreds

(continued)

Table 6.1 (continued)

RI source and activity	*Equipment*	*Main uses*	*Indian scenario*	*Global scenario*
^{60}Co, 5.27 y, 37–518 TBq (1–14 kCi)	Laboratory irradiators—gamma cells	For crop mutants, process development—validation, dosimetry services, R&D, etc	>25	A few hundreds
^{137}Cs, 30y, 111 TBq (3 kCi)			Very few	Limited numbers

63–70). This has generally remained confined to the more industrialised nations.

The safety and security of radioactive sources has been a subject of high importance to stakeholders and national authorities (IAEA 2004, 1–16; Ranajit Kumar 2013; Upreti 2013, 146–149). The 9/11 events in the USA became a wake-up call to all countries. It forced the world to identify and analyse vulnerable areas, potential threats, and any possible risk to society. The widespread use of high-intensity radioactive sources has been naturally recognised as a crucial area of risk in this context. The large programme involving the use of RI sources has to ensure the availability of their benefits to society while protecting them from terrorists and criminals, who could use them to endanger public life, property, and the environment.[3] In this context, this chapter tries to capture the various facets of applications and vulnerabilities, the importance of addressing the security of radioactive materials, effectively controlling and managing the use of RI sources, and measures for possible paths forward. This manuscript was prepared prior to the launch of U.S. National Academy

[3] It is pertinent to point out that well over a century ago Pierre Curie cited the danger due to potential abuse of radioactive materials in his Nobel Lecture (delivered on June 6, 1905) entitled 'Radioactive substances, especially radium'; he says in the last part of his talk: "*It can even be thought that radium could become very dangerous in criminal hands, and …*", https://www.nobelprize.org/uploads/2018/06/pierre-curie-lecture.pdf.

publication on Radioactive Sources (NAS 2021), an important reference on this subject (see Sect. 7.1).

6.1.2 *Control and Security of Radioactive Sources in Major Areas of Their Applications*

Three unique features of radioisotopes make them extremely valuable, predominantly for industry and healthcare (Gopinath and Ramamoorthy 2020). The first, popularly referred to as radiotracer principle, is based on open-source RI samples, mostly in liquid or solid form, and of low to medium level of radioactivity. These may not come under the high-risk category, unlike the other two areas where high-risk RI sources are commonplace (the categorisation of RI sources is covered later in this chapter). RI can use tracers to follow the movement of materials of interest with respect to time and space in both living and non-living systems, using the very high sensitivity for detection of RI radiation. This makes them one of the most powerful probes for non-invasive examination, often including imaging, in medicine, industrial processes and systems, civil structural integrity, biology, agriculture, drug development research, etc. Transmission and attenuation of radiation while penetrating through matter will reveal the inner details of the interposed objects depending upon their density, mass, atomic number, etc. This is the basic principle of all radiography procedures, whether it is in a medical or industrial area, or of civil construction and structures. Nucleonic gauges used in industries also fall in this category. The ability to deposit radiation energy (low-dose to high-dose) at the desired location inside exposed matter helps to bring about physical, chemical, and biological changes of the materials exposed to radiation. This enables applications ranging from cancer treatment to sterilisation of medical products, to disinfestation or hygienisation of food products, to manufacturing advanced materials (polymers, composites, cable insulation, etc.), to mitigation of certain pollutants.

A few specific areas of large-scale deployment of RI sources are discussed in the following sub-sections, keeping in mind practice-specific vulnerabilities.

6.1.2.1 *Industrial Gamma Radiography (IR) Sources and Practices*

The RI sealed sources of high-intensity ^{192}Ir 740 - 3700 GBq (20–100 Ci) and ^{60}Co up to about 11 TBq (300 Ci) are used in gamma radiography exposure devices, popularly known as radiography cameras. Industrial radiography (IR), as a key element of non-destructive testing/examination (NDT/NDE), is a vital feature of regular operations in several industries such as aviation, steel, oil and gas, and chemical large civil constructions such as bridges, dams, and many cases of establishing infrastructure (Venkatraman and Menaka 2020, 106–130). By the very nature of IR's utility, the procedures are often carried out in open areas. Furthermore, devices with radioactive sources must repeatedly be transported from one site to another, often at very short notice. There is also stiff competition amongst IR service providers to secure orders, make maximum utility of each source/device, and perform radiography and deliver results as and when demanded by the contract-awarding party (CAP).

Advanced RF-based tracking of sources and devices, which has recently emerged in the IR sector, is an important step towards ensuring additional control over them (IAEA CN269 December 2018). The application of sealed-source techniques for trouble-shooting industrial processes and systems, such as gamma-column scanning in petrochemical plants and refineries, is popular in many countries including India (Jung 2019, 52–59; Pant 2020, 210–249). The source strength in some of these cases can be high (tens of GBq, a few Ci ^{60}Co), coming under Cat. 2 and can warrant measures similar to those applicable for IR devices/sources.

Another challenge is retaining qualified manpower. Well-qualified operators tend to move to greener pastures for better wages and benefits. This increases the challenge of ensuring operational safety as well as security of sources.

The number of RI sources and devices globally in use runs into tens of thousands, with over 2000 in India alone (Table 6.1). This creates a serious danger of theft and sabotage, though the source strength involved in IR devices is much lower than in the case of gamma radiation plants (PBq level, 0.1–5 MCi) and tele-cobalt units (tens of TBq, 10–12 kCi) (Ramamoorthy, IAEA conf 2018; Ramamoorthy, IAEA conf 2019). The latter two have a much higher degree of physical protection measures in place, being located within a specific campus, apart from other inherent system strengths.

6.1.2.2 Irradiator Plants (Gamma Radiation Plants)

There are over 250 gamma radiation plants in the world (www.iiaglobal.com; iiA brochure 2020; iiA white paper 2020; IAEA Directory 2004) and the number in India is over 20. The total installed strength of ^{60}Co in radiation plants in the world is about 500 MCi, while the actual physical loading can conservatively be taken as 40% at any given time. In India, there are over 20 gamma radiation-based processing units (20–110 PBq level, 0.5–3 MCi capacity) set up and operating in the private sector, in most cases handling both food and medical products. Another seven are under construction.[4]

Most of the gamma radiation processing plants are operated with quality-standard certifications issued by an accredited entity. These certifications attest to the plants' compliance with well-established SOPs. They also indicate that the facilities have met source-security-related requirements against both theft and sabotage.

Despite these precautions, threats from malicious actors cannot be ruled out. Materials may be vulnerable to theft or tampering during transport. Such tampering could include the introduction of explosives into the shipment, resulting in damage to facilities. Because plant design and operation involves heavy shielding, any damage is likely to be contained. Nonetheless, malicious actors can cause damage.

Gamma radiation plants must undertake periodic source replenishment operations. For this purpose, large, heavy casks containing fresh-source pencils of high intensity are transported to and then handled within the premises. Spent sources may also be loaded into the same container and returned to the vendor, with adequate attention given to the security and safety of sources during transport (Nandakumar 2013, 131–134). Most of these operations with source pencils take place in the shielding water pool housing the source racks and are handled by experienced, qualified, and certified staff. Also, professional support is available from the vendor providing the sources, the personnel that provide regulatory oversight, and the radiation protection officers.

Though information on replenishment operations is not public, it could leak to malicious actors. They can target such operations, particularly through commando-type attacks, which can damage a facility and frighten the public. Sensitive information must therefore be shared

[4] See www.britatom.gov.in.

between stakeholders, the operator-licensee and their staff, the vendor, and the regulator on a strictly "need-to-know" basis.

6.1.2.3 Radiotherapy: RI Sources and Systems for Cancer Care

In the area of healthcare applications, radiotherapy facility housing ^{60}Co sources and brachytherapy sources, mostly ^{192}Ir and also ^{60}Co, is commonplace in medical centres or hospitals for treatment of cancer patients (Table 6.1) (Fidarova and Erbas 2019, 61–70). Blood irradiator units containing ^{137}CsCl (74–111 TBq, 2–3 kCi) or ^{60}Co (30–37 TBq, 0.8–1 kCi) are deployed in many hospitals and blood banks (Table 6.1) for low-dose radiation (25–35 Gy) inactivation of T-lymphocytes in blood samples meant for transfusion to immuno-compromised patients. Almost all of these facilities are located in specific campuses, where physical protection, access control, and personnel reliability assessment are operative, reducing the scope for theft and sabotage of sources and equipment.

There has been greater concern over ^{137}CsCl source among national authorities and academic experts. This is due to its dispersible nature, and the 30-year half-life and 0.66 MeV gamma emission of ^{137}Cs. This creates the potential for heavy, large-scale contamination in the event of sabotage to systems containing ^{137}CsCl source.

Also, medical centers and hospitals, containing large numbers of people and lacking robust security, are attractive targets for malicious actors. Miscreants can potentially make a large impact and intimidate the public by attacking these types of sites. However, the design features of telecobalt units and BI units in these facilities include heavy shielding *cum* storage casks, which may withstand the impact of explosions triggered by attackers.

6.1.2.4 Other Areas of RI Source Applications

Laboratory Research Irradiators, called gamma chambers or gamma cells (GC), contain ^{60}Co source and have an irradiation chamber volume of a few litres' capacity. They have played a central role in supporting radiation research studies focusing on food preservation, phytosanitary support for trade or shelf-life extension, polymer and composite development, treating seeds for preparing crop mutants, and sterilisation of male insects. In the past, such units housing ^{137}CsCl sources were also in use. In India, BRIT/DAE has since the 1990s developed and supplied gamma

chambers to facilitate and catalyse radiation science R&D and allied applications. Low-dose rate gamma chamber units of ^{60}Co have also been supplied and used.

The utilisation of most of these units is in R&D and academic centres. Thus, access to these types of units is more easily controlled. Research interests may change with time, however, and scientists may move to different locations. The possibility of radiation equipment like gamma cells being abandoned therefore cannot be ruled out, notwithstanding the regulations that should preclude this. The Mayapuri incident in India, involving abandonment of an old GC unit belonging to Delhi University, illustrates this danger, as well as the challenges that authorities face in tackling such situations and striving for mitigation measures (Kumar et al. 2015, 517–528; IAEA 2015).

6.1.2.5 Human Element/Factor-Related Aspects

The human element—in particular the problem of human reliability—is an essential aspect of the safety and security-related efforts discussed above (Ramamoorthy, NIAS 2021; Ramamoorthy 2022). Insider threats can result in theft or sabotage of radioactive sources. A number of measures can address such insider threats and related risks. A human reliability assessment programme, consistent with the potential risk level due to the nature of RI sources, equipment, and plant, needs to be adopted by the employers and licensees acquiring Cat.1 and 2 sources. This may include formal vetting procedures for staff induction, training, periodic reviews, medical examination including psychometric tests, counselling, and mentoring of key staff. Further, crucial high-risk operations, such as ^{60}Co source loading or replenishment in irradiator plants, should be undertaken only after additional checks have been conducted on the team undertaking such operations. In addition, sensitive information related to high-risk sources regarding operations, storage, access control, and transport should be shared on a strictly "need-to-know" basis. Instituting appropriate protective measures towards ensuring information security is imperative to the management of radioactive sources.

6.1.2.6 'Legacy Source'-Related Events and Lessons

The regulatory systems of many countries have evolved and matured over time, but in light of the rather long half-life of many RI, e.g., 30 years for ^{137}Cs (in gamma cells), 432 years of ^{241}Am (in neutron source), as well as RI-based nucleonic gauges received with industrial machinery, legacy

sources and equipment are present in many countries. While still in the early stages, a few applications involving radiation—mostly in medical and academic centres—have been established, preceding the formal regulatory system coming into vogue. The regulatory authority, or its delegated entity, has strived to map the legacy sources and equipment and to minimise the possibility of unregistered RI sources. However, this has not been an easy task. Incidents involving orphan and legacy sources have taken place.

Efforts to create a foolproof inventory of all high-risk (Cat. 1 and Cat. 2) RI sources assume great importance in this context. A comprehensive inventory scheme is essential for proper control and management of RI sources. Any sudden occurrence involving a newly recognised orphan source challenges the validity of the RI source inventory claims.

Cooperation and mutual support among all stakeholders will be crucial to efforts to track and inventory radiological materials, especially in regions experiencing instability due to conflict or the dissolution of states. The 2001 radiological accident involving orphaned sources in Lia, Georgia, is a case in point. In particular, help is needed to better control, track, and inventory unaccounted sources in conflict-ridden countries or regions; for example, the 2001 Georgia case (IAEA 2014) and the Mayapuri incident mentioned in the preceding sub-section. The technological tools adopted and experience gained in managing events like the one in Georgia have become useful additions to emergency preparedness in affected countries and around the world (IAEA 2014, 2015).

6.1.3 *Production of RI-Based Sources and Operation of Radiation Technology Facilities/Services—Indian Experiences with Control of Sources*

In India, Cobalt-60 is produced in large quantities (over 75 PBq level (2+ MCi) per annum) using some of the PHWR-type NPPs of NPCIL. Cobalt adjuster rods are used in place of the conventional SS adjuster rods enabling ^{60}Co production during NPP operation for power generation. A BRIT/DAE recovery *cum* processing facility, called RAPPCOF, is located in Rawatbhata. DAE/BRIT is one of the very few entities in the world that has large-scale ^{60}Co production and supply capacity as well as associated technology capabilities (www.britatom.gov.in).

BRIT/DAE has also established indigenously designed and constructed irradiator plants,[5] leveraging its very early entry (1974) into gamma radiation processing.[6] As cited in Sect. 3.2, there are over 20 gamma radiation-based processing units set up with DAE-provided technology and operating in the private sector, in most cases handling both food and medical products. BRIT/DAE expects to make available lifetime supplies of ^{60}Co indigenous sources for all these plants.

Bhabha Atomic Research Centre and BRIT have unique access to certain fission-product RI, which can be recovered only from the reprocessing stream of back-end fuel cycle operations. Exploratory efforts have delivered Cesium-137 (^{137}Cs) in vitrified form as a sealed source, for use in place of ^{60}Co in radiation equipment such as blood irradiators and low-dose laboratory research irradiators. BARC-developed vitrified ^{137}Cs source containing BI units also has been developed in the past few years (Patil et al. 2015, 55–63). The use of ^{137}Cs (30 y) obviates the need for source replenishment, which is required in the case of ^{60}Co-based BI units. Development of vitrified ^{137}Cs source provides technology superiority to ^{137}CsCl, which is vulnerable to sabotage due to its high solubility and dispersibility. It is, however, unlikely that such vitrified ^{137}Cs sources can find use in other applications such as radiation processing plants. This is due to the relatively larger dimensions of vitrified ^{137}Cs source pencils, lower penetration of 0.662 MeV gamma radiation (cf. 1.17 and 1.33 MeV of ^{60}Co), low density of radioactivity content, and likely non-homogeneity of radioactivity in the source matrix. In other words, the use of vitrified ^{137}Cs source will remain confined to low-dose-rate applications.

India's national regulatory authority, the Atomic Energy Regulatory Board (AERB), has instituted a number of steps toward enforcing regulatory oversight functions related to radiation facilities and their applications, in line with experience gained over time and stakeholder

[5] High-dose plant for disinfestation of spices (37 PBq (1 MCi) ^{60}Co, 2000, Vashi near Mumbai) and low-dose plant for preservation of onions, fruits (11 PBq (300 kCi) ^{60}Co, 2001, Lasalgaon, Maharashtra)—pool-type storage of ^{60}Co source racks.

[6] BARC set up in 1974 a 1 MCi ^{60}Co dry-storage type radiation processing plant (UNDP supported project) called ISOMED. This gave a boost to Indian pharma companies and medical devices manufacturers as well as led to launch of similar plants in the private sector for medical products sterilization. The plant (under BRIT management since 1989) provided services for 45 years, before being shut down for major renovation and upgrades.

feedback. The web-based e-LORA (e-Licensing of Radiation Applications) system has helped to enable registration, intimations, applications, approvals, accountability, and tracking.[7] An annual interactive event, the National Conference of Regulatory Interface (NCRI) is another process to encourage frank feedback, disseminate lessons and experience gained, and suggest possible strengthening measures to consider. This has helped to inculcate a safety and security culture among stakeholders using RI sources, contract-awarding parties, and higher management teams in institutions where the radiation equipment may be a small part of a department or laboratory.

The expertise and infrastructure required for nuclear and radiological emergency preparedness and response (EPR), built up by DAE over time (Pradeepkumar 2013, 138–145; Murali 2020, 1–5), enables mandated authorities to manage any exigencies involving radioactive sources (especially Cat. 1 and 2 type). A Crisis Management Group (CMG; https://dae.gov.in/writereaddata/CMG_contact.pdf), comprising high-level professionals and senior management and with linkage to government officials of the region, is also in place at the DAE headquarters in Mumbai. There are 25 Emergency Response Centres (ERC), set up in different parts of the country, well equipped to support field operations. The various units of DAE spread across the country can further augment the resources of ERCs to support EPR-related activities as required.

Training events and exercises, involving personnel beyond the nuclear/radiological domain, are carried out regularly. The Global Centre for Nuclear Energy Partnership[8] (GCNEP), located at Bahadurgarh, near New Delhi, has been functioning for over a decade and runs several training events both on and off campus. GCNEP schools dealing with Nuclear Security Studies and Radiological Safety Studies support the management and control of radioactive sources and offer necessary training and familiarisation to the various stakeholders. GCNEP is also helping to build expertise in nuclear forensics for managing EPR situations (Murali et al. 2014, 178–189).

[7] See www.aerb.gov.in.

[8] This Centre was set up in line with the then Indian PM's declaration at the Nuclear Security Summit of 2010. Initially, activities and events of GCNEP were held in off-campus locations. GCNEP has several cooperation agreements in place, including with national entities (e.g., USA) and the IAEA. http://www.gcnep.gov.in/index.html.

Radioactive sources from old or abandoned academic, medical, or industrial equipment have in some cases required extensive DAE support for safe disposal or suitable storage. With the concurrence of the Government of India, the experts in units like BRIT and BARC have undertaken to provide it. Such cases needing national-level support for managing the end-of-life-time RI sources or equipment are common in other countries too.

Entities handling large-scale scrap metal waste, including from foreign sources, pose another concern. At times, radioactive metal has been found in such waste. Lessons learnt from specific instances have prompted the establishment of radiation monitoring in key locations of large scrap yards. In this context, an apparent irony is evident. Invariably, there is monitoring of incoming goods for potential radioactive contamination by the ports in any country. However, there is little monitoring of outgoing cargo at most ports. This issue remains to be effectively addressed. Failure to control radioactive sources at the originating point is the main cause of radioactive waste contaminating traded scrap materials.

6.1.4 Strengthening Measures to Control the Use of Radioactive Sources and to Foster Alternative Technologies

Increasing concerns about the security of nuclear and other radioactive materials have led to calls for additional protection and control measures, especially while dealing with high-activity sources of Category 1 and Category 2. In this context, the utility of exploring and adopting alternatives to the use of radioactive sources needs to be highlighted. It is commendable that efforts and interest continue to grow regarding benefits of applications of ionising radiation, while fostering avoidance of RI-based sources to the maximum extent possible. This strategy can play a vital role in minimising the use of radioactive sources (especially of Category 1 and Category 2) and in increasing their security. Accordingly, international cooperative initiatives and investment of resources under different forums, including the IAEA and WINS, are noteworthy (IAEA December 2018, WINS December 2020). Advocacy of adopting non-RI sources, such as X-rays and electron accelerators, has grown over the past 10–12 years, as alternative options have emerged in important cases, such as external beam radiotherapy for cancer. It may however take time to become mature in some other cases, such as X-ray-based systems for field applications of industrial radiography. Furthermore, alternatives may not

be readily feasible for applications such as brachytherapy. More detailed discussion on alternative technologies for specific cases of applications will follow below.

6.1.4.1 Alternative Technologies to the Use of Radioactive Sources—Existing, Emerging, and Under-Development Options

It is important to distinguish between adopting "existing alternative technologies to RI use" and entirely "newly developed, i.e., emerging, alternatives," or "alternative technologies being developed" to RI use. This is further elaborated in the next sub-sections. An Expert Group Study organised by the U.S. National Academy (NAS 2021) has also identified the areas to be addressed in offering alternative technologies. The summary of the report lists 15 findings and 9 specific recommendations showing the status of alternative technologies and further efforts needed to make them more amenable for adoption. A brief quote from the synopsis of the report encapsulates the key message: "The committee found that alternative technologies do not provide a "one-size-fits-all solution." This is particularly evident in medical applications across high- and low- and middle-income countries, because of the stark disparities in access to health care and resources."

6.1.4.2 Medical Application Sources

There are a few non-RI technology options available as sources of ionising radiation for applications in medicine and industry, with some proven to be superior. For example, in cancer treatment, Linac-based radiotherapy systems have been widely used and possess distinct efficacy and safety advantages over systems using ^{60}Co sources, popularly known as "tele-cobalt" machines (IAEA and WHO 2021). However, Linac systems require continuous high-quality electric power supply, without fluctuations in voltage and frequency. This has posed a challenge for many developing nations, LMICs, and non-urban areas of some other countries.

Concerted efforts are hence needed to promote development of low-cost, basic-standard, highly rugged Linac EBRT systems—e.g., 6 & 10 MV—for wider adoption and sustainable use in all countries and regions. The point to highlight is that the reluctance to move away from the RI ^{60}Co source can be addressed, reiterating the benefits of alternative technologies accruing to both the patients and the country's healthcare system. The issue to address should be one of the "rugged, basic-standard

Linac EBRT systems for routine use" needed in large numbers by numerous countries versus "advanced, expensive Linac systems," which would be of interest to high-end medical institutions and the promoting industries.[9] The relevant issue is not "Linac versus tele-cobalt" systems.[10]

This strategy also requires mobilising adequate financial resources, as well as technical and logistical support, to dispose of spent sources of ^{60}Co of the tele-cobalt machines (or of ^{137}Cs) previously used in many centres. Campaign mode efforts over the next 2–3 years and global cooperation initiatives can help to make this goal reachable.

6.1.4.3 Industrial Application and Research Sources

In the area of industrial radiation processing applications, ^{60}Co-based gamma plants and electron Linacs have their own niche areas of application. In general, radiation processing involving continuous operation is better performed using gamma plants, while cases requiring very high-dose rate exposure or different depths of penetration are more suited to EB treatment. There are also certain areas where both can be deployed and this is where the advocacy for adoption of Linac alternative comes into the picture. In the latter case, ^{60}Co-based gamma plants continue to hold practical advantages in terms of ease and simplicity of operations, 24 X 7, about 330–350 days per year. This is essential for end-users in medical fields and the food industry. Here, the need for alternative technology involving electron Linacs, popularly called EB systems, warrants further development efforts to offer ease and economy to end-user industry and service providers. Currently, the techno-economic viability of adopting EB technology for all established applications of radiation processing remains another point of concern. The existing gamma plants,

[9] The medical equipment industry is known for making continuous (at times rapidly changing) advances in technologies and sophistication of systems. While this is understandable and even welcome, empathetic consideration is warranted from the point of view of decision-makers, hospital management, resource providers, etc. Advanced features invariably come with a price tag and the desire to avail the best of the options is strong among medical professionals. A balance is imperative and hence the advocacy of basic-standard EBRT system for large-scale deployment in practically every country in the world. Advanced systems can be more appropriate for high-end care providers like tertiary care referral centres.

[10] Why not seek to launch a system (under the auspices of a global sponsor of societal contribution) to be named after the former DG of the IAEA, (Late) Mr Yukiya Amano, who pioneered the IAEA efforts to expand and enhance its programmes on supporting cancer care deliverables to patients.

i.e., ^{60}Co plants, have up to 500 MCi of sources and these plants have more than a few decades of useful life ahead (iiA brochure 2020; iiA white paper 2020; IAEA CN269 2018). Hence a long-term strategy will be needed in this case.

Non-radioisotope technologies have also been developed in recent years to offer an alternative to the use of RI. Support for technology development and simplification and strengthening of X-ray-based systems would encourage its acceptance. End-users, including medical centres, researchers, academia, and national nuclear centres, can be relatively easily convinced of the alternatives' merits but they may need some support to avoid use of RI sources. One can also cite the need for portable X-ray-based industrial radiography (IR) devices for field applications of IR in this context. Fostering alternatives to RI in this case will involve persuading a highly-competitive, stressed service industry of the alternatives' advantages. A two-pronged approach to engage end-users is needed here. The practical logistics issues in open-field conditions, such as availability of the required electric power supply for IR practices, will be a considerable challenge in most developing countries and many other nations.

6.1.4.4 Envisaged Areas of Continuity in RI Source Applications

The final group of applications is the case where no viable alternative to RI exists or can be offered. The most important case is brachytherapy (BT) for treatment of certain cancers. This is a crucial wing of radiotherapy of cancer patients, especially cancers in women. The concept of electronic BT, or contact X-ray BT, continues to remain primarily in the realm of research, with limited demonstrations. High-dose-rate (>12 Gy/h) ^{192}Ir sources are mostly used in BT systems, which need replacement once every 2–3 months and involve periodic shipments (Table 6.1). The option to use ^{60}Co in place of ^{192}Ir may help avoid frequent replacement of sources, but may not be applicable or desirable for all BT applications and in all groups of patients, due to the penetrating nature of ^{60}Co radiation. For brachytherapy requirements of cancer treatment, RI-based systems are essential and it is not currently possible to replace them with machine sources of radiation. Such use should continue as a needs-based exception, while advocating the use of alternative technologies. Well-established security mechanisms for the radioactive sources should be employed by the end-users, with compliance overseen by the national regulators.

6.1.5 *Control of Radioactive Sources—Continuing Challenges and Path Forward*

This paper has described the wide use of radioactive sources for vital applications, practice-specific vulnerabilities posing dangers of various magnitude, lessons learnt from events involving radioactive sources, as well as other technology options available for certain applications. Discouraging the use of radioactive sources wherever alternatives are available will be the logical first option. Techno-economic and logistical issues create barriers to this approach, however, and its feasibility varies across issue areas (Ramamoorthy WNU 2019; IAEA—WHO 2021).

In the case of medical applications, alternatives to radioactive sources should be vigorously pursued, highlighting the advantages to patients. Financial support can be secured from large international and philanthropic sources. In the case of industrial applications, by contrast, practical operational challenges are much more severe. The operators in this group are private entities with significant resource constraints; they cannot receive government support. Industry could seek to transition during a longer period, adopting alternatives such as electron accelerators over time. Support for advances in this technology, such as enhancing ruggedness for 24/7 operation, increasing electric power efficiency, and improving reliability of components and sub-systems, will have to go hand in hand. Securing the buy-in of all concerned industrial stakeholders will be essential for sustainable enforcement of controls and security measures in the above-mentioned applications.

Industrial radiography has thousands of operators across multiple regions. This issue is compounded by the relatively low capital investment required to set up a new IR service entity. As earlier discussed, the IR group is the most vulnerable for exploitation by malicious actors (notwithstanding the relatively lower extent of potential harm and panic). Increased use of machine-based IR systems for industrial specimen inspections, except when required to be done in open-field conditions, can help considerably reduce the volume of IR devices and sources in use in the public domain.

The fact that IR service delivery is based on relatively low capital investment has increased the number of players in the field, which in turn has created a high degree of competition. Requiring a substantial deposit from licensees could help to mitigate these problems. IR licensees should also have adequate provisions of their own for secure storage

of their devices and sources at all times. Heavy penalties for violations like non-compliance with transport-related requirements for source safety and security could be helpful. Although national laws and practices may impede their implementation, these measures are worth considering in the interest of safety and security.

In the case of high-risk radioactive sources in research and academic centres, appropriate dissemination of risk-related information and inclusive management practices can help ensure that RI sources are not lost over time, when research priorities change or faculty moves to other locations. Similar techniques can be used in the case of large private entities using nucleonic gauges in their industrial processes. One can also target specific areas where large volumes of such gauges are in use and explore options to deploy X-ray-based gauging systems. Appealing to industry leaders and management to adopt this as part of their "responsible corporate practices" could be a worthwhile endeavour.[11]

6.1.6 Recommendations

This chapter concludes with two sets of recommendations to improve security around the challenges identified herein. First, it is possible and necessary to move away from using RI sources for external beam radiotherapy (EBRT) of cancer patients. This can be achieved by concerted efforts to build consensus around a standard, simple system for basic routine EBRT. Such efforts would seek large-scale deployment, including in locations with resource constraints of infrastructure, as well as to facilitate all aspects of transition from the old tele-cobalt machines. The partnership of industry is crucial in this context. Further, harnessing synergies among relevant entities, such as cancer care professionals and healthcare authorities, Linac system industries, professional entities like IARC, and inter-governmental organisations like IAEA & WHO, along with the support from international initiatives to strengthen nuclear security, will be required. Global philanthropic aid available for healthcare can be leveraged for this purpose. A time-bound action plan (2–3 years)

[11] While on the topic of appealing to the industries for showing objective, broad-minded perspective, simultaneously appealing for avoidance of certain undesirable practices is necessary. It is seen that advocacy to consider non-RI technology options has been conveniently (mis)quoted by some vested interests to promote one equipment or system over the other. This shows the involved industry in poor light and needs to be discouraged. As responsible leaders in industry, they should be urged to be sensitive to the topic of RI source-based applications and strengthening controls and security measures.

and implementation mechanism should be attempted, with the lead entity being determined through consensus among key stakeholders.

The second set of recommendations is related to the inevitable requirement of RI sources for certain vital applications, and the possibility of fostering adoption of alternative technologies to RI use for other applications wherever possible.[12] A transparent stakeholder process should clearly identify cases where alternatives to RI use are not feasible. Simultaneously strengthening the radioactive sources in these systems against theft and sabotage through design, shielded housing, tracking, physical protection, etc.), against theft and sabotage, should be given priority.

Another potential strategy would be supporting the deployment of rugged alternative technologies in place of equipment such as blood irradiators, research irradiators, and radiography devices containing RI sources. This would enable end-users to consider transition to non-RI-based options for applications wherever possible. The question of how to make such a transition adequately attractive for the licensee or employer delivering radiation-based services has to be addressed. Persuading industry to demonstrate the utility and reliability of offer alternative equipment and systems at IAEA labs in Seibersdorf can be an option.

The duration for these pursuits will be much longer than in the case of medical Linacs; a timeline of 5 years may be worth considering as a target. Bringing together all relevant stakeholders may pose challenges, due to commercial interests, and concerns regarding the techno-economic viability of new options. Nonetheless, it would be worthwhile to strive for a paradigm shift.

6.2 A U.S. Perspective

Christopher Boyd and Anne L. Willey

Christopher Boyd, Anne L. Willey

In the 20 years that have transpired since the terrorist attacks on September 11, 2001, there has been a growing awareness of the potential for the pernicious use of sealed sources—radioactive materials meant

[12] Seeking to switch over to EB machines in place of gamma radiation plants for every application—be it in medical or agro-food area, e.g., for sterilisation, food preservation—could be the toughest to achieve. It may take a long time to make significant progress in this case due to the large investments done by industry in several countries.

to be kept permanently sealed in a capsule or bonded and in solid form (IAEA). These materials emit excess energy (radiation); one of the forms this energy takes, gamma rays, is often used for life-saving treatments and critical infrastructure applications. However, if these sealed sources fall into the wrong hands, they can be deployed as weapons and cause serious harm. Concerns over the use of sealed sources in the making of radiological dispersal devices (RDDs), also known as "dirty bombs," have led to a re-evaluation of approaches to radiation security, especially regarding soft targets such as healthcare organizations, commercial and federal operations, and institutions of higher learning.

For the last 20 years, regulatory bodies at national, regional, and international levels have developed far-reaching policies and procedures to mitigate security risks associated with sealed sources. Enhancing security measures, while sometimes effective in reducing opportunities for malicious use, requires a permanent commitment to managing risk. A fundamental problem with this risk management approach is that it is very resource-intensive—not only in economic terms, but also in terms of technology, human power, and political capital. Risk management requires, at a minimum, continued upgrades in physical security controls, increased coordination with law enforcement at all levels of government, as well as expansion of personnel training, screening, and assessment programs.

Risk mitigation also can require cultures of safety and security within the nuclear enterprise and beyond IAEA. While very important and desirable, safety and security cultures must ultimately rely on human factors, such as attitudes, beliefs, and behaviors. These factors are often resistant to change and difficult to control.

Stakeholders in all sectors have come to recognize these problems with risk mitigation. They have concluded that permanent risk reduction approaches, which promote adoption of alternatives to sealed sources, are preferable. Replacing sealed-source devices with alternative technologies that do not require the same level of protection and vigilance provides the most effective and efficient means of increasing security.

Where viable alternatives exist (see Non-Isotopic Alternative Technologies Working Group 2019), the adoption of these alternative technologies should be encouraged. Denmark, France, and Norway, supported by strong legislative mandates, embraced a risk elimination approach and replaced all cesium blood irradiators by 2016. Japan replaced 80% of its cesium blood irradiators by 2017. Finland, Switzerland, and Sweden have strong programs promoting the adoption of alternative technologies,

which include requiring justification for seeking approval for acquiring new gamma devices.

Until recently, the United States had fallen behind other nations' efforts to replace cesium irradiators. This situation was due at least in part to the complexities of the country's governmental framework, in which regulations and interests at the federal (nation-wide) level overlap and occasionally conflict with those of its states (regions/provinces). However, intensifying concerns over security threats posed by malicious actors have led to a steady increase in support for alternative technologies. Indeed, the US offers an interesting case study in how a risk elimination approach targeted to open, low-security environments can become an integral part of a national risk management strategy. The United States' success in instituting a voluntary cesium irradiator replacement program that allocates financial and logistical resources to facilitate acquiring the new technologies, as well as removing and disposing of the sealed sources in a secure way, provides a model that could be emulated by other governments who wish to permanently eliminate risk but cannot secure a legislative mandate to do so.

This chapter begins by placing the regulatory landscape for sealed sources in the United States in both a historical perspective and an international perspective. Section 6.2.1, "Overview: the Regulatory Framework in the United States," discusses the emergence in the United States of the "risk management" approach to the regulation of sealed sources, in the context of the Cold War and also the "War on Terror." Section 6.2.2, "Challenges Within the Framework," highlights limitations and conflicts in current regulation, arising in part from the structure of the United States government, where federal, state, and occasionally cities can share jurisdiction over sealed sources. Section 6.2.3, "An Emerging Consensus," discusses the advantages of adopting a "Public Health" approach that reduces the reliance on radioisotopic technologies, especially in low-security settings, in favor of alternative technologies. The authors discuss one such program developed by the U.S Office of Radiological Security: The Cesium Irradiator Replacement Project (CIRP). The program offers meaningful financial and logistical support to stakeholders who voluntarily agree to adopt non-radioisotopic technologies. It has had great success in replacing high-activity radiological devices located in open, low-security environments, particularly within healthcare and research settings.

The paper concludes that seeking permanent threat reduction is both the most forward-looking and fiscally responsible approach to radiological materials management. Eliminating sources of risk in a categorical way produces better outcomes and greater safety than managing these sources of risk. Government regulation should facilitate the process of replacement and support institutions and organizations that are willing to transition to technologies that do not pose terrorism risks. During the interim period when regulatory and/or legislative direction has not been established, government agencies responsible for the regulation of radioactive sources should promote voluntary replacement as the preferred permanent risk reduction strategy. Strategies based on the long-term management of security risks should be adopted only when the potential for high-consequence events cannot be eliminated due to the absence of feasible alternatives to sealed-source devices.

6.2.1 Overview: The Regulatory Framework in the United States

The current regulatory landscape for radioactive materials in the United States is complex, due to the overlapping jurisdictions created by state and federal/national agencies and legislation. This was not always the case and it is instructive to examine legislative actions and social dynamics that shaped how radiological security in the United States evolved.

6.2.1.1 Federal Regulators: The Nuclear Regulatory Commission

The Atomic Energy Act of 1954, as amended in 1959, is the law that regulates civilian and military uses of nuclear materials. The law ended the federal government monopoly over nuclear power, allowing for the participation of the private sector in the expanding nuclear industry and shifting the federal role to one of promotion and regulation of private enterprise (Yates 1976, 399). All responsibility for both military and civilian uses of nuclear materials and technology fell under the control of the Atomic Energy Commission (AEC). This agency was put in charge of regulating both military and civilian uses of nuclear technology.

Jasper (1996, 31) claims that "the AEC interpreted its role less as regulation than as promotion of the new technologies." This posture was shared by many politicians and policy makers outside the AEC and led to the rapid growth of the nuclear industry during the 1960s and early 1970s. Nevertheless, many citizens, influenced by growing environmental

concerns, remained deeply skeptical of nuclear power. Quirk and Terasawa (1981, 833) describe the situation as follows:

> But even during the boom years for nuclear power, controversies were growing concerning almost every conceivable aspect of the industry, from the mining of uranium through reactor operations to disposing of nuclear wastes. Environmentalists and other intervenors argued that nuclear power was inherently unsafe, and that regulation of the industry was ineffective, so that the long run consequences of an economy powered by nuclear energy would be devastating.[13]

Much of the concern focused on a perceived conflict of interest in the AEC's dual role as promoter and regulator. Factors such as wildly inaccurate predictions about cost-savings (Jasper 1996, 29) and lengthening approval times for the licensing of new projects (Quirk and Terasawa 1981, 834) contributed to weakening governmental support for nuclear energy, which in turn further undermined public confidence. The situation was only made worse by the AEC's resistance to addressing environmental concerns (Greenberg 1996). In 1974, Congress addressed the perceived conflicts by creating the Nuclear Regulatory Commission (NRC) and entrusting it with regulatory functions over civilian nuclear technology, including source materials and the devices that rely on them. It is important to note that this agency was not given an official role in the promotion of nuclear technologies,[14] or in the regulation of mining.[15]

Rules governing use, access, security, transportation, storage, and decommissioning of sealed sources and byproduct materials in the United States are contained within the Code of Federal Regulations (CFR) title 10 parts 25–40. Following the terrorist attacks on September 11, 2001, additional security measures were instituted for Category 1 and Category 2 materials, which are contained within 10 CFR part 37. Other enhancements include a National Source Tracking System (NSTS), created to trace high-risk radioactive sources from the time they are manufactured or

[13] See also P. Greenberg, "Safety, Accidents and Public Acceptance," in *Governing the Atom: The Politics of Risk*, ed. J. Byrne and S. Hoffman (Transaction Publishers, 1996), pp. 127–156.

[14] That role as well as all other remaining functions of the AEC were given to the US Department of Energy (DOE).

[15] Conventional mining is regulated through the Mining Act of 1872.

imported through the time of their disposal or export, or until they decay enough to no longer be of concern, as well as a National Sealed Source and Device Registry (NSSDR), which contains summaries of engineering and radiation safety evaluations of sealed sources and devices conducted by both federal and state regulators under the conditions of their possession and use. NRC has resisted including Category 3 materials in any of these additional measures (GAO 2019, 5).

6.2.1.2 State-Level Regulation: "Agreement State" Compacts

The Atomic Energy Act of 1954, as amended in 1959, provides a statutory basis under which the NRC relinquishes to the States portions of its regulatory authority, allowing them to license and regulate health and safety impacts of sealed sources and devices. The mechanism for the transfer of NRC's authority to a State is an accord signed by the Governor of the State and the Chairman of the Commission of the AEC (later the NRC) in accordance with Section 274b of the Act. States that enter into such a compact become "Agreement States." This legislation recognized that localized health and safety risks associated with byproduct material were similar to other public health risks managed by local governments, and there was not a national interest requiring federal control. If specified, the compact can include a commitment to enforce on the NRC's behalf orders and requirements related to common defense and national security (Section 274i). In the later instance, the federal agency was not relinquishing authority, but merely delegating a duty. If a State did not enter into such an Agreement under any terms, all regulatory authority was left with the AEC/NRC.

Currently, the process of becoming an Agreement State takes approximately four to five years. Once the petition is approved, the NRC Management Review Board assesses each Agreement States' performance every four years to ensure that the state's program is adequately performing its regulatory obligations. The mechanism used by the NRC to oversee states is the Integrated Materials Performance Evaluation Program (IMPEP). The organizational structure of IMPEP teams nominally allows for Agreement State input. In practice, however, NRC staff outnumber Agreement State personnel (NRC Office of Inspector General). The NRC maintains reassertion authority in the case of accidents or emergencies, and there is a probationary period during which an Agreement State can lose its authority. To date, 39 out of 50 states have

joined the Agreement State program and one more is in the process of doing so.

The primary mechanism to organize, support, and facilitate the interactions between the Agreement States and the NRC is the Organization of Agreement States (OAS). The OAS is a private, not-for-profit professional society for the Agreement State radiation control program directors and their staff. The OAS is a voluntary organization, has no full-time staff, and is funded primarily through grants from the NRC. OAS has taken an active role in attempting to minimize conflicts between individual states and the NRC and pursuing a role for states in matters that have come to be seen as part of national security (Squassoni et al. 2014, 17). However, the OAS has limited administrative capacity. It relies on state regulators to volunteer staff, otherwise charged with regulatory responsibilities, to orchestrate engagement with the NRC's full-time administrative, legal, and policy planning personnel. This imbalance in administrative capacity clearly complicates dialogue between the two categories of regulators.

6.2.1.3 Agreements with the Armed Forces

The NRC's regulatory authority over sealed sources extends to devices under the jurisdiction of the Armed Forces. It delegates its authority to these agencies through a Master Materials License (MML). These licenses are designed to account for the diversity of sites, locations, and materials (byproduct, source, and/or special nuclear material) that might be under the jurisdiction of the armed forces (NRC, *Master Materials License*). Each military branch has its own centralized radiation control program responsible for ensuring regulatory oversight and compliance with the terms of the license. Under the authority of the MML, these centralized radiation programs can issue permits for the possession and use of sealed sources listed on the MML. In order to receive the MML, the licensee must agree to program inspections every two years. The NRC also has the authority to independently inspect permit holders.

6.2.2 Challenges Within the Framework

Edwards (2016, 151) argues that while the current radiation regulatory scheme has served the country well, the framework nevertheless "must periodically evolve and adapt to ensure that public health, workers, and the environment are properly protected in view of accepted societal values

and the advance of science, technology, and medical practices." In the United States, conflicts over the proper allocation of power between the federal government and the states are not uncommon. State law is not permitted to contravene federal law. At the same time, there is a widely held belief that federal laws should not encroach on matters best dealt with at the local level, and that all matters not explicitly regulated by federal law fall under state jurisdiction. State laws are necessarily complementary to federal regulation and there is substantial coordination between federal and state regulators in all manner of directives, oversight, and enforcement. Nevertheless, when it comes to regulating radioactive materials, including sealed sources, the stakes involved in any perceived conflict are significantly higher. Several factors are involved in making the dynamics of collaboration between federal and state regulators particularly fraught (see Aron 1997; Jones 2019).

Below, we will focus on challenges that arise within the Agreement State framework. Edwards (2016, 153) proposes several broad criteria that regulators should keep in mind when crafting directives and guidance. Among them is to ensure that regulations are protective yet flexible, that requirements are clear, and the directives are forward looking. We will first consider whether current regulations are sufficiently forward looking and whether they strike the appropriate balance between protection and flexibility when it comes to meeting specific local security needs within a nation-wide regulatory scheme. We will then consider whether the language used in creating compliance criteria is sufficiently clear and specific.

6.2.2.1 Compatible vs. Identical Regulations

Agreement States are expected to issue regulations that are "adequate and compatible" with those issued by the NRC (NRC "Security Orders and Requirements"). NRC's rigid interpretation of compatibility means that in practice they expect state regulation to be identical to their own Greer. This can lead to significant disagreements between state and federal regulators. Despite heightened security concerns relating to RDDs, states felt strongly that they continued to be the best option in regulating the security of sealed sources (GAO 03-804, 1). Furthermore, the vast majority of Category 1 and Category 2 licenses are regulated by the 39 Agreement

States. Nevertheless, despite the NRC's dwindling licensing responsibilities and the revenues tied to them,[16] its administrative and policy resources dwarf those of individual states. As a result, the NRC exercises significant control over both policy dialogue and regulation changes.

Currently, the NRC considers regulations that are more rigorous than its own to be incompatible with its requirements (NRC 2018).[17] This poses unique challenges for states with a high security risk profile tied to high population densities, their role in national or international economies, or simply the concentration of sealed sources located in low-security environments. States wishing to challenge IMPEP reviews must contend with a protracted process that can become administratively and financially burdensome. Mistrust between State and Federal regulators is heightened when federal decisions appear unduly influenced by stakeholders seeking a unified regulatory environment that facilitates the achievement of their commercial or professional interests, rather than promoting relevant health and safety concerns at national, regional, and local levels (Rojas-Burke 1992: 28; see also Jones 2019).

As the balance of direct regulatory activity for radioactive materials has shifted to the Agreement States, it could be argued that one of the NRC's primary roles has shifted to "overseeing the overseers"—the Agreement States. Given the imbalance of power between States and the NRC, the threat of increased audit schedules and negative findings that can result from the IMPEP process can further suppress open and honest communication between federal and state regulators. This makes the IMPEP process less a dialogue about best practices and more of an instrument to bring Agreement States into alignment with NRC policies and procedures. Establishing minimum national standards need not preclude states from addressing their own unique health, safety, and security risks.

[16] By law, 94% of NRC budget must be funded through licensing fees (GAO 03-804, 10).

[17] "Program elements in Compatibility Categories A and B adopted by Agreement States should be essentially identical to those of the NRC. If a requirement adopted by an Agreement State differs in any significant respect from that of the NRC, the State should explain how its requirement is essentially identical to the NRC requirement." NRC (2018) Dh 5.9 Adequacy and Compatibility of Program Elements for Agreement State Programs Dt-18-08, *U.S. NUCLEAR REGULATORY COMMISSION DIRECTIVE HANDBOOK*. https://www.nrc.gov/docs/ML1808/ML18081A070.pdf.

6.2.2.2 Prescriptive vs. Performance-Based Criteria

The NRC takes a performance-based approach to determining regulatory compliance (Medalia 2012, 26). Performance-based regulations focus on the ultimate outcome or the effect of the regulation and are designed to allow stakeholders greater flexibility in how they comply with the law, as long as the ultimate intent of the law is met. A prescriptive approach, as the name suggests, dictates the exact steps and procedures that must be followed in order to be considered in compliance. When it comes to dealing with safety measures, a performance-based approach can be frustrating to some state regulators who would prefer to provide more concrete guidance to licensees about what mechanisms and systems are likely to be most effective. It can also be frustrating to the licensees themselves, who may be uncertain as to what measures are sufficient to meet the standards.

The use of highly subjective terms contributes to the problem. NRC regulations require licensees to ascertain that persons with unescorted access to Category 1 and Category 2 materials are "trustworthy and reliable." It is left to HR personnel hired by the licensees to see that those standards are met. Decisions are expected to rely on routine information gleaned from law enforcement databases, previous employers, and character references. Psychological assessments are not included in review materials, and individuals are only re-evaluated every 10 years. Medalia (2012, 8) suggests the current standard can result in subjective judgements and inconsistencies in hiring practices.

A recent incident underscores the risks of relying on licensees' hiring practices and the potential for insider threats to result in the malicious use of radioactive materials. In 2019, Jared Atkins, an employee of an engineering firm who had been granted unescorted access to Category 2 materials, began experiencing a mental health crisis. He decided to steal three radioactive devices from his workplace in Arizona. Once in possession of the devices, he communicated to family and coworkers his intention to release the materials at a popular shopping area. Authorities were not aware of the theft until those who he had messaged about his malicious intentions contacted law enforcement. Catastrophe was only averted because the person ultimately changed his mind (Stern 2021; see also NRC 2019).

The safety regulations laid out in 10 CFR Part 37 require licensees to "provide *reasonable assurance* of the security of Category 1 or Category 2 quantities of radioactive material by protecting these materials

from theft or diversion" [emphasis added]. The regulation does not define what "reasonable assurance" would be. While it does prescribe the creation of security zones around Category 1 and Category 2 materials, commonplace security measures such as key card, passcode, and biometric technology systems are not required. Alarm systems to detect and record non-scheduled or after-hour removal are also not required. In the above incident, a standardized personnel reliability program (PRP) for staff with unescorted access to Category 1 material may have identified the insider threat prior to commission of the crime. Indeed, the Department of Defense requires further regulation of the reliability of its workforce than its civilian counterparts through the implementation of PRP in DoD Instruction Manual 5210.42 Nuclear Weapons Personnel Reliability Program (PRP).

This lack of prescriptive regulations might be explained by the fact that NRC gears the safety standards toward limiting the risk of short-term health exposures. However, when dealing with RDDs, it seems reasonable to also take into consideration health risks and societal costs relating to a large-scale evacuation, and the extremely high costs of environmental clean-up. Furthermore, the mental health effects of surviving an RDD attack should also be considered. Indeed, in the case discussed above, the economic and mental health impacts would have been felt long after the immediate health impacts were addressed and palliated.

Recent studies suggest that the deployment of an RDD in an urban center such as New York City would not only significantly impact the regional economy but also impact the United States Gross National Product (GAO 2019). Another recent incident makes abundantly clear that these predictions are no longer theoretical. In 2019, a vendor in the process of decommissioning a cesium irradiator in Washington State breached the sealed source, releasing an estimated 1 curie of cesium 137 and contaminating the seven-story research facility. Two years later, the costs of environmental remediation and reoccupation—for 1 curie in a single, modestly-sized structure—have soared to over $100 million. This staggering sum makes it abundantly clear that a continued focus on short-term health effects is insufficient[18] and calls for a reassessment of the economic models used to evaluate the impacts of a cesium or radioactive material release in a major urban center.

[18] This incident also highlighted the need for improvement in federal, state, and local collaboration (Department of Energy 2020).

In summary, the performance-based approach, while offering licensees flexibility in meeting the intent of the regulation, has significant limitations when dealing with the dangers posed by malicious or even accidental release of sealed-source materials. In our current national and global political climate, this is a risk that should not be underestimated.

6.2.3 An Emerging Consensus: Permanent Risk Reduction

The regulatory approaches to security discussed thus far focus on risk *management*. Such approaches necessarily assume high costs for securing sealed-source devices. These include not only one-time investments in equipment and infrastructure, but also recurring expenses such as licensing fees, liability insurance, security personnel, and administrative overhead. We propose instead to take a "public health" approach o security, prioritizing risk prevention and elimination, and adopting mitigation strategies only when elimination is not feasible. Such an approach calls for removing high-activity radiation materials from low-security, open access environments such as medical and healthcare facilities, research centers, and universities. Stakeholders at local, regional, national, and international levels are increasingly recognizing that reducing the use of sealed-source devices whenever alternatives are available is the most effective and financially sound security strategy.

The following section focuses on the significant success of a federal program that promotes permanent risk reduction by incentivizing organizations to exchange their sealed-source devices for comparable ones that use alternative technologies, such as X-rays. We also present case studies showing how federal, state, and local regulators collaborated with non-governmental organizations to promote large-scale adoption of this strategy.

6.2.3.1 The Cesium Irradiator Replacement Project (CIRP)

Given that the ability of Agreement States to establish prescriptive security measures as part of the "reasonable assurance" provision is limited, many states have sought to address structural security gaps through consensus-building mechanisms and voluntary programs provided by the Department of Energy's (DOE) National Nuclear Safety Administration (NNSA). Congress created the NNSA in 2000 as a semi-autonomous agency within the Department of Energy (DOE) responsible for reducing

the global danger from weapons of mass destruction, among other critical missions. Though the NNSA has no regulatory authority over civilian uses of sealed sources, its role in counterterrorism and nuclear nonproliferation lent itself to a concern with the safety and security of radioactive devices both nationally and internationally. Beginning in 2004 with the Global Threat Reduction Initiative (GTRI), and continuing with the creation of the Office of Radiological Security (ORS), NNSA became involved in the recovery of orphan and disused sources and enhancing security measures for high-activity radioactive materials both within and beyond U.S. borders.

While it held no regulatory authority, ORS became deeply involved in strengthening security protocols after the September 11 attacks. ORS strengthened collaboration between state radiological regulators, licensees, and local law enforcement agencies, offering workshops on responses to radiological theft alarms. It also worked directly with licensees to improve their security systems, instituting a voluntary program that provides protection upgrades, guidance, and training to enhance the security of high-activity radioactive sources. ORS also addressed the problem of disused sources, removing, and disposing of them at no cost to the licensee.

Over time, the security efforts of the ORS and the NNSA evolved from managing security risks to promoting permanent risk reduction. ORS now describes its mission as consisting of three "pillars": protect radioactive sources used for medical, research, and commercial purposes; remove and dispose of unwanted or abandoned sources; and reduce the reliance on highly active radioactive sources by encouraging development and use of alternative technologies such as X-rays whenever possible. Within its "Reduce" mission, the Cesium Irradiator Replacement Project (CIRP) offers a particularly successful model for promoting the voluntary adoption[19] of alternative technologies. This project has not only resulted in significant permanent risk reductions but encouraged important technological innovation in health services and in medical research.

Established in 2015, CIRP aims to persuade eligible U.S. organizations to voluntarily participate in the program by educating them on available

[19] This approach contrasts with that of France and Norway which achieved the replacement of sealed-source blood irradiators by banning or significantly curtailing access to cesium chloride.

alternative-technology devices and providing a wide range of resources: These resources include audit tools that support organizations in assessing the feasibility of transitioning to alternative technologies; access to experts who can answer questions about the transition to new technologies; opportunities for discussion with peers also considering this option; as well as compatibility studies between different technologies. Importantly, CIRP provides financial support to help fund the purchase of alternative technologies and arranges for the removal of disused gamma devices at no cost to the user. The program has had a significant impact in creating an industry-wide consensus about the benefits of X-ray devices in blood irradiation, which will be crucial in helping the United States meet its goal of eliminating the use of blood irradiation devices that rely on cesium chloride by December 31, 2027, as laid out by Congress (H.R. 5515 2018; Garrison et al. 2018).

6.2.3.2 Collaborations with Diverse Stakeholders

During the first four years of its existence, CIRP was responsible for replacing 20% of the gamma irradiators in the United States, a rate of roughly 40 irradiators per year. In addition, CIRP has commitments from licensees to replace another 20% of the inventory by 2023. This stunning success was achieved in large part through collaboration with the DOE/NNSA National Laboratories, state regulators, university systems, private sector stakeholders, and non-governmental organizations. The National Laboratories expanded their role from offering voluntary security enhancements to providing expertise in alternative technologies. The DOE/NNSA National Laboratories also expanded their capacity for removing and disposing of disused sealed sources at no cost. State regulators and non-governmental organizations also help coordinate outreach to commercial, public, and nonprofit users. CIRP supported Vitalant, the largest independent, nonprofit blood services provider in the United States with offices located throughout the country, as it committed to replace all its cesium blood irradiators with X-ray devices. Vitalant's example has been crucial in gaining the trust from other providers of blood irradiator services, who have come to appreciate that X-ray technology not only offers benefits in terms of reducing regulatory and security burdens, but also provides gains in quality and quantity of the blood supply.

CIRP's collaboration with the Nuclear Threat Initiative[20] (NTI) also deserves detailed discussion, as it provides a successful model for using consensus-building strategies to gain the support for the adoption of alternative technologies from a wide range of stakeholders. In New York City, NTI supported the local regulator[21] in convening discussions between ORS officials and representatives from universities, healthcare and research institutions to help them see beyond their individual organizational needs and move towards a city or region wide, public health understanding of risk reduction. Participants took the information back to their institutions, where they engaged in further consensus-building among researchers, radiological security officers, and administrators, allowing for open discussion of the promises and challenges of X-ray technology. In the end, these efforts will result in the replacement of 75% of the cesium irradiators within the city (Kamen et al. 2019; Iliopulos and Boyd 2019, 9–12). CIRP also collaborated with NTI to successfully obtain commitments from the University of California system to replace 90% of its cesium irradiators (MacKenzie et al. 2020; Iliopulos and Boyd 2019, 13–16). In a report published in 2019, NTI lists important lessons that can be learned from the success of these replacement endeavors. Recommendations include identifying and fostering local advocates and support networks; making information on alternatives to sealed-sources devices readily available; seeking consensus for the change from stakeholders using cesium devices within and among institutions; and increasing funding at federal levels to support the efforts (Iliopulos and Boyd 2019, 17, 20–23).

ORS is also engaged in international collaborations. Their focus is on reducing the reliance on radioactive sources used in medical, industrial, and commercial applications. Their efforts involve providing a range of financial incentives and support to stakeholders in partner countries who are interested in voluntarily replacing sealed-source devices with non-radioisotopic alternatives. It also works to repatriate radioactive sealed sources that originated in the U.S. and supports partner country efforts to remove disused sources to a secure location.

[20] A nonprofit whose mission is to prevent catastrophic attacks with weapons of mass destruction and disruption—nuclear, biological, radiological, chemical, and cyber (nti.org).

[21] The original agreement between the State of New York and the NRC designates the City of New York as its own regulatory entity within the State.

6.2.3.3 Elimination of Nuclear Threat Networks to National Security

The U.S. Federal government is heavily invested in the detection and elimination of materials capable of creating a nuclear or radiological threat to the American public and international partners. The Defense Threat Reduction Agency (DTRA) within the Department of Defense (DoD) acts to consolidate, secure, and eliminate weapons-usable radiological and/or nuclear materials abroad in efforts to prevent these devices from becoming weaponized by State or Non-State actors. These endeavors have been successfully accomplished by codifying umbrella agreements between the U.S. Department of State and foreign governments establishing mutual cooperation towards eliminating the nuclear and radiological threats posed by high-threat regions. Leveraging these international agreements, DTRA has focused efforts on the detection and interdiction of nuclear materials smuggling in these regions by providing radiological detection equipment, security training, logistics infrastructure, and nuclear dismantlement technology. These programs have shown particular success in threat reduction and elimination in nations such as Kazakhstan and Ukraine, which were historically inundated with dangerous materials from old nuclear reactors and weapons testing from the former USSR nuclear programs.

6.2.4 Conclusion

This chapter has highlighted how an effective regulatory framework must incorporate national, regional, and local levels. This framework must be based on fair collaboration practices, open channels of communication, and explicit division of responsibilities. Certainly, the advantages of having *minimum* nation-wide standards are indisputable. However, settling for *only minimum* requirements creates gaps in the regulatory regime and makes it difficult for local officials to fully meet the distinct needs of their populations. Federal regulators should value the knowledge that their state partners bring to discussions and should acknowledge that local and regional threat levels might require enhanced security protocols. While in some instances that might create a more complex regulatory landscape for licensees, it will ultimately yield benefits in terms of safety and preparedness.

We also made the case for including prescriptive measures, such as personnel reliability programs, within regulatory frameworks, to avoid

inconsistencies in oversight and compliance. The two recent incidents we discussed illustrate the dire consequences of such security gaps. As an alternative, we presented an example of a federal program that achieved security enhancements through fostering cooperation between diverse stakeholders, including offering financial and technical support.

Finally, we strongly recommended the creation and/or expansion of programs that facilitate the replacement of sealed-source devices. There is no question that high-activity radioactive materials provide many advantages to the industries that use them. Nevertheless, when housed in low-security, open environments, these advantages can be offset by the serious challenges their protection and potential malicious use pose. The dangers of accidental or intentional release of high-activity radiological materials are no longer hypothetical, nor are they decreasing. Thankfully, we currently have viable alternatives to many sealed-source devices, and research and development continues to offer promising new advances in these technologies.

References

Aron, J. *Licensed To Kill?: The Nuclear Regulatory Commission and the Shoreham Power Plant*. Pitt Series in Policy & Institutional Studies. Pittsburgh: University of Pittsburgh Press, 1997

Byrne, J. and Hoffman, S., eds. *Governing the Atom: The Politics of Risk*. Transaction Publishers, 1996.

Chmielewski, A. G. and Haji-Saeid. M. "Radiation Sources and Accelerators," in *Advanced Radiation Technology*, ed. N. Ramamoorthy (UK: WNU, 2019), pp. 37–44.

Edwards, J. D. "Federal Directions in Radiation Regulations," *Health Physics* 110, no. 2 (2016): 151–157.

Fidarova, E. and Erbas, B. "Medical Applications of Ionising Radiation," in *Advanced Radiation Technology*, ed. N. Ramamoorthy (UK: WNU, 2019), pp. 61–70.

Garrison, L, Itamura, M. T., Baumann, M. J., and Gilbert, L. J. (2018) *Radiological Security Through Cesium Irradiator Replacement in the United States*. Albuquerque: Sandia National Laboratories. https://www.osti.gov/servlets/purl/1592558.

Gopinath, D. V. and Ramamoorthy, N, ed. *Ionising Radiation and Mankind*. UK: Cambridge Scholars Publishing, 2020.

Greenberg, P. "Safety, Accidents and Public Acceptance," in *Governing the Atom: The Politics of Risk*, ed. J. Byrne and S. Hoffman (Transaction Publishers, 1996), pp. 127–156.

"IAEA 2004: Code of Conduct on the Safety and Security of Radioactive Sources," IAEA/CODEOC/2004, Vienna, 2004.
"IAEA 2005: Categorization of Radioactive Sources," Safety Guide No. RS-G-1.9, IAEA, 2005.
"IAEA 2014: The Radiological Accident in Lia, Georgia," IAEA STI/PUB/1660, 2014.
"IAEA 2015: Safety and Security of Radioactive Sources: Maintaining Continuous Global Control of Sources Throughout Their Life Cycle," STI/PUB/1667, 2015.
"IAEA 2021: IAEA Technical Report Series 1000, Nuclear Safety and Nuclear Security Interface: Approaches and National Experiences," 2021.
"IAEA and WHO 2021: Technical Specifications of Radiotherapy Equipment for Cancer Treatment," 2021.
"IAEA CN269," December 2018. https://www.iaea.org/newscenter/news/cooperation-coordination-and-communication-key-to-securing-radioactive-material-iaea-conference.
"IAEA CN270," November 2019. https://www.iaea.org/events/conference-on-effective-regulatory-systems-2019 and https://www.iaea.org/sites/default/files/20/01/cn-270-president-report.pdf.
"IAEA Directory," IAEA-DGPF/CD, 2004. https://www.iaea.org/publications/6914/directory-of-gamma-processing-facilities-in-member-states.
"iiA brochure," 2020. https://iiaglobal.com/wp-content/uploads/2020/06/FactSheet_Gamma-v5.pdf
Iliopulos, I. and Boyd, C. *Preventing a Dirty Bomb: Case Studies and Lessons Learned*. Foreword by L. Holgate. Washington DC: Nuclear Threat Initiative, 2019.
International Irradiation Association White Paper, "Uses and Applications of Radiation Processing," https://iiaglobal.com/resource/white-paper-uses-and-applications-of-radiation-processing/ and https://iiaglobal.com/wp-content/uploads/2020/11/iia_Uses_and_Applications_Radiation_Processing.pdf.
Jasper, J. "Nuclear Policy as Projection: How Policy Choices Can Create Their Own Justification," in *Governing the Atom: The Politics of Risk*, ed. J. Byrne and S. Hoffman (Transaction Publishers, 1996), pp. 47–67.
"John S. McCain National Defense Authorization Act for Fiscal Year 2019," Conference Report to Accompany H.R. 5515, 2018.
Jones, C. G. "The US Nuclear Regulatory Commission Radiation Protection Policy and Opportunities for the Future," *Journal of Radiological Protection* 39, no. 4 (2019): 51–59.
Jung, S.-H. "Application of Radioisotope Techniques for Industrial Process and Systems," in *Advanced Radiation Technology*, ed. N. Ramamoorthy (UK: WNU, 2019), pp. 52–59.

Kamen, J., Hsu, W., Boswell, B., and Hill, C. "Successful Migration from Radioactive Irradiators to X-ray Irradiators in One of the Largest Medical Centers in the US," *Health Physics* 117, no. 5 (2019): 558–570.

Kumar, R., Guest editor. "Nuclear Security," *IANCAS Bulletin* XI, no. 2 (2013).

Kumar, R., Panda, G. K., Singh, B. K., Rane, D. M., Sunil Kumar, J. V. K., and Sonawane, A. U. "Lessons Learned from the Radiological Accident in Mayapuri, New Delhi," IAEA/STI/PUB/1667 (2015): 517–528.

MacKenzie, C., Iwamoto, K. S., and Smith, K. "University of California Replacement of Cesium Irradiators with Alternative Technologies," *Health Physics* 118, no. 2 (2020): 209–214.

Medalia, J. *Nuclear Regulatory Commission 10 C.F.R. 37, A New Rule to Protect Radioactive Material: Background, Summary, Views from the Field*. Washington, DC: Congressional Research Service, December 14, 2012.

Murali, S. "Radiological Safety and Radiation Emergency Preparedness—Guest Editorial," *Radiation Protection and Environment* 43, no. 1 (2020): 1–5.

Murali, S., Anilkumar, S., Pradeepkumar, K. S., and Sharma, D. N. "Challenges on Prevention and Response to Nuclear/Radiological Threats and Nuclear Forensics," *IANCAS Bulletin* XII, no. 3 (2014): 178–189.

Nandakumar, A. N. "Security in Transport of Radioactive Material," *IANCAS Bulletin* XI, no. 2 (2013): 131–134.

NAS 2021: US National Academies of Sciences, Engineering, and Medicine. *Radioactive Sources: Applications and Alternative Technologies*. Washington, DC: The National Academies Press, 2021. https://doi.org/10.17226/26121

Non-Isotopic Alternative Technologies Working Group. "Non-radioisotopic Alternative Technologies White Paper." Washington DC: Cybersecurity and Infrastructure Security Agency, United States Department of Homeland Security, 2019.

Pant, H. J. "Radiotracer Applications in Industry, the Environment and Research," in *Ionising Radiation and Mankind* (UK: Cambridge Scholars Publishing, 2020), pp. 210–249.

Patil, S. B., Jha, J., Srivastava, P., Mishra, S., Datta R., and Khan, S. S. "Design & Development of Facility for Production of Active Cs-137 Source Pencils for Blood Irradiator," BARC Newsletter, November-December, 2015, 56–63.

Pradeepkumar, K. S. "Development of National Level Preparedness for Response to Radiological Emergencies/Threats," *IANCAS Bulletin* XI, no. 2 (2013): 138–145.

Public Health England. "Alternatives to Caesium Irradiators for Biological Sciences and Blood Transfusion Services," CRCE-RED-001-2020. Oxfordshire: Centre for Radiation, Chemical and Environmental Hazards. Public Health England, 2020.

Quirk, J. and Terasawa, K. "Nuclear Regulation: A Historical Perspective," *Natural Resources Journal* 21 (1981): 833–855.

Ramamoorthy, N. "Fostering Synergy of Security of Radiography Sources and Radiation Safety in Industrial Applications," IAEA Conf. CN-269 Book of Abstracts, 2018.

Ramamoorthy, N., ed. *Advanced Radiation Technology*. UK: WNU, 2019.

Ramamoorthy, N. "Practice-Specific Challenges in the Management of Regulatory Functions of Radiation Sources and Medical Facilities," IAEA Conf. CN-270 Book of Abstracts, 2019.

Ramamoorthy, N. "Radioisotopes and Radiation Technology and Their Applications: An Overview," in *Advanced Radiation Technology* (UK: WNU, 2019), pp. 1–12.

Ramamoorthy, N. "Impact of Human Element Aspects on Crucial Industrial Functions," NIAS, 2021. https://www.nias.res.in/publication/summary-meetings-human-reliability-program-industries-national-importance, https://www.nias.res.in/sites/default/files/2021-MR-02-SaiBaba.pdf.

Ramamoorthy, N. "Vulnerability of Human Reliability—Impact on Crucial Industries and Services," in *Human Reliability Programs in Industries of National Importance for Safety and Security*, ed. Sunil S. Chirayath and M. Sai Baba (2022, In Press)

Rojas-Burke, J. "Agreement States Still Chafing Under NRC Compatibility," *Journal of Nuclear Medicine* 33, no. 3 (1992): 27–28.

Squassoni, S., Cooke, S., Kim, R., and Greenberg, J. *Governing Uranium in the United States*. A Report of the Center for Strategic and International Studies (CSIS) Proliferation Prevention Program. New York and London: Rowman & Littlefield, 2014.

Stern, R. "Man Who Planned to Release Radiation at Scottsdale Fashion Square Mall Gets 15 Years," *Phoenix New Times*, March 5, 2021. Accessed April 26, 2021

United States Department of Energy. "Sealed Source Recovery at the University of Washington Harborview Training and Research Facility Results in Release of Cesium-137 on May 2, 2019," Joint Investigation Report, National Nuclear Safety Administration and Triad National Security LLC, March 20, 2020. https://www.energy.gov/sites/prod/files/2020/04/f73/JIT-Seattle-Cesium-Event-2019-05-02.pdf. Accessed April 28, 2021.

United States Government Accountability Office. "Nuclear Nonproliferation: Further Actions Needed by U.S. Agencies to Secure Vulnerable Nuclear and Radiological Materials," Report to Congressional Committees. GAO-12–512T, 2012, pp. 16–18. http://www.gao.gov/assets/590/589345.pdf.

United States Government Accountability Office. "Nuclear Security: NRC Has Enhanced the Controls of Dangerous Radioactive Materials, but Vulnerabilities Remain," GAO-16–330. Report to the Ranking Member Committee on Homeland Security, House of Representatives, 2016. https://www.gao.gov/products/gao-16-330.

United States Government Accountability Office. "Combating Nuclear Terrorism: NRC Needs to Take Additional Actions to Ensure the Security of High-Risk Radioactive Material," Report to Congressional Committees GAO-19–468, 2019. https://www.gao.gov/products/gao-19-468.

United States Nuclear Regulatory Commission. "DH 5.9 Adequacy And Compatibility Of Program Elements For Agreement State Programs Dt-18–08," U.S. Nuclear Regulatory Commission Directive Handbook, 2018. https://www.nrc.gov/docs/ML1808/ML18081A070.pdf.

United States Nuclear Regulatory Commission. "Agreement State Report—Theft of Cat 2 Material," Event Number: 54033. Event Notification Report For May 6, 2019. https://www.nrc.gov/reading-rm/doc-collections/event-status/event/2019/20190506en.html#en54033. Accessed May 15, 2021.

United States Nuclear Regulatory Commission. "Audit of NRC's Integrated Materials Performance Evaluation Program," Office of the Inspector General, Defense Nuclear Facilities Board, OIG-20-A-10 June 15, 2020.

United States Nuclear Regulatory Commission. "Agreement State Program." https://www.nrc.gov/about-nrc/state-tribal/agreement-states.html.

United States Nuclear Regulatory Commission. "Frequently Asked Questions About the National Source Tracking System." https://www.nrc.gov/security/byproduct/ismp/nsts/faqs.html#f1. Accessed on April 27, 2021

United States Nuclear Regulatory Commission. "History." https://www.nrc.gov/about-nrc/history.html. Accessed April 20, 2021.

United States Nuclear Regulatory Commission. "Security Orders and Requirements." https://www.nrc.gov/security/byproduct/orders.html. Accessed April 20, 2021.

Upreti, A. "The IAEA Nuclear Security Series," IANCAS Bulletin XI, no. 2 (2013): 146–149.

Venkatraman, B. and Menaka, M. "Ionising Radiations for Industrial Applications," in *Ionising Radiation and Mankind* (UK: Cambridge Scholars Publishing, 2020), pp. 106–130.

"WINS 2020: Event Report—Virtual Workshop on Strengthening the Coordination of International Programmes and Organisations Involved in the Adoption of Alternative Technologies to Radioactive Sources in Support of Radiological Security," December 10, 2020. https://www.wins.org/wp-content/uploads/2021/04/Dec-2020-Roundtable-on-Strengthening-Coordination-International-Programmes-involved-in-Alt-Tech-Report.pdf; https://www.wins.org/event/7804/virtual-roundtable-on-strengthening-the-coordination-of-international-programmes-involved-in-the-adoption-of-alternative-technologies.

"WINS 2021: Special Report Series—"Considerations for the Adoption of Alternative Technologies to Replace High Activity Radioactive Sources"," January

2021. https://www.wins.org/document/considerations-for-the-adoption-of-alternative-technologies-to-replace-high-activity-radioactive-sources-2/.

Yates, R. "Preemption Under the Atomic Energy Act of 1954: Permissible State Regulation of Nuclear Facilities' Location, Transportation of Radioactive Materials and Radioactive Waste Disposal," *Tulsa Law Review* 11, no. 3 (1976): 397–419.

CHAPTER 7

Cybersecurity and Nuclear Facilities

Pulkit Mohan, Cliff Glantz, Guy Landine, Sri Nikhil Gourisetti, and Radha Kishan Motkuri

7.1 An Indian Perspective

Pulkit Mohan

With the digital revolution, the interconnectedness between humans and machines has become significantly more complex. This has resulted in an exponential increase in the risks and vulnerabilities associated with the use of cyber technologies in our everyday lives. These cyber risks are no different in the case of nuclear materials and facilities. They present a unique and dynamic challenge to the nuclear security environment and therefore command attention. Effective nuclear security architectures are predicated upon accounting for vast and varied threats to nuclear materials and associated activities. Emerging threats in critical sectors such as nuclear have demonstrated the susceptibility of nuclear infrastructure to

P. Mohan
Observer Research Foundation, New Delhi, India

C. Glantz (✉) · G. Landine · S. N. Gourisetti · R. K. Motkuri
Pacific Northwest National Laboratory, Richland, WA, USA
e-mail: cliff.glantz@pnnl.gov

S. P. Kapur et al. (eds.), *The Challenges of Nuclear Security*, Initiatives in Strategic Studies: Issues and Policies,
https://doi.org/10.1007/978-3-031-56814-5_7

cyberattack. Such an attack can be disastrous, rendering many safety and security mechanisms ineffective.

The concern surrounding cyber threats to nuclear infrastructure has further been fueled by the sophistication of cyber operations employed to disrupt Iran's nuclear activities, specifically the 2010 cyberattack on Iran's Natanz uranium enrichment plant, which infiltrated the plant's computer software and infected and damaged its nuclear centrifuges. With the rise in the number of instances of cyberattacks over the years, there has been an emphasis on a deeper integration of cybersecurity measures into nuclear security frameworks. In the Indian context, cybersecurity in nuclear infrastructure garnered substantial attention as a result of 2019 cyber breaches at the Kudankulam nuclear power plant in Tamil Nadu, as well as the Indian Space Research Organisation (ISRO) headquarters.

Cybersecurity can be understood as "the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access. Cyber security may also be referred to as information technology security."[1] Cyberattacks are a category of risk that may disrupt or seize control of nuclear facilities, their control systems, and administrative systems and provide access to the facility itself, nuclear materials, or associated systems.[2] Given this danger, states must deploy robust security measures to tackle cyber threats and their subsequent consequences.

India's extensive nuclear infrastructure requires enhanced and dynamic safety and security measures to protect against associated threats, risks, and vulnerabilities. With the integration of cyber technologies into the fabric of India's security architecture, the vulnerability to cyber threats is amplified. An effective response to the emerging cyber threats requires wide-ranging attention at national level, as well as cooperation with international organisations and actors with similar challenges. With the greater risks of nuclear escalations and the repercussions associated with cyberattacks, countries must strike a balance between protecting critical

[1] Juliana De Groot, "What Is Cyber Security? Definition, Best Practices & More," *Digital Guardian*, https://digitalguardian.com/blog/what-cyber-security.

[2] Caroline Baylon, Roger Brunt and David Livingstone, "Cyber Security at Civil Nuclear Facilities: Understanding the Risks," *Chatham House*, September 2015, iv, https://www.nonproliferation.eu/wp-content/uploads/2019/11/20151005CyberSecurityNuclearBaylonBruntLivingstoneUpdate.pdf.

systems infrastructures and transparency in their cybersecurity safeguards and policies.

7.1.1 Identifying Risks and Vulnerabilities

To appropriately understand the cyber risks associated with nuclear facilities, a comprehensive analysis of possible negative outcomes is essential. A number of indicators can help us to make an informed risk assessment, increase protection of nuclear facilities, and decrease the likelihood of cyberattacks.[3] These include:

- Importance of Instrumentation and Control (I&C) system functions for both safety and security
- The identified and assessed threats to the facility
- Attractiveness of the I&C system to potential adversaries
- Vulnerabilities of the I&C system
- Operating environment
- Potential consequences that could result from a compromise of the system[4]

Additionally, the IAEA Nuclear Security Series offers a technical guide, "Computer Security of Instrumentation and Control Systems at Nuclear Facilities," which provides methods to implement cyber security programmes at nuclear facilities.[5] The key systems that control processes and equipment at nuclear facilities require rigorous cybersecurity safeguards. These systems are:

- SCADA (supervisory control and data acquisition) systems
- Distributed control systems
- Centralized digital control systems
- Control systems composed of programmable logic controllers

[3] "India Subindicators Detail," 2020 NTI Nuclear Security Index, Nuclear Threat Initiative, Accessed 28 June 2021, https://www.ntiindex.org/subindicator/?data_country=IN&data_indicator=INDICATOR_SECURITY_6&data_model=2020_NSI_T1&year=2020.

[4] Pickering and Davies, "Cyber Security."

[5] "Computer Security of Instrumentation and Control Systems at Nuclear Facilities," IAEA Nuclear Security Series No. 33-T, 2018, 2, https://www-pub.iaea.org/MTCD/Publications/PDF/P1787_web.pdf.

- Micro-controllers and "smart" devices
- Systems using programmed logic devices (e.g., field programmable gate arrays, complex programmable logic devices, and application-specific integrated circuits)[6]

It is also important to identify the origin of cyber threats to nuclear facilities. Cyber threats, like other threats to nuclear facilities, can occur from state actors,[7] non-state actors (such as terrorists, extremists, hackers, or lone-wolf actors), and insiders.[8]

One of the main challenges that cyberattacks present is the unpredictability of their effects on a country's nuclear infrastructure. A cyberattack may directly affect a nuclear facility or its systems, or it may act as a precursor or supplement to a more catastrophic threat or attack. The impact of a cyberattack and the best ways to address them, therefore, need to be based on an assessment of high-risk scenarios. These scenarios include:

- Unauthorized access to/theft of radioactive sources, such as highly enriched uranium. Adversaries can use cyberattacks to distract authorities and facilitate efforts to steal such materials.
- Radiation discharge. Cyber infiltration of a nuclear facility's instrumentation or control systems could enable an adversary to release radiation into the environment. This could pose a serious threat to nearby populations.
- Theft of sensitive/confidential information about specific facilities, including reactor designs. Theft of information on nuclear plants, their instrumentation, and plant controls, along with specifics of security measures and safeguards, can constitute a grave threat to a nuclear facility, with potential consequences reaching the national

[6] Ibid., 4.

[7] States that do not possess nuclear material or specific technical or confidential information on nuclear technologies and systems may try to illegally acquire it through cyber warfare, cyber terrorism, or hacking.

[8] Insider threat presents a unique challenge, where the risk is associated with individuals within the organisation. The threat can emerge from current or former employees or from third-party actors like contractors or temporary workers who have access to the plant's digital interface or networks.

or international level. For example, adversaries could use this information to plan a direct physical attack on a nuclear facility. They also could use such information to build or improve their own nuclear capabilities.

- Cause for public panic. Incidents or accidents pertaining to nuclear facilities often incite intense public reactions. Knowledge of cyber infiltration at a nuclear facility could result in public hysteria, potentially leading to chaos or the spread of dangerous misinformation.
- Reputational damage. A cyberattack can undermine the reputation of a nuclear facility, or even of the state as responsible nuclear actor. This can damage crucial relationships with international organisations, other countries, contractors, and suppliers, as well as with the public.
- Economic and operational costs. The nuclear industry, its maintenance, and its safety and security are costly. A cyberattack exposes vulnerabilities in the entire system and could require extensive and expensive changes to the existing systems and mechanisms.
- Theft of personal information of employees/leaders. Cyber infiltration into administrative or employee networks by adversaries may provide access to sensitive or personal information of employees. Adversaries can use this information to threaten employees, forcing them to provide unauthorised access to additional confidential information, or even to plant controls and instrumentation.

7.1.2 Cybersecurity in India: An Overview

In India, cyber security poses a serious challenge; the country suffered an estimated 394,499 cyberattacks in 2019 alone.[9] Yet, prior to 2013, India's cybersecurity architecture received inadequate attention. Cybersecurity gained greater salience in India as a result of the information uncovered during the Snowden leaks in June 2013. This brought India's attention to the United States National Security Agency (NSA)'s surveillance programs. India posited that the agency was spying on Indian citizens using digital surveillance tools.

[9] "CERT-In Annual Report (2019)," Indian Computer Emergency Response Team (CERT-In), Ministry of Electronics & Information Technology (MeitY) Government of India, Accessed June 28, 2021, https://cert-in.org.in/.

The Indian government's Ministry of Electronics and Information Technology published the first and only "National Cyber Security Policy" in 2013. Through this policy, the government aims "to protect information and information infrastructure in cyberspace, build capabilities to prevent and respond to cyber threats, reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology and cooperation."[10] The policy identifies the need for a national nodal agency responsible for all matters pertaining to cybersecurity in India and lists out a set of objectives required to build an ecosystem. These objectives include[11]:

- Creating a secure cyber ecosystem in the country, capable of generating adequate trust and confidence in IT systems and transactions in cyberspace and thereby enhancing adoption of IT in all sectors of the economy
- Creating an assurance framework for design of security policies and for promotion of compliance with global security standards and best practices by way of conformity assessment (product, process, technology, and people)
- Strengthening the regulatory framework for ensuring a secure cyberspace ecosystem
- Enhancing and creating national and sectoral level 24/7 mechanisms for obtaining strategic information regarding threats to ICT infrastructure and for creating scenarios for response, resolution, and crisis management through effective predictive, preventive, protective, response, and recovery actions; and enhancing the protection and resilience of the nation's critical information infrastructure by operating a 24/7 National Critical Information Infrastructure Protection Centre (NCIIPC) and mandating security practices related to the design, acquisition, development, use, and operation of information resources
- Developing suitable indigenous security technologies through frontier technology research, solution-oriented research, proof of

[10] "National Cyber Security Policy-2013," Ministry of Electronics & Information Technology (MeitY) Government of India, July 2013, 3, https://www.meity.gov.in/writereaddata/files/downloads/National_cyber_security_policy-2013%281%29.pdf.

[11] Ibid, 4.

concept, pilot development, transition, diffusion, and commercialisation that leads to widespread deployment of secure ICT products/processes in general and specifically for addressing national security requirements
- Improving visibility of the integrity of ICT products and services by establishing infrastructure for testing and validating security of such products
- Creating a workforce of 500,000 professionals skilled in cybersecurity in the next 5 years through capacity building, skill development, and training
- Providing fiscal benefits to businesses for adoption of standard security practices and processes
- Enabling protection of information while in process, handling, storage, and transit so as to safeguard privacy of citizen's data and to reduce economic losses due to cybercrime or data theft
- Enabling effective prevention, investigation, and prosecution of cybercrime and enhancing law enforcement capabilities through appropriate legislative intervention
- Creating a culture of cybersecurity and privacy that enables responsible user behaviour and actions through an effective communication and promotion strategy
- Developing effective public-private partnerships and collaborative engagements through technical and operational cooperation and contributions for enhancing the security of cyberspace
- Enhancing global cooperation by promoting shared understanding and by leveraging relationships for furthering the cause of security of cyberspace

India's cybersecurity policy is an effort to establish standard (best) practices, mechanisms of identification and classification of threats and risks, verification processes, and testing the effectiveness of this ecosystem and the security measures within. It endeavours to promote the welfare of the country's public and private infrastructures through appropriate safeguards and institutions.

7.1.3 India's Cyber and Nuclear Infrastructure

In India, the importance of integrating cyber security measures within nuclear security mechanisms has increased with the growing reliance on

digital technologies across functions as well as the global uptick in cyber risks and incidents. In order to engage with cybersecurity in the context of India's nuclear infrastructure, it is important to identify the key agencies and actors that are involved in maintaining the country's cybersecurity architecture. Understanding the organisation structure and its integration with India's nuclear security culture helps better understand the nexus in the Indian context.

One of the key institutions involved in building and maintaining cybersecurity mechanisms in India's nuclear infrastructure is the Computer Information and Security Advisory Group (CISAG). CISAG is responsible for conducting periodic audits on information systems as well as providing guidelines for countering cyberattacks and mitigating their impact on India's nuclear infrastructure.[12] Cybersecurity mechanisms are supplemented by agencies such as the national-level "Computer Emergency Response Team (CERT-In), National Technical Research Organisation (NTRO), and a Defence Cyber Agency (DCyA)."

CERT-In, operationalised in 2004, is the national nodal agency tasked with cybersecurity incidents in the form of analysis, emergency response measures, guidelines, and coordination on security practices, procedures, prevention, response, and reporting.[13] The NTRO, which draws inspiration from the United States' NSA, "reports to the national security advisor and is tasked with technical intelligence-gathering, signals interception, and influence operations."[14] CERT-In also conducts "cyber security exercises comprising of tabletop exercises, crisis management plan mock drills, and joint cyber security exercises with organizations from key sectors to enable participating organizations to assess their preparedness in dealing with cyber crisis situations" (Fig. 7.1).

In 2014, the National Critical Information Infrastructure Protection Centre (NCIIPC), a unit within the NTRO, was set up. NCIIPC is responsible for protecting critical information infrastructure "from unauthorized access, modification, use, disclosure, disruption, incapacitation

[12] "Nuclear Security in India," Ministry of External Affairs Government of India, Accessed June 28, 2021, https://www.mea.gov.in/Images/pdf/Brochure.pdf.

[13] "ICERT," Ministry of Electronics & Information Technology (MeitY) Government of India, accessed June 28, 2021, https://www.meity.gov.in/content/icert.

[14] "Cyber Capabilities and National Power: A Net Assessment," International Institute for Strategic Studies, June 2021, 134, https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power.

Security Incidents	2019
Phishing	472
Unauthorized Network Scanning /Probing/Vulnerable Services	305276
Virus/ Malicious Code	62163
Website Defacements	24366
Website Intrusion & Malware Propagation	417
Others	1805
Total	394499

Fig. 7.1 Types of security incidents handled in India

or distraction through coherent coordination, synergy and raising information security awareness among all stakeholders."[15] Additionally, the Defense Cyber Agency (DCyA), created in 2019, is a command within the Indian Armed Forces. DCyA handles all cyber threats pertaining to the military and develops and implements the security measures required to tackle cyber infiltration into India's defence networks. The DCyA was created as a result of the joint doctrine released by the Indian Armed Forces, which brought significant emphasis on the importance of protecting India's cyberspace and technologies, similar to the importance accorded to physical territories.[16]

The aforementioned institutions are key actors in India's efforts to address cybersecurity concerns and threats. However, it is important to emphasise the need for enhanced inter-agency coordination and collaboration between cybersecurity institutions and the traditional establishments within India's nuclear infrastructure. Institutions tasked with

[15] "Mission," National Critical Information Infrastructure Protection Centre, Government of India, https://nciipc.gov.in/.

[16] IISS, "Cyber Capabilities."

cybersecurity require extensive collaboration and coordination with key institutions such as the Atomic Energy Regulatory Board (AERB) and the Department of Atomic Energy and its many units.

7.1.4 Case Study: The Kudankulam Breach

The 2019 Kudankulam cyber breach can help us better to understand the Indian approach to protecting its nuclear facilities. The incident, which took place in September 2019, was an infection of a known malware called Dtrack, which had been used to attack financial institutions in India previously. According to government statements and reports, the breach did not directly attack the plant control and instrumentation system, and access was limited to the administrative network.[17]

The incident is important for a number of reasons. First, the incident received an unusual degree of public attention, given the relative lack of public information on cybersecurity in India's nuclear facilities. There were considerable speculation and discussion around the causes of the incident and its level of severity. The malware attack was particularly concerning due to its potential ability to perform reconnaissance and gather sensitive information on plant systems.

Second, the breach was limited to administrative systems. The government explained that "the Kudankulam Nuclear Power Project (KKNPP) and other Indian Nuclear Power Plants Control Systems are stand alone and not connected to outside cyber network and internet. Any Cyber-attack on the Nuclear Power Plant Control System is not possible."[18] The fact that the control systems were not breached through the attack is noteworthy. This was the result of air gaps, which are a common method of cyber protection in which the main plant control system is not connected to the internet or intranet.[19] It is important to note, however, that such

[17] Utpal Bhaskar, "India Confirms Malware Attack at Kudankulam Nuclear Power Plant," *Mint*, Updated November 20, 2019, https://www.livemint.com/news/india/india-confirms-malware-attack-at-kudankulam-nuclear-power-plant-11574262777163.html.

[18] "Press Release," Kudankulam Nuclear Power Project, Nuclear Power Corporation of India Ltd., October 29, 2019, https://i0.wp.com/www.opindia.com/wp-content/uploads/2019/10/Kudankulam-Nuclear-Power-Plant-statement.jpg?ssl=1.

[19] Air gaps are software-designed firewalls that deny any external networks to connect with the isolated computer network. See: https://scroll.in/article/943954/what-happened-when-the-kudankulam-nuclear-plant-was-hacked-and-what-real-danger-did-it-pose.

air gaps, despite their apparent efficacy in this case, are not impossible to overcome.

Third, the breach resulted in a robust governmental response. CISAG and the CERT-In were called in to investigate the incident and strengthen cybersecurity. As a result, a number of measures were implemented. These included hardening of internet and administrative intranet connectivity, implementing restrictions on removable media, and blocking malicious websites and IPs.[20]

The limited infiltration levels and the implementation of additional cybersecurity measures in this case are reassuring. Nonetheless, the case does highlight the need for robust and adaptive cybersecurity mechanisms to counteract inevitable vulnerabilities in critical infrastructure in nuclear systems.

7.1.5 Important Considerations and Recommendations

Nuclear security and safety are of paramount importance in India due to the severity of consequences as a result of accidents or incidents. The nuclear industry, however, has placed cybersecurity at a relatively low priority compared to traditional aspects of nuclear security like physical protection of facilities or insider threats. As the nuclear industry is heavily regulated, the incorporation of standardised cybersecurity rules, assessment, and training has been slow.[21] Furthermore, the Indian discussion around cybersecurity and nuclear infrastructure is restricted due to the national security sensitivities associated with the nuclear industry. The limited information on cyber incidents within the nuclear industry may lead to the belief within the community that cybersecurity is not a real or immediate threat. Lack of engagement with cybersecurity and complacency regarding existing structures to counter the cyber threat are some of the biggest challenges to effective mitigation of cyber threats and attacks.

India's nuclear industry must consider a number of challenges it faces as it becomes increasingly reliant on digital systems. At an industry level, there is insufficient interaction with cybersecurity experts from other industries; more collaboration to better understand how technology

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

[21] Baylon, Brunt and Livingstone, "Cyber Security," 14.

and technological advancements impact cybersecurity broadly would be beneficial for those charged with securing nuclear infrastructure. More investment into training personnel across nuclear facilities in India is also essential.

For the physical protection of nuclear facilities in India, a national Design Basis Threat (DBT)[22] document helps individual facilities to counter both internal and external threats. Similar national guidelines are required to deal with cyber threats to nuclear systems, facilities, and security systems. Cybersecurity should be accorded similar standing in risk and threat assessments, and more resources should be invested into building a robust security plan to counter cyber threats. This would entail a deeper look into the vulnerabilities that come with any critical infrastructure, such as the complexity of design and systems, the lack of verification, periodic assessment, and appraisals. Additionally, the nuclear industry has to engage more deeply with regulatory authorities and promote information exchange to better assuage the concerns associated with cyber risks.

The human factor also impacts cybersecurity within India's nuclear industry. The role of nuclear security culture, for example, is critical. Poor understanding of cybersecurity is detrimental to maintaining an effective security culture at facilities. This issue requires both the creation of a cadre of competent security personnel who are well acquainted with cybersecurity challenges and a larger effort to educate all nuclear facility personnel so they better understand why cybersecurity should be treated as a priority.

Complacency among nuclear plant personnel can impact cyber operations negatively as well. The lack of cognisance in terms of cybersecurity risks may lead to poor cyber practices among nuclear personnel, such as the use of personal electronic devices. The dangers of insider threats must also be acknowledged. Cyber threats can arise from deliberate malicious intentions of rogue or disgruntled employees at a nuclear facility. In the aftermath of the Kudankulam attack, the Indian nuclear industry has taken steps to restrict the exposure to cyber risks as a result of physical access to plant and security personnel.

[22] DBT describes "the capabilities of potential insider and external adversaries who might attempt unauthorized removal of nuclear and other radioactive material or sabotage." See: https://www.iaea.org/topics/security-of-nuclear-and-other-radioactive-material/design-basis-threat.

In addition to the risks posed by facility personnel, India suffers from supply-chain vulnerabilities. Vendors, contractors, or subcontractors could exploit digital equipment during transport, assembly, or even within facilities. Cybersecurity measures must be incorporated into supply-chain management in order to reduce these dangers.

Finally, India's nuclear infrastructure would benefit greatly from strengthening international cooperation and agreements regarding cybersecurity issues. India is party to a number of these agreements. In 2020, for example, India and Japan finalised an agreement to "boost cooperation on 5G technology and critical information infrastructure, and the two countries pledged… to work for a free and open Indo-Pacific with diversified supply chains."[23] Further, the United States and India have engaged in an annual Cyber Dialogue, dedicated to "exchanging and discussing international cyber policies, comparing national cyber strategies, enhancing our efforts to combat cybercrime, promoting capacity building and R&D, thus promoting cybersecurity and the digital economy."[24] More such agreements and discussions would be helpful, particularly if they focus specifically on the cyber threat to nuclear infrastructure.

Deeper bilateral engagement is helpful in learning from the cybersecurity experiences and expertise of similar countries. Additionally, India has civil nuclear cooperation with several countries, including the United States and Japan. Given the scope for cooperation with like-minded partners, India can engage more deeply to boost information and knowledge exchange to improve its cyber-nuclear infrastructure. Additionally, international organisations like the IAEA provide guidance and training to develop comprehensive measures. The IAEA "conducts advisory missions, trains inspectors, and provides planning expertise in conducting computer

[23] Rezaul H. Laskar, "India, Japan Finalise Key Cyber-Security Deal to Boost Cooperation on 5G, AI," *Hindustan Times*, October 7, 2020, https://www.hindustantimes.com/india-news/india-japan-finalise-key-cyber-security-deal-to-boost-cooperation-on-5g-ai/story-WCMa9En3NFPkQMWClGNFJI.html.

[24] "The Governments of the United States and India held the Fifth U.S.-India Cyber Dialogue in New Delhi (September 28, 2016)," Ministry of External Affairs, Government of India, September 30, 2016, https://www.mea.gov.in/press-releases.htm?dtl/27448/The+Governments+of+the+United+States+and+India+held+the+Fifth+USIndia+Cyber+Dialogue+in+New+Delhi+September+28+2016.

security exercises as part of the nuclear security programme."[25] Engaging with international organisations, multilateral forums, and regulatory frameworks is essential to a building robust cybersecurity mechanisms and practices.

7.1.6 Conclusion

The challenges posed by digital technologies and their advancement will continue to grow as an essential aspect of nuclear security that must be managed. The acknowledgement of cyber risks as a real and present threat to India's nuclear infrastructure must lead to increased awareness of the challenge and to more robust efforts to counter it. Particularly against the backdrop of the 2019 incident at the Kudankulam Nuclear Power Plant, developing appropriate guidelines to enhance the visibility and importance of cyber in nuclear security culture and in risk assessment methods is vital. Effective security measures are required to tackle the industrial, technical, and cultural challenges associated with cyber risks. Given the dynamic nature of cyber risks and threats, complacency regarding cybersecurity mechanisms and practices is dangerous. As India expands its nuclear industry, assessing the risks, vulnerabilities, and areas for improvement must be a fundamental part of its nuclear security practice.

7.2 A U.S. Perspective

Cliff Glantz, Guy Landine, Sri Nikhil Gourisetti and Radha Kishan Motkuri

Cybersecurity is the "art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability" of digital devices and information (U.S. Cybersecurity & Infrastructure Security Agency [CISA] 2019). The threat of cyberattacks is a growing concern for national, regional, and local governments; industry; and the public. Effective cybersecurity programs are needed to secure all types of critical infrastructure, including nuclear facilities.

[25] "Computer and Information Security," International Atomic energy Agency, Accessed June 29, 2021, https://www.iaea.org/topics/computer-and-information-security.

Reports of criminal organizations mounting cyberattacks against critical infrastructure are common. Cyberattacks attributed to nation-states, with the goal of gathering information or in some cases disrupting the operation of critical infrastructure, have been reported by government agencies, industry, and the news media. Ransomware and extortion attempts are a significant concern, made worse by the advent of electronic currency, making the tracking of payments and the identification of specific attackers exceedingly difficult. In this threat environment, it has become imperative for governments and industries to focus on resources to assess and address cybersecurity risks. This problem is exacerbated for the nuclear sector by the growing prevalence of digital control systems deployed in all aspects of nuclear facility operation.

This chapter discusses the potential perpetrators of cybersecurity threats against nuclear facilities; cybersecurity risks that nuclear facilities face, including vulnerabilities in their information technology (IT) and operational technology (OT) systems; and risk-based, cost-effective methods to protect nuclear facilities.

As leaders and innovators in cybersecurity, the U.S. and India need to support nuclear cybersecurity programs and provide impactful nuclear cybersecurity guidance in their respective countries. The U.S. and India also need to work together to support and assist other countries in developing and implementing appropriate nuclear cybersecurity programs. This effort can involve the publication of technical guidance documents, the presentation of training courses, the development and sharing of cybersecurity technologies, and the implementation of effective supply-chain security programs.

7.2.1 Background

Twenty years ago, many in the U.S. nuclear sector discounted the cybersecurity threat to nuclear facilities because of the largely analog nature of facility control systems, the perceived isolation of those digital control systems that were present, and the lack of any credible cyberattacks on the nuclear industry. Today, none of those arguments are compelling. Many control systems at nuclear facilities are now digital and use contemporary operating systems, communication protocols, and commercial-off-the-shelf hardware and software. This has increased efficiencies and capabilities for nuclear operations, engineering, and maintenance. It has also raised significant security challenges owing to the vulnerabilities inherent

in these technologies. This problem is further complicated by the rapid pace in the evolution of technologies and the increasing capabilities of cyberattackers. As a result, cybersecurity regulations and guidance must also rapidly evolve to maintain an appropriate and up-to-date level of protection. This creates a substantial burden for both the competent regulatory authority and the licensees they support.

To understand the need for cybersecurity at nuclear facilities, it is helpful to review selected incidents that have occurred within the last 20 years. In 2003, the SQLSlammer worm infected Ohio's Davis-Besse Nuclear Power Plant. The worm traveled from a contractor's system to the operating utility's corporate network (using a connection that bypassed the protecting firewall) before arriving at the process control network for the plant (U.S. Nuclear Regulatory Commission [NRC] Office of Nuclear Reactor Regulation 2007). The traffic generated by the worm clogged the plant control network and other systems. For nearly five hours, plant staff could not access the Safety Parameter Display System, as the worm interfered with, and eventually crashed, the system along with other monitoring systems at the nuclear plant. Fortunately, there were no immediate safety implications from this event because the plant was down for extensive repairs when the incident occurred (Markey 2003).

In August 2006, the Browns Ferry Nuclear Power Plant underwent a manual shutdown because of an overload of network traffic. This overload resulted in the failure of reactor recirculation pumps and the condensate demineralizer controller because microprocessors are prone to failure in high traffic environments. Although the failure of these controllers was not the result of a cyberattack, this incident shows that a cyberattack on the plant network can affect the operation of key systems even if those systems are not directly targeted (U.S. NRC 2007).

In March 2008, the Hatch Nuclear Power Plant experienced an automatic shutdown after a software update on its business network. The update was intended to synchronize data collection between a diagnostic system and the process control network. When the business network computer was rebooted, it reset the data on the control network, triggering an automatic plant shutdown. This incident was not a cyberattack, but it illustrated how changes to business network systems could affect the operation of process control networks for the facility in ways that plant personnel might not anticipate (U.S. NRC 2011).

In 2010, Iran's Natanz nuclear facility was infected by the Stuxnet computer worm. Stuxnet targeted the Siemens control systems operating the facility's centrifuges, damaging this equipment. The worm exploited several previous unknown and/or unpatched vulnerabilities and appeared to have spread to the controllers via malware on infected USB flash drives (U.S. CISA 2010; Hemsley and Fisher 2018).

In December 2014, a cyber incident was reported by the Korea Hydro and Nuclear Power Company. A cyberattack exfiltrated information on the design and operation of the South Korea company's nuclear reactors. The attack began with phishing emails. An employee's accidental click on the malicious link given in the email allowed malware to download, infecting the company network (U.K. National Cyber Security Centre 2016).

In March 2018, the U.S. Cybersecurity & Infrastructure Security Agency (CISA) reported that Russian-government cyber actors targeted multiple U.S. critical infrastructure sectors, including the energy and nuclear sectors (U.S. CISA 2018). CISA did not release specific information on targeted nuclear facilities. The report states that attacks first involved "peripheral organizations" such as trusted third-party suppliers with less secure networks. The attackers used these initial attacks to access systems within the networks of critical infrastructure facilities, conduct reconnaissance, and collect information. It was not reported whether the malware had the capability to allow the attackers to affect nuclear power operations if activated during a future international confrontation.

In September 2019, a cyberattack on the Kudankulam Nuclear Power Plant in Tamil Nadu, India, was reported by the Nuclear Power Corporation of India. They stated that the nuclear plant's administrative network was breached in the attack, but it did not cause any operational, safety, or critical damage. In theory, information acquired in this type of cyberattack at a nuclear plant could assist attackers in planning a future attack focusing on the critical systems within that nuclear plant. In reassuring the public about the Kudankulam cyberattack, plant officials stated that their nuclear power plants are "stand alone" and are not connected to any outside cybernetwork or the internet. They further asserted that any cyberattack on the plant's control system was impossible (India Department of Atomic Energy 2019). While air gapping is an excellent way to reduce cybersecurity risks, it is not foolproof. Air-gapped systems, like those targeted by Stuxnet, can be compromised when data, software, firmware, etc., are physically exchanged (e.g., using memory sticks or

direct connections to portable devices) between infected and air-gapped devices or systems as part of routine operations and maintenance.

7.2.2 *Threat Agents and Vulnerabilities*

Cyber threats to nuclear facilities may come from different categories of adversaries. The traditional list of cyber threat actors includes[26]:

- ***Nation-States***: They may be part of a government organization or receive direction, funding, or technical assistance from a nation-state. Nation-state adversaries can be well resourced and patient in their activities. They may be motivated to gather sensitive information, steal intellectual property, or install malware that can be activated during a future conflict. Their goals could be military, political, or economic. They may be assisted by insiders motivated by financial, political, or other motives.
- ***Cybercriminals***: They may be individuals or large groups that are financially motivated. They may have the resources to acquire significant capabilities and to recruit or coerce insiders. They may be willing to extort money from their victims, manipulate financial markets, or steal intellectual property.
- ***Terrorists***: They may have motivations equivalent to that of nation-states or cybercriminals. Their capabilities and resources may be less than that of nation-states but could still be significant. Like criminal organizations, they may be able to hire or coerce the support of technical experts of nuclear facility insiders. Limited offensive cyber activity is typically disruptive or harassing in nature. The terrorist organization primarily uses the internet for communications and recruitment.
- ***Hacktivists***: They are politically, socially, or ideologically motivated and may mount cyberattacks to harm a company, influence public opinion, or cause a political change. Hacktivists typically have fewer resources and capabilities than nation-states or larger criminal organizations, but they may acquire significant attack capabilities, and they may entice insiders to provide support.

[26] See https://www.cisecurity.org/spotlight/cybersecurity-spotlight-cyber-threat-actors/.

- ***Insiders***: They are current or former employees, contractors, or other partners who have access to an organization's networks, systems, or data. Insiders may intentionally perform malicious actions, be enticed or coerced to support other categories of attackers, or perform actions without malicious intent that can permit or support a cyberattack. Malicious insiders might take actions to seek revenge or financial gain.

Threat agents exploit vulnerabilities to execute an attack. "Vulnerability" may be defined as a weakness in a system, process, or a procedure that could be exploited by a threat source. Vulnerabilities may exist at the business level (or management level) and at the system or network level. An example of a business-level vulnerability is the lack of well-defined policy for organization-wide access control. An example of a system-level vulnerability is the use of default or simplistic passwords (e.g., "password," "0123456") on digital devices.[27]

Vulnerabilities can be introduced unwittingly by suppliers/vendors. An example of a vulnerability introduced by the supplier might be a flaw or "bug" in the firmware or software that a cyberattack could exploit. Most systems are built with several hardware, software, and firmware subcomponents and libraries. They are often procured from other suppliers, rather than developed at the vendor location, because it is cost-effective to the vendor. Therefore, it is not uncommon to find vulnerabilities associated with inadequate supply-chain security. At the time of the product's release, vendors are expected to address any known vulnerabilities. However, new vulnerabilities may be discovered after the system is widely deployed. These new vulnerabilities are referred to as the zero-day vulnerabilities.[28] To address these newly discovered vulnerabilities, vendors often release software and firmware patches. To ensure secure design and development of a system, vendors should follow security best practices throughout the system life cycle.

[27] See https://csrc.nist.gov/glossary/term/vulnerability#:~:text=Definition(s)%3A,VULNERABILITY%20from%20CNSSI%204009%20%2D%20Adapted.

[28] Note that the zero-day vulnerabilities and zero-day exploits are different. A zero-day exploit refers to a cyberattack that occurs on the same day a vulnerability is discovered. In other words, this implies that the vulnerability is exploited by a threat actor before the vulnerability is mitigated.

Vulnerabilities can be introduced unwittingly by users, who must be careful to protect their systems from cyberattack. A misconfiguration or other error can increase the risks from a cyberattack. Users are expected to follow network-level and system-level best practices to protect their systems (e.g., implementing network segregation, using principle of least privilege, applying need-to-know security controls). Users also are expected to maintain good cyber hygiene by applying strict password rules, multi-factor authentication, and if possible, using zero trust architecture. Users should use external information sources (e.g., Industrial Control System-Cyber Emergency Response Team [ICS-CERT], U.S.-Computer Emergency Response Team [US-CERT]) to stay up to date on security alerts and to immediately develop mitigations to address a relevant alert. When vendors release a patch, users should perform thorough testing and implement the patch accordingly.[29]

7.2.3 U.S. Regulatory Approach

The U.S. is often viewed as a model within the international nuclear community for nuclear cybersecurity. Many nations have taken their lead from the cybersecurity rule and regulatory guidance published by the U.S. Nuclear Regulatory Commission (NRC). Therefore, it is instructive to review the history of the U.S. cybersecurity program and regulatory actions.

The U.S. approach to cybersecurity for the nuclear sector has evolved as the U.S. Nuclear Regulatory Commission (NRC) issued cybersecurity regulations and guidance, observed real-world outcomes, and strived to incorporate lessons learned.

Several months after the September 11, 2001, terrorist attacks, an NRC security order (EA-02–026, "Interim Safeguards and Security Compensatory Measures for Nuclear Power Plants") directed nuclear power plant licensees to address issues concerning cybersecurity. A year later, another NRC security order (EA-03-086, "Design Basis Threat for Radiological Sabotage") directed nuclear power plants to address cyberattacks in their design basis threat assessments. After conducting series of pilot cybersecurity assessments at several nuclear facilities, in October

[29] Information on patch management can be found at https://csrc.nist.gov/Topics/Security-and-Privacy/security-programs-and-operations/patch-management.

2004, a cybersecurity team from Pacific Northwest National Laboratory in October 2004 published NUREG/CR-6847, "Cyber Security Self-Assessment Method for U.S. Nuclear Power Plants."

The Nuclear Energy Institute (NEI) is the policy organization of the U.S. nuclear technologies industry. NEI's members include companies that operate nuclear power plants, reactor designers, engineering firms and manufacturers, fuel suppliers and service companies, consulting service companies, and others (https://www.nei.org/about-nei). The NEI cybersecurity task force developed guidance (NEI 04-04 Rev. 1, "Cyber Security Program for Power Reactors") to provide a programmatic framework to manage a nuclear power plant's cyber security program. It included support for use of NUREG/CR-6847 and outlined defensive strategies and techniques to protect nuclear plants from cyber threat. The NRC staff evaluated NEI 04-04 and in December 2004 determined it to be an acceptable approach for licensees to formulate their cybersecurity programs. The U.S. nuclear industry uniformly embraced the use of NEI 04-04 and voluntarily agreed to implement the program—in part to make it unnecessary for the NRC to implement cybersecurity regulatory actions.

In January 2006, the NRC released Regulatory Guide 1.152 Rev. 2, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants." The guidance provided the licensee with security controls that could be embedded within the safety system development process to address potential security vulnerabilities in each phase of the digital safety system life cycle. In March 2007, the NRC released Branch Technical Position (BTP) 7-14 Rev. 5, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems." This position paper provided guidelines for evaluating software life-cycle processes for computer-based instrumentation and control systems. Also, in 2007, the NRC conducted composite reviews at several U.S. nuclear facilities to determine whether licensees were faithfully implementing the programmatic requirements and cybersecurity measures specified within NEI 04-04 Rev. 1. The reviews identified significant deficiencies within the licensees' implementation of their agreed-to program. As a result, the NRC initiated rule-making activities to institute a regulation addressing cybersecurity for power reactors.

In March 2009, the NRC, with technical assistance from PNNL, issued 10 CFR 73.54 "Protection of Digital Computer and Communication Systems and Networks." This two-page performance-based rule required

licensees to provide high assurance that digital computer and communication systems and networks are adequately protected against cyberattacks, up to and including the design basis threat. It included requirements to incorporate the cybersecurity program as a component of the physical protection program, maintain defense-in-depth protective strategies, mitigate the adverse effects of cyberattacks, ensure that critical functions are maintained, provide cybersecurity training and awareness, assess cyber risks, test system modifications prior to deployment, and develop and maintain a detailed cybersecurity plan.

Prior to the publication of 10 CFR 73.54, PNNL and NRC began work on Draft Guide (DG) 5022, "Cyber Security Programs for Nuclear Facilities," to outline a detailed, performance-based (i.e., risk-based), defense-in-depth method for implementing nuclear cybersecurity. Based on material in NEI 04-04 and NUREG/CR-6847, it included a description of a network security architecture that could be used for the protection of plant systems and networks and incorporated the use of a defensive model that defined formal communication boundaries (or security levels) where defensive measures could be deployed to detect, prevent, delay, mitigate, and recover from cyberattack. Also included in DG-5022 was a compendium of defensive strategies that could be utilized by licensees to address a variety of issues common to the application of cybersecurity within a nuclear plant environment.

In June 2008, the NRC released a first draft of DG-5022 and subsequent versions were released later that year and in January 2009. After receiving extensive stakeholder comments, the NRC opted to take a different approach. Rather than continuing with the performance-based approach outlined in DG-5022, the final version of the document, now entitled Regulatory Guide (RG) 5.71, "Cyber Security Program for Nuclear Facilities," embraced a compliance-based approach to cyber security. RG 5.71 was published in January 2010 and lists over 100 security controls (obtained from NIST SP 800-53 Rev 2, "Recommended Security Controls for Federal Information Systems") for application to each critical digital asset (CDA) in the nuclear facility. A CDA is a component of a "critical system" that consists of or contains a digital device, computer, or communication system or network. A critical system performs or is associated with a "safety-related, important-to-safety, security, or emergency preparedness function." At a nuclear power plant, there may be hundreds to thousands of CDAs.

Licensees experienced difficulties attempting to apply all the security controls identified in the RG 5.71 compliance-based approach. While the concept of "more security equals better security" sounds plausible, in some cases it is actually contrary to good security engineering practices. The blanket application of security controls without analysis of their benefits and drawbacks can result in unintended consequences that can negatively impact system performance and cybersecurity. The following are examples of the drawbacks to the compliance-based approach in RG 5.71:

- Not all controls can be applied in all situations. For instance, implementing virus protection on a real-time operating system (RTOS) is often impossible because technical limitations prevent installation of antivirus elements into an RTOS environment. In cases like these, RG 5.71 directs the licensee to perform an engineering justification analysis and identify an "alternative" control that is as "effective or better than the original control." Unfortunately, there is no guidance on what "alternative" controls are acceptable and what they must achieve. Licensees complain they are spending an inordinate amount time and resources explaining why they cannot apply a particular control or set of controls, rather than using those resources to reinforce existing, or investigate new types, of security controls.
- The compliance-based approach of RG 5.71 does not consider cost-benefit ratios. RG 5.71 requires the application of all its specified security controls to each CDA, and little discretion is allowed regarding the use of alternative, creative, cost-effective solutions. As a result, the compliance-based approach does not permit performance-based decisions that would divert resources from ineffective security controls toward measures that would provide much greater risk reductions.
- The only time that a licensee is required to perform an analysis of security controls for a CDA is when a required security control cannot be applied. This can limit creativity and flexibility in applying security controls. RG 5.71's compliance-based approach does not provide incentives for doing more to address pressing cybersecurity issues (Securicon 2020).

- RG 5.71 specifies that a digital asset that acts to protect a CDA also becomes a CDA. This circular logic can cause confusion in the evaluation process, dramatically expanding the number of CDAs at the licensee's facility, and unnecessarily complicating their cybersecurity program. If a CDA is defined by its ability to impact the design base function of a compromised critical system, how can the same be said of a digital asset used to protect the critical system?[30]
- Security controls often involve digital hardware or software that may contain their own vulnerabilities. One recent example of this is the SolarWinds attack detected in late 2020. The SolarWinds Orion platform monitors the health, security, and performance of a system's network. Investigators determined that an adversary infiltrated the supply chain of SolarWinds, inserting a backdoor into the product. As customers downloaded installation and update packages from SolarWinds containing the malware, the attackers were able to access the systems running the SolarWinds product(s). This example illustrates that the implementation of some security controls may introduce new vulnerabilities that attackers can exploit.[31]

Having a performance-based rule (10 CFR 73.54) supported by a compliance-based regulatory guide (RG 5.71) creates a mismatch. Compliance-based approaches are easy for regulators to assess and work in situations where the domain is understood and relatively static. However, these approaches do not fare well for problems like cybersecurity, where the domain is not well understood and the conditions are dynamic.

In contrast, performance- or risk-based approaches, like that described in NIST SP 800-37 (U.S. NIST 2018), are more difficult for regulators

[30] For example, assume a firewall has been installed to protect a critical system from an attack originating from a different connected system. If the firewall is de-energized by a cyberattack, is the critical system it is supposed to be protecting more or less secure? Interestingly, it may be more secure because all communication along the compromised attack pathway is halted, preventing the attacker from reaching the critical system. Further, if implementation of the firewall did impact the design-base function of the critical system, then a new, unanalyzed failure mode has been created that was not originally accounted for in the commission and acceptance of the system.

[31] https://www.cisecurity.org/solarwinds.

to inspect. However, these approaches may be more helpful and cost-effective for organizations because they encourage the licensees to:

- Explore new approaches to keep up with the evolving threats, vulnerabilities, and security technologies
- Prioritize their security efforts to focus resources on the most productive and cost-effective security controls for their facility
- Prioritize their security efforts to focus on the most at-risk systems and spend correspondingly less time and resources on those systems that pose low risks
- Eliminate excessive paperwork needed to document in detail why some security controls may not be applicable for specific devices and systems
- Connect cybersecurity and other business risks so that cybersecurity can be seen in the broader context of the facility's operation, as part of its risk-management program (Securicon, 2020).

Recognizing the limitations of a compliance-based approach to cybersecurity, the NRC is working on transitioning to an approach that adopts risk-based elements into its compliance-based program. In this regard, the NRC may be somewhat behind some other nations. For example, the United Kingdom already incorporates risk-based elements in its cybersecurity regulations.

7.2.4 Potential Risks from a Cyberattack

Cyberattacks may jeopardize the confidentiality, integrity, and availability of nuclear facility assets, systems, or networks. Confidentiality is protecting information from unauthorized access or disclosure (https://csrc.nist.gov/glossary/term/confidentiality). "Integrity" is defined as the "quality of a system reflecting the logical correctness and reliability of the operation of the system, the logical completeness of the hardware and software implementing the protection mechanisms, and the consistency of the data structures and occurrence of the stored data. Additionally, integrity includes protection against unauthorized modification or destruction of information" (U.S. NRC 2010). "Availability" is defined as "the property of being accessible and usable upon demand by an authorized entity" (International Atomic Agency [IAEA] 2011).

For information systems, the "confidentiality" of information is typically the most important thing to protect. However, for operational technology, integrity and availability of these control systems are typically more important than the confidentiality of their information (IAEA 2017).

When the confidentiality, integrity, or availability of a system at a nuclear facility is compromised, there may be significant consequences. These may involve:

- Impacts on worker health and safety—for example, from cyberattacks that manipulate control systems and result in an explosion or fire within the facility
- Impacts on public health and safety such as the release of radioactive or hazardous chemicals outside the facility owing to the cyber manipulation of plant systems, and radiological exposure resulting from the theft, diversion, or misuse of radiological materials
- Environmental impacts resulting from the release of radiological or hazardous materials to the environment fully or partly facilitated by a cyberattack
- Damage to the facility and equipment, requiring expensive replacements and repairs
- Economic impacts such as an extended shutdown of a nuclear facility with the resulting loss of revenue or facility productivity, payment of ransom to cyberattackers, or cyber theft of valuable intellectual property
- Public perception impacts, such as loss of public confidence in the nuclear facility, which could undermine public support for the continued operation of the facility or for new facility construction
- Regulatory impacts, making operation of the facility more difficult and expensive

Regulatory compliance might focus on activities to protect human health and safety and pay little attention to other potentially costly impacts for the nuclear facility, such as extensive downtime from facility operation. As a result, organizations operating nuclear facilities often need to take risk-based actions in their cybersecurity program that exceed regulatory requirements or address systems not covered by their regulator.

The existence of a vulnerability does not by itself increase the risk to the organization. Instead, risk increases if the existence of a vulnerability is combined with the existence of a threat actor capable of exploiting that vulnerability. Therefore, when a nuclear facility reviews its known vulnerabilities, it should seek to mitigate risk in the context of threat-actor capabilities.

There are three types of cybersecurity risk analysis:

1. Quantitative risk analysis
2. Qualitative risk analysis
3. Relative-quantitative or hybrid risk analysis.

The first two types of analysis are commonly discussed in the literature, but the third type is an evolving topic. Performing quantitative risk analysis involves probabilistic analysis. Most forms of quantitative risk analysis require at least the estimated values of the assets and probabilities pertaining to vulnerability exploration and impact.[32]

Because quantitative risk analysis requires extensive information, some of which may be difficult to quantify, a less intensive and more subjective qualitative risk analysis approach is often used. This often involves round-table discussion between subject matter experts (SMEs) using well-recognized cybersecurity frameworks. Examples of such frameworks are the NIST Cybersecurity Framework (CSF) and the U.S. Department of Energy's cybersecurity capability maturity model (C2M2).[33]

To minimize the subjectivity pertaining to qualitative risk analysis, researchers have been experimenting with methods to combine the best attributes of quantitative and qualitative approaches. This combination is often referred to as hybrid risk analysis. Hybrid models include:

1. C2M2- and CSF-driven hybrid risks analysis: The method uses the qualitative outcomes from frameworks such as C2M2/CSF

[32] More information on quantitative risk analysis can be found at https://resources.infosecinstitute.com/topic/quantitative-risk-analysis/#:~:text=It%20contains%20information%20about%20the,where%20EF%20is%20exposure%20factor.&text=ALE%20is%20calculated%20as%20follows,(once%20in%20two%20years.

[33] See https://www.nist.gov/cyberframework and https://www.energy.gov/ceser/energy-security/cybersecurity-capability-maturity-model-c2m2-program, respectively.

and transforms the outcomes to relative-quantitative values.[34] The quantities obtained are used to prioritize mitigations. This method reduces the financial cost of risk reduction.

2. Consequence-driven hybrid risk analysis: This method focuses on the potential consequences of exploiting a vulnerability and prioritizes the mitigation of such vulnerabilities based on their potential cost.[35]
3. Vulnerability-driven hybrid risk analysis: This method uses widely agreed-upon numerical factors associated with system-level vulnerabilities.[36] These numerical factors are defined under the common vulnerability scoring system (CVSS) and are assigned to all the discovered common vulnerabilities and exposures.[37]

After performing risk analysis, the nuclear facility should make risk management decisions. This involves determination of its risk tolerance and takes proactive actions based on the available resources and organizational constraints. Nuclear facilities can make risk management decisions to exceed minimum regulatory compliance because such decisions lower risks and reduce the likelihood of negative events/outcomes over the lifetime of the facility.

7.2.5 Defense and Response

Cybersecurity is a shared responsibility between nuclear facilities; their larger organizational entities such as companies; and government, including competent authorities, review boards, commissions, and other agencies. Effective cybersecurity involves addressing the vulnerabilities associated with people, processes, and technology. It also involves an appropriate integration with other types of security, including physical security and information security (IAEA 2011).

The key to effective cybersecurity is to take actions to deter, detect, delay, and deny attacks and to be resilient in the face of a cyberattack. All of these important capabilities should be part of an effective

[34] See https://www.sciencedirect.com/science/article/pii/S0167739X19307344.

[35] See https://patents.google.com/patent/US20210110319A1/en.

[36] See https://scholarspace.manoa.hawaii.edu/bitstream/10125/71455/0678.pdf.

[37] See https://www.first.org/cvss/ and https://cve.mitre.org/ for more.

cybersecurity program, and all have long been addressed in the physical security programs for nuclear facilities. In support of deterrence, warning signs, fences, other barriers, and the visible presence of security guards are used to deter physical attacks. The same holds for cybersecurity. Screen warning messages for those attempting to log into computer systems, video cameras monitoring access to key computers, and training that informs facility workers that computer usage is being monitored are examples of cybersecurity deterrence activities.

Detection of unauthorized or abnormal activities on computer systems is needed to trigger a defensive response. The physical security analogy is having watchmen in the towers of a castle. Thick walls are an excellent defense for a castle, but if you cannot spot a group of engineers digging a tunnel under your walls or see an approaching army before it starts scaling your walls, your defensive capabilities become ineffective. An effective cybersecurity program should detect malicious activity in a timely matter. Continuous monitoring programs, automated assessment of computer logs, network and host intrusion detectors, and other approaches support attack detection.

Delay is important because it allows time for defenders to respond to an attack and bring additional defensive measures online before the attackers can achieve their goals. Multiple defensive boundaries, honeypots to lure attackers and study their efforts, and other measures can delay an attack in addition to supporting other defensive goals.

Denial is the successful defense against a cyberattack. It means that the attackers are unable to achieve their goals and the nuclear facility is able to maintain safe and secure operations. A comprehensive and integrated cybersecurity program is needed to deny attacks.

The resilience capability is an often neglected but critically important approach for dealing with a cyberattack. Resilience includes both robustness, defined as the ability to resist a successful attack and to fail safely and securely if a system is affected, and recovery, defined as the ability to safely, quickly, and efficiently restore operations after an attack.

A key element in supporting cybersecurity is embodied in the concept of “defense-in-depth.” The U.S. NRC defines defense-in-depth as “an approach to security in which multiple levels of security and methods are deployed to guard against failure of one component or levels” (U.S. NRC 2010). Defense-in-depth is implemented primarily by combining a number of independent levels of protection that would have to be circumvented before the compromise of a computer system could occur. If one

level of protection or barrier were to fail, the subsequent level or barrier would remain to protect key assets. When properly implemented, defense-in-depth ensures that no single failure of people, processes, or technology could lead to an unacceptable compromise. It also reduces the likelihood that combinations of failures could give rise to a cyber incident. The independent effectiveness of the different levels of defense is a necessary element of defense-in-depth.

Defense-in-depth can be visualized as a series of concentric layers of security in which the vulnerabilities in a given layer are prohibited from existing within the adjacent layers. An attacker seeking to penetrate such a system would be forced to identify and exploit nonidentical vulnerabilities existing at each successive layer, as illustrated in Fig. 7.2.

One way to implement defense-in-depth is to use a graded, risk-based approach for the security of computer systems. A graded approach applies security measures proportional to the potential consequences of

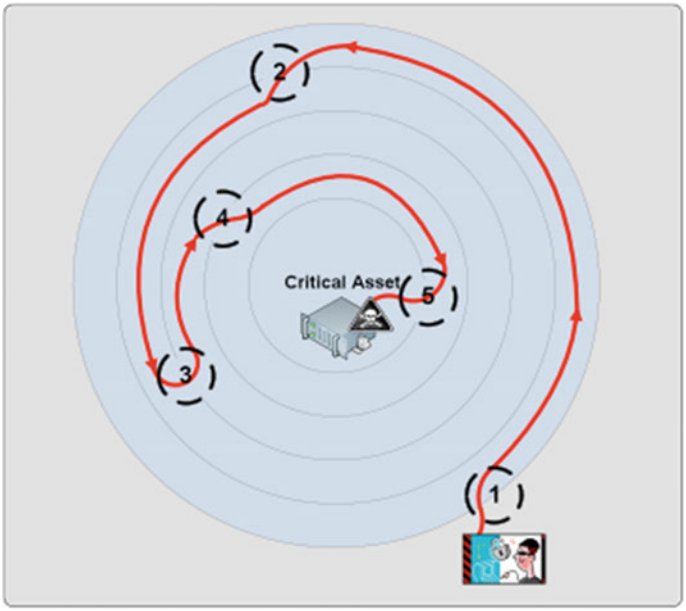

Fig. 7.2 Illustration of defense-in-depth. Multiple barriers must be overcome before the attacker can reach its objective

an attack. One practical implementation of the graded approach is to divide computer systems into zones, where graded protective principles are applied for each zone based on safety, operations, and business concerns (IAEA 2020).

Security levels are abstractions that define the degrees of protection required by various computer systems in a facility. Each level in a graded approach will require different sets of protective measures to satisfy the computer systems in all levels, while others are specific to a certain level(s). The security-level model allows easier assignment of protective measures to various computer systems, based on the categorization of the system and the definition of the set of protective measures appropriate to that level.

Zones are a logical and physical concept for grouping computer systems for administration, communication, and application of protective measures. The zone model allows computers with the same or similar importance concerning the safe and secure operation of the plant to be grouped together for administration and application of protective measures, as illustrated in Fig. 7.3 (Pacific Northwest National Laboratory 2015).

The application of a zone model should comply with the following guidelines:

- Each zone comprises systems that have similar importance for the facility's security and safety.
- Systems belonging to a zone have similar demands for protective measures.
- Different computer systems belonging to one zone build a trusted area for internal communication within that zone.
- Zone borders featured decoupling mechanisms for data flow built on zone-dependent policies.
- Zones can be partitioned into subzones to improve the configuration (Pacific Northwest National Laboratory 2015).

Because zones are comprised of systems with the same or comparable importance for facility safety and security, each zone can have a level assigned, indicating the protective measures to be applied for all computer systems in that zone. However, the relationship between zones and levels is not one-to-one; a level may have multiple zones assigned to it when

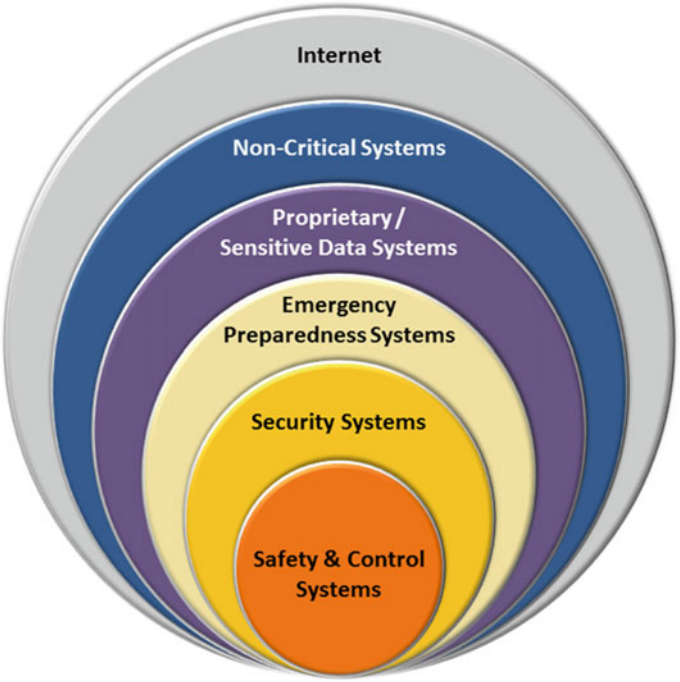

Fig. 7.3 Concentric security levels and the sorts of systems assigned to them

multiple zones require the same degree of protection (see Fig. 7.4). Zones are a logical and physical grouping of computer systems, while levels represent the degree of protection required. Each level consists of graded security requirements, such as limits on the communication permitted between different security levels. The graded approach assists the nuclear facility in directing the application of limited security resources to those zones and levels that perform the most critical functions (IAEA 2020).

Level 1 includes computer systems and assets vital to the safe and secure operation of the facility. Level 2 includes operational control systems and other systems that require a high level of security. Level 3 includes process and other real-time systems not required for operations. Level 4 includes technical data management systems used for maintenance or operation activity, such as work permit, work order, tag out, and documentation management. Level 5 includes systems not directly important

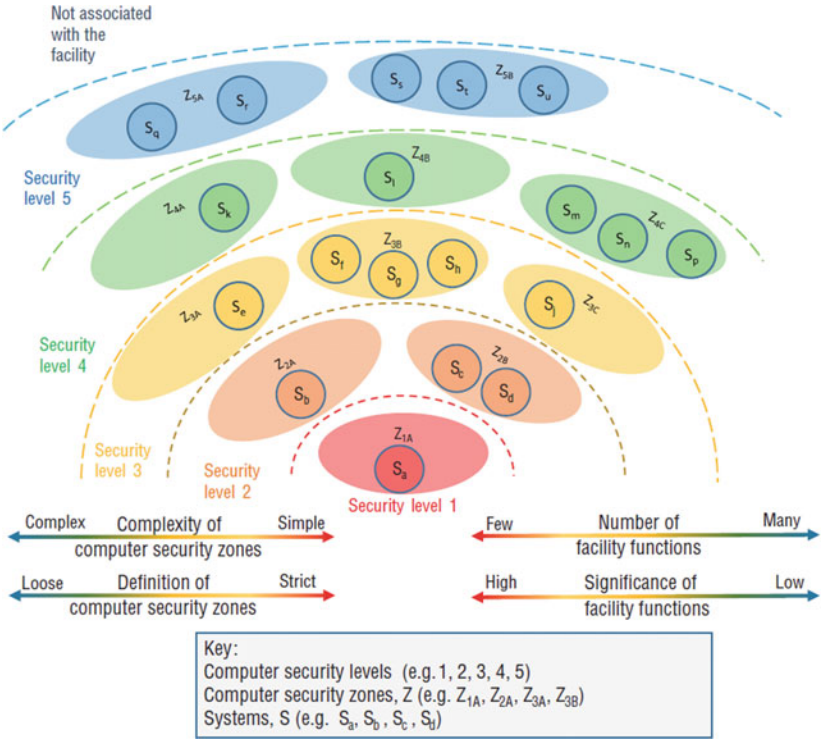

Fig. 7.4 Conceptual model of computer security level and zones (IAEA NR-T-3.30)

to technical control or operational purposes, such as business systems like email, calendars, and financial accounting (IAEA 2011).

Only one-way data flow is allowed from Level 1 to Level 2 and Level 2 to Level 3. Two-way communication is allowed between Levels 3, 4, and 5. However, the initiation of communications between levels can only occur from an inner level, with higher security, to an outer level, whistle-blower security. Data only flow from one level to other levels through

a device or devices that enforce security policy between each level (U.S. NRC 2010).[38]

Although cybersecurity threats are evolving and exhibiting increasing sophistication, so are security technologies that can provide defense-in-depth capabilities. In the past, communication between security levels was restricted by firewall devices that rely on complex rule sets to permit and prevent certain types of communications. Firewalls are only as effective as their technology and rule sets permit. A poorly implemented a firewall poses little challenge to a skilled attacker. New technologies, such as data diodes, can be more effective than firewalls. Data diodes are hardware-based devices that enforce unidirectional communication. Data flows only in a single pre-defined direction, from a more secure-level to a less secure-level network. They contain no physical mechanism that could permit communication in the reverse direction. The design of the data diode "makes it invulnerable to mismanagement by any user" or IT or OT system (Siemens 2020).

7.2.6 Supply-Chain Security

Supply-chain security has long been a concern of nuclear facilities and governing regulatory bodies. The IAEA notes that "Effective and efficient oversight of the global nuclear supply chain is crucial in both nuclear new build and operating nuclear facilities… In recent years, both the construction and operation of nuclear power plants have experienced difficulties related to their supply chains."[39]

An example of a breakdown in supply-chain security is the 2020 SolarWinds cyberattack. SolarWinds is a software company that primarily deals in systems management tools used by IT professionals. In 2020, the most widely deployed SolarWinds product was Orion, a network management system that monitored and managed computer systems for tens of thousands of customers. Attackers broke into the SolarWinds computer systems and inserted malware into Orion software. The corrupted software was deployed to customers as part of an update from SolarWinds servers. The malware opened a backdoor pathway into the infected

[38] Additional information on how to define security levels and implement security controls is provided in IAEA (2020).

[39] See https://www.iaea.org/topics/management-systems/management-of-the-nuclear-supply-chain.

computer systems. The attackers used this to install additional malware that collected and transmitted valuable internal data to the attackers (U.S. CISA 2021).

The United Kingdom (U.K.) National Cyber Security Centre proposed 12 principles for effective control and oversight of supply-chain security. These principles hold for a nuclear supply chain that includes hardware, firmware, and software products purchased from vendors or supplied by contractors. These principles cannot eliminate all supply-chain security risks, but their diligent application will reduce cybersecurity risks. The 12 principles are:

1. Understand what needs to be protected and why. This includes assessing the sensitivity of the information in the contract and understanding the value of the nuclear facility's information or assets that the suppliers will hold as part of the contract.
2. Know who the suppliers are and build an understanding of their security. This includes knowing the maturity and effectiveness of your suppliers' current security arrangements and what they expect from their subcontractors.
3. Understand the security risk posed by the supply chain. Assess the risks these arrangements pose to your information or assets, to the products or services to be delivered, and to the wider supply chain.
4. Communicate security needs to suppliers and contractors.
5. Set and communicate minimum security requirements for all suppliers and contractors.
6. Build security considerations into the contracting processes and require suppliers to do the same.
7. Follow the same security requirements when serving as a supplier and service provider to others.
8. Raise awareness of security within the supply chain.
9. Provide support for security incidents.
10. Build assurance activities into supply-chain management. This includes requiring suppliers to report their security performance, adhering to any cybersecurity risk management policies and processes, and accepting your right to audit suppliers and contractors to ensure they are meeting their cybersecurity performance requirements.
11. Encourage the continuous improvement of security within the supply chain.

12. Build trust with suppliers. This includes building strategic partnerships with key suppliers, sharing issues with them, and encouraging and valuing their input.[40]

A bill of materials (BOM) is an emerging concept to support supply-chain security, including cybersecurity for nuclear facilities. It is applicable for the purchase of digital assets, including hardware, firmware, and software. A software bill of materials (SBOM) is a "formal, machine-readable inventory of software components and dependencies, information about those components, and their hierarchical relationships" (U.S. National Telecommunications and Information Administration [NTIA] 2021). The primary purpose of an SBOM is to uniquely and unambiguously identify software components; document where each component was obtained; and characterize the relationship between components. At a basic level, an SBOM is akin to an ingredients list like one found on a box of food purchased at your local grocery store (U.S. NTIA 2021).

Commercially available firmware and software are directly purchased by nuclear facilities or installed on computers and other digital devices purchased by the facility to play an operational role in a nuclear facility. These software products often include third-party components, such as libraries, executables, or source code. If nuclear facilities don't know what components are in software they are purchasing, it is extremely difficult to identify vulnerabilities or determine if the software contains a component that comes from a potential adversary. This makes it extremely difficult for a nuclear facility to determine the level of risk associated with using acquired software. This lack of transparency increases cybersecurity risks and can result in unexpected costs during a product's operational life cycle (U.S. NTIA 2020).

Given the significance of this problem, guidance is being prepared to help organizations identify the components in hardware and software, determine their purpose and where they came from, and evaluate the cybersecurity risks associated with their use.

[40] See https://www.ncsc.gov.uk/collection/supply-chain-security.

7.2.7 *Assessing Cybersecurity*

Assessment and auditing play a key role in cybersecurity programs. Assessment is "the testing or evaluation of policies, procedures, or controls to determine the extent to which the policies, procedures, or controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the cybersecurity requirements" (U.S. NRC 2010). Audits are conducted by the competent authority or other government or industry regulator to determine whether requirements are being met. Deficiencies are reported, and facility actions are monitored until the issue is resolved. In some cases, severe penalties can be imposed for failure to meet requirements.[41]

Auditors will typically conduct checklist-based inspections to assess regulatory compliance. Nuclear facilities and their governing organizations will want to self-assess their performance against regulatory requirements. Still, they should also perform risk-based assessments to implement and maintain a cybersecurity program that meets regulatory requirements and protects the facilities against undue operational and business disruptions that are not covered by regulations.

U.S. NUREG/CR-6847 was specifically designed for cybersecurity self-assessments of nuclear facilities. The method outlined in NUREG/CR-6847 provides a systematic and phased approach that enables organizations to conduct a thorough assessment of cybersecurity at their respective facilities to understand their relative cybersecurity posture. While the focus of the assessment method concentrates on systems associated with safety, security, and emergency preparedness, it can also be extended to other systems within a nuclear facility. These include operational control systems associated with secondary or balance-of-plant operation, traditional IT systems related to business functions, and systems related to business continuity.

The NUREG/CR-6847 assessment method allows the users a fair amount of latitude in the selection of tools and techniques that work best for their specific needs. Completed assessments may be used to support or validate the selection of security controls to mitigate cyber threats as well as demonstrate compliance with established regulations. The assessment method can be incorporated as part of the organization's ongoing cybersecurity program.

[41] See https://www.nrc.gov/insp-gen/auditpro.html.

The method begins with the formation of a multidisciplinary assessment team and continues with the following six steps:

1. Examine facility-wide cybersecurity practices. In this stage, the assessment team gathers information on the facility's cybersecurity policies, procedures, and practices. Information is also gathered on facility resources that can play a role in the cybersecurity of critical systems.
2. Identify critical systems and assets to be assessed. These will include systems associated with safety, security, and emergency preparedness. Other systems important to facility operation may also be assessed. These systems are then analyzed and decomposed by the team to understand and identify the digital assets that comprise the design base function of the system. An initial consequence analysis for each identified critical system or asset is performed to determine whether the system and facility's potential consequences could compromise confidentiality, integrity, or availability.
3. Conduct tabletop reviews and validation testing. In this stage, the team works with various facility personnel responsible for designing, operating, and maintaining identified critical systems and assets. Validation involves physical inspections (walk-downs) and electronic testing of critical systems.
4. Conduct assessments of susceptibility. The team uses tabletop reviews and validation testing results to assess each critical system and asset's susceptibility to cyber exploitation. Pathway analysis is used to understand the various vectors of attack that may exist for the system. Both direct and indirect pathways of compromise are considered. The product of this stage is an estimate of the overall susceptibility level for each critical system and asset.
5. Conduct risk assessment activities. The team reassesses the initial consequence analyses that were performed in Stage 2 and uses these results in conjunction with the results of susceptibility assessments to estimate the risks of cyber exploitation for each identified critical system and asset.
6. Conduct risk management activities. In this stage, the team identifies and characterizes potential new security controls that could be implemented to enhance cybersecurity. A cost–benefit analysis is performed to identify those countermeasures that maximize adequate protection and minimize risk to the operation. Effective

risk management options and recommendations are prepared for senior facility management approval and implementation (U.S. NRC 2004).

The NUREG/CR-6847 has been successfully applied at nuclear facilities, such that those applying the method have typically performed at the top of their class during audits by their competent authority.

7.2.8 Summary and Conclusions

The threat of cyberattacks is a growing concern for governments, industry, and the public. Effective cybersecurity programs are needed to secure all types of critical infrastructure, including nuclear facilities. As leaders and innovators in cybersecurity, the U.S. and India must support nuclear cybersecurity programs and provide impactful nuclear cybersecurity guidance in their respective countries. The U.S. and India should work together to support and assist other countries in developing and implementing appropriate nuclear cybersecurity programs. This effort can involve the publication of technical guidance documents, the presentation of training courses, the development and marketing of cybersecurity technologies, and the implementation of effective supply-chain security programs.

Risk assessment and management should go beyond simple compliance activities to appropriately protect nuclear facilities from cyberattack. In addition to the human health and environmental concerns, nuclear facilities should consider the cybersecurity risks associated with potential damage to their facility and equipment, economic impacts, public perception impacts, and the governmental response to an attack—consequences that are generally not factored into the compliance requirements issued by the competent authority or other regulatory agencies. Models and tools exist to help nuclear facilities evaluate their risks and guide them in making effective risk management decisions. These include simple qualitative models, more sophisticated quantitative models, and hybrid approaches that can assist facilities in characterizing risks and making risk-based and cost-effective cybersecurity decisions.

Effective cybersecurity involves addressing the vulnerabilities associated with people, processes, and technology. It also involves an appropriate integration with other types of security, including physical security and information security. The key to effective cybersecurity is to take actions

to deter, detect, delay, and deny attacks and to be resilient in the face of a cyberattack. All these important capabilities are not new for nuclear facilities—they should already be part of mature physical security programs.

One key design consideration for cybersecurity is to employ defense-in-depth—a graded, risk-based approach to secure computer systems. This involves categorizing computer systems into zones, where graded protective principles are applied for each zone based on the required level of security given safety, operations, and business concerns (IAEA 2020).

Supply-chain security has long been a concern of nuclear facilities and governing regulatory bodies. The UK National Cyber Security Centre proposes 12 principles for effective control and oversight of supply-chain security. These principles hold for a nuclear supply chain that includes hardware, firmware, and software products purchased from vendors or supplied by contractors. These principles cannot eliminate all supply-chain security risks, but their diligent application will reduce cybersecurity risks.

A bill of materials is an emerging concept to support supply-chain security, including cybersecurity for nuclear facilities. Its primary purpose is to uniquely and unambiguously identify components, document where each component was obtained, and characterize the relationship between components.

Assessment and auditing play a key role in cybersecurity programs. Auditors will typically conduct checklist-based inspections to assess regulatory compliance. Nuclear facilities and their governing organizations will want to self-assess their performance against regulatory requirements and assess their ability to protect their facilities from undue operational and business disruptions that are not covered by regulations. The NRC has developed a method (U.S. NRC 2004) that can assist nuclear facilities in conducting cybersecurity self-assessments.

References

"Addressing Cyber-Nuclear Security Threats," *Nuclear Threat Initiative*, Accessed June 29, 2021. https://www.nti.org/about/projects/addressing-cyber-nuclear-security-threats/.

Baylon, Caroline with Roger Brunt and David Livingstone, "Cyber Security at Civil Nuclear Facilities: Understanding the Risks," *Chatham* House, September 2015, iv. https://www.nonproliferation.eu/wp-content/uploads/2019/11/20151005CyberSecurityNuclearBaylonBruntLivingstoneUpdate.pdf.

Bedi, R.S., "NTRO: India's Technical Intelligence Agency," *Indian Defence Review*, April 23, 2015. http://www.indiandefencereview.com/spotlights/ntro-indias-technical-intelligence-agency/.

Bhaskar, Utpal, "India Confirms Malware Attack at Kudankulam Nuclear Power Plant," *Mint*, updated November 20, 2019. https://www.livemint.com/news/india/india-confirms-malware-attack-at-kudankulam-nuclear-power-plant-11574262777163.html.

"CERT-In Annual Report (2019)," Indian Computer Emergency Response Team (CERT-In), Ministry of Electronics & Information Technology (MeitY) Government of India, Accessed June 28, 2021. https://cert-in.org.in/.

"Computer and Information Security," International Atomic Energy Agency, Accessed June 29, 2021. https://www.iaea.org/topics/computer-and-information-security.

"Computer Security of Instrumentation and Control Systems at Nuclear Facilities," IAEA Nuclear Security Series No. 33-T, 2018, 2. https://www-pub.iaea.org/MTCD/Publications/PDF/P1787_web.pdf.

"Cyber and Nuclear Security," *Chatham House*, Accessed June 28, 2021. https://www.chathamhouse.org/about-us/our-departments/international-security-programme/cyber-and-nuclear-security.

"Cyber Capabilities and National Power: A Net Assessment," International Institute for Strategic Studies, June 2021, 134. https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power.

De Groot, Juliana, "What Is Cyber Security? Definition, Best Practices & More," *Digital Guardian*. https://digitalguardian.com/blog/what-cyber-security.

Decker, Debra, Rauhut, Kathryn, Kutchesfahani , Sara Z. and Connolly, Erin, "Nuclear Cybersecurity: Risks and Remedies," *Fissile Materials Working Group and Stimson Center*, March 2019. https://armscontrolcenter.org/wp-content/uploads/2019/03/FMWG_CyberReport_webready.pdf.

"Design Basis Threat," International Atomic Energy Agency, Accessed June 29 2021. https://www.iaea.org/topics/security-of-nuclear-and-other-radioactive-material/design-basis-threat.

Giaurov, Vesselin, "The Cyber-Nuclear Security Threat: Managing the Risks," *Vienna Center for Disarmament and Non-proliferation,* January 2017. http://large.stanford.edu/courses/2017/ph241/bunner2/docs/giaurov_2017.pdf.

Greenwald, Glenn and Saxena, Shobhan, "India among top targets of spying by NSA," *The Hindu,* September 23, 2013. https://www.thehindu.com/news/national/india-among-top-targets-of-spying-by-nsa/article5157526.ece.

Hemsley, Kevin E. and Dr. Fisher, Ronald E., *History of Industrial Control System Cyber Incidents*. INL/CON-18-44411-Revision-2. Authors: Kevin Hemsley and Ronald Fisher. Idaho Falls, Idaho: Idaho National Laboratory, 2018. https://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0054.html.

"ICERT," Ministry of Electronics & Information Technology (MeitY) Government of India, Accessed June 28, 2021. https://www.meity.gov.in/content/icert.

"India Country Page" 2020 NTI Nuclear Security Index, Nuclear Threat Initiative, Accessed 28 June 2021. https://www.ntiindex.org/wp-content/uploads/2020/06/India.pdf.

India Department of Atomic Energy, "Cyber Attack on KKNPP." Press Information Bureau, November 20, 2019. https://pib.gov.in/Pressreleaseshare.aspx?PRID=1592498.

"India Subindicators Detail", 2020 NTI Nuclear Security Index, Nuclear Threat Initiative, Accessed 28 June 2021. https://www.ntiindex.org/subindicator/?data_country=IN&data_indicator=INDICATOR_SECURITY_6&data_model=2020_NSI_T1&year=2020.

International Atomic Energy Agency, *Computer Security Aspects of Design for Instrumentation and Control Systems at Nuclear Power Plants*. Nuclear Energy Series No. NR-T-3.30. Vienna, Austria: International Atomic Energy Agency, 2020.

International Atomic Energy Agency, *Computer Security at Nuclear Facilities*. Technical Guidance Reference Manual, Nuclear Security Series No. 17. Vienna, Austria: International Atomic Energy Agency, 2011.

International Atomic Energy Agency, *Computer Security for Nuclear Security*. Draft Implementing Guide, NST045. Vienna, Austria: International Atomic Energy Agency, 2017.

Kesler, Brent, "The Vulnerabilities of Nuclear Facilities to Cyber Attack," *Stanford Strategic Insights,* 2011.

Laskar, Rezaul H., "India, Japan Finalise Key Cyber-Security Deal to Boost Cooperation on 5G, AI," *Hindustan Times*, October 7, 2020. https://www.hindustantimes.com/india-news/india-japan-finalise-key-cyber-security-deal-to-boost-cooperation-on-5g-ai/story-WCMa9En3NFPkQMWClGNFJI.html.

Leverett, Éireann, "Cyber Insurance for Civil Nuclear Facilities: Risks and Opportunities," *Chatham House*, May 8, 2019.

Markey, Edward J., "Infection of the Davis Besse Nuclear Plant by the 'Slammer' Worm Computer Virus—Follow-up Questions: EDO Principal Correspondence Control," 2003. https://www.nrc.gov/docs/ML0329/ML032970134.pdf.

"Mission," National Critical Information Infrastructure Protection Centre, Government of India. https://nciipc.gov.in/.

Mohan, Pulkit, "Cyber Security in India's Nuclear Systems," *ORF Issue Brief No. 412*, October 2020, Observer Research Foundation.

"National Cyber Security Policy-2013," Ministry of Electronics & Information Technology (MeitY) Government of India, July 2013, 3. https://www.meity.gov.in/writereaddata/files/downloads/National_cybersecurity_policy-2013%281%29.pdf.

Nuclear Energy Institute, "Cyber Security Program for Power Reactors." NEI 04-04 Rev. 1. Washington, DC, USA, 2004.

"Nuclear Security in India," Ministry of External Affairs Government of India, Accessed June 28, 2021. https://www.mea.gov.in/Images/pdf/Brochure.pdf.

Pacific Northwest National Laboratory, "Cyber Security Programs for Nuclear Facilities. U.S. Nuclear Regulatory Commission Office of Nuclear Regulatory Research. Draft Guide 5022." Washington D.C. USA, 2008.

Pacific Northwest National Laboratory, "Cyber Security Self-Assessment Method for U.S. Nuclear Power Plants." U.S. Nuclear Regulatory Commission Office of Nuclear Security and Incident Response NUREG/CR-6847. Washington. DC, 2004. https://adamswebsearch2.nrc.gov/webSearch2/main.jsp?AccessionNumber=ML15111A054.

Pacific Northwest National Laboratory, "How to Implement Security Controls for an Information Security Program at CBRN Facilities." Pacific Northwest National Laboratory. Richland, WA, USA, 2015. https://www.pnnl.gov/main/publications/external/technical_reports/PNNL-25112.pdf.

Palani, Kartik and Anantharaman, Prashant, "What happened when the Kudankulam nuclear plant was hacked—and what real danger did it pose?," *Scroll India*, November 20, 2019. https://scroll.in/article/943954/what-happened-when-the-kudankulam-nuclear-plant-was-hacked-and-what-real-danger-did-it-pose.

Pickering, Susan Y. and Davies, Peter B., "Cyber Security of Nuclear Power Plants: US and Global Perspectives," *Georgetown Journal of International Affairs*, January 22, 2021. https://gjia.georgetown.edu/2021/01/22/cyber-security-of-nuclear-power-plants-us-and-global-perspectives/.

"Press Release," Kudankulam Nuclear Power Project, Nuclear Power Corporation of India Ltd., October 29, 2019. https://i0.wp.com/www.opindia.com/wp-content/uploads/2019/10/Kudankulam-Nuclear-Power-Plant-statement.jpg?ssl=1.

Protection of Digital Computer and Communication Systems and Networks, 10 C.F.R. 73.54, 2009. https://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0054.html.

Rajagopalan, Rajeswari Pillai, "Nuclear Security in India," *Observer Research Foundation*, 2015. https://www.orfonline.org/wp-content/uploads/2015/02/NUCLEAR_SECURITY_IN_INDIA.pdf.

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

Securicon, "Why a Compliance-Based Approach to Cybersecurity Is Not Enough," July 27, 2020. https://www.securicon.com/why-a-compliance-based-approach-to-cybersecurity-is-not-enough/#:~:text=Compliance%20is%20siloed%20%E2%80%93%20a%20compliance,t%20communicate%20with%20one%20another.

Siemens, "Protecting OT Networks: Data Diodes vs Firewalls," 2020. https://www.mobility.siemens.com/global/en/portfolio/rail/automation/reports/difference-data-diode-and-firewall.html.

"Strengthen Cybersecurity at Nuclear Facilities," *NTI Nuclear Security Index*, Accessed June 28, 2021. https://www.ntiindex.org/recommendation/recommendation-4-2/

"Terminology Used in Nuclear Security Guidance," IAEA Nuclear Security Glossary, August 2020, 22. https://www.iaea.org/sites/default/files/21/06/nuclear_security_glossary_august_2020.pdf.

"The Governments of the United States and India held the Fifth U.S.-India Cyber Dialogue in New Delhi (September 28, 2016)," Ministry of External Affairs, Government of India, September 30, 2016. https://www.mea.gov.in/press-releases.htm?dtl/27448/The+Governments+of+the+United+States+and+India+held+the+Fifth+USIndia+Cyber+Dialogue+in+New+Delhi+September+28+2016.

U.K. National Cyber Security Centre, "Weekly Threat Report 17th October 2016." The UK National Cyber Security Centre, 2016. https://www.ncsc.gov.uk/report/weekly-threat-report-17-october-2016.

U.S. Cybersecurity & Infrastructure Security Agency, "Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations." Department of Homeland Security, Alert: AA20-352A. Washington, DC, USA, 2021. https://us-cert.cisa.gov/ncas/alerts/aa20-352a.

U.S. Cybersecurity & Infrastructure Security Agency, "Primary STUXNET Advisory." Department of Homeland Security ICS Advisory: ICSA-10-272-01. Washington, DC, USA, 2010. https://us-cert.cisa.gov/ics/advisories/ICSA-10-272-01.

U.S. Cybersecurity & Infrastructure Security Agency, "Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors." Last updated March 16, 2018. Department of Homeland Security, Alert: TA18-074A. Washington, DC, USA, 2018. https://us-cert.cisa.gov/ncas/alerts/TA18-074A.

U.S. Cybersecurity & Infrastructure Security Agency, "What is Cybersecurity?" Last updated November 14, 2019. Department of Homeland Security, Security Tip: ST04–001. Washington, DC, USA, 2019. https://us-cert.cisa.gov/ncas/tips/ST04-001.

U.S. National Institute of Science and Technology. 2007. "Recommended Security Controls for Federal Information Systems." NIST Special Publication (SP) 800-53 Rev 2. Gaithersburg, MD, USA. https://csrc.nist.gov/publications/detail/sp/800-53/rev-2/archive/2007-12-19.

U.S. National Institute of Science and Technology. 2018. *Risk Management Framework for Information Systems and Organizations: A System Life Cycle*

Approach for Security and Privacy. NIST Special Publication 800-37 Revision 2. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf.

U.S. National Telecommunications and Information Administration. 2020. "Software Bill of Materials (SBOM)." Washington D.C., USA. https://www.ntia.gov/files/ntia/publications/sbom_overview_20200818.pdf.

U.S. National Telecommunications and Information Administration. 2021. "Software Bill of Materials (SBOM) at a Glance." Washington D.C., USA. https://www.ntia.gov/files/ntia/publications/sbom_at_a_glance_apr2021.pdf.

U.S. Nuclear Regulatory Commission Office of Nuclear Reactor Regulation. 2007. "Effects of Ethernet-based, Non-safety Related Controls on the Safe and Continued Operation of Nuclear Power Stations." Nuclear Regulatory Commission, NRC Information Notice: 2007-15. Rockville, Maryland, USA. https://www.nrc.gov/reading-rm/doc-collections/gen-comm/info-notices/2007/in200715.pdf.

U.S. Nuclear Regulatory Commission Office of Nuclear Regulatory Research. 2006. "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants." Regulatory Guide 1.152 Rev. 2. Rockville, Maryland, USA. https://www.nrc.gov/docs/ML0530/ML053070150.pdf.

U.S. Nuclear Regulatory Commission. 2001. "Interim Safeguards and Security Compensatory Measures for Nuclear Power Plants". Security Order EA-02–026. Rockville, Maryland, USA.

U.S. Nuclear Regulatory Commission. 2002. "Design Basis Threat for Radiological Sabotage. Security Order EA-03-086. Rockville, Maryland, USA.

U.S. Nuclear Regulatory Commission. 2004. *Cyber Security Self-Assessment Method for U.S. Nuclear Power Plants*. NUREG/CR-6847. Prepared by Pacific Northwest National Laboratory (Lead author: CS Glantz) for the Nuclear Regulatory Commission, Rockville, Maryland, USA.

U.S. Nuclear Regulatory Commission. 2007. "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems". Branch Technical Position (BTP) 7-14 Rev. 5. Rockville, Maryland, USA. https://www.nrc.gov/docs/ML0706/ML070670183.pdf.

U.S. Nuclear Regulatory Commission. 2010. *Cyber Security Programs for Nuclear Facilities*. Regulatory Guide (RG) 5.71. Rockville, Maryland: Nuclear Regulatory Commission. https://www.nrc.gov/docs/ML0903/ML090340159.pdf.

U.S. Nuclear Regulatory Commission. 2011. "Advisory Committee on Reactor Safeguards Digital Instrumentation and Control Systems." Official Transcript of Proceedings, February 23, 2011. Regulatory Commission. Rockville, Maryland, USA.

Unal, Beyza and Lewis Patricia, "Cybersecurity of Nuclear Weapons Systems: Threats, Vulnerabilities and Consequences," *Chatham House International Security Department*, January 2018. http://www.menacs.org/wp-content/uploads/2018/01/Beyza_Cybersecurity-nw.pdf.

Van Dine, Alexandra, Assante, Michael and Stoutland, Page, Ph.D., "Outpacing Cyber Threats: Priorities for Cybersecurity at Nuclear Facilities," *Nuclear Threat Initiative*, 2016. https://media.nti.org/documents/NTI_CyberThreats__FINAL.pdf.

World Nuclear Association, Accessed June 28, 2021. https://world-nuclear.org/information-library/country-profiles/countries-g-n/india.aspx.

Index

S. P. Kapur et al. (eds.), *The Challenges of Nuclear Security*, Initiatives in Strategic Studies: Issues and Policies,
https://doi.org/10.1007/978-3-031-56814-5