

Assessing Military and Terrorist Threats against Indian Civilian Nuclear Facilities

Charles D. Ferguson
Fellow for Science and Technology
Council on Foreign Relations

Growing Dangers

While the controversial U.S.-India nuclear deal has focused attention on the potential for sparking nuclear war or an arms race in East or South Asia, little or no attention has been paid to how the deal's implementation might increase the threats of terrorism and military attack against Indian nuclear facilities. These threats could grow in three ways. First, the deal can facilitate a substantial expansion of India's plutonium stockpile in the civilian and military sectors. Plutonium, a toxic and fissile material, could, in the hands of skilled terrorists, fuel improvised nuclear devices—crude but devastating nuclear bombs—or radiological dispersal devices—one type of which is popularly called a “dirty bomb.”¹ Second, the deal can spur expansion of India's civilian nuclear facilities, thereby increasing the number of targets for terrorist or military attacks. Third, the deal brings India into much closer alignment with the United States. This alliance has already stirred animosity toward India from Osama bin Laden, the leader of al Qaeda. Moreover, closer Indo-American relations could also breed resentment in Pakistan and result in a more vulnerable India, especially in armed conflict involving India and Pakistan.

Al Qaeda-affiliated operatives may have launched or helped perpetrate the July 11, 2006, terrorist bombings in Mumbai. Soon after these attacks, the U.S. Embassy in New Delhi issued a warning about possible terrorist assaults against Indian government facilities, including nuclear sites. In response, New Delhi boosted security at its nuclear complex by early August.² Perhaps security requires further strengthening. For instance, in late August, villagers near the Kakrapar nuclear facility reported seeing two men armed with automatic weapons inside a prohibited area, but still outside the most sensitive area of the facility.³

India's extensive nuclear complex both in the civilian and military sectors already presents a target-rich environment. Moreover, India has ambitious plans for a major expansion of this complex. This expansion could increase the risks of accidents, attacks, or sabotage. Without adequate quality controls in training, the risk of accidents increases, and even with high quality of training, a rapid influx of workers into the nuclear program increases the probability of saboteurs entering the program.

¹ This chapter does not analyze the radiological dispersal device or dirty bomb threat in India. For a recent report that assesses that threat, see Kishore Kuchibhotla and Matthew McKinzie, “Nuclear Terrorism and Nuclear Accidents in South Asia,” in Michael Krepon and Ziad Haider, editors, *Reducing Nuclear Dangers in South Asia*, Henry L. Stimson Center Report No. 50, January 2004.

² “India's N-Plants Turned into Fortresses after U.S. Alert,” Islamic Republic News Agency, August 14, 2006.

³ “India Nuclear Plant Combed for Armed Intruders,” Gulf Daily News, August 23, 2006.

Shaken by sectarian strife and terrorism for many decades, India resides in one of the most violence prone regions of the world. Jihadist groups have caused much of this violence. Some of these groups have ties to al Qaeda, which has considered using nuclear and radiological terrorism. Pakistan has sponsored terrorist groups to further its aims in the separatist region of Jammu and Kashmir and could consider using such groups as proxies in a military attack against other regions of India, including those containing nuclear facilities.

The focus here is on the military and terrorist threats to India's civilian nuclear facilities, but because Indian civilian and military nuclear programs are intertwined, the analysis will consider significant areas of overlap notably the growing plutonium stockpiles that can fuel both programs. First, this chapter examines India's civilian nuclear infrastructure, assessing potential vulnerabilities to attack. Second, the chapter discusses terrorism and sectarian violence involving India and whether this violence is likely to be directed against nuclear facilities. Finally, after reviewing efforts India has reportedly taken to protect these facilities, the chapter recommends further urgently needed security measures.

In sum, the major recommendations are that India should:

- Ensure that the different modes of a terrorist or military attack are fully considered and continually evaluated in assessing the safety and security of its nuclear facilities;
- Separate more of its civilian nuclear facilities, including breeder reactors, from connections to the military program to reduce the target profile of these facilities and to help remove them from the shroud of secrecy surrounding the military program;
- Work with China and Pakistan toward a fissile material cap to limit the amount of plutonium potentially available to terrorists;
- Develop cooperative nuclear security by sharing and implementing best practices with the United States, the International Atomic Energy Agency, and other partners;
- Apply to new facilities and retrofit to the extent possible in existing facilities sabotage-resistant safety systems as well as additional safety and security measures such as extra diesel generators and relatively low-cost fortifications around spent fuel pools and vulnerable buildings in addition to active and passive air defenses for critical nuclear sites; and
- Create a more transparent and self-critical civilian nuclear infrastructure that would empower an independent regulatory agency and would continually be vigilant about insider threats.

India's Civilian Nuclear Infrastructure

Understanding the potential vulnerabilities of India's civilian nuclear program to military or terrorist attack first requires understanding the vision behind the program. For decades, India has envisioned a three-pronged approach to developing its civilian nuclear infrastructure. First, it would exploit its limited indigenous deposits of uranium to fuel thermal reactors. These reactors are called "thermal" because they rely on slowed down neutrons, or neutrons possessing thermal or relatively low energies, to power the nuclear

reactions in these reactors' cores. Second, India would harvest the plutonium produced in the thermal reactors to make fuel for fast breeder reactors. The "harvesting" is called reprocessing, which uses chemical processes to extract plutonium from highly radioactive spent nuclear fuel. Fast reactors use high speed, or high-energy, neutrons to power the reactions. Breeder reactors can produce, or breed, more plutonium fuel. Third, India wants to create a fleet of thorium-reactors that would use the fertile element thorium to produce uranium-233, a fissile material that can power reactors. India is estimated to possess one-third of the world's deposits of thorium.

Many aspects of this three-pronged plan can increase India's risk of militaries or terrorists targeting civilian nuclear assets. The sheer complexity of the enterprise could complicate management of ensuring adequate security throughout the program. The different reactor designs, for instance, would require detailed attention to differences in vulnerability to various modes of attack. For instance, one type of reactor might have adequate protection against attacks from the air because the reactor design might have a strong containment building around the reactor core. In contrast, a different design might have a weaker containment structure, but might present vulnerabilities to truck bombs. Protecting against these differing vulnerabilities demands a highly technically trained guard force as well as a regulatory agency that is vigilantly and continually conducting rigorous security tests, probing for and correcting any weaknesses.

The second prong involving bulk processing and handling of tons of separated plutonium can increase the risk of diversion of this bomb-usable material. In contrast, keeping plutonium embedded in spent nuclear fuel provides a highly radioactive and lethal barrier against theft. In the event of an accident or an attack that results in radioactivity release to the environment, reactors fueled with plutonium could cause greater harm to health than reactors fueled with uranium because plutonium is a much more toxic material.⁴

The third prong, if not managed properly, could raise the risk of uranium-233, a fissile material that can power the easiest to make nuclear bomb, a gun-type device, falling into the wrong hands. The thorium cycle produces uranium-232, which decays to highly radioactive daughter products. Even relatively small concentrations of uranium-232 and its daughters can emit lethal doses of gamma radiation.

Because U-232 and U-233 have essentially the same chemical properties, separating the one isotope from the other is very difficult. One method involves limiting the daughter products of U-232 by chemically removing thorium and other daughter products from the uranium mixture. However, within two years after this chemical separation, the buildup of highly radioactive daughter products can lead to a lethal dose in 20 minutes to a person within one meter of a critical mass of uranium-233. This assumes that uranium-232 is present at least to the level of 0.1 percent. Another method is to remove U-232 by using laser isotope separation (LIS) methods. Employing powerful lasers, LIS selectively excites and ionizes uranium-233 to separate it from uranium-232. India's Department of Atomic Energy (DAE) has stated that its long-term ambition is to use LIS to remove enough U-232 to reach a level of a few ppm. At this level, workers could handle a mixture of U-233 and U-232 for tens to hundreds of hours without

⁴ Edwin S. Lyman, "Public Health Risks of Mixed Oxide Fuels," *Science and Global Security*, Vol. 9, 2001.

exceeding their annual occupational radiation exposure doses. But terrorists could also safely handle such a mixture.

A uranium-233 mixture can be de-natured to make it less bomb-usable. To do that, sufficient U-238 can be mixed into the mixture to greatly increase the critical mass needed to make a bomb out of the mixture. This isotopic denaturing depends on the reactor design as well as the reprocessing method used with the U-233 mixture. Nuclear physicists Jungmin Kang and Frank von Hippel have concluded, "The proliferation resistance of thorium fuel cycles depends very much upon how they are implemented."⁵ For instance, they found that pressurized light water reactors fueled with a mix of low enriched uranium and thorium fuel at high burnup produce high U-232 contamination levels. Thus, this type of usage is commensurate with proliferation resistance. In contrast, heavy water reactors operated in a low burnup mode can produce low concentrations of U-232.

India has plans to develop an advanced heavy water reactor using the thorium/uranium-233 cycle. Presently, India has been operating since 1996 the Kamini research reactor on uranium-233 fuel. This reactor has a modest power rating of 30 kWth. Notably, the Kamini reactor is located at the Bhabha Atomic Research Center (BARC), which is part of the Indian nuclear weapons complex. Like the plutonium program, the thorium program blends into India's weapons program.

By design, the Indian civilian and military nuclear programs are intertwined. An attack on India's military program would also likely adversely affect India's civilian program and vice versa. The analysis turns to an examination of the different components of India's civilian nuclear program and the different potential modes of attack or sabotage against the program.

Indian Nuclear Facilities

India has several types of nuclear facilities, including nuclear power plants, plutonium production reactors, research reactors, spent fuel storage areas, high-level radioactive waste storage facilities, and reprocessing plants.

Nuclear power plants

Despite the ambitious three-pronged plan, India has struggled to build even a small fraction of the nuclear power plants envisioned.⁶ Once the 540-MWe Tarapur-3 reactor supplies power to the grid, expected to occur in mid-2006, India will have about 3,900 MWe of installed nuclear power capacity.⁷ Under the optimistic planning scenario, New Delhi wants 11,000 MWe by 2010 and 29,000 MWe by 2020. Of the 29,000 MWe, 20,000 MWe are intended to come from indigenous development. It is uncertain whether India will follow through on acquiring 9,000 MWe of power from foreign sources. New

⁵ Jungmin Kang and Frank N. Von Hippel, "U-232 and the Proliferation-Resistance of U-233 in Spent Fuel," *Science & Global Security*, Volume 9, 2001, pp. 1-32.

⁶ A complete list of the currently operating Indian nuclear power plants and other relevant information can be found at Nuclear Power Corporation of India, Ltd., <http://www.npcil.nic.in/>

⁷ Sunil Saraf, "Npcil Takes Tarapur-3 Critical, Foresees Early Completion," *Nucleonics Week*, May 25, 2006, p. 7.

Delhi apparently put forward that figure prior to the March meeting between Prime Minister Singh and President Bush to help sweeten the U.S.-India nuclear deal.⁸ However, for many years, India has announced plans for 20,000 MWe of nuclear power by 2020, and with the soon-to-be-completed two Russian VVER-1000 reactors, imported reactors will produce at least 2,000 MWe of the planned increase in nuclear power capacity. India's Nuclear Power Corporation has sent dozens of engineers to be trained in Russia to operate the VVER-1000 reactors.⁹ New Delhi has discussed buying additional reactors from Moscow.

Past performance or shortfalls do not dictate future success or failure. Still, India has repeatedly failed to reach its nuclear power production goals by substantial margins.¹⁰ Within the next few years, India plans to complete construction of at least eight indigenously built nuclear power plants with a cumulative capacity of 2,780 MWe. Adding this amount to the 2,000 MWe from the Russian reactors, India would more than double its current nuclear power capacity. Nonetheless, even if India does not increase its use of nuclear energy by almost nine times by 2020, a growth of one-half or even one-fourth as great would significantly challenge India's ability to train enough competent nuclear engineers, technicians, plant managers, and security guards without the next fourteen years. According to India's top civilian nuclear management, the Department of Atomic Energy has had a functioning nuclear engineering school since the late 1950s and is taking steps to ensure that India can adequately train enough engineers to meet the projected growth in nuclear energy development.¹¹ India's Nuclear Power Corporation reported in 2003 that it has more than 11,000 employees working at its nuclear power plants.¹² That number was for a total power capacity of about 3,000 MWe, implying the need for 3 to 4 employees per MWe. If this ratio holds roughly constant as the power increases, India would need 60,000 to 80,000 employees in 2020 for a goal power capacity of 20,000 MWe. The actual number of employees needed would probably be less than that amount because the newer plants would tend to have a higher power rating and would, therefore, need fewer employees at fewer higher-power rating plants. Still, the overall conclusion is that DAE will need to train several thousand to tens of thousands of new employees. Assuming DAE can train sufficient competent engineers, it also needs to take into account the increased risk of the insider threat if the nuclear workforce expands exponentially.

The next generation of Indian nuclear engineers and plant managers would at least have to receive training on three types of thermal reactors or additional reactor designs depending on what types of foreign reactors India would import, if those import deals are actualized. Presently, the predominant type of Indian commercial reactor is the pressurized heavy water reactor (PHWR), based on the CANDU, or Canadian Deuterium

⁸ Sunil Saraf, "Hope for U.S.-India Nuclear Deal by March Fading on FBR Impasse," *Nucleonics Week*, January 26, 2006, p. 9.

⁹ Director's Report, *Annual Report 2003-2004*, Nuclear Power Corporation of India, Ltd., p. 47; in particular, this report notes that about 30 engineers had been trained prior to 2003; 18 more were undergoing training in 2003; and another 37 will be sent to Russia in 2004.

¹⁰ M. V. Ramana, "Nuclear Power in India: Failed Past, Dubious Future," Presentation to the Non-Proliferation Education Center, May 10, 2006.

¹¹ Anil Kakodkar, "Nuclear Power in India: An Inevitable Option for Sustainable Development of a Sixth of Humanity," World Nuclear Association Annual Symposium, September 4-6, 2002, p. 5.

¹² Director's Report, *Annual Report 2002-2003*, Nuclear Power Corporation of India, Ltd.

Uranium, design. Fourteen of India's sixteen thermal reactors are PHWRs. These PHWRs provide about 3,500 MWe, or more than 90 percent, of installed capacity. Boiling water reactors (BWRs) provide the remainder. The third type of thermal reactor that India will have in the coming years is the Russian-designed VVER-1000, which is a pressurized water reactor (PWR) design.

Reactor designs determine much of the inherent strengths and weaknesses of a reactor. Nonetheless, reactors of the same design can differ in their characteristics because of differences in construction. Engineers can vary the construction among reactors of the same design due to many considerations. One of the foremost considerations is site selection. Every reactor site is unique. Proximity to other reactors at the site or location of cooling sources such as bodies of water, for example, can significantly affect the layout of a nuclear power plant and lead to deviations from a standard design. Because detailed information on particular Indian nuclear power plant sites is not openly available, this chapter discusses the general characteristics that can affect the safety and security of India's commercial reactors.

Designers of nuclear power plants rely on the concept of defense-in-depth, which means using redundant systems to provide increased protection against accidents. Almost all systems inside a nuclear power plant have one or more backup systems to ensure that if the main system fails, a replacement or emergency system will quickly provide protection. For example, if the primary coolant system ruptures, an emergency cooling system is available to prevent the reactor core from melting and possibly leading to a release of radiation to the environment.

In general, there are two exceptions to the defense-in-depth practice. A reactor has only one pressure vessel surrounding the highly radioactive core. If the pressure vessel would rupture, a backup pressure vessel would not be available to contain the core. Nonetheless, the radioactivity in the core would not necessarily be released to the environment because most commercial reactors have a strong containment building surrounding the reactor. The containment is the last line of defense for a nuclear power plant preventing a release of radiation to the environment. But here is the second exception to defense-in-depth. A commercial reactor, if it has a containment structure, usually has one. (As discussed later, the newer Indian PHWRs have a double-domed containment structure.) Thus, in assessing whether a nuclear power plant can withstand an attack, it is vitally important to know how strong its containment building is.

CANDU-type reactors, such as the Indian PHWRs, have certain safety features that make them more resistant to surviving attack or sabotage. CANDU cores are typically subdivided into two thermo-hydraulic loops. Each loop has hundreds of individual pressure tubes. This feature would help localize a loss-of-coolant incident caused by accident, attack, or sabotage. Moreover, the large-volume, low-pressure, and low-temperature heavy water moderator surrounding the coolant would provide a large heat sink to further protect the reactor fuel from melting down in a loss-of-coolant incident. Furthermore, because the steam generators are located above the core, natural thermo-siphoning would help carry away heat from the core and mitigate the effects of a loss of coolant incident.¹³

Containment buildings using a minimum of four-foot thick concrete walls typically enclose CANDU reactors. India's most recently built PHWRs have an added

¹³ Canadian Nuclear FAQ, Section D: Safety and Liability, www.nuclearfaq.ca, accessed on July 15, 2006.

safety feature: double-domed containment structures.¹⁴ These PHWRs are the Kaiga-1 and 2 reactors, the Rajasthan-3 and 4 reactors, and the Tarapur-3 and 4 reactors. But developing the double-domes did not occur without incident. In 1994, Kaiga-1 experienced a partial collapse of its inner dome during construction. In response, Indian engineers revised the design. These PHWRs use microsilica-based high performance concrete.¹⁵ The newer PHWRs also have other safety features, including an automatic, quick acting poison injection system to shut down the reactor in an emergency and microprocessor-based systems for reactor protection and control.¹⁶

India's oldest commercial reactors are located at Tarapur, which is about 100 kilometers from Mumbai. India bought these U.S.-designed reactors from General Electric, which manufactured boiling water reactors. Tarapur-1 and 2 began operation in 1969. After more than thirty years of operation, these reactors would normally be nearing their end of life. But Indian engineers have made more than 300 modifications to the Tarapur BWR plant to improve its safety. The DAE believes that these improvements would allow Tarapur-1 and 2 to run for another thirty years. Safety problems had plagued these plants in the past. In particular, the tubes in the secondary steam generators had developed cracks. Technicians could not plug the leaks without running a significant risk of receiving large doses of radiation. Consequently, these generators were shut off from the plant, and in 1985, the reactors were de-rated from 210 MWe each to 160 MWe.¹⁷ The containment structures of these reactors are not as robust as more modern BWRs. The earliest generation GE BWR used the torus or inverted light-bulb-shaped containment design, which relies on a pressure suppression system. This system, in the event of a loss of coolant accident, is intended to absorb steam and prevent a buildup of pressure that could rupture the containment building. Thus, designers reasoned that the pressure suppression system would allow for a weaker containment building, saving on construction costs. As early as 1972, safety officials were recommending that this containment system be discontinued because of concerns about the failure of the system during an accident.¹⁸ Even if the system would function properly during a loss of coolant accident, a weak containment building might not withstand the crash of a large airplane.

India has purchased two Russian light water reactors to supplement its indigenous reactor production. The older indigenous reactors are typically rated at about 220 MWe (with two notable exceptions, mentioned above). The newer indigenous reactors, such as Tarapur-3 and 4, that are coming online within the past are rated around 500 MWe. In contrast, the Russian PWRs being built at Kudankulam are 1,000 MWe each. Thus, the foreign supplied reactors would offer a significant boost to India's power capacity. The Russian VVER-1000 reactor has a relatively large coolant-to-power ratio; thus, like a CANDU reactor, it has some inherent protection in the event of a loss of coolant incident. However, the VVER-1000 has some inherent weaknesses. Vulnerabilities include: steam lines and isolation valves too close together, which a single blast could knock out; the control room located at the lower level of the reactor building, potentially prompting

¹⁴ Department of Atomic Energy, *Nuclear India*, July-August 2000, available at: <http://www.dae.gov.in/ni/nijul00/nijul00.htm>

¹⁵ Elkem Microsilica, "Nuclear Power Stations in India," Reference Project Fact Sheet, March 2003.

¹⁶ Department of Atomic Energy, *Nuclear India*, op. cit.

¹⁷ T. S. Subramanian, "TAPS at Thirty," *Frontline*, September 29-October 12, 2001.

¹⁸ Reactor Watchdog Project, "Hazards of Boiling Water Reactors in the United States," Nuclear Information and Resource Service, March 1996.

quick evacuation if the containment is breached, thus minimizing the amount of time operators have to control the reactor; and relatively weak containment structures that an airplane might penetrate.¹⁹ The VVER-1000s are being constructed in Tamil Nadu, where a number of terrorist groups are based.

Research reactors

Compared to commercial nuclear power plants, research reactors do not at first glance appear to offer tempting targets. Research reactors typically contain much less radioactivity than commercial reactors. Also, the former facilities do not usually have the high symbolic or economic value as the latter facilities. However, an attacker might strike a research reactor because it tends to be weaker than a commercial reactor. While the vast majority of commercial reactors, including all Indian commercial power plants, employ strong containment structures, many research reactors do not use containment buildings, and if they do, the containments tend to be not as strong as those surrounding commercial reactors. Research reactors, especially those at universities, also tend to have less security forces than commercial power plants.

Indian research reactors, however, are usually located within institutions that perform both civilian and military work. If security at these dual-use institutions remains strong because of their role in India's military program, attackers would likely decide to target relatively weaker nuclear facilities unless they had assistance from workers inside the institutions. Conversely, because these institutions have a dual-use role, military or terrorist attackers might find striking against facilities attractive. A successful attack would deal a blow against India's civilian and military nuclear infrastructure. At the Bhabha Atomic Research Center at Trombay, there are two operating research reactors (the Apsara LWR and the Purnima-3 LWR), three decommissioned reactors (the Purnima-1 critical assembly, the Purnima-2 LWR, and the Zerlina PHWR), and one planned to start operating in 2010 (the compact high temperature reactor). The decommissioned reactors, while not operating, could still present potential targets because of the possible presence of radioactive materials on-site. At the Indira Gandhi Center for Atomic Research (IGCAR) at Kalpakkam, there is the Kamini test reactor, which, as mentioned earlier, uses uranium-233.

Plutonium production reactors

Indian plutonium production reactors employ the technology in certain types of research reactors to make plutonium for nuclear weapons. While plutonium production reactors are part of the military program, these reactors are considered here because they are also intertwined with the civilian program. Currently, India uses the Cirus and Dhruva research reactors to produce plutonium. Both of these reactors are located at BARC in Trombay. Also, BARC contains a plutonium separation plant that can process 30 to 50 tons of spent fuel annually and a plutonium weapon component facility.²⁰ Even six

¹⁹ Helmut Hirsch, "Vulnerability of VVER-1000 Nuclear Power Plants to Passenger Aircraft Crash," WISE, November 2001, available at: <http://www.antenna.nl/wise/terrorism/112001vver.html>.

²⁰ David Albright and Susan Basu, "Separating Indian Military and Civilian Nuclear Facilities," Institute for Science and International Security, December 19, 2005.

kilograms of plutonium would be sufficient to make a nuclear bomb. This is a very small amount compared to the bulk of plutonium that India processes. Terrorists who have enlisted the help of insiders might be able to sneak out enough plutonium to build an improvised nuclear device or a radiological dispersal device.

Plutonium, however, poses significant technical challenges for terrorists wanting to make a relatively high-yield nuclear bomb with an explosive yield of roughly one to twenty kilotons. An implosion nuclear device, or the Nagasaki-type bomb, demands use of high-speed electronic switches and precisely shaped and specialized conventional explosives, for example.²¹ Nonetheless, Pakistani nuclear scientists who are sympathetic to terrorist causes might help terrorists construct a bomb from Indian plutonium. This scenario is not farfetched. Osama bin Laden reportedly met with two Pakistani nuclear physicists in 2001 and asked about nuclear bomb making.²²

If terrorists could not enlist expert assistance or would face insurmountable technical hurdles to making an implosion bomb, they could decide to build a much less powerful plutonium-fueled gun-type nuclear bomb. By using highly enriched uranium, the Hiroshima bomb, a gun-type device, achieved a nuclear yield of about 13 kilotons. The gun-type device is the easiest to build nuclear weapon. However, it would still pose technical challenges to terrorists, but technically skilled terrorists have a greater chance of making this type of nuclear weapon than an implosion-type weapon.

Because plutonium emits more spontaneous neutrons than highly enriched uranium, it cannot power a high-yield gun-type bomb. Nonetheless, a plutonium gun-type bomb can produce an explosive yield of two to ten tons.²³ While such a bomb would be about one thousand times less explosive than a plutonium implosion bomb, it would still be much more powerful than a typical conventional bomb. Thus, an expanding stockpile of bomb-usable plutonium can increase the risk of terrorists building an improvised nuclear explosive.

Breeder reactors

Faced with limited supplies of indigenous uranium, as noted earlier, India envisions fueling a fleet of commercial reactors with plutonium. Consequently, India has researched breeder reactors, a technology that most of the world has abandoned. Presently, a fast breeder test reactor is operating at IGCAR in Kalpakkam and is helping India gain research experience with this technology. A much larger 500 MW breeder reactor is slated to begin operation in 2010 at Kalpakkam. New Delhi pointedly left its breeder reactor program outside of its list of designated civilian reactors to be under international safeguards. Although the breeder program would likely produce fuel for civilian reactors, the fact that this program remains on the military side of India's nuclear

²¹ Charles D. Ferguson and William C. Potter with Amy Sands, Leonard S. Spector, and Fred L. Wehling, *The Four Faces of Nuclear Terrorism* (New York: Routledge, 2005), pp. 135-138.

²² Ron Suskind, *The One Percent Doctrine: Deep Inside America's Pursuit of Its Enemies Since 9/11* (New York: Simon & Schuster, 2006).

²³ Stanislav Rodionov, "Could Terrorists Produce Low-Yield Nuclear Weapons?" in Committee on Confronting Terrorism in Russia, Office for Central Europe and Eurasia Development, Security, and Cooperation, National Research Council in Cooperation with the Russian Academy of Science, *High-Impact Terrorism: Proceedings of a Russian-American Workshop* (Washington, DC: The National Academies Press, 2002).

complex has raised concern that it could increase the stockpile of plutonium for nuclear weapons. As with the plutonium production reactors, a major problem with the breeder program is the possibility that terrorists could steal plutonium to make nuclear bombs or dirty bombs.

Spent fuel pools

Spent fuel pools are tanks full of water that store spent, or used, nuclear fuel that has been discharged from a reactor. These pools are typically located near the reactor at a power plant site. While commercial reactors usually contain millions of curies of highly radioactive materials that could cause significant harm if released to the environment, spent nuclear fuel pools can contain several times this amount of radioactivity because a spent fuel pool can store several reactor cores. The radioactivity build up can climb even higher. If spent fuel is not moved from the pool and transferred to dry storage casks, the pool can fill up beyond its original design capacity. For example, the pool at Tarapur-1 was initially designed to store at most 72 metric tons of spent fuel. But according to the International Nuclear Safety Center, this pool contains more than twice that amount. Storing more than the originally designed amount of spent fuel can increase the risk of the spent fuel catching fire in the event of a loss of coolant incident.

If an attack causes a propagating zirconium cladding fire, large amounts of radioactivity could be released. After assessing the two types of spent fuel pools at U.S. nuclear power plants, the U.S. National Research Council concluded: “successful terrorist attacks on spent fuel pools, though difficult, are possible.”²⁴ That study recommended to reduce the risk of such attacks, the pools should be properly secured; effective means of cooling should be available under emergency conditions; as soon as permissible, spent fuel should be stored in dry storage casks; and the remaining spent fuel should be reconfigured in the pools to minimize the risk of a propagating fire.

India has the boiling water reactor type of U.S. power plant. The General Electric Mark I BWR plants, related to the Indian Tarapur BWR plant, were designed to have their spent fuel pools located inside of the containment structure. This configuration would provide a hardened protective layer for the pool. But the countervailing factor is that BWR spent fuel pools are generally well above ground level and thus in the event of a rupture a BWR pool could more easily drain than a pool that is partially or fully below ground level.²⁵

The majority of Indian spent fuel pools at PHWRs most likely follow the CANDU design. The typical CANDU plant has its spent fuel pool outside of the containment building; thus it is more exposed to attack than a BWR pool. But the CANDU pools are generally partially or fully below ground level, making them harder to drain.²⁶

²⁴ Committee on the Safety and Security of Commercial Spent Nuclear Fuel Storage, National Research Council, *Safety and Security of Commercial Spent Nuclear Fuel Storage U.S. National Academy of Sciences: Public Report* (Washington, DC: National Academies Press, 2006).

²⁵ U.S. General Accountability Office, *Spent Nuclear Fuel: Options Exist to Further Enhance Security*, GAO-03-426, July 2003.

²⁶ Canadian Nuclear FAQ, “CANDU Nuclear Power Technology,” www.nuclearfaq.ca, accessed on July 15, 2006.

Reprocessing plants

Reprocessing plants extract plutonium from spent nuclear fuel. Presently, India uses the PUREX reprocessing method, which is considered by nonproliferation experts to be proliferation-prone because it completely separates plutonium from the self-protecting highly radioactive materials in spent fuel. Thieves or terrorists can carry separated plutonium without suffering near-term harm to health.

India presently has two bulk, or industrial-scale, reprocessing plants: the Power Reactor Fuel Reprocessing Plant at Tarapur and the Kalpakkam Reprocessing Plant. Each plant can reprocess about 100 tons of spent fuel annually, which translates into nearly one ton of plutonium, assuming that about one percent of the spent fuel is plutonium.²⁷ This estimate also assumes that the reprocessing is very efficient. In reality, there will be some losses, but because India has had decades of experience in reprocessing, it likely can operate the reprocessing plants at high efficiency. But in any plant, there will be losses and material unaccounted for (MUF). MUF can add up to many kilograms of plutonium not properly tracked especially in a bulk handling facility. As India's rate of reprocessing and production of plutonium-based fuel increase, the likelihood for large amounts of MUF will increase. This situation will increase the potential for plutonium diversion. Even under strict International Atomic Energy Agency accounting, a one percent MUF could easily occur. This relatively rigorous accounting would probably still result in up to 20 kilograms of plutonium unaccounted for in India's two existing industrial-scale plants. This amount of plutonium could conceivably power two to three first-generation implosion nuclear explosives. Reducing the MUF to below bomb-usable amounts is next to impossible at bulk reprocessing facilities. Increasing the amount of reprocessed plutonium can also increase the chance of hazardous release of radioactivity and plutonium dispersal.

High-level radioactive waste storage areas

Reprocessing plants also pose another danger to an attack that can release massive amounts of radioactivity to the environment. The highly radioactive fission products removed from spent nuclear fuel during reprocessing are stored in large high-level liquid waste tanks. Rupturing these tanks could result in millions of curies of radioactivity released. In comparison, the Chernobyl accident released more than two million curies of radioactive cesium. Thus, a worst-case attack on a high-level waste storage facility could be comparable to the contamination from the Chernobyl accident. India has developed the capability to immobilize this liquid waste in glass. Such immobilization would create hard to disperse radioactive materials and would provide significant protection against radioactivity release from an attack on a high-level waste storage facility. To make effective use of this protection, India would have to operate the immobilization at a rate commensurate with the production of liquid waste.

Uranium enrichment facilities

²⁷ David Albright and Susan Basu, op. cit.

Usually uranium enrichment facilities would not pose significant threats for attack because uranium, unlike plutonium, is not very radioactive and would not result in significant harm to public health if it were dispersed. Also, low enriched uranium used in commercial light water reactors and certain other types of reactors cannot fuel nuclear weapons. Although little is openly known about India's secretive uranium enrichment program, the Rare Materials Project (RMP) at Mysore has a gas centrifuge plant that apparently is devoted to enriching uranium for nuclear submarine fuel. India's nuclear submarine program has been stuck in low gear for decades and might not require weapons-grade uranium for fuel. However, some analysts have suggested that India might employ the RMP to make weapons-grade uranium for its weapons program.²⁸ The amount of highly enriched uranium, if any, produced at the RMP is unknown, but even as little as 40 kilograms in terrorists' hands could fuel a gun-type nuclear bomb.

Electricity Distribution Grid

A terrorist or military attack that disabled a nuclear power plant could have far-reaching effects on India's electrical power system. Although New Delhi has been striving to improve the stability and reliability of the national electrical grid, this distribution system has suffered from frequency and voltage fluctuations.²⁹ On an unstable grid, loss of a major generator such as a nuclear power plant could bring down much of the electrical distribution system. In addition to causing a major blackout, this event could jeopardize the safety of the affected nuclear plant because external sources of power typically provide reliable means of running safety equipment such as reactor coolant pumps. Knocking out the grid connected to the plant would decouple the plant from external sources of power.

Under that scenario, on-site diesel generators would have to provide backup power to operate safety equipment. According to the U.S. Nuclear Regulatory Commission (NRC), "The reliability of the diesel generator is strongly dependent on the interaction of the following factors: design, testing and operational requirements, operational history, inspections, maintenance, and the personnel qualifications of operators."³⁰ In 1977, the NRC cautioned, "The demonstrated reliability of standby diesel generator (DG) units in operating nuclear power plants has been less than anticipated."³¹ Although in recent years, the NRC has cited a 97.5 percent reliability rate, independent analysts have estimated that the actual reliability rate is about 90 to 95 percent. While there are no openly available estimates of India's diesel generator reliability, even a 95

²⁸ M. V. Ramana, "India's Uranium Enrichment Program," International Network of Engineers and Scientists Against Proliferation, Bulletin 24, available at: <http://www.inesap.org/bulletin24/art21.htm>, accessed on February 24, 2006; and David Albright and Mark Hibbs, "India's Silent Bomb," *Bulletin of the Atomic Scientists*, September 1992, pp. 27-31.

²⁹ Alexander's Gas & Oil Connections, "India's Sasaram Project to Complete National Electricity Grid," News & Trends: E & SE Asia, May 29, 2002, available at: <http://www.gasandoil.com/goc/news/nts22270.htm>, accessed on August 24, 2006; Address by Shri Sushil Kumar Shinde, Indian Minister of Power, "India Electricity 2006," May 11, 2006, available at: www.ficci.com, accessed on August 24, 2006.

³⁰ U.S. Nuclear Regulatory Commission, Letter to All Power Reactor Licensees about Reliability of Diesel Generators, GL79021, June 4, 1979.

³¹ U.S. Nuclear Regulatory Commission, Letter to All Power Reactor Licensees about Demonstrated Reliability of Diesel Generators, GL77007, December 15, 1977.

percent reliability rate means that a major grid failure that knocked out ten or more reactors would translate into a more than 40 percent chance that one diesel generator would not operate at a nuclear reactor. A 90 percent reliability rate would translate into a 65 percent failure chance under that scenario. To provide additional reliability, a nuclear power plant could have additional diesel generators. However, even this added backup does not provide absolute protection because the diesel generators at a plant could experience common-mode failure.

Modes of Attack or Sabotage

A military or terrorist strike against an Indian nuclear facility can make use of a variety of attack modes or sabotage, including airplane crashes or bombings, truck bombs, commando-type attacks, insider collusion, and cyber-terrorism.

Airplane crashes or bombings

In the immediate wake of 9/11, nuclear regulatory officials admitted that containment structures were not designed to withstand the impact of large commercial aircraft. But nuclear industry representatives have emphasized the strength of containment structures and have expressed confidence in the capability of containments to protect against airplane crashes. The nuclear industry in the United States has sponsored studies to assess whether containments would remain intact after an airplane crash. In perhaps the most prominent and widely reported of these studies, which was commissioned by the Nuclear Energy Institute, the Electric Power Research Institute (EPRI) in June 2002 determined that containment buildings “can safely protect the reactor against most commercial aircraft,” including 757s (the type used in the 9/11 attack) and 777s.³² Then in December 2002, EPRI reported the results of a related study in which it simulated the impact of a Boeing 767-400 into four types of structures: containment buildings, spent fuel storage pools, spent fuel dry cask storage facilities, and spent fuel transportation containers. Although the containment building experienced “some crushing and spalling (chipping of material at the impact point) of the concrete” and the spent fuel pools suffered “localized crushing and cracking of the concrete wall,” all simulations showed that the aircraft was not able to breach the protection structures.³³ Industry officials have also scoffed at the notion that hijackers could direct large airplanes traveling at fast speeds onto a containment structure, which is a relatively low profile target.

Outside the nuclear industry, critics made their own calculations of the effects of airplane crashes on nuclear facilities. Among the independent analysts, Edwin Lyman, a nuclear physicist, has assessed that the engines of large aircraft traveling at high speeds “would penetrate the containment, leading to a fuel spill within the building and most

³² “Nuclear Plant Damage from Air Attacks Not Likely,” *Nuclear News*, August 2002, p. 21.

³³ Electric Power Research Institute, “Deterring Terrorism: Aircraft Crash Impact Analyses Demonstrate Nuclear Power Plant’s Structural Strength,” Nuclear Energy Institute, December 2002.

likely a severe jet fuel fire and/or explosion.”³⁴ These fires or explosions could cause multiple system or common mode failures. Even if containment structures are strong enough to withstand the direct impact of a large aircraft, many other buildings at nuclear facilities are much softer targets. For example, auxiliary buildings at nuclear power plants are typically not hardened. Smashing airplanes into these targets could result in many lives killed and substantial property and financial damage.

Perhaps terrorists will never use airplanes to attack nuclear facilities. In contrast, some militaries have already crossed this threshold and attacked nuclear reactors. In 1981, for example, Israel launched a preemptive attack by bombing and destroying Iraq’s Osirak research reactor, which was believed to become a plutonium production reactor. Later in the 1980s, Iraq bombed Iran’s Busheher nuclear power plant site during the Iran-Iraq War. Also, in the 1980s, Bennett Ramberg drew attention to nuclear power plants as Achilles heels offering relatively weak structures, but valuable symbols, for an enemy to attack.³⁵

Truck bombs

Over the past three decades, terrorists have increasingly used trucks to deliver devastating explosives to targets. Trucks are advantageous because they are hard to slow down once they gain momentum, allowing them to crash through un-reinforced barriers and can carry large amounts of explosives. India has suffered from many truck bomb attacks. Such attacks carried out by Islamic extremists in Kashmir have killed scores of people and damaged some hardened structures. Although terrorists would probably prefer trucks because of the large hauling capacity, they have also used car bombs on several occasions. For example, on August 25, 2003, Mumbai was rocked by two powerful car bombs. Also, many car bombs have detonated in Kashmir.

Commando-type attacks

Most militaries, including the Pakistani military, have highly skilled special fighters or commandos who are trained to attack and penetrate well-protected facilities. One of the most daring and famous military commando attacks was the Allied effort during World War II to destroy the Norsk Hydro plant that was producing heavy water for the Nazis’ nuclear program. British commandos at first tried to hang-glide to the Norwegian plant, but they failed because of the difficulties of landing on the rocky terrain. Finally, Norwegian commandos parachuted to a spot near the plant and then scaled steep, ice-covered cliff faces to place explosives at the plant.³⁶

Commandos are usually trained in multiple means of attack. For instance, they could barrage nuclear facilities with rocket propelled grenades, mortars, or artillery. Also, they could conduct attacks by air, land, or water routes. In addition, highly skilled commandos could disable external power supplies to a nuclear plant just prior to

³⁴ Nuclear Control Institute, National Press Club Briefing, September 25, 2001, statement by Edwin Lyman.

³⁵ Bennett Ramberg, *Nuclear Power Plants as Weapons for the Enemy: An Unrecognized Military Peril* (Berkeley: University of California Press, 1984).

³⁶ Dan Kurzman, *Blood and Water: Sabotaging Hitler’s Bomb* (New York: Henry Holt & Co., 1997).

launching a coordinated, multiple onslaught. Knocking out external power would reduce the capability of a nuclear plant to provide for adequate cooling to the reactor core.

While there have not been any reported commando attacks against Indian nuclear facilities, terrorists trained in commando techniques broke through tight security to attack the Indian parliament in New Delhi on December 13, 2001. Parliament was in session at that time. This attack brought India and Pakistan to the brink of war. A similar type of attack against a nuclear facility might spark an armed conflict between the two nuclear-armed countries.

Cyber-attacks

Nuclear power plants and other nuclear facilities rely on computer systems to operate. Consequently, military or terrorist attackers can attempt to use cyber-methods, such as hacking into computer systems or unleashing computer worms or viruses, to strike at India's nuclear infrastructure. According to a 2002 report in the *Indian Express*, major Indian nuclear research institutions such as the Indira Gandhi Centre for Atomic Research and BARC have experienced repeated attempts at cyber-attack. Notably, in 1988, cyber-attackers stole critical data from BARC. Many Indian computer experts point to Pakistan as a sponsor of cyber-attackers. Al Qaeda is also believed to support and encourage cyber-terrorism. Some of the cyber-groups that have targeted India include Anti India Crew, G-Force, World's Fantabulas Defacers, Pakistan Hackerz Club, Kill India, and Death to India.³⁷

Cyber-attacks can provide many advantages to an attacker. A cyber-attack is cheap compared to traditional methods. Tracking the attack can be very difficult. Attackers can mask their identities and locations and can launch an attack off-site. Cyber-attacks can easily cross borders because of the global nature of the Internet. For militaries, the Internet offers a virtual battlefield.³⁸ Increased frequency of computer attacks between India and Pakistan has often tracked times when the two countries have prepared for possible physical attacks. The rapid growth of software engineering and other computer specialties has spurred an exponential growth in the number of Indians who have advanced computer skills. Even if only a tiny fraction of these specialists turns to cyber-terrorism, New Delhi would face an increased internal security threat. Even though the Indian parliament passed the Information Technology Act of 2000 to, in part, address cyber-threats, Praveen Dalal, an Indian legal and computer expert, has called for the Indian legislature to amend this law because it does not adequately protect against cyber-attacks.³⁹

Insider collusion

³⁷ Subimal Bhattacharjee, "War in Cyberspace: When Hackers Turn Terrorists," *Indian Express*, May 31, 2002.

³⁸ Mudawi Mukhtar Elmusharaf, "Cyber Terrorism: The New Kind of Terrorism," Computer Crime Research Center, April 8, 2004.

³⁹ Praveen Dalal, "Cyber Terrorism and its Solutions: An Indian Perspective," May 14, 2005, available at: http://www.naavi.org/praveen_dalal/pd_cyber_terrorism_oct25_04_02.htm, accessed on July 20, 2006.

Workers at nuclear facilities have knowledge about the detailed operations and vulnerabilities at these places that outsiders would not usually possess. Thus, insider collusion would serve as a multiplier effect for outside attackers. To boost the chances of causing devastating damage, terrorist or military attackers would devote significant effort to recruit insiders. Skilled and highly trained insiders, such as nuclear engineers, would likely know how to disable emergency cooling systems and emergency sources of power such as diesel generators. Such disablement would increase the likelihood of a reactor meltdown and radiation release. Insiders could sabotage other vital plant systems while outside attackers are placing guard forces under siege.

India has experienced the betrayal of insiders. One of the most high profile insider attacks was the assassination of Prime Minister Indira Gandhi by her own guards. A major theme of Indian legends and literature is the fear of betrayal. For example, the *Artha Shastra*, a classic Indian Machiavellian text, which predated Machiavelli's *The Prince* by about 1,500 years, advises its prince to use an army of spies to keep watchful eyes on the loyalty of wives and officials. Also, according to Stanley Wolpert, a leading scholar of India, Chanakya's *Artha Shastra* "remained the standard text for several Indian Empires ... almost a timeless tribute to human treachery, banality, and the corrosive pettiness of power. There was even an elaborate 'Circle' (Mandala) theory of foreign policy that Chanakya developed, teaching every Indian monarch that the king ruling the circle of his immediate neighbor was his 'Enemy,' while just beyond lived his 'Friend.'"⁴⁰ To cite another prominent example from literature, the famous epic *Ramayana* pitted the virtuous Prince Rama against the villainous Ravana. Rama feared betrayal and forced his bride Sita, who had been abducted by Ravana, to prove her chastity in a trial by fire. After Rama became king, he continues to believe gossip that Sita is disloyal.

Even if a devastating event is not a clear act of insider sabotage, the public can be primed to view such events in that light, searching for scapegoats. Many have viewed the Bhopal chemical catastrophe, one of the worst industrial accidents in history, as an act of sabotage. On December 3, 1984, hazardous chemicals spilled out of the Union Carbide plant at Bhopal, killing thousands of mostly poor Indians. This event underscored the potential for complex technology to wreak havoc. These technological tragedies can lead to loss of faith in humanity's ability to control its inventions and can have profound socially disruptive effects as Paul Slovic observed in the journal *Science*:

An accident that takes many lives may produce relatively little social disturbance (beyond that experienced by the victims' families and friends) if it occurs as part of a familiar and well-understood system (such as a train wreck). However, a small accident in an unfamiliar system (or one perceived as poorly understood), such as a nuclear reactor or a recombinant DNA laboratory, may have immense social consequences if it is perceived as a harbinger of further and possibly catastrophic mishaps.⁴¹

⁴⁰ Stanley Wolpert, *India* (Berkeley: University of California Press, Third Edition, 2005), p. 35.

⁴¹ Paul Slovic, "Perception of Risk," *Science*, April 17, 1987, Vol. 236, p. 280.

Managerial and operator errors contributed to the Bhopal disaster and further eroded public confidence in corporate competence.⁴² An accident at or sabotage of an Indian nuclear power plant could be perceived as a nuclear Bhopal, potentially damaging public acceptance of nuclear energy in India. The public or the government might also try to pin the blame of a nuclear Bhopal on Pakistan, possibly stimulating a war between India and Pakistan.

Indian officials have taken measures to guard against the insider threat at nuclear power plants. In particular, India's Nuclear Power Corporation has instituted a Vigilance Directorate to, in part, "strive towards achieving zero degree tolerance to corruption" and also "encouraging whistle blowing arrangements."⁴³ According to the corporation, it has maintained surveillance on employees who have access to sensitive parts of the plants and has done regular and surprise inspections to try to detect possible misconduct.

Although vitally important and necessary, personnel reliability programs such as the Vigilance Directorate are not foolproof. In the United States where the military has had a decades-long practice with a personnel reliability program (PRP), between 2.5 and 5 percent of the PRP certified personnel are decertified and shut out from nuclear related duties.⁴⁴

Regulation, Safety, Secrecy, and Security

A safe nuclear facility is not necessarily a secure facility and vice versa. Nonetheless, common nodes for both safety and security are the regulatory agency and the culture of operations at the facilities. Concerning the culture of operations, key factors are whether management instills safety and security culture and fosters trust among employees so that they feel that they can raise safety and security concerns without fear of reprimand or reprisal. An assessment of how safety incidents are handled by the regulator can indicate how security incidents are addressed.

The Atomic Energy Regulatory Board (AERB) is the regulatory agency for India's civilian nuclear facilities. But because the many of the civilian facilities are embedded in the weapons program, BARC reviews the functioning of the military-related facilities. From the beginning of India's nuclear program, the Official Secrets Act has shrouded the program and blocked needed safety improvements, according to safety advocates. In 1999, T. S. Gopi Rethinaraj, a safety advocate, wrote, "India's nuclear establishment has grown into a monolithic and autocratic entity that sets the nuclear agenda of the country and yet remains virtually unaccountable for its actions."⁴⁵

During the 1990s, then-AERB chairman Dr. A. Gopalakrishnan led the charge that safety had fallen short. Soon after raising questions about safety problems, the Indian government decided to not renew his contract.⁴⁶ In 1996, he cited, "there were 130

⁴² Robert P. Gephart, Jr., "Review of Bhopal: Anatomy of a Crisis," *Science*, May 22, 1987, Vol. 236, p. 979.

⁴³ Director's Report, *Annual Report 2004-2005*, Nuclear Power Corporation of India, Ltd., p. 17.

⁴⁴ Ryan Crow, "Personnel Reliability Programs," Report for Project Performance Corporation, 2004, p. 3.

⁴⁵ T. S. Gopi Rethinaraj, "In the Comfort of Secrecy," *Bulletin of the Atomic Scientists*, November/December 1999, p. 52.

⁴⁶ K. S. Jayaraman, "Head of Indian Nuclear Agency Loses Job After Going Critical," *Nature*, June 27, 1996.

safety-related issues in various nuclear facilities, of which 95 belonged to the NPC [Nuclear Power Corporation] alone.”⁴⁷ The Official Secrets Act prevented him from being fully open about the specific issues. The Chief Engineer of the NPC responded that Gopalakrishnan was an alarmist and that his accusations have played into the hands “of vested interests internationally who are running down India’s self-reliant achievements in nuclear energy and have been periodically using the international media to create fear psychosis.”⁴⁸ But the Indian nuclear establishment was not carrying out an open investigation of Gopalakrishnan’s safety concerns. A conflict of interest, for example, arose when Raja Ramanna was appointed to an inquiry committee even though he was chairman of the Atomic Energy Commission when many of the safety incidents took place.

In the 1990s, headlines about India’s nuclear safety or lack thereof blazoned “Doomsday averted,” “Headed for a meltdown,” and “Sugarcoating nuclear power.”⁴⁹ Some of the known incidents are: in 1991, the switch gear room in the first unit of the Kakrapar Atomic Power Station caught fire and caused a complete loss of the emergency power system and partial loss of the electrical power supply; in 1991, for almost a month, the Dhruva plutonium production reactor operated without a functioning emergency core cooling system; on March 31, 1993, a major fire happened in the turbine room of the Narora Atomic Power Station; in September 1997, the workers union charged that there were high radiation levels at the Madras Atomic Power Station; and on March 26, 1999, large quantities of radioactive heavy water leaked out of the Madras Atomic Power Station. By the late 1990s, India had sunk to the lowest bracket of efficiency and performance in a *Nuclear Engineering International* survey of the world’s nuclear programs.

A plethora of safety incidents can point to shortcomings in the defense-in-depth protective functions of nuclear plants. Weaker defense-in-depth safety system would make these plants less able to withstand damage from a military or terrorist attack. Safety failures could be blamed on saboteurs supported by terrorists or by Pakistan.

Since the 1990s, there have been few reported safety incidents. The lack of reported incidents could either point to a secrecy clampdown or improvement in safety. A combination of the two factors might be the correct explanation. The Indian nuclear program, according to outside safety and regulatory experts, still is burdened with a regulatory agency that is not fully independent. Moreover, the Official Secrets Act probably still exerts a chilling effect. These barriers to self-critical appraisal of safety shortcomings could also lead officials to not take a hard examination of security culture.

However, safety appears to have improved in India’s nuclear program in recent years. For instance, since the late 1990s, a number of India’s nuclear power plants have received peer reviews by the World Association of Nuclear Operators (WANO). WANO grew out of the industry’s goal of striving to prevent a repeat of the 1986 Chernobyl

⁴⁷ As quoted in T. S. Gopi Rethinaraj, “In the Comfort of Secrecy,” op. cit.

⁴⁸ M. Das, “An Alarmist View on Nuclear Safety: NPC Speaks,” *Frontline*, May 8-21, 1999.

⁴⁹ Nayan Chanda and Kathy Wilhelm, “Doomsday Averted,” *Far Eastern Economic Review*, February 4, 1999; Nayan Chanda, “Headed for a Meltdown,” *World Press Review*, June 1999; and Mohammed Ahmedullah, “India: Sugarcoating Nuclear Power,” *Bulletin of the Atomic Scientists*, September/October 1999.

accident. In addition to peer reviews of particular plant operations, WANO has also conducted technical exchanges involving India to help instill best safety practices.⁵⁰

In May 2005, Gopalakrishnan addressed safety concerns and responded to his past critics who had raised the issue of alleged undue influence of foreigners in India's nuclear activities. He wrote, "In fact, without any foreign technical assistance, the DAE engineers have rectified almost all the safety deficiencies which I had documented and submitted to the government ... in 1995. Therefore, invoking the need for safety assistance from the U.S. is merely a ploy to indirectly plant doubts in the minds of the Indian public that DAE's capability to maintain safety in our reactors is inadequate in comparison to U.S. expertise."⁵¹ His article was published in the lead up to the unveiling of the controversial U.S.-India nuclear deal in July 2005. Gopalakrishnan believes firmly in India maintaining its self-reliance, especially in a world dominated by the United States. Other former and current Indian nuclear officials have expressed similar resistance to outside nuclear safety assistance. Such resistance would also tend to block India from receiving nuclear security assistance from outsiders.

Still, in the same article, Gopalakrishnan underscored some current safety issues. In particular, he warned against DAE's consideration of operating Tarapur reactors "with plutonium-based indigenous fuel" because this "is impractical and dangerous" and "world-wide studies have established that introducing more than 30-35 percent plutonium into boiling water reactors could bring adverse changes in their safety-related physics and kinetics parameters." Despite his reservations about relying on foreign assistance, he encouraged DAE "to initiate detailed technical discussions and consultations" with France and Russia "to further ensure public safety" about the breeder reactor program.⁵² While those countries have breeder reactor programs, the French Superphenix breeder reactor had to be shutdown soon after completion because of sodium coolant leaks. There has been an extensive history of safety problems in breeder reactor programs. Without rigorous attention to safety, India could experience numerous safety issues if it moves ambitiously with its breeder program as it has planned to do.

Terrorism and Sectarian Violence

Since independence in 1947, India has suffered repeatedly from terrorism and sectarian violence. While New Delhi has made great strides in creating the world's largest democracy and in officially ending the caste system, centuries of religious strife and caste discrimination lie just below the surface, ready to boil over.⁵³ In the past few decades, tens of thousands have died in India because of sectarian and terrorist violence.⁵⁴ Even though South Asia has experienced several wars in the past sixty years,

⁵⁰ Director's Report, *Annual Report 2001-2002*, Nuclear Power Corporation of India, Ltd., as well as other subsequent annual reports.

⁵¹ A. Gopalakrishnan, "India-U.S. Nuclear Mismatch," *The Asian Age*, May 31, 2005.

⁵² *Ibid.*

⁵³ Stanley Wolpert, *India* (Berkeley: University of California Press, Third Edition, 2005).

⁵⁴ Walter Laqueur, *The New Terrorism: Fanaticism and the Arms of Mass Destruction* (Oxford: Oxford University Press, 1999), p. 150.

terrorism has killed more people than all the wars in South Asia during that time period.⁵⁵ In recent years, the cycle of terror among disaffected groups continues and arguably has increased in its fury. Although the West has recently experienced high profile terrorist events including the 9/11 attacks in the United States, the March 11, 2004, or 3/11, attacks in Spain, and the July 7, 2005, or 7/7, attacks in Britain, there have not been continual attacks in these countries. In contrast, as terrorism analyst Swati Parashar has underscored, “India on the other hand barely recovers from one attack when another is successfully launched. It is a never ending saga of terror that needs to be examined.”⁵⁶

Religious terrorism has caused the largest number of terrorist incidents and killings. Much of this terrorism has arisen from the Sikh separatist movement wanting to create an independent Khalistan and from the strife in Jammu and Kashmir. While the former movement raged prior to 1995, the latter conflict continues to flourish. Pakistani-linked pan-Islamic groups operate in Jammu and Kashmir.

Four Pakistani pan-Islamic organizations, the Lashkar-e-Toiba (LET), the Harkat-ul-Mujahideen (HUM), the Harkat-ul-Jihad-al-Islami (HUJI), and the Jaish-e-Mohammad (JEM), which are active in India, have joined Osama bin Laden’s International Islamic Front (IIF), which formed in 1998. Osama bin Laden is also the leader of al Qaeda. All of these terrorist groups have safe havens in Pakistan, and two of them, LET and HUJI, also have found shelter in Bangladesh. While these groups had at first recruited their members from Pakistan, they have since 2003 drawn recruits from the Indian Muslim Diaspora community in the Gulf region and from the Indian Muslim community within India. Muslims in India are generally opposed to al Qaeda and the pan-Islamic terrorist groups.⁵⁷ However, with more than 140 million Muslims in India, which has the second largest Muslim community in the world, al Qaeda affiliated groups need only recruit a tiny fraction to create a formidable force operating inside India.

The connection of these Pakistani pan-Islamic groups to al Qaeda increases India’s risk of nuclear and radiological terrorism. Bin Laden has proclaimed that al Qaeda has a religious duty to acquire weapons of mass destruction.⁵⁸ He has also cited the American bombing of Hiroshima to rationalize al Qaeda’s drive for nuclear weapons.⁵⁹ Lending support to bin Laden’s call to nuclear arms, in May 2003, Shaykh Nasir bin Hamid al-Fahd, a young Saudi cleric, wrote the religious paper “A Treatise on the Legal Status of Using Weapons of Mass Destruction” to try to justify Muslims’ use of such weapons in the defense of the Umma, the Islamic community.⁶⁰ This rhetoric mirrors bin Laden’s modus operandi. Like the Prophet Mohammed, bin Laden purposefully warns foes before they subjected to attack. This behavior also tracks the Prophet Mohammed’s conviction of trying to convince the enemy of the error of his ways and to give him an opportunity to surrender or make restitution. For example, bin Laden warned Spain and

⁵⁵ Waheguru Pal Singh Sidhu, “Terrible Tuesday and Terrorism in South Asia,” *South Asian Survey*, Vol. 10, No. 2, December 2003.

⁵⁶ Swati Parashar, “Varanasi Blasts: The Unending Saga of Terror,” Paper no. 1742, South Asia Analysis Group, March 20, 2006.

⁵⁷ B. Raman, “Al Qaeda in India,” Rediff.com, April 4, 2003.

⁵⁸ Osama bin Laden interview with *Time* magazine, December 23, 1998.

⁵⁹ Steve Coll, “What bin Laden Sees in Hiroshima,” *Washington Post*, February 6, 2005, p. B1.

⁶⁰ Anonymous, *Imperial Hubris: Why the West is Losing the War on Terror* (Washington, DC: Brassey’s, 2004), pp. 154-158, and references therein. Since publication of that book, anonymous has been revealed to be Michael Scheur, a former CIA analyst.

Britain before the 3/11 and 7/7 attacks. Both countries were apparently primary targets of al Qaeda-affiliated groups because they were closely aligned with the United States, especially in the war in Iraq.

Until April 23, 2006, neither bin Laden nor his deputy Ayman al-Zawahiri had directly criticized India. On that date, bin Laden, in a video aired by the Al Jazeera TV channel, spoke about India's involvement in Kashmir and referred to an alleged Crusader-Zionist-Hindu war against the Muslims. A prominent South Asian terrorism analyst believes that the bin Laden message was provoked in part by President Bush's visits to India and Pakistan in early March 2006.⁶¹

Other Islamic extremists have warned Muslims about Hindus allegedly colluding with the United States and Israel. Notably, Professor Khurshid Ahmad, a leading ideologue for the Jamaat-e-Islami, has written about the Islamist "axis of evil," revolving around Christians, Jews, and Hindus.⁶² Such rhetoric may have inspired al Qaeda or an al Qaeda-affiliated group to bomb commuter trains on July 11, 2006. These bombings killed about 200 people in Mumbai. Soon after the attack, a self-described al Qaeda representative said that al Qaeda had established a cell in Kashmir and that the bombings were "a reaction to what is happening to the minorities, especially Muslims in India."⁶³

Early backlash against India cozying up to the United States occurred on October 29, 2005, when three precisely coordinated bombs detonated in Delhi, killing about 50 people. These bombings had the mark of al Qaeda and the IIF because of the well-synchronized nature of the multiple attacks and the occurrence close to Al Quds Day, which is on the last Friday of the Ramadan fasting period. Many Muslims commemorate Al Quds Day by protesting against the Israeli occupation of East Jerusalem where the Al Quds mosque is located. The bombings also happened two days before Diwali, a major Hindu festival. Moreover, the blasts follow on the heels of a propaganda campaign against India launched by al Qaeda, the Taliban, and the IIF. For example, on August 9, 2005, the Al Arabiya TV channel broadcast an alleged al Qaeda video that showed interviews with jihadists in Afghanistan saying that they are avenging the killing of Muslims by the United States, Britain, Israel, and India.⁶⁴ The propaganda campaign ramped up soon after Prime Minister Singh's high profile visit to the United States in July 2005.⁶⁵ During that visit, Singh and Bush unveiled the U.S.-India nuclear deal.

So far, religious terrorists in India have not attacked nuclear facilities or used nuclear or radiological materials in their attacks. However, on September 12, 2001, Sheikh Jamil-ur-Rehman, the leader of the Tehrik-ul-Mujahideen, a terrorist group in Kashmir, promised to attack nuclear facilities in India.⁶⁶ Although some religious terrorist organizations, such as al Qaeda, have expressed strong interest in nuclear terrorism, all of the religious terrorist groups have favored well-proven techniques of improvised explosive devices, suicide bombings, hostage taking, as well as hijacking and blowing up aircraft. South Asian terrorist groups who are mainly influenced by non-

⁶¹ B. Raman, "Bin Laden Targets India," Paper No. 1776, South Asia Analysis Group, April 25, 2006.

⁶² Husain Haqqani, "The Ideologies of South Asian Jihadi Groups," *Current Trends in Islamist Ideology*, published by the Hudson Institute, Volume 1, April 2005, pp. 19-20.

⁶³ Amelia Gentleman, "Al Qaeda Link to Kashmir Worries India," *International Herald Tribune*, July 13, 2006.

⁶⁴ B. Raman, "Al Qaeda & India," Paper No. 1498, South Asia Analysis Group, August 13, 2005.

⁶⁵ B. Raman, "Delhi Blasts: The Message," Paper No. 1591, South Asia Analysis Group, October 30, 2005.

⁶⁶ "Terrorists Vow to Hit Indian N-Sites," *Times of India*, September 12, 2001.

religious motivations also have employed these non-nuclear methods and have notably introduced to the Subcontinent one of the more radical methods: suicidal terrorism. In May 1991, suicidal terrorism first appeared in India with the assassination of Prime Minister Rajiv Gandhi by the Liberation Tigers of Tamil Eelam (LTTE), a national-separatist group in Sri Lanka. However, after the Pakistani pan-Islamic groups of LET, HUM, HUJI, and JEM teamed up with bin Laden's International Islamic Front in 1998, they have embraced and expanded the use of this method. Terrorists' willingness to covet martyrdom may be required for them to penetrate a nuclear facility. Certainly, an airplane crash into a nuclear plant would call for suicidal terrorists. Also, a truck bomb would likely require a terrorist martyr to drive to the designated target at the nuclear facility and ensure the detonation of the explosive.

At least one terrorist who wanted to crash airplanes into nuclear power plants had lived in neighboring Pakistan. Khalid Shaikh Mohammed, a Pakistani and one of the chief planners of the 9/11 terrorist attacks, told interrogators that his ambitious original plan for 9/11 involved ten airplanes instead of the four that were used. In addition to smashing airplanes into the World Trade Center and the Pentagon, he wanted to crash planes into the CIA and FBI headquarters as well as nuclear power plants.⁶⁷ He was captured in Rawalpindi, Pakistan, in March 2003 and had connections to al Qaeda-affiliated groups throughout South and Southeast Asia. Mohamed Atta, the leader of the 9/11 hijackers, also reportedly "considered targeting a nuclear facility he had seen during familiarization flights near New York ... referred to as 'electrical engineering.'"⁶⁸ But the 9/11 report notes:

According to Binalshibh [one of the 9/11 planners], the other pilots did not like the idea. They thought a nuclear target would be difficult because the airspace around it was restricted, making reconnaissance flights impossible and increasing the likelihood that any plane would be shot down before impact. Moreover, unlike the approved targets, this alternative had not been discussed with senior al Qaeda leaders and therefore did not have the requisite blessing.⁶⁹

Some terrorist attacks in India have brought it close to war with Pakistan. In particular, the December 13, 2001, attack on the Indian parliament and the following January 2002 attack on the Kaluchak army camp spurred New Delhi to mobilize its military along the India-Pakistan border. Many Indian leaders believed that Islamabad was responsible for allowing the perpetrators of these attacks to operate within Pakistan. The military mobilization spurred U.S. intervention with Islamabad. In response, Pakistan temporarily stemmed the flow of militants into India. According to V. R. Raghavan, a retired general in the Indian army, this experience in part shifted Indian strategy "from defensive to proactive, offensive responses to terrorism."⁷⁰ As a consequence, in the future, India may use "punitive military actions such as air strikes against terrorist

⁶⁷ 9/11 Commission Report, p. 154.

⁶⁸ 9/11 Commission Report, p. 245.

⁶⁹ Ibid.

⁷⁰ V. R. Raghavan, "The Double-Edged Effect in South Asia," *The Washington Quarterly*, Autumn 2004, p. 150. In an earlier paper, Jon P. Dorschner, "An Indian Assault on Terrorism—The Military Option," Department of Social Sciences, United States Military Academy, August 2002, examines India's strategic shift.

infrastructure and military forays to take out terrorist bases in Pakistani territory.”⁷¹ In light of this new more aggressive strategy, a terrorist attack on or sabotage of an Indian nuclear facility could spark a war between India and Pakistan, particularly if New Delhi suspects Islamabad’s involvement in the initiating event.

Concerns about Pakistan attacking nuclear facilities have influenced decisions on where to build Indian nuclear power plants. For example, on June 23, 2006, the Indo-Asian News Service reported that New Delhi was forced to rethink its original plans to locate a new nuclear plant in Punjab after concerns were raised about the proposed site’s close proximity to Pakistan. Instead, the new plant will be built in Haryana.⁷²

Al Qaeda or al Qaeda-affiliated groups in South Asia could try to blackmail India to “liberate” Kashmir from India. Blackmail is most effective when it targets what someone cherishes. It would not have been lost on jihadi terrorists in South Asia that India believes dearly in its nuclear program. Moreover, a blow delivered to this program would also strike at the United States, which has invested much of its foreign policy clout in promoting India’s civilian nuclear development. Jihadis seeking the liberation of Kashmir would not want to commit nuclear terrorism inside that region because of fear of harming their constituents. Instead, they would target Indian nuclear facilities outside that region of which there are many. The blackmail scenario could play out in a number of ways. Conceivably, a terrorist group could forewarn Indian authorities before the attack demanding surrender of Kashmir. Alternatively, the group might believe that a more effective method is to prove its capability by launching an attack on a nuclear facility and then make its demand. The blackmail would take the form of threats against other facilities. New Delhi would probably suspect Islamabad’s involvement especially because Indian leaders would likely reason that successful terrorist strikes against nuclear facilities would require financial and technical assistance from a state sponsor. This scenario could then spiral into a war between India and Pakistan.

While non-religious terrorist groups in India are not apparently motivated to acquire and use weapons of mass destruction, possible exceptions are Marxist and Maoist groups. These groups intend to right the wrongs of economic and social injustice experienced by hundreds of millions of India’s poor people. Marxist groups in India have linked up with Maoist groups in Nepal, Sri Lanka, and Bangladesh.⁷³ This network could lend means of financial and technical support among these groups. Although Marxist and Maoist terrorist organizations in South Asia have not openly expressed interest in chemical, biological, radiological, or nuclear terrorism, one group has drawn attention recently to its targeting of India’s economic infrastructure. During the past four years, the Naxalites, a Maoist-inspired group, have spread throughout parts of eastern and southern India. Their numbers have recently increased, and they are held responsible for attacks that killed about 900 people in 2005. The Naxalites and some Marxist groups have recently threatened to attack mining operations.⁷⁴ A major uranium mining and milling site in Jaduguda is located in the Indian region of Jharkhand, a stronghold of the Naxalites. The Naxalites have already attacked railways and could turn their sights on nuclear power plants because of these facilities high-profile economic significance.

⁷¹ Ibid.

⁷² “Haryana Selects Nuclear Power Plant Site,” Indo-Asian News Service, June 23, 2006.

⁷³ B. Raman, “Terrorism: India’s Unending War,” Rediff.com, April 4, 2003.

⁷⁴ “India’s Revolutionaries: The East is Red,” *The Economist*, April 15, 2006, p. 45.

Protective Measures

The Ministry of Home Affairs is the lead agency in managing internal Indian security. A major part of the Home Ministry, the Central Industrial Security Force (CISF) is responsible for defending nuclear installations and is independent of the Department of Atomic Energy. But the CISF, a paramilitary force, has many additional responsibilities. It protects oil refineries, ports, airports, steel plants, and many other places that are vital for India's economy. The CISF currently consists of more than 95,000 personnel guarding more than 250 industrial locations. It has a specially trained fire wing that provides fire-fighting services to the government. With all of these duties, there are concerns that CISF is stretched too thin.⁷⁵ Even the Indian government's official Web site for the CISF acknowledges, "CISF is increasingly being called upon to perform important duties beyond its charter such as internal security, airport security, security of highway, election duties, etc." While not discussing the details of its training methods, the CISF Web site mentions that its seven training institutions are trying "to keep the force abreast of the latest trends in threat perception and its management vis-à-vis the technological advancement in the field."⁷⁶ It is not openly reported as to what types and frequency of testing the CISF undergo at nuclear facilities.

In 2004, India's Border Security Force (BSF) announced that it is forming a battalion with special skills in countering nuclear, biological, chemical threats. The special battalion will receive training from nuclear experts at BARC. At that time, the BSF also pointed to increased concerns about militant camps in Bangladesh. While the battalion has established its main base of operations near Bangladesh, BSF reported that the battalion could deploy in any part of India if and when needed.⁷⁷

In April 2002, the Chairman of India's Nuclear Power Corporation announced that he was cognizant of the terrorist threat and mentioned that the DAE and CISF have performed security drills at nuclear facilities.⁷⁸ Within a month after 9/11, New Delhi promulgated no-fly zones around nuclear power plants.⁷⁹ However, it is uncertain whether these facilities are adequately protected by anti-aircraft defenses.

The Indo-U.S. Working Group on Counterterrorism has discussed a variety of issues including nuclear terrorism. The United States has reportedly brought up the issue of assistance to secure Indian nuclear facilities.⁸⁰ But such assistance faces the hurdle of appearing to place India in a subservient position. Indian officials pride themselves on trying to become self-reliant. To have a greater chance of being accepted, U.S. help with nuclear plant security would have to at least be perceived as a cooperative venture.

Crises have often spurred India and Pakistan to enhance cooperative efforts to address mutual security concerns. In the 1980s, for instance, Indian fears about Pakistan's

⁷⁵ Rajesh M. Basrur and Hasan-Askari Rizvi, *Nuclear Terrorism and South Asia*, Cooperative Monitoring Center Occasional Paper No. 25, Sandia National Laboratories, SAND 98-0505/25, February 2003.

⁷⁶ DefenceIndia, "Central Industrial Security Force," Web site, available at: <http://www.defenceindia.com/defenceind/cisf.html>, accessed on July 12, 2006.

⁷⁷ Marcus Dam, "BSF Battalion to Counter Nuclear, Chemical Threat," *The Hindu*, September 17, 2004.

⁷⁸ R. K. Radhakrishnan, "Security Concerns Will Not Stop New Nuclear Plants," *The Hindu*, April 4, 2002.

⁷⁹ Kalyan Ray, "move to Put Nuclear Plants Under Restricted Zone," *Deccan Herald*, October 13, 2001.

⁸⁰ Rajesh M. Basrur and Hasan-Askari Rizvi, op. cit., p. 71.

nuclear weapons program were rising. During the early 1980s, New Delhi considered preemptive strikes against Pakistan's nuclear facilities, especially the Kahuta plant. Rumors were circulating that Israel would carry out the attack if India requested.⁸¹ As noted earlier, Israel had bombed the Osirak reactor in Iraq in 1981. During this time period, New Delhi had yet to diplomatically recognize Israel because of not wanting to rile India's large Muslim population. A possible buildup to a preemptive attack heightened already growing tensions on the Subcontinent.

A partial defusing of the crisis atmosphere came about with the 1988 agreement between the two adversaries to refrain from attacking each other's nuclear facilities in the event of war. The agreement entered into force in 1991. Since January 1, 1992, the two sides have annually exchanged a list of their nuclear facilities. Although this agreement has served as a confidence building measure, it has its shortcomings. It does not define "nuclear facility," and it does not specify when a facility should be included on the list, that is, when construction has started or been completed. The lists have never been openly published. Outside observers suspect that the lists are incomplete and most likely do not include many military facilities. If possible, it would be interesting to compare the list India has sent Pakistan to the list of civilian facilities India has sent to its parliament and the United States with respect to the U.S.-India nuclear deal.⁸²

Although India is not a signatory of the Nuclear Non-Proliferation Treaty, it is a member of the International Atomic Energy Agency (IAEA). The IAEA has provided some security training using seminars for Indian officials. Also, both Indian and Pakistani experts have participated in the IAEA-sponsored International Training Course on the Physical Protection of Nuclear Facilities and Materials operated by the Sandia National Laboratories.⁸³ But India and Pakistan could make more effective use of the IAEA by requesting International Physical Protection Advisory Service missions in which an international team makes confidential vulnerability assessments that result in specific recommendations to improve physical security. But Indian and Pakistani concerns about the leakage of sensitive information from civilian facilities embedded in the military complex are likely creating resistance to fully opening up to the IAEA.⁸⁴

The two countries are also parties to the Convention on the Physical Protection of Nuclear Material (CPPNM). A major shortcoming of the CPPNM was that for many years, it only applied to protection of nuclear material during international transit. But amendments to the CPPNM in 2005, once ratified, would require parties to protect nuclear material at their domestic facilities. Still, independent security experts have expressed concern that security requirements, associated with the CPPNM and related IAEA guidance, are not rigorous enough.⁸⁵

Increasing the Number of Guards does not Always Increase Security

⁸¹ Wolpert, op. cit, p. 246.

⁸² E-mail communication with Michael Krepon, April 17, 2006.

⁸³ Arian L. Pregoner, Securing Nuclear Capabilities in India and Pakistan: Reducing the Terrorist and Proliferation Risks, *Nonproliferation Review*, Spring 2003, p. 125.

⁸⁴ Sharon Squassoni, *Nuclear Threat Reduction Measures for India and Pakistan*, CRS Report for Congress, RL31589, Updated February 17, 2005, p. 8.

⁸⁵ George Bunn, "Raising International Standards for Protecting Nuclear Materials from Theft and Sabotage," *Nonproliferation Review*, Summer 2000.

While increasing the number of guards might appear to always increase security, certain countervailing human behaviors might actually weaken security if guard forces are increased. Scott Sagan, a Stanford University professor, has challenged the conventional thinking on guard forces. In a 2003 paper that won Columbia University's Institute for War and Peace Studies best paper award, he identified three ways in which more security forces could result in less security.⁸⁶

First, more guards could increase the threat from insiders. If recently hired guards are not thoroughly screened, saboteurs could infiltrate the nuclear facility. Even if the new guards are well screened, screening procedures are not foolproof, and a rapid increase in new hires increases the probability of some malicious people being admitted. India's ambitious plan to rapidly increase the number of its nuclear plants could unintentionally allow penetration by saboteurs. While India would likely insist that it is only recruiting loyal employees for its nuclear facilities, Sagan cautions, "Unfortunately, organizations that pride themselves on high degrees of personnel loyalty can be biased against accurately assessing and even discussing the risk of insider threats and unauthorized acts." After an employee clears a background check, he could become the target of coercion by terrorists.

Second, Sagan observes that guard redundancy can diffuse responsibility through the phenomenon of social shirking. Citing examples from even elite military units, he points out that it is a common human tendency to assume that others will "take up the slack." Third, Sagan cautions that increasing security forces at a nuclear plant could lead to overconfidence that the security system is stronger than it really is. This unintended consequence can lead to the risky behavior of building and running more nuclear facilities than the security system can manage. Sagan concludes, "Predicted increases in nuclear security forces should not be used as a justification of maintaining inherently insecure facilities or increasing the number of nuclear power plants, storage sites, or weapons facilities." Still, he does not mean that "redundancy never works in efforts to improve reliability and security." He advises that greater awareness of the potential pitfalls in simply adding more security forces would likely increase vigilance.

Recommendations

Over many decades, India has developed a widespread and multifaceted nuclear infrastructure. While New Delhi has instituted security practices, including a paramilitary guard force and a personnel reliability program, it must continually reevaluate the rigorousness of its security system as it forges ahead with an ambitious expansion of its nuclear enterprise. It is not clear whether India has reexamined its design basis threat (DBT) in light of al Qaeda's growing influence on terrorist activity in India. The DBT is the particular level of threat from outside attackers and inside saboteurs.

Another complicating factor for Indian nuclear security is the tight interconnection between India's civilian and military nuclear programs. A commercial reactor would likely pose more of a target for military attack if it were associated with the

⁸⁶ Scott D. Sagan, "The Problem of Redundancy Problem: Why More Nuclear Security Forces May Produce Less Nuclear Security," *Risk Analysis: An International Journal*, August 2004. All quotations referenced to Sagan appear in that article.

military nuclear sector. Moreover, this blurring between the programs shrouds the civilian nuclear activities in more secrecy than a purely civilian program would experience. Although secrecy can keep sensitive information from the enemy, too much secrecy can silence questioning that leads to improvements in security.

Separate Civilian and Military Nuclear Programs

India should move more of its civilian nuclear facilities into a separate civilian program. While New Delhi, under the U.S.-India nuclear deal, has designated an additional handful of its commercial reactors as subject to IAEA safeguards, many more of its reactors remain in the military sector. The United States should use what influence it has to urge India to place more of its commercial reactors as well as its breeder reactors under the civilian program. Other nuclear-armed countries such as France and Russia have designated their breeder programs as civilian. New Delhi has objected to designating its breeder program as purely civilian because it foresees this program as potentially providing a huge source of plutonium for weapons. Such potential plans should provide further incentive for the United States and other nuclear-armed countries to bring India and Pakistan into serious negotiations for a fissile material cutoff. Such negotiations would also have to involve China, which is believed to have stopped making fissile material for nuclear weapons but has never formally announced it has.

Develop Cooperative Nuclear Security

India prides itself on having developed a largely indigenous nuclear program. Many Indian leaders bristle at the suggestion that their country needs security assistance. The United States, the IAEA, and other relevant entities should work cooperatively with India to improve its nuclear security. Perhaps the United States could leverage the U.S.-India nuclear deal to encourage New Delhi to engage in this issue.⁸⁷ U.S. security experts could brief Indian officials about security practices in the United States. In the spirit of true cooperation, India would be encouraged to discuss its practices. While the non-nuclear part of the U.S.-India deal mentions greater cooperation on fighting terrorism in South Asia, the United States and India should strive to ensure that more work is done in this area as the region confronts severe threats from numerous terrorist groups.

New Delhi would likely have to be convinced to accept a cooperative security program. A relevant precedent is the opening up of India's civilian nuclear program to outside peer review of the safety systems and operational practices at its nuclear power plants. WANO has conducted several such confidential reviews in India. A WANO-like security peer review could confidentially identify shortcomings in India's security system. The peer reviewers could involve IAEA security experts as well as experts from other countries' nuclear programs. Indian experts could take part in serving as peer reviewers of other nuclear programs. Thus, the peer review program would not single out a particular country but would serve as a global network to exchange best security

⁸⁷ Kenneth N. Luongo and Isabelle Williams, "Seizing the Moment: Using the U.S.-India Nuclear Deal to Improve Fissile Material Security," *Arms Control Today*, May 2006.

practices.⁸⁸ At a minimum, India should request more security reviews and seminars from the IAEA, especially through the IAEA's IPPAS program.

Implement Best Safety and Security Practices

While IAEA and WANO-type peer reviews are important in identifying safety and security shortcomings, safety and security will not improve without implementation of the recommended enhancements. Indian nuclear power plants should incorporate safety systems resistant to insider sabotage.⁸⁹ India should apply this sabotage-resistance to future plants and, to the extent possible, retrofit current plants. In general, vital safety equipment could require a two-person rule in order to allow access to the equipment. For example, make sure that emergency core cooling systems cannot be turned off unless at least two nuclear operators agree.

Inherent safety systems can be expensive. But there are inexpensive measures that can improve safety and security. For instance, passive air defenses such as barrage balloons or steel beams secured in concrete foundations could provide cost effective protection against airplane crashes.⁹⁰ Placing a berm around vulnerable nuclear plant structures, fortifying spent nuclear fuel pools, and transferring spent fuel to dry storage casks, and supplying extra diesel generators for reliable emergency power can be other relatively easy to implement methods. The extra diesel generators should be configured and maintained in a manner that minimizes the probability of common mode failure.

Create a More Open Civilian Nuclear Infrastructure

While cooperative ventures can help enhance security, for this cooperation to be effective, openness to change is essential. In addition, openness to self-criticism is equally as important. A self-critical nuclear system requires a truly independent regulator. Although India's AERB appears independent on paper, New Delhi should ensure that the AERB is independent in practice. New Delhi should also make sure, by amending as appropriate, that the Official Secrets Act does not have a chilling effect on silencing concerns about safety and security. As India continues to build up its nuclear program, it should continually assess whether its DBT is adequate to counter military and terrorist threats. Also as the Indian nuclear complex scales up, New Delhi should prepare to counter potentially hazardous unintended consequences, including increases in the insider threat and the dangers of a growing stockpile of weapons-usable plutonium.

⁸⁸ Arian L. Pregoner, op. cit., pp. 126-127; Charles B. Curtis, "Promoting Global Best Practices," Paper presented at the Institute for Nuclear Materials Management, 46th Annual Meeting, July 11, 2005; and Charles D. Ferguson, "Nuclear Lessons for Today," *Christian Science Monitor*, April 26, 2006.

⁸⁹ Paul Leventhal and Brahma Chellaney, "Nuclear Terrorism: Threat, Perception, and Response in South Asia," Nuclear Control Institute's Nuclear Terrorism Prevention Project, October 10, 1988.

⁹⁰ Joel Hirsch, "Beamhenge?" *Bulletin of the Atomic Scientists*, May/June 2003.