



TERRORISM THREAT AND NUCLEAR POWER: RECENT DEVELOPMENTS AND LESSONS TO BE LEARNED

Dr. Edwin S. Lyman, President, Nuclear Control Institute, 1000 Connecticut Avenue, NW Ste. 410, Washington, DC 20036 USA

Introduction

On the morning of 11 September, American Airlines Flight 11 flew directly over the Indian Point nuclear plant, 35 miles north of New York City, on its way to the World Trade Center. It is an unmistakable fact that if Al Qaeda had desired it, one or even both of the hijacked airlines from Boston could have directed their enormous destructive energy at the Indian Point reactors or spent fuel pools. This realization has dramatically focused the attention of the American public, politicians and the media on nuclear power issues that had not been prominent since the great anti-nuclear demonstrations of the late 1970s. Industry and government assurances that the risk of nuclear power accidents are low are meaningless when the threat of deliberate attacks is considered.

The threat of aircraft attack has also made the public aware of the other ways that terrorists could attack nuclear plants to cause a meltdown. Nuclear plants are vulnerable to attacks by well-trained and equipped groups from land or sea, large vehicle bombs, or insider sabotage.

Despite the level of public concern, the U.S. Nuclear Regulatory Commission (NRC), has been extremely reluctant to order systematic upgrades of security at nuclear plants to protect against 11 September-scale assaults. The NRC's lackadaisical attitude stems from a combination of pressure from the nuclear industry and an apparently sincere belief among some NRC Commissioners that nuclear plants pose little threat to public health and safety, even in the event of a successful terrorist attack. Without unrelenting public pressure and stringent Congressional oversight, it is unlikely that the glaring security vulnerabilities at U.S. nuclear plants will be corrected in a timely manner. Thus the risk that terrorists will be able to cause an "American Chernobyl" is not likely to go away any time soon.

Nuclear Plant Security Before 11 September

The NRC has had regulations in place since the 1970s for protecting nuclear plants against commando attacks, but the regulations were not designed with the current level of terrorist threat in mind. Nuclear plants licensees are required to protect against the "design-basis threat" (DBT): an attacking force consisting of "several" well-trained individuals, operating as a single team, armed with automatic weapons and explosives and assisted by an insider (who either actively participates in the attack or only supplies information). Following the 1993 car bomb attack on the World Trade Center, the DBT was enhanced to include a "four-wheel drive vehicle bomb." Airborne attack of any sort, including the use of a helicopter to gain entry, is not considered. More detailed information about the DBT, including the number of attackers, the types of weapons carried, and the size of the vehicle bomb is considered "safeguards information" and is not publicly available.

The objective of the attacking force is "radiological sabotage" — that is, damage to the plant causing a radiological release that could endanger the public health and safety. In operational terms, this is assumed to be equivalent to causing a core meltdown. Although not every core melt accident would lead to a large radiological release to the environment, terrorists would be able to facilitate such a release by mechanically breaching the reactor containment or causing a containment bypass.

The consequences of a Chernobyl-type radiological release at a U.S. reactor could be devastating. Many reactors are located in close proximity to large cities, or are in the midst of suburban areas with rapidly growing populations. NRC computer models predict that protective actions, such as potassium iodide administration and evacuation, would be required for individuals well beyond fifty miles from plant sites. The models also estimate the occurrence of hundreds to thousands of fatalities from acute radiation exposure, and tens to hundreds of thousands of eventual cancer deaths from lower doses.

To protect against the DBT, nuclear plant licensees must develop a security plan, describing in detail the strategies that would be used by armed responders to prevent the attackers from destroying enough



equipment to cause a meltdown. Procedures must also be in place for controlling access of persons and vehicles to the plant, including vehicle barriers to maintain safe setbacks from truck bombs. To guard against the insider threat, licensees must also have procedures for granting unescorted access to sensitive areas of the plant.

However, simply having a security plan on paper is not a guarantee that the plan will work in practice. For this reason, in 1991 NRC introduced a program to test nuclear plant security by carrying out exercises involving mock attacks, known as the Operational Safeguards Response Evaluation (OSRE). The OSRE program was intended to test both the effectiveness of the protective strategy and the skills of the armed response force.

In OSRE exercises, the mock attacking force does not work for NRC, but is hired by the nuclear plant licensee. However, NRC employs "contractors" with highly specialized knowledge to assess the security of each plant and advise the mock attacking force on strategy. Before the OSRE, a series of "tabletop" exercises are conducted, in which elements of the licensee's protective strategy are probed by the NRC contractors. This is meant to simulate the role of a "passive insider" who provides detailed security information to the attackers. Finally, four different "force-on-force" exercises are conducted over a two-day period. A number of different scenarios are conducted, ranging from a lone adversary (the so-called "Farmer Brown" scenario) to a group with capabilities close (but not identical) to that of the full DBT. The scenarios are chosen by NRC and its contractors, based on their observations of the tabletops.

The goal of the attacking force in OSRE is the destruction of a "target set." A target set is defined as the smallest combination of pieces of equipment that, if simultaneously disabled or destroyed, would result in damage to the reactor core. Therefore, the attackers are judged to have "won" the exercise only if all elements of a target set are reached. Conversely, the defending force is considered to have "won" if it is able to protect a single element of a target set. However, a nuclear plant presents many different possible target sets, so the design of a protective strategy that can defend the plant against any possible attack scenario is a complex task.

At some nuclear plants, a target set may consist of only one element — that is, a single location with enough safety equipment in close proximity that a single well-placed explosive could result in a meltdown. The existence of such vulnerabilities is a clear indication that sabotage resistance was not a consideration when the current generation of nuclear plants was designed.

The OSRE exercises obviously have little in common with a real attack. They typically are scheduled six to ten months in advance, allowing considerable time for advance preparations and security force training. (In fact, in some cases additional guards were hired simply to participate in the OSRE.)

In spite of these advantages to the defensive force, OSRE performance has been poor. According to the NRC, from 1991 to 2001, 81 OSREs were run. At least one target set was destroyed in 46% of the exercises, meaning that the security force was unable to prevent the attacking force from gaining access to vital areas and destroying enough equipment to cause a meltdown. In most of these cases, the plant was fully in compliance with the security regulations. In a number of these exercises, the mock attackers also used explosives to breach the reactor containment; if the attack had been real, there would have been no barrier to release of radionuclides into the environment once the core began to melt.

Overall OSRE performance did not improve over time. Over the last two years of the program (2000-2001), the failure rate remained at 46%. In fact, the last OSRE to take place before the 11 September crisis led to a suspension of the program, at the Vermont Yankee plant, was the worst one on record.

The nearly 50% OSRE failure rate at U.S. nuclear power plants was largely due to the fact that the nuclear industry long regarded security as an unnecessary expense, and had drastically cut security budgets to reduce operating costs during the 1990s to try to make nuclear power more competitive with other sources of electricity. During this time, the NRC looked the other way.

The NRC has tried to downplay the significance of the OSRE test results, arguing that the OSREs are not "pass-fail" exams but merely learning experiences. However, some of the results, as documented in NRC inspection reports, reflect an incompetence so profound that the word "failure" is perfectly appropriate. To quote from a June 2001 inspection report at one plant,



“the licensee failed to prevent the mock adversaries from gaining access to two target sets...numerous responders were unable to deploy ... without being vulnerable to the adversary.”

Armed assault is not the only threat that nuclear plants are not equipped to handle. Although plants are required to defend against vehicle bombs of a certain size (the “design-basis” bomb), at a number of plants the level of protection is not adequate. For instance, the regulations require that all vehicles must be searched and declared free of explosives before they reach a point where a design-basis vehicle bomb could threaten safe plant operation. However, at 15-20% of plants in the U.S., the physical layout of the plant and its surroundings make this requirement difficult or impossible to meet.

Personnel access authorization programs at nuclear plants also have problems. Although NRC and the industry often say that no one is allowed unescorted access to sensitive areas of nuclear plants unless they have undergone an FBI background check, this is an untrue statement. At U.S. nuclear plants, contract workers can obtain “temporary” unescorted access for up to six months before their background checks have been completed. This provides a loophole that could be exploited by terrorists.

The response of the nuclear industry to the significant security vulnerabilities uncovered by the OSRE program was to try to kill the program. In 1998, as a result of industry pressure, NRC quietly cancelled OSRE, only to have to restore it promptly after word of the cancellation was leaked to the press. However, the industry did not cease in its efforts to discredit the OSRE program, and its complaints got a sympathetic hearing in NRC. In fact, before the events of 11 September, NRC and the industry were collaborating to weaken the program by it by giving the nuclear plant operators themselves the responsibility to conduct and grade the exercises.

The cavalier attitude toward security in the nuclear industry is best expressed in the following quote from Lynette Hendricks of the Nuclear Energy Institute (NEI), the chief lobbying organization for the U.S. nuclear power industry, which appeared in the magazine *U.S. News and World Report* on 10 September:

“We believe the [nuclear] plants are overly defended at a level that is not at all commensurate with the risk.”

Then came the events of 11 September, which one would think might cause a reevaluation of this position. However, there is no indication that such a reevaluation has taken place, since even now, the industry is fiercely opposing more stringent security requirements. Ms. Hendricks would likely make the same statement today.

Nuclear Plant Security After 11 September

Immediately following the World Trade Center attacks, the NRC “advised” its licensees to go to the highest level of security, but refused to issue a mandatory order, saying that it was unnecessary. In the absence of NRC guidance, some states called out National Guard troops to augment plant security forces, but others did nothing. Increased demands on security guards were largely met by compelling existing guards to work overtime, rather than hiring new guards. The result was spotty and inconsistent security.

Also, NRC suspended OSRE exercises after 11 September, arguing that it was dangerous to engage in such games when the U.S. was at high risk of a real terrorist attack. There may have been some merit to this argument in the aftermath of 11 September, but while the U.S. has largely returned to normal, OSREs still have not resumed. Thus there is no means of confirming whether plant security is up to the task of defending against the level of terrorist threat that is now known to exist.

More than five months after 11 September, the NRC did issue a mandatory order — at the prompting of



the White House — but gave plant operators six months to comply. Each plant was required to provide a schedule within 20 days for implementing the measures specified in the order, but nearly 75% missed the deadline, primarily because they had not carried out blast analyses to determine if their facilities were adequately protected from vehicle bombs. This implies that the state of technical knowledge of the resistance of nuclear plants to terrorist attack is still rife with uncertainty.

As a result of the terrorist attacks, the NRC initiated a “top-to-bottom” review of its security regulations and procedures, which still has not reached a conclusion. One key unresolved issue is whether the DBT should be revised. The DBT traditionally consists of only a small number of individuals working in a single team, based on an outdated assessment that any coordinated group of terrorists would be detected by intelligence activities once it reached a certain size. The 11 September attacks, which involved a coordinated assault of nineteen individuals in four teams, clearly shows the fallacy of this argument. The DBT also does not include the threat of aircraft attack. Despite the inadequacy of the current DBT, there is little indication that the NRC intends to make it more challenging in the near future.

In fact, there is an effective legal limit on the severity of the DBT. Protecting against threats posed by “enemies of the United States,” such as missile attacks from a foreign country, are not the responsibility of private entities. NRC and nuclear plant owners have asserted that protection against terrorist groups like Al Qaeda is the responsibility of the U.S. military, because such groups are “enemies of the state.” However, the U.S. military has not assumed this responsibility by providing armed forces or anti-aircraft weaponry at nuclear plants. The issues of who will set the necessary level of security, who will provide it and who will pay for it are difficult and far from being resolved. Meanwhile, the ability of nuclear plants today to protect against 11 September -scale threats remains a great unknown.

One thing the U.S. government has not hesitated to protect is basic information on nuclear plant safety that was routinely accessible by the public before 11 September. The NRC website was shut for several weeks, and only a fraction of the material that was formerly on the site has been restored. NRC argues that much nuclear plant safety information could be used as a blueprint for terrorist attacks and a guidepost to choosing targets. A new, sweeping category of “sensitive homeland security information (SHSI, or sushi)” has been created to encompass any materials that might be helpful to terrorists in seeking weapons of mass destruction. Unfortunately, this standard is so broad that it can be interpreted to include information that is important for public understanding of the safety of nuclear power plants. There is a great danger that the SHSI label will be used to restore the opaque screen behind which the nuclear industry operated during the height of the Cold War.

Legislation introduced in the U.S. Congress and recently approved by a Senate committee, calls for an interagency review of nuclear plant security, including an upgrading of the DBT, and establishes a Federal nuclear counterterrorism force to supplement the private guard forces at nuclear plants. This may be the only realistic means of bypassing the entrenched bureaucracy at NRC and forcing nuclear plants to apply the level of security needed to protect the public against radiological sabotage by sophisticated terrorists.

However, it may well be the case that this level of security is simply too expensive or infeasible. If plant operators are unwilling to pay the necessary security costs, then taxpayers would be stuck with the bill, effectively subsidizing nuclear energy by providing public funds for protection of private facilities. If the public objects to this use of taxpayer dollars, the viability of nuclear power as a long-term energy option must be called into question.