Protecting reactors from terrorists

by Daniel Hirsch, Stephanie Murphy, and Bennett Ramberg

THE NUCLEAR Regulatory Commission's (NRC) official "design basis threat"—the maximum terrorist attack for which nuclear power plants are required to be protected—was promulgated roughly a decade ago. It has not been revised since then, despite a dramatic shift in the nature and frequency of terrorism. A review of the available data regarding changing terrorist trends suggests that the design basis threat assumed by the NRC and the security and safeguards precautions that flow from them are dangerously out of step with the current reality of the terrorist threat.[1]

NRC security regulations 10 CFR 50.13 and 73.1 mandate that nuclear power plants need not provide protection against radiological sabotage attempts by:

- more than one insider;
- more than three external attackers;[2]
- attackers capable of operating as more than one team, that is, of employing "effective team maneuvering tactics";
- a group or individual utilizing weapons of greater sophistication than hand-held automatic weapons or equipment or explosives in quantities larger than can be carried by hand;
- "an enemy of the United States."

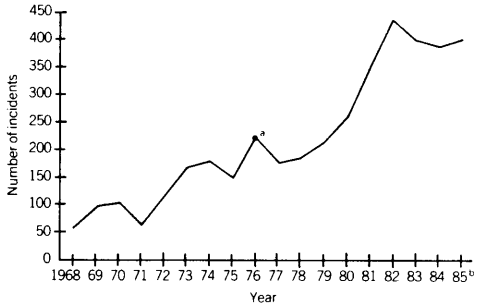
Power reactors therefore are required to have a minimum of only five guards, a number deemed by the NRC to be sufficiently "conservative" to repel the maximum "three-and-one" threat (three outsiders and one insider). Most facilities, however, employ more than the required five guards, apparently not accepting the NRC's assertion that its design basis threat is conservative. This modest level of threat against which plants are required to be protected was rationalized when originally promulgated in the 1974–1976 period on the following bases:

- intelligence information that there were no known groups "having the combination of motivation, skill, and resources to attack a fuel facility or a nuclear power reactor";[3]
- controversial studies asserting that redundant safety measures made severe core damage of such low probability as to be "non-credible";
- the belief that prospective terrorists had demonstrated an unwillingness to undertake actions that would result in large numbers of casualties and the assertion that moral and political constraints prevent terrorist actions which would result in large damage.

Each of these assumptions has been called into question since promulgation of the threat level for which protection was required, and thus nuclear plants may be unprepared for the kinds of threats that exist today. The Three Mile Island accident demonstrated that the assumptions of severe fuel damage being noncredible were in error even for accidental destruction. The consequences of an attack on a reactor facility or of an accident could, of course, be far worse than that at Three Mile Island since that incident was terminated prior to full core melt and the containment structure was not breached. The capabilities, motivations, and resources of terrorist groups appear to have grown significantly in the period since the NRC arrived at its threat basis. And most importantly, any assumption of moral and political constraints preventing terrorists from taking large numbers of lives seems mere wishful thinking in the wake of such incidents as the apparent sabotage of the Air India airliner off the coast of Ireland and the Beirut truck bombings. Terrorists today seem not to care about their own lives, let alone about others'.

Figure 1.

Terrorist incidents



RAND analysts defined terrorist acts as crimes involving violence or the threat of violence, usually directed against civilian targets, the motivation for which is political, and carried out in a way that will achieve maximum publicity. Certain discrepancies exist in the published RAND data; in such cases, we have used the data obtained directly from RAND.

[a]The "design basis threat" was developed by the Nuclear Regulatory Commission 1974-1976; the findings were published in Feb. 1977.

[b]As of Nov. 1985.

Sources: Gail Bass and Brian Jenkins, "A Review of Recent Trends in International Terrorism and Nuclear Incidents Abroad," N-1979-SL (Santa Monica, Calif.: RAND Corporation, April 1983); Bonnie Cordes et al., "Trends in International Terrorism, 1982 and 1983," R-3183-SL (Santa Monica, Calif.: RAND, Aug. 1984); and personal communication with the RAND team, Dec. 1985.

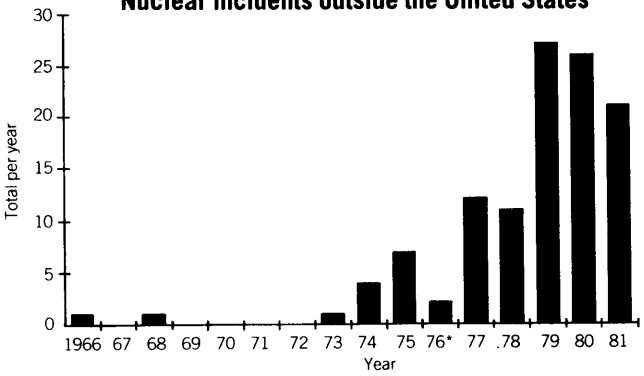
Daniel Hirsch is director of and Stephanie Murphy a research assistant at the Adlai E. Stevenson Program on Nuclear Policy at the University of California, Santa Cruz. Bennett Ramberg, senior research associate at the Center for International and Strategic Affairs at the University of California, Los Angeles, is the author of Nuclear Power Plants as Weapons for the Enemy: An Unrecognized Military Peril *(1984). This article is based on a study by the Nuclear Policy Program entitled "Nuclear Terrorism: A Growing Threat."*

Perhaps the most important factor undermining the validity of the NRC's current design basis threat and associated security requirements is the radical change in the incidence and nature of terrorism since those determinations were originally made. According to one measure, the number of international terrorist incidents has risen from an average of approximately 130 annually in the nine years before the NRC's design basis threat was finalized to about 400 such incidents during each of the last four years (figure 1). Similarly, the number of nuclear-related incidents abroad has risen an order of magnitude since promulgation of the threat basis (figure 2). Domestically, NRC data likewise indicate an increase, although not as pronounced, in nuclear related incidents.[4]

In addition to the quantitative trends, the nature of terrorism itself has changed. The presumption of moral or political constraints has vanished in the face of the dramatic rise in the numbers of fatalities involved—from about 10–20 per year in the late 1960s to a high of nearly 700 in 1983. The number of incidents with fatalities averaged a little more than 20 per year before the design basis threat was codified; thereafter, the number jumped, in recent years averaging over 70 annually. The capabilities of terrorists also increased, with simultaneous multiple events coordinated with considerable precision. These trends force one to conclude that the current design basis threat established a decade ago by the NRC for nuclear power plants is outdated, perhaps dangerously so.

Figure 2.

Nuclear incidents outside the United States



Nuclear incidents are defined by RAND as including events such as bombings, sabotage, arson, or assaults directed at nuclear facilities, or diversion, theft, or malevolent use of nuclear materials. RAND has complete data only through 1981.

*The "design basis threat" was developed by the NRC 1974-1976; the findings were published in Feb. 1977.

Source: Bass and Jenkins, 1983.

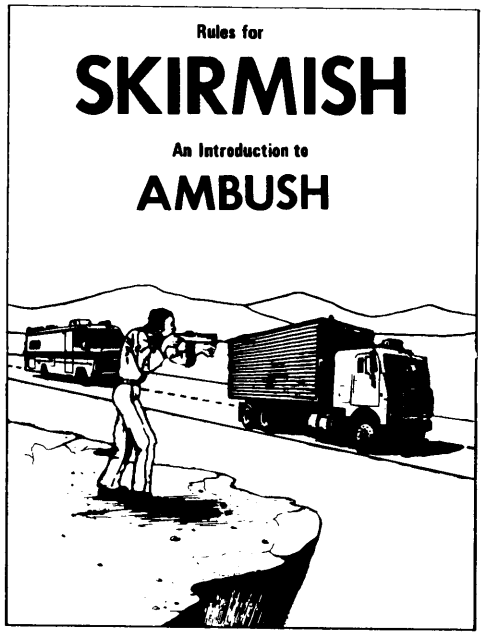
An important case in point is the agency's handling of the truck bomb threat. Documents obtained under the Freedom of Information Act reveal a troubling picture of the NRC's inner workings on this important matter. After the truck bomb incidents in the Middle East, many U.S. agencies took prompt action to put in place appropriate domestic precautions. An NRC survey of the Defense Department, the Secret Service, the State Department, and the Department of Energy found that "all four agencies believe that the 'truck bomb' threat in the U.S. is sufficient to prompt action."[5] Indeed, all four agencies implemented measures to counter the threat in the United States. Only the NRC has not.

In the wake of the Beirut truck bombings, the NRC safeguards staff concluded that this was a major new domestic risk and that the design basis threat should be changed to encompass it.[6] In January 1984 the process was begun to expedite promulgation of an "immediately effective rule"; the package was scheduled to reach the commissioners for approval in June of that year. In late April, that process was abruptly halted, and all action was deferred, supposedly "pending results of research" into the effects of truck bombs on reactors.[7] However, the research results had already come in, and with rather frightening conclusions. The study, performed by Sandia for the NRC and presented to the NRC staff on April 13, concluded, according to the Weekly Information Report to the commissioners: "The results show that unacceptable damage to vital reactor systems could occur from a relatively small charge at close distances and also from larger but still reasonable size charges at large setback distances (greater than the protected area for most plants)."

This research finding is particularly disturbing because it indicates that even a truck bomb detonated offsite could cause unacceptable damage to vital reactor systems. Inexplicably, however, two weeks after the Sandia briefing, the NRC staff decided to defer any action to include protection from vehicle bombs in the design basis. Nearly two years have passed, and the Commission has yet to take action, making it the only comparable agency not to do so. The NRC, however, did send out a nonbinding information notice, "suggesting" that licensees "review vehicle access procedures," but not requiring them to take any actions to redress vulnerabilities that might be identified.

In addition to NRC's inaction causing problems in assuring adequate protection against sabotage, two areas of NRC action may also have the effect of worsening the security situation at some reactors:

- After at least 15 years of requirements that some measure of sabotage protection be provided at research and test reactors, the NRC staff has undertaken action to eliminate



The box cover of Skirmish, a board game designed to simulate ambush attacks on moving vehicles, including those transporting nuclear materials. Robert Renne, of Sandia Laboratory in Livermore, California, explained that all security personnel "can't spend years taking the Army Special Forces course." The game was developed as an alternative to expensive computer simulation games.

A Skirmish game in progress. Sandia Laboratory wanted "a wide dissemination of information on how to protect facilities. . . . The Japanese, Germans, French, and ourselves should share the technology," said Robert Renne of Sandia. Developers of security techniques are concerned about how to "make sure terrorists can't use [publicly available training information] against you," he added. But the game did not pose a security threat, he offered, because "most terrorist groups [already] do a good job of what Skirmish was designed to do": scout the terrain surrounding a proposed attack site.

all such requirements.[8] This would be quite serious, because, unlike power reactors, many of these reactors are urban-sited. Although far smaller than power reactors, the dose to the public from successful sabotage of research or test reactors could be very high because there is generally neither a containment to trap the radioactivity nor a buffer zone to disperse it before exposing people. It is therefore troubling that despite the refusal by the NRC commissioners to approve staff-requested changes to the regulations that would have eliminated sabotage protection for research reactors, the NRC staff has proceeded to issue instructions to its inspectors to stop enforcing sabotage requirements at such facilities.

• The second concern regards the kind of sensitive security information the NRC routinely issues in public documents. The NRC and various support agencies have published an astonishing array of material on the nature of security at these facilities and the best way to bypass it. One can obtain from the Government Printing Office, by phone, charged to a credit card: generic training manuals for site security personnel and for transportation security personnel; detailed design guidance for physical protection systems at power reactors; board games to simulate terrorist attacks, for example one set called "Skirmish and Ambush"; detailed manuals for generic security communications systems, intrusion and duress alarm systems, key and lock systems, physical barriers, closed-circuit television systems, vehicle search procedures, and so forth.

Perhaps the most disturbing documents publicly available are a series of scientific assessments of how to penetrate security barriers. The government has tabulated the best ways to get through various protective barriers, even to the point of describing the optimal tools and explosives to use for each, the weight of such tools (so the attacking team knows how much each member can carry), and the amount of time, to the fraction of a minute, it would take.

While it is no doubt useful to let licensees know the weak points of security systems and the most effective ways an adversary might penetrate those barriers, it is inexplicable that the NRC would make that information fully available to adversaries as well.

As other studies make clear, the 1981 Israeli bombing of the Osirak reactor in Iraq and the 1984–1985 Iraqi bombing of nuclear power plants under construction in Iran demonstrate that whatever psychological barrier might once have existed against the destruction of reactors appears to have been broken. Destruction of reactors is now a far more credible threat than before, and a dangerous escalation of nuclear destruction might well have begun. The provisions of the regulations exempting reactors from protection against attack by "an enemy of the United States" seem particularly obsolete, given these new developments.

It seems quite unrealistic to require protection of power reactors from only one insider and/or three outside adversaries, working only as a single team, with nothing more sophisticated than hand-held automatic weapons and with no more explosives than can be carried by hand. The NRC's

A Nuclear Regulatory Commission book designed to offer suggestions for protecting nuclear storage facilities also show how to break into them. In the photos here, men from the U.S. Army's Aberdeen Proving Ground use an axe to break in after an explosive charge has exposed part of the mock facility's plywood wall (above); at right, the attacker has successfully penetrated the facility.

assessment of potential terrorist threats to nuclear facilities and the measures required to protect against that threat remain stuck in the assumptions of a decade ago—assumptions which, if they were ever valid, no longer are. □

1. Detailed discussion and documentation can be found in Daniel Hirsch, Stephanie Murphy, and Bennett Ramberg, "Nuclear Terrorism: A Growing Threat," SPNP-85-F-1 (Santa Cruz, Cal.: Stevenson Program on Nuclear Policy, 1985) and "The Failure to Provide Adequate Protection against Nuclear Terrorism," SPNP-85-F-3 (Santa Cruz, Cal: Stevenson Program on Nuclear Policy, 1985).

2. Title 10, Code of Federal Regulations, Part 73, Section 1 requires protection against an attack by "several" persons. In the Diablo Canyon case, the appeal board rejected claims by the governor of California that the facility should be able to protect against an attack by up to 12 people, finding that the NRC had intended several to mean three. Although the specific number was expurgated from the published decision, it is readily inferred from unexpurgated material and other documents cited in the decision which were made public.

3. NRC's Statement of Consideration accompanying the final rule, 42 FR 10836, Feb. 24, 1977.

4. Data from the NRC's *Safeguards Summary Event List*, NUREG-0525, Rev. 9, indicate that the number of domestic "nuclear safeguards events" went from an average of approximately 70 annually for the first three years for which data are available to an average of about 120 for each of the five years thereafter. Assessments are more difficult than from the RAND data (see figures 1 and 2) because the pre-1976 figures are not tabulated. The NRC uses the term "nuclear safeguards event" to refer to events at nuclear facilities which are bomb-, transportation-, or firearms-related, involve arson or sabotage, or involve nuclear materials missing or allegedly stolen. Differences in definition make the RAND and NRC data not readily comparable. It should be noted, however, that to date domestic incidents have generally been of a lower order of severity than incidents abroad, although it is not at all clear that this will remain the case.

5. NRC, "Comparison of Agency Response to 'Truck Bomb' Threat in the U.S.," internal memorandum, May 9, 1984, released under the Freedom of Information Act.

6. NRC, "Design Basis Threat," internal memorandum from Robert Burnett, director, Division of Safeguards, to George McCorkle, chief, Power Reactor SG Licensing Branch, Division of Safeguards, Jan. 27, 1984, released under the Freedom of Information Act.

7. Memorandum, Burnett to McCorkle, April 26, 1984, released under the Freedom of Information Act.

8. In late 1983, the NRC staff petitioned the commissioners to rewrite the 1973 regulations and overturn the 1970 and 1983 adjudicatory decisions that required sabotage protection for research reactors: memorandum SECY-83-500, Dec. 6, 1983. On June 6, 1984, the commissioners rejected the staff request: CLI-84-10, 19 NRC 1330. Notwithstanding the commissioners' refusal to change the requirement, the staff directed its inspectors to stop enforcing it: ACRS transcript, May 7, 1985, pp. 121–30.