The Truck Bomb and Insider Threats to Nuclear Facilities

Daniel Hirsch

There are two primary safeguard and security risks associated with fixed-site nuclear facilities and with nuclear materials in transit the theft of weapons-grade nuclear materials or fully assembled nuclear devices and sabotage The potential consequences to the public from either action can be surprisingly similar

In the field of nuclear safeguards and security, there is a tendency to protect against threats that are relatively easy to address and to ignore those that are somewhat more difficult However, overall security is a function of the weakest links in the security chain, links that societies ignore at their own peril In the nuclear field, two of these weak links in the security chain are the truck bomb threat and the insider threat The risks associated with terrorist use of vehicular bombs against nuclear targets surfaced (actually, resurfaced) following the terrorist attacks on the U S Embassy annex and the Marine compound in Lebanon Concern was expressed that similar attacks against nuclear facilities could result in substantial damage and release of radioactivity Since the current regulations of the NRC require licensees to protect only against attacks on foot (and even then, only against very small attacking forces), shortly after the Lebanon bombings, that agency commenced an urgent rulemaking to require its licensees to protect against truck bombs Inexplicably, that rulemaking was called off after research results indicated that the truck bomb threat to nuclear facilities was even more serious than previously thought [1]

Even were nuclear facilities adequately protected against external attack, be the aim theft or sabotage, the greatest security risk to these sites—the threat of action by insiders—would remain The insider threat is particularly difficult to resolve because nuclear facilities typically employ large numbers of people, and certain employees must have access to vital areas of the facility in order to perform their work Some employees could take advantage of that access to perform acts of sabotage or theft that could be immensely

destructive The traditional methods of protecting against the insider threat—such as the two-person rule, strict compartmentalization of vital areas, and design features that make damage to two or more redundant systems by one individual difficult—are generally expensive and have encountered substantial resistance from the nuclear industry, which has restrained the NRC from requiring them

Truck Bomb Threat

The NRC established most of its security regulations for nuclear facilities and materials in the mid-1970s Those regulations required power reactors to be protected only against three external attackers, working as a single group, moving on foot, with weapons no more sophisticated than hand-carried automatic weapons and with the possible assistance of no more than one insider NRC-licensed facilities with weapons-usable nuclear materials were required to meet only a marginally higher standard that primarily involved a slightly larger attack group capable of operating as two teams Research reactors, even those using highly enriched (weapons-grade) uranium, as well as those reactors posing a substantial sabotage risk because of their urban siting and lack of a containment structure, were, according to NRC staff, exempted from both requirements [2]

Basing security at power reactors on a defined maximum threat of a very small group with only those explosives they can hand carry (10 CFR §73 1) leaves these facilities highly vulnerable to vehicular bombs This omission was not, however, an oversight The original proposed security regulations had included a provision requiring "appropriate barriers" to obstruct ready access by ground vehicles, but it was explicitly deleted from the final regulation on the following basis "The Commission has decided that this proposed provision should be further studied before being considered for inclusion in the regulations. This proposed amendment has been deleted from the rule "[3] Whether those studies were ever conducted is unclear What is clear, however, is that ten years later, the NRC security regulations still require protection against only a small group of adversaries on foot, despite a marked rise in international terrorism, including acts against nuclear targets

A mounting series of truck bombings directed at U S installations in the Mideast led the NRC to reexamine the issue in early 1984, with considerable urgency In a press release at the time, the NRC noted the

> publicized events where U S installations overseas have been the target of terrorists using vehicle bombs and the Executive Branch's recent announcement that security precautions at certain government facilities in this country

> have been upgraded as a result [NRC] *Licensees currently are not required to protect against such attacks*
>
> As a matter of prudence, the staff is reviewing this matter on a continuing basis to ensure that security requirements provide for the continued protection of the public health and safety[4] (Emphasis added)

The review by NRC safeguards staff concluded that the regulations needed to be changed rapidly They directed the development of "an immediately effective rule which revises the design basis threat for both radiological sabotage and theft to include the introduction by an adversary of explosives and other equipment by vehicle"[5] Because of the urgency of the situation, the rule was to be written in the shortest possible time and to go into effect immediately upon publication, without the usual delays At the same time, the NRC contracted with Sandia National Laboratories to study the potential damage that truck bombs of various sizes could cause at various distances from a power reactor

Three months later, on April 26, 1984, all action on the proposed rule was deferred, "pending the results of research"[6] The research results had actually been provided to the NRC two weeks earlier, however A review of those findings raises troubling questions about the manner in which the NRC has tended to deal (or not deal) with difficult terrorism problems

The task the NRC gave Sandia was as follows

> Terrorist activity in other parts of the world has exemplified the destructive consequences of an explosives-laden vehicle i e , a truck used as a weapon against a facility Given this threat, the NRC seeks to evaluate the potential vulnerabilities of nuclear facilities in this country against such action, to determine the "worst case" potential consequences, and to develop *easily implemented, cost-effective safeguards mechanisms* for preventing facility access of such a vehicle (Emphasis added)[7]

On April 13, 1984, the NRC was provided the results of the Sandia study As the staff subsequently reported 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)"[8]

Why did the NRC, which had initiated an urgent rulemaking to address the truck bomb threat, suspend action on the matter only two weeks after these results, which were extremely disquieting, came in Its action might be easier to understand had the sequence of events been reversed—for example, a January 1984 decision to commence research to see whether truck bombs could cause serious damage to a reactor, with action suspended pending the research results, followed by a subsequent decision to go ahead

with an urgent rulemaking to address the problem when the research indicated the threat was serious It is hard, however, to comprehend why, if the NRC viewed the truck bomb threat as sufficiently serious to commence an immediate rulemaking before the research findings were available, it called off action when the study's conclusions confirmed serious problems

An explanation for this state of affairs can perhaps be found in the original direction the NRC provided to Sandia The NRC gave Sandia three research tasks evaluate the vulnerability of U S nuclear facilities to a truck bomb attack, determine the potential consequences of such an attack, and develop easily implemented inexpensive mechanisms for preventing access of explosive-laden vehicles

Sandia's research produced unpleasant findings regarding each of the questions posed It concluded that nuclear facilities in the United States are extraordinarily vulnerable to truck bomb attacks, that such an attack could result in "unacceptable damage," and that addressing the problem would require more than just a few concrete flower pots or barricades near the reactor because of Sandia's extraordinary finding that "unacceptable damage to vital reactor components" could result even if the truck bomb were detonated off-site Thus the problem was graver than previously thought (and therefore more needy of prompt action) and required costly corrective measures (which were therefore likely to be resisted more vigorously by licensees)

As members of the Advisory Committee on Reactor Safeguards (ACRS) have pointed out, there is a difference between the NRC and other federal agencies, which had already taken measures to protect against truck bombs (including the DOE for its reactors)[9] That difference can help explain why the NRC is the only comparable federal agency not to have taken domestic precautions against truck bombs The expense of the security measures adopted by the other agencies was borne by taxpayers, whereas if the NRC expanded its design basis threat regulations to require protection against vehicular bombs, the added security costs would have to be covered by the utilities that own the nuclear facilities[10] Here is a unique situation where the level of protection at a nuclear facility is determined by who owns it rather than by how many people could be hurt by a failure of its security

As long as the proposed NRC truck bomb rule involved only a few extra concrete barricades on-site, the cost to the licensees would have been minimal and the political cost to the NRC acceptable When research revealed that the problem was considerably more serious than previously thought and the solution therefore more expensive, the regulatory agency apparently felt it could not afford to require action proportionate to the problem

This situation raises the peculiar paradox of contemporary regulatory agencies such as the NRC with regard to large problems such as the risk of nuclear terrorism As long as the problem is small and the solution not costly to those being regulated (and thus not politically costly to the agency doing

the regulating), the agency feels it can act Should the problem turn out to be major, with significant risks to the public, and the solution therefore consequential in terms of costs to the licensees, the agency comes under substantial internal and external pressure to leave the problem unattended

Thus, ironically, it is only those links in the security chain that are already relatively strong that the commission feels it can address because they are inexpensive, both economically to the licensees and politically to the agency The weak links, such as vulnerability to truck bombs, remain "deferred pending further study" Yet it is the weak links that create the bulk of the risk to the public and to the nuclear industry itself

Insider Threat

The second critical weak link in nuclear security is the insider threat Indeed, ACRS members have justified their inaction on the truck bomb issue, in part, on the basis that resolving it would still leave nuclear facilities extremely vulnerable to acts by insiders [11] Yet as little action has been taken to mitigate the insider threat as that of the truck bomb problem

Examples of past incidents involving the insider threat range from the relatively inconsequential (such as theft and attempted extortion involving low enriched and only mildly radioactive uranium dioxide powder or theft of kilogram quantities of depleted uranium and subkilogram quantities of highly enriched uranium) through events costly to the company involved but not dangerous to the public (destruction of a large quantity of fresh fuel assemblies at a nuclear power plant) to occurrences that are potentially very serious (such as intentional disabling of a power reactor's emergency core cooling system or the backup diesel generators) All point to the difficulties in protecting nuclear materials and facilities from insiders [12]

> In 1981 at the Beaver Valley nuclear power plant near Liverpool, Ohio, someone shut a valve to the high head safety injection pumps, a crucial part of the emergency core cooling system (ECCS), an act that disabled the high-pressure portion of the ECCS This act could have been serious had there been an incident in which that system were needed (for example, a small loss of coolant accident where high-pressure injection of emergency cooling water would have been necessary) The consensus of opinion was that the act was intentional [13]
>
> Also in 1981, at the Nine Mile Point Unit I nuclear power plant in Oswego, New York, the NRC found what it described as a "major degradation" of the backup power supply needed in case of a loss of off-site power Diesel generators failed to start when tested because of an apparently deliberate closure of the drains on the fuel oil filters The utility concluded that the problem was the result of tampering [14]

At the Salem Unit II nuclear power plant in Salem, New Jersey, in August 1982, the manual isolation stop valves to the air start motors to the number 2C diesel generator were found closed This condition would have prevented both automatic and manual start-up of the diesel generator were it needed in an emergency (such as loss of off-site power) The event occurred despite increased precautions by the licensee put in place after an act of suspected sabotage the previous week [15]

On July 1, 1969, four depleted uranium plates and a smaller quantity of highly enriched uranium were reported lost from a nuclear facility at MIT The materials were subsequently found on the desk of an MIT professor following police questioning of a suspect The consensus was that a master key was probably used to gain access to the material, presumably by an MIT graduate student who was the prime suspect [16]

In January 1979, the general manager of the GE nuclear facility in Wilmington, North Carolina received an extortion letter with a sample of uranium dioxide powder The letter stated that the writer had two five-gallon containers of low enriched uranium dioxide that had been taken from the plant The containers were identified in the letter by serial number and were subsequently authenticated as being missing from the plant The letter demanded $100,000 or else the material would be dispersed in an unnamed U S city An employee of a GE subcontractor was arrested and sentenced to fifteen years in prison [17]

Also in 1979, two plant operator trainees at the Surry nuclear power station in Newport News, Virginia, entered the fuel storage building, which was locked and alarmed, and poured sodium hydroxide on sixty-two of sixty-four new fuel assemblies stored there, damaging them Both individuals had authorized access to the storage building [18]

Insiders pose a dual threat theft of nuclear materials and sabotage of the facility The amount of material unaccounted for (MUF, now referred to as the inventory difference, or ID) from facilities in the United States handling highly enriched uranium or plutonium is enough to fabricate hundreds of bombs It is uncertain whether all that material has merely been lost through faulty accounting procedures or whether some has been stolen or diverted It is clear, however, that the risk of the theft of these materials by insiders, or with the assistance of insiders, is substantial It is widely believed, for example, that the large apparent diversion of highly enriched uranium from the NUMEC facility in Apollo, Pennsylvania, was accomplished with the assistance of a well-placed insider [19] The continuing long-term problem with inventory differences outside acceptable statistical margins at the Erwin, Tennessee, facility, which handles large quantities of highly enriched uranium, is particularly worrisome in this regard, as is the NRC's willingness to permit continued operation of the plant without resolution of the problem

An insider or conspiracy of insiders could cause immeasurable harm through sabotage The fuel in a nuclear power reactor must be cooled con-

tinually, otherwise it can melt and release large quantities of fission products to the environment This requirement holds true even after the reactor is shut down because decay heat is generated long after the control rods stop the fission process Loss of either the coolant or the electricity to power the pumps to move the coolant could be disastrous Although all reactors have backup systems, it is precisely the attack on important backup systems that makes insider sabotage attempts such a concern

In this regard, the published probabilistic risk assessments (PRAs) performed for a number of nuclear plants are problematic They are of questionable use for their principal purpose the estimation by the NRC and the nuclear industry of quantitative values for absolute risk from particular facilities Worse, they could provide virtual road maps for saboteurs PRAs and much of the recent source term research identify the worst possible sequence of events at nuclear facilities that could result in large releases of radioactivity to the environment Some argue that the probability of the most serious of these release sequences occurring accidentally is very small Whatever the truth of that hotly contested matter, no such statement can be made about the probability of their being made to occur intentionally As former NRC chairman Palladino has remarked, unlike reactor accidents involving human error, sabotage is not mathematically random and involves deliberate attempts to defeat safety systems [20]

The regulatory and industry responses to the insider threat have been remarkably similar to the response to the truck bomb threat. they hope that it goes away on its own Indeed some proposed actions appear to be making matters worse For example, rather than further compartmentalizing vital areas so that there is greater control of access to crucial portions of nuclear plants, vital areas are proposed to be combined into larger islands Once through a single access point, workers would be free to wander through large areas of the plant

A recent event at the Turkey Point nuclear power station is indicative of the inadequacies in current practices designed to prevent insider sabotage While sabotage has not been ruled out as the cause, the preponderant belief is that this particular incident was the result of personnel error It is, however, illustrative of how sabotage could take place and remain undetected for long periods of time At Turkey Point, a shared auxiliary feedwater system supplies two reactors at the site The system provides feedwater when the main system is not in service or when only small feedwater flows are required While one reactor was down for maintenance, someone valved out the feedwater system for the operating unit For five days, no one noticed that the system had been rendered inoperable, despite a requirement that a thorough check be performed twice per shift The failure to detect the disabling of the feedwater system occurred apparently because the checks were not adequately detailed in instructions and because appropriate "out for maintenance" tags had been

placed on the inappropriately closed valves. Had normal feedwater flow been interrupted during that period, a serious situation, including the potential for core damage, could have resulted because the auxiliary system was valved off.[21]

A traditional approach to the insider problem, the two-person rule (prohibiting unaccompanied presence in vital areas), has met with great resistance from industry and within the NRC. Even existing regulations designed to provide some measure of protection against insiders seem to be enforced and complied with inadequately. Violations of access controls are commonplace, and the small fines imposed when such violations are detected seem to offer little deterrent to repetition of the infractions.

It is troubling that the current proposed NRC rule on insider safeguards, weak though it is, is being opposed by the nuclear industry and the ACRS. The ACRS has endorsed an alternative proposed by the Nuclear Utility Management and Human Resources Committee (NUMARC), which both groups argue is preferable to the issuance of a commission rule. NUMARC proposes that the minimal actions suggested by the NRC staff not be made a binding regulation but rather that there be "industry oversight of the program based on a policy statement issued by the commission endorsing some guidelines."[22] The NRC staff says that "the more effective way to go is the rule" because "policy statements have a tendency to wither up and go away."[23] Nevertheless the ACRS opposes the staff proposal for a binding rule.

An important method of reducing the insider risk is careful attention at the design stage to the inclusion of features that make insider-induced sabotage difficult. An example of a design problem that would make the work of an insider easier rather than harder is reported by NRC security officials to have occurred recently at the Wolf Creek nuclear plant. A security officer at that facility is said to have entered a command into the security computer erroneously, which had the effect of unlocking the doors to all the protected and vital areas of the plant. It was fifteen minutes before anyone realized that, having pushed this button, all the doors were unlocked.[24]

One approach to designing nuclear plants to make them more resistant to insiders is to ensure that redundant safety features are located in different vital areas such that access to both areas by the same individual is difficult. In this regard, the NRC's recent policy statements regarding severe accidents and reactor standardization are troubling. By declaring the current generation of nuclear plant designs safe enough and by indicating that new standardized designs need be no safer than current models, much of the impetus to improve reactor safety and security by a new standardized design has been undercut. Attention to sabotage protection at the design stage is, however, important to dealing with the terrorist threat.

Stricter regulation, stricter enforcement, better security controls at nuclear facilities, and more attention to protection against sabotage at the design

stage can help reduce the insider threat It is not a problem, however, that will go away on its own

Potential Consequences and Implications

The risks associated with the theft of weapons-usable nuclear materials and/or a fully assembled nuclear device are well recognized A clandestine fission explosive could kill on the order of the same number of people as died at Hiroshima or Nagasaki (Various accounts give the dead as approximately 70,000 and 40,000, respectively, within the first thirty days of the bombings, with deaths resulting from injuries or radiation-induced cancer occurring for extended periods thereafter [25]) This would be a calamity of awesome scale An additional risk is the potential for triggering a larger nuclear war

The risks associated with the intentional destruction of nuclear energy facilities are not so well appreciated Not generally recognized is that the potential consequences of sabotage of a power reactor are not so different from those of a clandestine fission explosive In fact, one of the arguments raised (successfully) against publishing revised Atomic Energy Commission (AEC) casualty estimates for severe reactor accidents in the mid-1960s was precisely that point the comparability of potential casualties from a severe reactor incident and an atomic weapon explosion

In the mid-1960s, Brookhaven National Laboratory (BNL) was asked by the AEC to assess the potential consequences of severe reactor accidents in preparation for congressional consideration of extending the Price-Anderson nuclear liability legislation, given the considerably larger reactors then being built. The BNL study concluded that a large accident could result in as many as 45,000 deaths, significant radioactivity levels extending over an area of 10,000 to 100,000 square kilometers (the famous conclusion about contaminating an area the size of the state of Pennsylvania), thyroid dose levels greater than the prescribed limits of the Federal Radiation Council extending beyond 1,000 kilometers, and $17 billion in damage [26] AEC memoranda pointed to the "dangers of publishing" these conclusions and advised against their release, a prime reason being that "the results of the hypothetical BNL accident are more severe than those equivalent to a good sized weapon and this correlation can readily be made by experts if the BNL results are published "[27]

Subsequent site-specific estimates of severe incidents at nuclear power reactors have produced even larger casualty estimates For example, an NRC environmental impact statement for the San Onofre nuclear powerplant near Los Angeles estimated up to 130,000 acute fatalities, plus 300,000 latent cancers and 600,000 genetic effects The cost of off-site mitigating actions was estimated at $35 billion [28]

Some argue that the accidental combination of failures necessary to produce such massive consequences is highly unlikely Even if true—and it is a matter hotly disputed in nuclear safety circles—that does not mean it could not happen intentionally PRAs provide something of a manual for would-be saboteurs intent on creating the largest effect [29]

Attacks on reactors may have an escalatory effect as well As Bennett Ramberg, perhaps the leading scholar on the subject, has argued, attacks on nuclear reactors with conventional weapons may provide nonnuclear nations or subnational groups a near-nuclear capability [30] A power reactor contains about 1,000 times the long-lived radioactivity of a Hiroshima bomb Use of conventional attacks on nuclear energy facilities as a form of radiological warfare may provide the escalatory link between conventional attack and nuclear response

Thus, nuclear terrorism aimed at the sabotage of nuclear energy facilities and nuclear terrorism involving clandestine fission explosives may be comparably destructive

Conclusions and Recommendations

Nuclear terrorism in the form of the theft of weapons-usable nuclear materials or sabotage of nuclear facilities poses substantial societal risks, particularly in an age of escalating terrorism Protection against these forms of nuclear terrorism is only as strong as the weakest links in the nuclear security chain Two of the weakest links at present are the dangers associated with truck bombs and insiders Regulatory agencies do not appear to be focusing on the weak links in the chain but rather on those problems for which the solutions are cheap and easy Unfortunately, the major contributors to nuclear terrorism risks are generally not conducive to solutions that are either cheap or easy Doubly unfortunate is that deferring action on the central contributors to nuclear terrorism risks makes the probability of such catastrophic events considerably more likely

What should be done? A nonexhaustive list includes a number of policy recommendations

First, revise the decade-old design basis threat regulations (10 CFR §73 1) to include consideration of vehicular bombs and attacking groups considerably larger and more sophisticated than the current, unrealistically modest three-and-one threat, which assumes attackers capable of acting only as a single team and traveling only on foot [31]

Second, repeal the two-decades-old regulation (10 CFR §50 13) prohibiting consideration in licensing and regulatory matters of potential sabotage by "enemies of the United States, whether a foreign government or other person"

Third, reverse the 1984 directive sent by NRC staff to the regional inspection and enforcement offices ordering them to stop inspection and enforcement activities related to sabotage protection requirements at research reactors, issued despite a decision by the commissioners refusing a staff request to repeal the regulation requiring such protection

Fourth, tighten insider protection requirements forgo consideration of vital islands, institute and enforce a strict two-person rule, require protection against more than one insider, significantly increase the penalties for violations of access controls, and make all insider requirements mandatory regulations rather than industry-supervised guidelines

Fifth, require substantial sabotage-resistant design features as a condition for construction permits for any new nuclear plants and for approval of any standardized reactor design

Sixth, make regulations consistent across agencies It is of questionable logic that DOE reactors should be required to protect against truck bombs but NRC reactors not, that shipments of Canadian-origin Taiwanese spent fuel across the United States under DOE jurisdiction not be required to have security, whereas NRC-supervised shipments must, and that highly enriched, weapons-grade uranium at university reactors is exempt from the security requirements that the same material must meet if located at other fuel cycle facilities

Seventh, expeditiously remove all highly enriched uranium from NRC-licensed research reactors and replace it with low enriched uranium Despite the new NRC rule, resistance from NRC staff and from the DOE is likely to slow the process substantially The provision in the regulation that the DOE must certify the availability of funding to pay for all conversion costs, including those of commercial reactors, means that Congress must continue annually to appropriate the funds and the DOE must spend those funds as intended Until the conversions are completed, the security requirement in 10 CFR §73 67 must be changed from a posttheft detection and reporting requirement to a genuine theft prevention standard

Eighth, require all DOE research reactors to convert to low enriched uranium and stop all shipments of highly enriched uranium abroad now that low enriched uranium replacement fuels are available Conversion of research reactors worldwide would remove hundreds of formula quantities of highly enriched uranium from approximately 150 sites in dozens of countries

Ninth, clarify the law regarding the right of security forces at nuclear facilities to use deadly force Even the guard force at the Lawrence Livermore National Laboratory is reportedly uncertain whether it is legally permitted to use lethal force [32] The guards are employed by the University of California, a state institution that operates the lab for the DOE and whose employees are prohibited from using lethal force However, the laboratory at which the guards are stationed is a federal installation where, under guidelines estab-

lished in 1985 lethal force would normally be permitted if necessary to prevent the theft of plutonium. The matter is even more unclear at commercial power reactors, which are generally not located at federal installations Currently guards at some of these nuclear plants have informed NRC inspectors that if an attack were directed against their facility, they would not resist it because of uncertainty as to whether they would thereafter be held to have used lethal force illegally

Tenth, the most important change necessary is a change in attitude and personnel on the part of the nuclear industry and its regulators The current extraordinary pressures for deregulation of the nuclear industry in the long run can only work against the interests of both the industry and the public Regulators and those they regulate must take security far more seriously Troubling issues such as the truck bomb and insider threats can no longer be dealt with by sending them back for further research or by asking for voluntary compliance with nonbinding guidelines The complaisance within some circles of the NRC, the DOE, and the nuclear industry cannot be permitted to continue, given the current nature of the threat It is hard to understand, for example, why the S site at Los Alamos was permitted to continue operating for four years with grossly inadequate security and despite repeated critical safeguards reviews, culminating in one where the facility failed three out of three security tests In two of the simulations, terrorists would have gotten away with weapons-grade plutonium; in the third, they would have successfully obtained an unlocked nuclear test device constructed for the Nevada test site that could have been detonated within hours of its theft [33] When failures of this sort are detected, the responsible parties should be rapidly removed from their posts, and the same should be true for the regulators who fail strictly to enforce the regulations New officials who are serious about the risks of nuclear terrorism and the need to protect adequately against its occurrence are needed at the NRC and DOE and within the nuclear industry

Last, proposals to reduce the size of the emergency planning zones (EPZs) around nuclear power plants by 95 percent should be denied Whatever the merits of the claims by the nuclear industry of a reduced source term in nuclear accidents—and they seem questionable at best—the claims do not apply to sabotage, particularly in situations in which early containment failure is the aim EPZs should be based on the distances at which radiation levels would exceed federal protective action guidelines for the worst possible intentional or accidental destruction of a reactor As a society, the United States needs to take considerably greater measures to reduce the likelihood of reactor destruction It also needs, however, to have workable emergency plans in place in case those measures fail

Notes

1 For more detail, see Daniel Hirsch, Stephanie Murphy, and Bennett Ramberg, "The Failure to Provide Adequate Protection against Nuclear Terrorism," Stevenson Program on Nuclear Policy, Santa Cruz, Cal., December 1985, printed in a slightly different version as "Protecting Reactors from Terrorists," *Bulletin of the Atomic Scientists* 42 (March 1986) See also "Nuclear Terrorism A Growing Threat," report presented by the same authors in support of testimony before the Safeguards and Security Subcommittee of the NRC's Advisory Committee on Reactor Safeguards, May 7, 1985 The contributions by Ms Murphy and Dr Ramberg to the research on which this study is based are gratefully acknowledged

2 NRC staff assert that research reactors are not required to provide protection against theft of weapons-grade uranium, merely posttheft detection and reporting, and need have no sabotage protection whatsoever These assertions have been quite controversial The NRC's Atomic Safety and Licensing Board, for example, has ruled that protection against sabotage is required, the NRC staff position on the issue being at odds with NRC regulations and case law NRC staff subsequently requested that the NRC commissioners eliminate the sabotage protection regulation, a request that was denied The staff has nevertheless unilaterally directed its inspectors to cease inspection and enforcement activities related to sabotage protection at research reactors

3 NRC,"Amendments to 10 CFR Part 73 to Specify Measures for Physical Protection of Nuclear Power Reactors from Industrial Sabotage and to Provide Clarification of the Applicability of 73 50 to Nuclear Reactors," SECY-76-242 (Washington, D C , April 26, 1976), encl A, p 4

4 NRC, "NRC Staff Suggests Licensees Should Review Vehicle Access Procedures," NRC press release no 84-18 (Washington, D C , February 6, 1984)

5 See internal memorandum, Robert F Burnett, director, Division of Safeguards, Office of Nuclear Material Safety and Safeguards (NMSS), to George W McCorkle, chief, Power Reactor SG Licensing Branch, Division of Safeguards, NMSS, "Design Basis Threat," January 27, 1984, NRC, Washington, D C , obtained under the Freedom of Information Act

6 See internal memorandum, Robert F Burnett, director, Division of Safeguards, NMSS, to George W McCorkle, chief, Power Reactor SG Licensing Branch, Division of Safeguards, NMSS, "Design Basis Threat," April 26, 1984, NRC, Washington, D C , obtained under the Freedom of Information Act

7 NRC, "Statement of Work Investigation of 'Truck Bomb' Threat at Nuclear Facilities," n d , document obtained under the Freedom of Information Act

8 From "Weekly Information Report to the NRC Commissioners," April 20, 1984, enclosure E, p 3

9 See the transcript of the meeting of the ACRS Subcommittee on Safeguards and Security, May 7, 1985, during my testimony The ACRS subsequently recommended against revising the design basis threat regulations to include consideration of vehicular bombs See "ACRS Comments on Provisions for Protection against Sabotage," (Washington, D C NRC, July 17, 1985)

10 This point was made rather explicitly in an internal NRC memorandum that

discussed reasons why NRC staff opposed upgrading security regulations to require nuclear powerplants to undertake truck bomb protective measures or contingency planning In the memorandum, obtained under the Freedom of Information Act, the director of the NRC's Division of Safeguards argues succinctly that "protection against truck bombs should not be a responsibility of commercial entities " See memorandum, Robert F Burnett, director, Division of Safeguards, NMSS, to John G Davis, director, NMSS, "Truck Bomb Threat," August 14, 1984

11 See ACRS Safeguards and Security Subcommittee transcript

12 I am indebted to Steve Sholly of MHB Technical Associates for identifying the first three examples

13 See NRC, "Report to Congress on Abnormal Occurrences, July–September 1981," NUREG-0090, vol 4, no 3 (Washington, D C , January 1982), NRC inspection report 50-334/81-16 for the Beaver Valley power station, December 10, 1981, NRC, "Summary of Incidents That May Have Involved Deliberate Acts Directed against Plant Equipment in Vital Areas of Operating Reactors (1980–1982)," attachment to letter from then NRC Chairman Nunzio J Palladino to Congressman Edward J Markey, February 7, 1983

14 NRC, "Summary of Incidents "

15 Ibid

16 See S A Mullen, J J Davidson, and H B Jones, Jr , *Potential Threat to Licensed Nuclear Activities from Insiders (Insider Study),* NUREG-0703 (Washington, D C Office of Nuclear Material Safety and Safeguards, U S Nuclear Regulatory Commission, July 1980)

17 Ibid

18 Ibid

19 See, for example, Steve Weisman and Herbert Krosney, *The Islamic Bomb* (New York Times Books, 1981)

20 See *Inside NRC,* February 6, 1984, p 17

21 See Sheryl A Massaro, Office for Analysis and Evaluation of Operational Data, U S Nuclear Regulatory Commission, "Power Reactor Events March–April 1983," NUREG/BR-0051, vol 5, no 2 (Washington, D C , October 1983), Office for Analysis and Evaluation of Operational Data, U S Nuclear Regulatory Commission, "Report to Congress on Abnormal Occurrences, April–June 1983," NUREG-0090, vol 6, no 2 (Washington, D C , November 1983), and Florida Power and Light Company, "Reportable Occurrence Report 250-83-07," Turkey Point nuclear plant, May 3, 1983 I am grateful to Steve Sholly for pointing out the significance of the Turkey Point event

22 *Inside NRC,* March 17, 1986, pp 2–3

23 Ibid

24 See ACRS transcript

25 See Samuel Glasstone and Philip Dolan, *The Effects of Nuclear Weapons* (Washington, D C U S Department of Defense, 1977), J Carson Mark, "Nuclear Weapons Characteristics and Capabilities," in *The Final Epidemic Physicians and Scientists on Nuclear War,* ed Ruth Adams and Susan Cullen (Chicago University of Chicago Press, 1981)

26 For a discussion of the Brookhaven study, see Henry W Kendall, *Nuclear Power Risks* (Cambridge, Mass Union of Concerned Scientists, 1975) pp 35–36,

Daniel Ford, *The Cult of the Atom* (New York Simon and Schuster, 1982, 1984), pp 67–82 See also "Minutes of Steering Committee on Revision of WASH-740—December 16, 1964," as well as the memorandum of January 28, 1965, for U M Staebler, Office of the Assistant General Manager for Reactors, from Stanley Szawlewicz, chief, Research and Development Branch, Division of Reactor Development and Technology, "Trip Report—Meeting of the Steering Committee on the Revision of WASH-740 Theoretical Possibilities and Consequences of Major Accidents," both documents obtained by the Union of Concerned Scientists pursuant to the Freedom of Information Act

27 See memorandum of November 13, 1964, for U M Staebler from Stanley Szawlewicz, "Discussion with BNL Staff on the Revision of WASH-740," obtained by the Union of Concerned Scientists pursuant to the Freedom of Information Act

28 *Supplement to Draft Environmental Statement, San Onofre Units 2 and 3,* NUREG-0490 (Washington, D C NRC, January 1981)

29 In the last several years representatives of the nuclear industry have made a number of claims that nuclear accident source terms—estimates of the amount of radioactivity that could be released in severe accidents—should be reduced by orders of magnitude across the board The technical bases for these claims have been roundly criticized, particularly by a panel of the American Physical Society See R Wilson et al , "Report to the American Physical Society of the Study Group on Radionuclide Release from Severe Accidents at Nuclear Power Plants," *Reviews of Modern Physics* 57, 3 pt II (July 1985) See also Daniel Hirsch, "The NRC's Reassessment of Consequences of Catastrophic Nuclear Accidents," Stevenson Program on Nuclear Policy, Santa Cruz, Ca , January 1986, and my testimony before the NRC commissioners, April 3, 1985 A number of recent empirical studies have called into question the fundamental premise of the reduced source term claims that radioiodine is released as cesium iodide rather than elemental iodine Furthermore, tremendous uncertainty exists regarding the adequacy of containment performance during severe accidents However, even were the claims for accidental releases to hold up, which now appears quite unlikely this fact would not make much difference regarding risk estimates for sabotage of nuclear facilities The reason is that much of the hoped-for reduction in the estimated radioactivity release from accidents is based on the assumption that containments fail much later than previously thought, during which time it is asserted that radionuclides would settle out in the containment Saboteurs however, have it in their power to ensure early containment failure and thus very large radionuclide releases to the environment

30 See Bennett Ramberg, *Destruction of Nuclear Energy Facilities in War The Problem and the Implications* (Lexington, Mass Lexington Books, 1980) reissued in paperback as *Nuclear Power Plants as Weapons for the Enemy An Unrecognized Military Peril* (Berkeley University of California Press, 1984) Ramberg estimates casualties associated with intentional destruction of a power reactor as ranging up to 60,000 deaths, 450,000 cases of thyroid nodules, temporary agricultural restrictions on 175,000 square miles of land, and decontamination or long-term restrictions on the occupation of 5,300 square miles, depending on the nature of the destruction produced, the location of the reactor, and weather conditions

31 The lack of realism in this regulatory threat basis was underscored recently by a serious sabotage attempt at the Palo Verde nuclear plant in Arizona A group of

attackers successfully and skillfully disabled three of four off-site power sources for the plant, each located about 35 miles from the plant Since the transmission lines converge on the site from four different directions and since the power loss for each line was accomplished within a few minutes of each other, it appears to have been a coordinated effort of people operating as several teams, probably with vehicles, and perhaps utilizing in excess of three people In other words, the Palo Verde attempted sabotage event exceeded the maximum threat to a nuclear power plant deemed credible by current NRC regulations Until the regulations are made more realistic, no U S plant is required to protect against such an incident because it goes beyond the official design basis threat For a discussion of the Palo Verde event, see "Suspected Sabotage Loss of Three of Four Offsite Power Sources," Preliminary Notification of Safeguards Event, PNS-V-86-03 (Washington, D C NRC, May 15, 1986)

32 See "Security Conflict at Lab Rules Vary on Use of Deadly Force," *San Jose Mercury News,* January 24, 1986

33 See Congressman John Dingell to DOE Secretary Donald Hodel, May 7, 1984