Clandestine Nuclear Trade and the Threat of Nuclear Terrorism

Leonard S. Spector

Clandestine nuclear dealings have long threatened international efforts to halt the spread of nuclear arms and could contribute to the risk of future nuclear terrorism. Today, this nuclear netherworld embraces a broad range of activities, including outright smuggling, the quiet exploitation of loopholes in nuclear export controls, the purchase of nuclear goods under false pretenses, and secret R&D work on nuclear weapons themselves.

Fortunately, these activities fall short of constituting a black market comparable to that for illicit drugs or conventional arms. For now, virtually all the activities in the nuclear underground are pursued at the behest of a small number of national governments rather than by criminal, dissident, or terrorist groups. There appear to be few, if any, independent, free-standing smuggling networks. Furthermore, the commodities ultimately being sought—nuclear weapons and nuclear weapons material—do not appear to be for sale, only the equipment and technology needed by national governments to build the plants to produce them are commercially available.[1]

Still, this nuclear netherworld may ultimately contribute to the danger of nuclear terrorism in at least three ways. First, as national governments exploit this underground market and nuclear weapons spread to additional states, the possibility that terrorists will gain access to them will grow. Such weapons in nuclear threshold countries are likely to be more vulnerable to terrorist seizure than they are in today's more advanced nuclear weapons states. Moreover, depending on its alignment, an emerging nuclear weapons state could conceivably seek to advance its own political goals by sharing those weapons with ostensibly independent terrorist groups whose actions it could later disclaim.

The author wishes to thank Theodore Hirsch, an intern at the Carnegie Endowment for International Peace, for his help in preparing this report.

Second, terrorist groups might seek to exploit the nuclear gray market themselves, using the same subterfuges that national governments use. Although in today's nuclear netherworld, subnational groups cannot obtain nuclear arms or nuclear weapons material and cannot hope to build the complex installations needed to produce the latter, they might be able to engage in a form of barter with sympathetic emerging nuclear states (for example, offering raw materials or needed nuclear hardware in return for nuclear weapons material).[2] No cases of such barter arrangements involving terrorist groups have come to light, but it has been reported that one national government, Libya, provided uranium concentrate to Pakistan in the possible hope of receiving nuclear weapons or sensitive nuclear technology in return.[3] U.S. officials disclaim the possibility that Pakistan would have offered such a quid pro quo.

Finally, there is always the risk that nuclear arms or nuclear weapon materials will someday become available on the nuclear black market. There is evidence indicating that terrorist organizations might well be interested in acquiring such items. Understanding underground nuclear commerce in its current form is essential to preventing such future dangers.

Rules for Legitimate Nuclear Commerce

The cornerstone of current nuclear export controls is an agreement among the nuclear suppliers—in essence, the advanced industrialized nations, including those in the Eastern bloc—to require that their nuclear exports be subject to audits and inspections in recipient nations by the International Atomic Energy Agency (IAEA). Suppliers have adopted this requirement for IAEA safeguards under the Nuclear Suppliers' Guidelines they negotiated in 1976. The requirement is also mandated by the 1970 Non-Proliferation Treaty (NPT), which has been signed by all the suppliers except France.[4]

The commodities that trigger the application of safeguards in recipient countries are worked out in negotiations among the suppliers and are specified in an agreed-upon trigger list, which is updated from time to time. Manufacturers seeking to export items on this list must report their proposed sales to the supplier country authorities and obtain export licenses so that these authorities can verify the intention of the recipient country to apply the required safeguards.

Many recipient countries are themselves parties to the NPT and as such have agreed to place all their nuclear activities under IAEA inspection. However, Argentina, Brazil, India, Israel, Pakistan, and South Africa have not joined the pact. To support their growing nuclear weapon capabilities, many of these nonsignatories have quietly attempted to obtain nuclear commodities

without being subject to IAEA safeguards Iraq, although an NPT signatory, may have done likewise

In addition to the safeguards requirement, the supplier nations have agreed to exercise restraint in the sale of the most sensitive nuclear facilities These include reprocessing plants, which extract weapons-usable plutonium from spent reactor fuel, and enrichment installations, which can upgrade uranium from its natural state to weapons grade Since France cancelled its proposed sales of reprocessing plants to the Republic of Korea and Pakistan in the late 1970s, there have been no sales of those installations The very success of these efforts to curtail commercial sales of sensitive nuclear plants, however, has driven would-be purchasers to the nuclear underground, where at least the components for these facilities can sometimes be obtained

The export of related dual-use commodities—items having both nuclear and nonnuclear uses—is controlled partly through the suppliers' trigger list In the West, many of these items are also controlled through a separate export control system (known as the COCOM regime), established to prevent exports of strategic items to the Soviet Union and Eastern Europe [5] Licenses are required for these exports, but IAEA safeguards need not necessarily be applied in the recipient nation because the basis for granting the relevant export license is often that the export not be destined for a nuclear end use Dual-use items controlled through these mechanisms include advanced computers potentially useful for designing nuclear weapons, equipment for nuclear weapons testing, and electronics and hardware potentially usable in nuclear weapons themselves

Despite their seeming comprehensiveness, these controls are far from being wholly effective As a stream of recent prosecutions has shown, they are subject to continuous assault by a number of emerging nuclear nations intent on using the nuclear netherworld The prosecutions provide hard evidence of clandestine nuclear trade and also show the relative leniency accorded offenders, a factor that may encourage would-be nuclear terrorists to exploit the nuclear gray market in the years ahead

Illicit Nuclear Trade

Perhaps the most egregious case of nuclear smuggling in the recent past took place between 1977 and 1980, when Albrecht Migule, a West German businessman, shipped a nuclear plant to Pakistan in sixty-two truckloads and provided a team of West German engineers to supervise its construction The facility processes natural uranium into easily gasified uranium hexafluoride so that it can be enriched for possible use in nuclear arms Thus the plant is a critical building block in Pakistan's nuclear weapons program— in the words of one West German official, providing the "yeast for the cake "[6]

Unlike many other nuclear smugglers, Migule was tried and convicted for exporting the $6 million plant in 1985 He received only a $10,000 fine

and an eight-month suspended sentence [7] The facility he supplied, now believed to be operating in the town of Dera Ghazi Khan, contributes to fears that Pakistan will soon have the bomb

Similarly, in 1976 and 1977, the Dutch automobile transmission manufacturer, Van Doorne Transmissie, exported 6,500 tubes of specially hardened steel to Pakistan, despite warnings from the Dutch government The tubes were intended to encase high-speed centrifuges at Pakistan's sensitive Kahuta enrichment plant, a facility that may soon produce weapons-grade uranium [8] Although Van Doorne executives had acknowledged to one Dutch official that the tubes were destined for the Pakistani enrichment program, the businessmen were acquitted at their 1985 trial because of ambiguities in Dutch regulations implementing the Nuclear Suppliers' Guidelines [9]

Other recent criminal and civil proceedings for similar acts of nuclear smuggling include the following

> The prosecution of the Dutch firm Fysisch Dynamisch Oderzoekslaboratorium (Physical Dynamics Laboratory) for illegally exporting in 1976 specially designed measuring equipment for Pakistan's classified Kahuta uranium enrichment plant [10]
>
> The prosecution of Henk Slebos in the Netherlands for illegally exporting to Pakistan in 1983 a wide-band oscilloscope potentially useful in helping run the Kahuta plant [11]
>
> The prosecution in Canada of Abdul Aziz Khan and two accomplices for the illegal export to Pakistan in 1980 of electronic components for inverters, devices used to regulate the speed of centrifuges of the type used in the Kahuta plant [12]
>
> U S Commerce Department proceedings against Sarfaz Mir and Albert Goldberg for illegally attempting in 1981 to export zirconium metal (used to sheathe uranium fuel for reactors) to Pakistan, labeled as "mountain-climbing equipment" [13]
>
> The prosecution in Houston, Texas, of Nazir Vaid for attempting illegally to export to Pakistan in 1984 50 krytrons (high-speed electronic switches used in nuclear weapons) [14]
>
> The prosecution of Richard Smyth for illegally exporting 810 krytrons to Israel between 1980 and 1983 [15]
>
> The prosecution of Man Chung Tong, in Los Angeles, for attempting to export high-technology equipment to the People's Republic of China in 1983 and 1984, including special Polaroid film, measuring devices, and computers said to be destined for China's nuclear test site at Lop Nor [16]

In April 1986, the West German weekly *Stern* carried a lengthy account of yet another nuclear smuggling operation involving Pakistan that was con-

cluded in August 1985—and whose perpetrators have apparently not been brought to justice The account offers a detailed look at the intricacies of such operations

On August 10, 1985, according to *Stern*, a shipping company, Global International Transport, moved 880 kilograms (1,936 pounds) of specially hardened maraging steel to a Karachi address [17] The steel had been fabricated into round bars whose diameter exactly matched that of a German-designed uranium enrichment centrifuge of the type Pakistan is believed to be building at Kahuta [18] Maraging steel is on the list of items of the Nuclear Suppliers' Group that require special export licenses to ensure either that the export will not be used for nuclear purposes or that it will be used only in a nuclear installation covered by IAEA safeguards The Kahuta enrichment plant is not so covered

According to *Stern,* a small London steel-trading firm, Lizrose Ltd , originally ordered the maraging steel from the Arbed Corporation of Voelklingen, West Germany, in October 1984 Lizrose is run by Inam Ullah Shah, a man of Pakistani descent Western intelligence agents learned of the order and persuaded Arbed not to go through with it Two weeks afterward, Arbed received a second order for the same material from Mark Blok, a Cologne steel dealer, who is married to a Pakistani and is said to be a friend of Inam Shah Blok had the material delivered to a Cologne warehouse, thus avoiding the need for Arbed to obtain an export license The material was then shipped to Hamburg and on to Karachi by Global Transport, presumably under false labeling [19]

Although these episodes all involve smuggling activities undertaken to advance the nuclear weapons programs of national governments, one case that has been the subject of a prosecution initiated in 1984 by the Italian government raises the possibility that a subnational group, the Palestine Liberation Organization (PLO), may have sought to exploit the nuclear netherworld The case is also unusual because it involves an offer to sell nuclear weapons and nuclear weapons-usable plutonium rather than merely the technology and equipment needed to derive these coveted products Fortunately, it appears virtually certain that the would-be purveyors never actually possessed these items

The central figure in these illicit dealings, and a defendant named in the Italian indictment, was Glauco Partel, an Italian rocket engineer who served as an intermediary for back-channel suppliers of conventional arms In early 1982, Partel, at the initiative of an Australian arms dealer, Eugene Bartholomeus, began offering three atomic weapons for sale—weapons that Partel subsequently acknowledged did not exist—to a series of potential buyers with connections to Arab interests in the Middle East [20] In all likelihood, Partel and Bartholomeus intended to use the nuclear weapons as bait to attract buyers, who would then be told that these weapons were not available

but that Partel and company could provide a variety of conventional arms instead

One telex from Partel in the prosecutor's dossier on the case gave the following details on the offering of the weapons to another intermediary with close contacts to the Syrian government

> Terms of offer Power of units same as Japanese original ones (20kt) Delivery will be effected in buyer's country The 3 units are being assembled now and will be ready for delivery in the first week of March [1982] Testing [without a detonation] will be effected in a neutral country of Europe at [*sic*] the presence of the seller and buyer reps/experts Selling people will arrange for transportation This unit have [*sic*] not been offered elsewhere Net price for the 3 units delivered is USD 924 millions Deposit of 462 millions On delivery the balance will be paid [21]

Other telexes to or from Partel obtained by the prosecution specified that the weapons weighed 90 kilograms (198 pounds) each, contained 40 kilograms (88 pounds) of weapons-grade uranium (sufficient for a Hiroshima-size weapon), and measured 41 inches by 11 inches [22]

Although Partel's approach to Syria apparently fell through, telexes from the prosecutor's file grouped under the heading "A-bombs, Arabs" appear to indicate that Partel did bring one and possibly more groups into serious negotiations for the weapons One of these initiatives sent Partel and a colleague on a trip to Iraq In a March 30, 1982, cable to Bartholomeus while he was in Sydney, Australia, Partel linked the PLO to the "three toys," a term considered by the Italian prosecutor and others who have examined the entire court file to be a code for the three atomic bombs

> This is the first in a series of TLXS reporting on our trip to Baghdad presenting the general picture of the whole situation It was apparent that the first operation—the supply of specific armaments to Iraq—is the security key for the men involved in the operation of the three toys By successful completion of the first operation the men in question are to receave [*sic*] the official protection of the Iraqi services throughout the Middle East and Europe (not only with regard to Israel but also with nonfriendly Arab countries) In other words, the two deals were interconnected *We were introduced at the top Iraqi military and political levels by the PLO men responsible for the three toys and by the Iraqi services* [23]

This reference to the PLO is the only one in the dossier in connection with nuclear devices While hardly conclusive evidence (Partel may have been inflating the accomplishments of his trip), it is at least an indication of PLO interest in the acquisition of nuclear arms, either directly or through the organization's ties with the Iraqi government

The same telex describes Iraq's apparent interest in acquiring 33 9 kilograms (74 pounds) of plutonium from Partel's group—plutonium Partel later maintained was available to the smugglers, although this possibility seems extremely unlikely "As for the offers submitted to Iraq, the Chief of Armaments told us they are interested in SAM-7 [surface-to-air missiles] mortars, AH-1s [helicopters] armed with TOWS [wire guided anti-tank missiles], plutonium, Glauco's secret rocket system "[24] Although Partel stated in a subsequent interview that Iraq continued to pursue the plutonium offer through the summer of 1982 (a claim seemingly supported by telexes among Partel and his cohorts in the court file), the deal fell through in August, when Partel's group proved unable to supply samples of the material for inspection

In the end, the episode seems to reveal that at least one terrorist group, and at least one nation that has supported such groups in the past, are interested in acquiring nuclear weapons clandestinely On the other hand, the Partel affair also supports the view that despite the existence of seemingly willing buyers, such weapons and the key materials needed for their fabrication remain unavailable in the international marketplace

Preventive Measures

Clandestine trade in nuclear-related commodities that are further removed from nuclear weapons may still contribute to nuclear terrorism in the future Curtailing such clandestine trade is essential to reducing these risks As a first step, efforts to prosecute nuclear smugglers must be intensified and the penalties increased In Western Europe, criminal laws and export regulations need strengthening, and the United States is urging its allies to move in this direction In the United States, where statutory penalties are already tough, the problem is inadequate coordination and follow-through of law enforcement efforts [25] The best remedy for such case management shortcomings is more active oversight by senior officials in the executive branch and Congress One approach would be to designate a ranking nonproliferation aide at the State Department as responsible for coordinating with appropriate Justice Department officials all nuclear prosecutions and for reporting annually on these activities to Congress

At least as important is the need to take diplomatic action against the national governments that are directing and benefiting from today's nuclear smuggling activities These nations should be condemned in international fora, and aggrieved nuclear supplier states, particularly when they have obtained convictions for smuggling, should strongly confront the nation responsible and demand that the illegally obtained goods be returned, mothballed, or placed under IAEA safeguards so they cannot contribute to the development of nuclear arms

Fortunately the nuclear netherworld remains fraught with obstacles as a route to nuclear terrorism The existing regime of export controls and international safeguards continues to restrict merchants in the nuclear gray market to the sale of components for production that are many steps removed from the coveted atomic weapons themselves Nevertheless, this success should not be taken as a cue for complacency The continued circumvention of nonproliferation measures by national governments not only increases the risk of nuclear terrorism by facilitating the spread of nuclear arms, it also invites subnational groups to enter the world of clandestine nuclear trade themselves, if only to obtain items for barter Thus, the tightening of proliferation constraints must be part of any long-term strategy for curbing the threat of nuclear terrorism

Notes

1 This may not always have been the case In the mid-1960s, Israel is believed to have diverted weapons-usable highly enriched uranium from a plant in Apollo, Pennsylvania, run by the Nuclear Materials and Equipment Corporation (NUMEC) No additional diversions of nuclear weapons material are believed to have occurred Although offers to sell such material have been made from time to time, apparently they have all been hoaxes

2 Nuclear commodities could, of course, be bartered for nonnuclear implements of terrorism, such as high explosives or rockets thereby contributing to an intensification of terrorist activities, although not at the nuclear level

3 John J Fialka, "West Concerned by Signs of Libyan-Pakistani A-Effort," *Washington Star,* November 25, 1979

4 The suppliers' guidelines are set forth in International Atomic Energy Agency document INFCIRC/254, the parallel requirements applicable to NPT parties are specified in IAEA document INFCIRC/209/Add 2

5 COCOM is an acronym for Coordinating Committee, an informal organization of Western governments that meets periodically to ensure consistency in the implementation of member nations' respective export control systems In the United States the principal statutes establishing export controls over strategic goods are the Arms Export Control Act and the Export Administration Act

6 "Waffenschmied Deutschland" [Weaponsmaker Germany], *Stern,* November 14, 1984, and interview with a West German official, March, 1985

7 "Achte Monate au Bewahrung fur Albrecht Migule" [Albrecht Migule receives eight months' probation], *Badische Zeitung* (Freibourg), March 12, 1985, and interviews with the presiding judge and West German foreign ministry officials, May 1985

8 "Report of the Inter-Ministerial Working Party for Investigating the 'Khan Affair,'" Foreign Ministry of the Netherlands (mimeo, English version), p 16, and interviews with Dutch prosecutors and foreign ministry officials, May 1985

9 The defendants had little to fear in any event Had they been convicted, each would have received a $6,000 fine and a one-month suspended sentence

10 The firm was also acquitted because of ambiguities in Dutch law Violet Cotterell, "Boetes geeist voor verboden export" [Fines demanded for forbidden exports], *Parool* (Amsterdam), October 30, 1984

11 Slebos received a six-month suspended sentence and a modest fine Details of the Slebos prosecution are based on interviews with Dutch and U S officials, July 1985, see also "Israel's Uranium," *Foreign Report,* July 19, 1985

12 Khan was acquitted after the prosecution failed to prove the inverters had been exported The others pleaded guilty and received $3,000 fines John J Fialka, "How Pakistan Secured U S Devices in Canada to Make Atomic Arms," *Wall Street Journal,* November 26, 1984, and interview with the Canadian prosecutor, July 1985

13 Mir was never apprehended, Goldberg's export privileges were suspended indefinitely Leslie Maitland, "U S Studying Foiled Bid to Export a Key Reactor Metal to Pakistan," *New York Times,* November 20, 1981

14 Vaid pleaded guilty after three months' pretrial detention and was deported to Pakistan Seymour M Hersh, "Pakistani in U S Sought to Ship A-Bomb Trigger," *New York Times,* February 25, 1985

15 Smyth disappeared before his trial, the krytrons not in use were returned by Israel, which told the United States that the others were being employed for nonnuclear purposes John M Goshko, "L A Man Indicted in Export of Potential Nuclear Bomb Component to Israel," *Washington Post,* May 17, 1985, U S House Subcommittee on Europe and the Middle East, *Hearings on Developments in the Middle East,* 99th Cong , 1st sess , July 24, 1985, and John J Fialka, "Investigators in Pollard Case Confront History of Accommodation by U S , Israeli Spy Agencies," *Wall Street Journal,* December 18, 1985

16 Tong jumped his $350,000 bail and did not appear for trial Ronald L Soble, "U S Investigates Illegal High-Tech Exports to China," *Los Angeles Times,* April 11, 1984 Regarding other alleged high-technology smuggling for China, see Maureen Dowd, "5 Named in Plot to Send Peking High-Tech Gear," *New York Times,* February 13, 1984, and telephone communication with the assistant U S attorney in charge of the prosecution, winter 1985

17 Egmont Koch and Simon Henderson, "Auf dunken Wegen zur Atommacht" [Secret routes to the bomb], *Stern,* April 30, 1986, p 52

18 "Report of the Interministerial Working Party Responsible for Investigating the 'Kahn Affair,'" Foreign Ministry of the Netherlands Dr A Q Khan, a German-trained metallurgist, is thought to have obtained classified information on this design in the course of his work in 1975 for the Dutch enrichment program at Almelo, where the West German design was being vetted

19 The Pakistani embassy in Bonn, the *Stern* report states, was involved in the operation from the beginning A few weeks after the first order was placed with Arbed, Pakistan's military attaché visited the steelworks and showed considerable interest in specialized steels The most damning piece of evidence of involvement by the Pakistan government, however, is that Global International Transport sent the shipping documents and its invoice for shipping the material to the Pakistani embassy in Bonn for payment According to a short note dated August 20, which authors Koch and Henderson apparently obtained in the course of their investigation, the shipping documents and the invoice, numbered 12240 in the amount of deutschemark (DM) 1,373 38

(about $660), were sent to embassy counselor Azmat Ullah "per telephone conversation with Mr Shaw," an alias of Inam Shah

20 This discussion is based on an examination of the documents in the prosecutor's file on the indictment, an in-person interview with one defendant (Glauco Partel) and a telephone interview with a second (Carlo Bertoncini), talks with journalists covering the case, and the following news reports "Iraq's Bid for Plutonium Foiled," *Energy Daily,* June 15, 1984, "Bombes A d'Occase" [Second-hand A-bombs], *Le Matin,* June 20, 1984, p 11, "Le Marché noir de la mort atomique," [The black market in atomic death], *Le Nouvel observateur,* June 22, 1984, p 35, "Unfassbar! Europaische Waffenmafia Liefert Atombomben frei Haus" [Incredible! European weapons mafia delivers atomic bombs C O D], *Bunte,* August 9, 1984, p 102, Peter Nichols, "Judge in a Hurry Indicts 37," *Times* (London), November 19, 1984, E J Dionne, Jr "Italian Case Uncovers an Alpine Heart of Darkness," *New York Times,* November 24, 1984, and "Atomica Connection" [Atomic connection], *Il Mondo,* February 25, 1985, p 42 Significant assistance was also provided to the author by the ABC "Closeup" television documentary team that investigated this story in depth in the course of preparing a three-hour documentary, "The Fire Unleashed," which aired on June 6, 1985

21 Prosecutor's file, p 3762

22 Ibid , p 3754

23 Ibid , p 3783 Emphasis added

24 Ibid

25 Nazir Vaid, for example, was apparently let off lightly because the prosecutor in that case thought that evidence clearly linking Vaid's krytrons to the Pakistani nuclear program was lacking As investigative journalist Seymour Hersh has brought out, however, the prosecution had subpoenaed a cable showing that the krytrons were ordered in Pakistan by one S A Butt—a figure unknown to the prosecutor in the Vaid case but known well to State Department experts as a man long involved in Pakistan's clandestine nuclear affairs Although it was supposedly monitoring the case closely, State apparently failed to alert the prosecutor to this key fact Hersh, "Pakistani in U S " In the Smyth and Tong proceedings, a different case management problem arose the failure to take adequate measures to prevent the flight of the defendants

Prospects for Nuclear Terrorism: Psychological Motivations and Constraints

Jerrold M. Post

Comprehensive analyses of the prospects for nuclear terrorism inevitably address two major considerations technological and psychological What is striking about these analyses, however, is the great disparity between the scrupulous attention devoted to technological considerations and the cursory attention given to psychological ones An example of this disparity is the frequently cited study *Nuclear Theft Risks and Safeguards* by Mason Willrich and Theodore Taylor, prepared for the Energy Policy Project of the Ford Foundation The authors provide rigorous analyses of the materials, technology, skills, and resources necessary to construct a crude fission bomb or radiological weapon They also give thorough attention to the requirements and elements of nuclear safeguards systems Their attention to detail is scrupulous In contrast, only 10 of the book's 252 pages are devoted to examining terrorist motivations and intentions, and even that limited treatment is descriptive and superficial

Thus, we are in the paradoxical position of having a clearer understanding of the interior of the atom than we do of the interior of the mind of the terrorist As is the case in the broader area of nuclear strategy, absent a clear understanding of the adversary's intentions, the tactics and strategies developed are based primarily on knowledge of terrorists technological capabilities and give insufficient weight to psychological motivations

Irrational Act or Rational Choice?

In considering the potential for nuclear terrorism, Brian Jenkins observes that the historical record does not contain incidents in which terrorist groups have attempted to acquire fissile material for use in a nuclear device [1] More-

over, he observes that inflicting mass casualties is usually inconsistent with the goals of terrorist groups On the other hand, when Jenkins considers the category of psychotic individuals, he is led to observe that "nuts are probably responsible for many of the low-level incidents and nuclear hoaxes" and that "lunatics have been perpetrators of many schemes of mass murder" He concludes that on the basis of intentions alone, psychotics are potential nuclear terrorists, but in terms of capabilities, they are the least able to acquire nuclear weapons

Although I agree with the overall thrust of Jenkins's arguments, an overly quick reading of his analysis could lead to the false conclusion that the major danger is from irrational actors—from psychotic individuals acting alone or in small groups One could go on to conclude—again falsely—that there is little or no danger from political terrorists, since political terrorist groups tend to guide their decision making in accordance with rational political considerations and it does not seem to be in the rational interest of political terrorist groups to engage in nuclear terrorism But, as Jenkins would be the first to agree, this thinking revolves around a false dichotomy In reality, there is a great deal of territory between irrationality and rationality Moreover, rational terrorists may reason quite logically, but the fixed premises that are at the basis of their rational calculus can lead to a "psycho-logic" with dreadful consequences

Terrorist Psycho-logic

In examining terrorist psycho-logic, it is necessary to utilize three levels of analysis individual psychology, group psychology, and organizational psychology

Individual Psychology

Comparative studies of terrorist psychology do not indicate a unique terrorist mind Terrorists do not fit into a specific psychiatric diagnostic category Indeed, most would be considered to fit within the spectrum of normality But it is difficult to conceptualize a psychologically normal individual who would carry out an act of mass destruction An attempt to construct a psychology that would lead an individual to be motivated to carry out an act of nuclear terrorism and have the wherewithal to implement it quickly reveals a paradox On the one hand, to be motivated to carry out an act of mass destruction suggests profound psychological distortions usually found only in severely disturbed individuals, such as paranoid psychotics On the other hand, to implement an act of nuclear terrorism requires not only organizational skills but also the ability to work cooperatively with a small team To

be suffering from major psychopathology, such as paranoid psychotic states, is incompatible with being able to work effectively with a small group

On the basis of my understanding of terrorist psychology, I agree with Jenkins's observation that the psychotic individuals most strongly motivated to commit acts of nuclear terrorism would be the least able to carry them out, although psychotic individuals could be—and have been—responsible for nuclear hoaxes

Psychosocial Vulnerabilities

Although there is no unique terrorist mind-set, there is a pattern of psychosocial vulnerabilities that renders those who become terrorists particularly susceptible to the powerful influences of group and organizational dynamics In particular, some data suggest that the act of joining a terrorist group represents an attempt to consolidate an incomplete psychosocial identity Within the broad array of terrorist groups with their disparate causes, a common feature is an unusually strong motivation to belong that is coupled with a tendency to externalize by seeking outside sources for personal inadequacies

A major study sponsored by the Ministry of the Interior of the Federal Republic of Germany is illustrative [2] The study of the epidemiology of terrorism found that one-fourth of terrorists had lost one or both parents by age 14, that a third had been convicted in juvenile court, and that those studied evinced a high frequency of job and educational failure The lives of the terrorists before joining were characterized by social isolation and personal failure For these lonely, alienated individuals on the margins of society, the terrorist group was to become the family they never had

Alienation from the family is characteristic of a major class of terrorists whom I term the anarchic ideologues [3] This class, of which the Red Army Faction and the Red Brigades are examples, have turned against the generation of their parents, which is identified with the establishment They are dissident to parents loyal to the regime

In apparent contrast, the nationalist separatists, such as ETA of the Basques and the Armenian Secret Army for the Liberation of Armenia (ASALA), are carrying on a family mission they are loyal to families dissident to the establishment They are not, however, at one with their societies in spite of their family identification Thus they too have fragmented psychosocial identities, and for them too, joining a terrorist group is an attempt to consolidate their identities

To recapitulate, from the perspective of individual psychology, terrorists are not in the main suffering from serious psychopathology They do not suffer from mental illness that could lead to the profound distortions of motivation and reality-testing one would expect to be associated with the

driven desire to carry out an act of mass destruction At the same time, they suffer from psychosocial wounds that predispose them to seek affiliation with like-minded individuals This strong affiliative need, coupled with an incomplete personal identity, provides the foundation for especially powerful group dynamics

If this line of reasoning is correct, it suggests that the terrorist group is an unusually powerful setting for producing conforming behavior Insofar as the individual psychosocial identity is incomplete or fragmented, the only way the member feels reasonably complete is in relation to the group Belonging to the terrorist group for many becomes the most important component of their psychosocial identity Indeed, data from terrorist memoirs and from interviews with terrorists suggest that individuals have a tendency to submerge their personal identity into a group identity The fact that individual terrorists subordinate their own judgment to that of the group has major implications for the question of whether a terrorist group would engage in an act of nuclear terrorism

A summary review of the evidence, direct and indirect, bearing on the group dynamics of political terrorism helps clarify this issue The strong need to belong becomes a major lever for ensuring the compliance of group members Andreas Baader, a founder of the Baader-Meinhof gang, used the threat of expulsion to ensure compliance In response to members who expressed doubt about the group's violent tactics, he indicated that "whoever is in the group simply has to be tough, has to be able to hold out, and if one is not tough enough, there is not room for him here "[4] Wanda Baeyer-Kaette, who had unusual access to members of the Heidelberg cell of the Red Army Faction, cites the example of a new recruit discussing an operation that had a high probability of producing a high casualty rate[5] When he questioned whether it was ideologically proper to conduct an operation where innocent blood would be shed, a heavy silence fell over the room It quickly became apparent that to question the decision was to be seen as disloyal Moreover, to question the group judgment was to risk losing his newly won place in the group

The risks may be much more consequential than the mere loss of one's membership Several conveyed the fear that to disagree actively with the group and be perceived as dissident was to risk not just membership but life itself Baumann stated that withdrawal was impossible except "by way of the graveyard "[6] Boock, a former Red Army Faction member, commented that the intensity of the pressures "can lead to things you can't imagine the fear of what is happening to one when you say, for example, 'No, I won't do that, and for these and these reasons ' What the consequences of that can be."[7]

Thus there are great pressures for compliance and conformity that mute dissent Consider the dilemma of the doubting group member, at once de-

sirous of belonging yet uncomfortable about an action that runs counter to his or her principles For this person, ideological rhetoric plays an especially important role, providing the justification for the contemplated antisocial act Indeed, as Baeyer-Kaette has noted, a remarkable upside-down logic characterizes terrorist group discussions But there is a psycho-logic to the reasoning if one accepts the basic premise that what the group defines as good is desirable and what the group defines as bad is evil If the group cause is served by a particular act, no matter how heinous, the act is good by definition

Absolutist Rhetoric

The rhetoric of terrorism is absolutist, idealizing, and devaluing, polarizing "us versus them," good versus evil What is within the group is ideal and not to be questioned. What is without—the establishment—is the cause of society's ills and is bad

Throughout the broad spectrum of terrorist groups, no matter how diverse their causes, the absolutist rhetoric is remarkably similar The absolutist rhetoric is characterized by splitting,[8] an important psychological characteristic of the borderline personality, a personality disorder disproportionately represented in the terrorist population Lorenz Bollinger, who has had the unusual opportunity of conducting in-depth psychoanalytic interviews of Red Army Faction terrorists, found a striking preponderance of borderline mechanisms, especially splitting and projecting onto the establishment the devalued aspects of the self while concomitantly idealizing the group[9] To the extent that the terrorist ideology devalues and dehumanizes the establishment and identifies it as the cause of society's (the terrorists') problems, it is not only not immoral to attempt to destroy the establishment, it is indeed the highest order of morality By the terrorists' upside-down logic, destroying the establishment is destroying the source of evil, and only good can result

A brief excursion into indirect evidence is also in order Studies of the membership of the Unification church of Reverend Sun Yung Moon are particularly instructive[10] They indicate that the more isolated and unaffiliated the individual was in terms of family and friends before joining, the more likely he or she was to find membership in the church attractive And the greater was the emotional relief the new member found, the more likely he or she was to accept instruction to participate in antisocial acts For the purposes of this comparison, recall the remarkable mass engagement ceremony in Madison Square Garden, where Reverend Moon assigned fiancés to 1,410 members The individuals who found in the Unification church their entire self-definition were the individuals willing to accept blindly an assigned

marital partner, a step contrary to the social mores to which these individuals had been socialized

A further major contribution to the power of the group over its members derives from the relationship between the group and its surrounding society For the underground group isolated from society in particular, group cohesion develops in response to shared danger In the words of a member of the Red Army Faction, group solidarity was "compelled exclusively by the illegal situation, fashioned into a common destiny"[11] According to the testimony of another member, "the group was born under the pressure of pursuit" and that pressure was "the sole link holding the group together"[12]

Thus, the terrorist group represents an almost caricature version of the fight-flight group Bion described[13] The fight-flight group acts in opposition to the outside world, which both threatens and justifies its existence The group perceives that the only way it can preserve itself is to fight against or flee from the enemy seeking to destroy it This belief that the enemy is out to destroy it is not merely a paranoid delusion Although initially it may derive from internal psychological assumptions, as a consequence of terrorist acts, the psychological assumption becomes a self-fulfilling prophecy The terrorist group successfully creates an outside world that indeed is out to destroy it

The psychological pressures within the individual terrorists and the psychological tensions within the group are externalized Terrorist groups require enemies in order to cope with themselves If such enemies do not exist, they create them, for if they cannot act against an outside enemy, they will tear themselves apart

The evidence on terrorists thus indicates a pattern of behavior in which the predominant determinant of terrorist actions is the internal dynamics of the terrorist group If the terrorist group does not achieve recognition as a feared opponent of the establishment, it loses its meaning If the terrorist group does not commit acts of terrorism, it loses its meaning A terrorist group needs to commit acts of terrorism to justify its existence, and it needs to be recognized as a feared opponent in its fantasy war against society

Terrorist Decision Making

If this characterization of terrorist group psychology is correct, what are the implications for group decision making? Would a group able to rationalize that its causes justify—indeed require—wreaking violence on innocent victims be similarly able to rationalize the mass destruction of nuclear terrorism? Is it a quantum leap, an unbridgeable gulf, or merely an incremental and inevitable step as terrorist acts escalate in magnitude? Can we construct a terrorist psycho-logic that not only permits but requires nuclear terrorism?

In addressing this question, it is important to emphasize that more than most other decision-making groups, individual judgment in terrorist groups tends to be suspended and subordinated to the group process Thus the focus of this inquiry is not whether individual terrorists could make such a catastrophic decision but whether a group deciding as a group could do so

This approach requires us to address the phenomenon Janis identified as groupthink [14] Occurring when groups make decisions in times of crisis, it is defined as

> high cohesiveness and an accompanying concurrence-seeking tendency people engage in when they are deeply involved in a cohesive in-group, when the members' strivings for unanimity override their motivation to realistically appraise alternative courses of action a deterioration of mental efficiency, reality testing, and normal judgment that results from in-group pressures [15]

Groupthink is the characterized by the following features

> Illusions of invulnerability leading to excessive optimism and excessive risk taking
>
> Collective rationalization efforts to dismiss challenges to key assumptions
>
> Presumption of the group's morality
>
> Unidimensional perception of the enemy as evil (thereby denying the feasibility of negotiation) or incompetent (thereby justifying risky alternatives)
>
> Intolerance of challenges by a group member to shared key beliefs
>
> Unwillingness to express views that deviate from the perceived group consensus
>
> A shared illusion that unanimity is genuine
>
> The emergence of members who withhold adverse information concerning the instrumental and moral soundness of its decision from the group

This cluster of traits would seem to epitomize the decision making of the terrorist group Of particular importance are the reduction of critical judgment, the assumption of the group's morality, and the illusion of invulnerability leading to excessive risk taking

Semel and Minix have investigated the effects of group dynamics on risk taking [16] In a group problem-solving task, they found that U S Army groups shifted in the direction of riskier policy choices than individual members

preferred privately Individual tendencies were strongly reinforced and intensified as a result of interactions within the group Also, the tendency of group members to conform to the preferences of the group was found to increase with the length of their interaction with the group

The phenomena described by Janis and by Semmel and Minix occur with psychologically healthy mature adults If mature adults with healthy self-esteem and appreciation of their own individuality can slip into such flawed decision making under the pressures of group dynamics, what of groups composed of individuals with weak self-esteem who depend on the group for their sense of significance? Does this circumstance not suggest that these groups would be subject to distorted decision making to a magnified degree?

Distorted decision making is not equivalent to total irrationality, however Looking at the world through distorted lenses is not equivalent to being blind or being subject to visual hallucinations Is there a psycho-logic that, under the pressure of distorted decision-making processes, could lead a terrorist group to opt for weapons of mass destruction? Jenkins has noted that "terrorists want a lot of people watching, not a lot of people dead Mass casualties may not serve the terrorist goals and could alienate the population "[17] But are there circumstances in which the upside-down logic of terrorists could lead them to want a lot of people dead, where they could be drawn to conclude that mass casualties could serve their goals and could do so without alienating the population? If there is a psycho-logic that could lead a group down that path, might not the distorted decision making make the difference in a close decision?

It is useful to invoke here a proposition advanced by Ariel Merari, who has made an important distinction between domestic terrorists acting on their own territory and those acting on the soil of other nations [18] Such groups as the Red Army Faction and the Red Brigades believe they are in the vanguard of a social-revolutionary movement They aspire to persuade their countrymen to join their fantasy war against the establishment, and they depend on their countrymen for both active and passive support In attempting to draw attention to their cause through acts of terrorism, it is their countrymen they are trying to influence The same is true for the terrorist group ETA when it is acting in the Basque region

In vivid contrast, when a group operates across borders, the rules of the game in terms of the target of influence are quite different As Merari has emphasized, when Palestinian terrorists operate in Israel, the horror and disapprobation of the population in the target country are not a disincentive, they are a reward

The issue of audience comes into play too In the media age, each act has multiple audiences If a group of moderate Palestinians, in considering a particular action, comes to believe that the act would invoke international opprobrium, that belief would mitigate against the action, for they much

value and need Western approval and would see the act as having the potential for being a setback to the Palestinian cause In contrast, for radical Shiite terrorism, different weights are probably attached to the reactions of different sectors of the international audience The degree to which the West is alienated by a particular act is probably not a major disincentive The key point is that a group acting across borders is significantly less constrained than one operating within its own national boundaries I believe it is with these groups that the greatest dangers lie

The Potential for Nuclear Terrorism

An examination of the historical record provides some comfort However distorted their reasoning, their special psychological calculus, thus far terrorist groups have concluded that nuclear terrorism would not advance their cause and have rejected that option Lest we draw false comfort from that historical record, however, let me suggest a scenario where a group might well have concluded that honor compelled it to perpetrate an act of mass violence and that such an act would advance its just cause Indeed the scenario is not a product of fantasy but might have occurred had it not been for the alertness of the Israeli counterintelligence forces In the spiraling cycle of violence begetting violence that characterizes the Middle East, an act of terrorism was planned and set into motion that, had it succeeded, would have had catastrophic consequences and could easily have provided a plausible rationale for nuclear terrorist response

When we think of Middle East terrorists, we are prone to think of radical Palestinian groups or Shiite groups such as Amahl or Hizballah In this case, the terrorists were zealous Jewish fundamentalists—millenarian Kabbalists—who had formed a cell within Gush Emunim [19] Reasoning with a fundamentalist logic that has been analyzed by Ehud Springzak, an Israeli political scientist, they planned to destroy the two holiest Islamic mosques in Jerusalem—in fact, two of the holiest sites in the Islamic world—the El Aksa Mosque and the Mosque of Omar (the Dome of the Rock) [20] Only the holy sites in Mecca and Medina are more important than the El Aksa Mosque, which is described in the Koran as the site at which Mohammed began his ninth journey Built in 732 A D , it has been the scene of violence in the past, for it was on its steps that King Abdullah of Trans-Jordan was assassinated in 1951, to be succeeded after a brief interregnum by his grandson King Hussein, who was at his side Built in 1691, the Mosque of Omar is considered by many to be the most magnificent shrine in Jerusalem

The logic of the Jewish terrorists is an example—and a horrifying one—of the psychological blinders that terrorists can wear, of the twisted psychologic that can lead to actions that can shape history In planning the destruc-

tion of the holy sites, these Jewish terrorists did not consider the holiness of the sites, nor did they define their planned action as an anti-Arab act Nor did they dwell on the consequences in the Arab world to any significant degree Their perspective was quite simple The El Aksa Mosque stood on the temple mount, the holiest place in Judaism The mosque was believed to stand on the very place where Abraham was instructed to sacrifice his son Isaac and was the site of the First Temple (built by Solomon in 970 B C) and of the Second Temple

The millenarians believe that redemption and the coming of the messiah are due for the year 6000 (in the Jewish calendar) The Kabbalist millenarians feel that they can help these events occur, and if they do not, the coming of the Messiah may be postponed for another thousand years This is why the Kabbalist band thought they had to help by removing the Muslim shrines, since according to their belief, the Messiah will rebuild the Jewish temple For the fundamentalist Jewish terrorists, the planned destruction of the Islamic holy sites was necessary to restore the temple mount to its original form Had they succeeded, there is little doubt that a *jihad* of worldwide proportions would have resulted In that climate, nuclear terrorism against Israel would have been considered fully justified by many in the Islamic world

There is another scenario worth considering—perhaps less extreme but potentially as far-reaching in its consequences Is it beyond the pale to imagine a terrorist cell in West Germany, obsessed with an escalating arms race, persuading itself that the only way to avoid a nuclear holocaust would be forcibly to call attention to its humanitarian cause, and that the most effective way to do that would be to seize a nuclear weapon, not for the purpose of detonating it but as a means of capturing the world's attention? Such an event could have profoundly destabilizing effects on the North Atlantic Treaty Organization (NATO) and the polities of the NATO countries most concerned with the forward deployment of Pershing IIs

In the two examples considered above, I have moved from considering terrorists' actually detonating a nuclear device to their seizing a device in order to dramatize a cause The next logical step in this progression is one that, from the point of view of the terrorist group, would involve even less profound consequences and hence would be more readily considered the nuclear terrorist hoax If it is technically feasible for a group with a certain range of scientific and engineering abilities to construct a primitive nuclear device, it is certainly much less complicated for it to mount a plausible hoax

Although there have been a number of such episodes, it is puzzling that they have not been more frequent A highly persuasive nuclear terrorist threat can have major consequences The probability may be judged quite low, but were a group to provide plausible evidence that it had fissile material, could decision makers afford to ignore its demands? One of the major difficulties

with the low probability–high consequence act of high-technology terrorism is that it tends to throw normal procedures out the window It is generally recommended that senior policy makers should avoid becoming involved in terrorist incidents But should a plausible nuclear terrorism threat be raised, it would be difficult, if not impossible, for them to avoid becoming actively involved in dealing with the crisis High-level involvement automatically changes the nature of the crisis and would in itself constitute success from the terrorists' perspective

The possibility of nuclear terrorism is usually discounted because of the historical record and the logic that it would not serve the terrorists' goals I believe it is highly likely that plausible nuclear hoaxes will occur with increasing frequency It is a contingency that requires more active planning and preparation than it has been given

One final class of actors must be considered terrorist losers Despite a stated commitment to various causes, the central priority for any terrorist group or organization is to survive And surviving means committing acts that justify and call attention to its existence What can be said of the terrorist group or faction on its way out, that has lost its support and its headlines, and, in a factional struggle, has lost its influence to a rival group? Desperate for success, might not such a group ask, "What have we got to lose?" Could the pressures of group decision making coupled with the requirement for organizational survival not argue for a nuclear spectacular as a way of regaining prominence? While the constraints raised earlier would continue to operate, in this case, I would suggest they would be significantly weakened

Summary

To understand the psychological motivations and constraints of terrorists considering nuclear terrorism, it is necessary first to identify the important features of their individual, group and organizational psychology Although there is no one terrorist mind-set, there is a pattern of psychosocial vulnerabilities that renders terrorists especially susceptible to the powerful influences of group and organizational dynamics In particular, the act of joining a terrorist group represents for many an attempt to consolidate an incomplete psychosocial identity A common feature is an unusually strong motivation to belong, coupled with a tendency to externalize, to blame the establishment for personal failures

These characteristics set the stage for terrorist group members to be unusually susceptible to the forces of group dynamics As a consequence, there is a tendency for individual judgment to be suspended so that conforming behavior results Many of the features of "groupthink" are present, with its accompanying tendency toward risky decision making

In considering the implications of these psychological understandings to the specific case of nuclear terrorism, it is emphasized that distorted decision making does not equate to totally irrational decision making In certain circumstances, however, the distorted individual and group decision-making psychology could influence the group toward a high-risk option such as nuclear terrorism

For terrorists operating within their own national boundaries, a terrorist act producing mass casualties would generally be counterproductive For groups acting across national boundaries, however, this constraint does not apply to nearly the same degree Although the opprobrium of the West will be a constraint for some, it will not be equally so for all terrorist groups The degree of disincentive will relate in particular to the major audience of influence Thus, Shiite fundamentalist terrorists would be less constrained than radical Palestinians, who would in turn be less constrained than more moderate Palestinian groups Finally, there are the terrorist losers who are being shunted aside and losing the recognition they seek Such a group could justify a terrorist spectacular in order to regain influence on the basis of a "what have we got to lose" rationale Other scenarios are possible in which terrorist groups could conclude that an act of nuclear terrorism was required

In thinking about the possibility of nuclear terrorism, it is important to distinguish between the actual detonation of a device and the use of a device for extortion and influence The constraints against the latter are significantly reduced in contrast to acts producing mass casualties The constraints are even more reduced in the case of the plausible nuclear hoax, an option that can be expected to become more frequent

Notes

1 Brian Jenkins, "The Potential for Nuclear Terrorism," P-5876, Santa Monica, The Rand Corporation, May 1977

2 Jager, Schmidtchen, and Suellwold, eds , *Lebenslauf-Analysen* vol 2, *Analysen zum Terrorismus,* (Wiesbaden Westdeutscher Verlag, 1981)

3 Jerrold Post, "Notes on a Psychodynamic Theory of Terrorist Behavior," *Terrorism* 7(3)(1984)

4 W Baeyer-Kaette, D von Classens, H Ferger, and F Neidhardt, eds , *Gruppenprozesse,* vol 3, *Analysen Zum Terrorismus* (Wiesbaden Westdeutscher Verlag, 1982)

5 Ibid

6 Ibid

7 Ibid

8 Psychoanalytic studies of individuals with "borderline" personalities reveal reliance on the primitive psychological mechanism of "splitting " Individuals who are narcissistically wounded in early childhood development do not develop a healthy

self concept Unable to integrate the good and the bad aspects of themselves and their environment into a realistic whole, as children they *split* off the bad as the "not me," thereby maintaining a grandiose self concept

9 Personal communication from L Bollinger, 1982

10 M Galanter, "'The Moonies' A Psychological Study of Conversion and Membership in a Contemporary Religious Sect," *American Journal of Psychiatry* 139(2)(February 1979), M Galanter, "Psychological Induction into the Large Group Findings from a Modern Religious Sect," *American Journal of Psychiatry* 137(12)(December 1980), and M Galanter, "Engaged Members of the Unification Church Impact of a Charismatic Large Group on Adaptation and Behavior," *Archives of General Psychiatry* (1984)

11 Ibid

12 Ibid

13 W R Bion, *Experiences in Groups* (London Tavistock Publications, 1961)

14 Irving Janis, *Groupthink* (Boston Houghton-Mifflin, 1982)

15 Ibid

16 A K. Semel and D A Minix, "Group Dynamics and Risk-Taking An Experimental Examination," *Journal of Experimental Politics* (January 1977)

17 Jenkins, "The Potential for Nuclear Terrorism"

18 A Merari, "A Classification of Terrorist Groups," *Terrorism* 1(3-4)(1977) 331

19 Gush Emunim is a religious redemptionist Zionist group within Israel that has played a leading role in settling the West Bank and Gaza It bases its political actions on Jewish religious sources

20 See Ehud Springzak, "Democracy, Fundamentalism, and Terrorism The Jewish Terrorism of Gush Emunim," Wilson Center Occasional Papers, Smithsonian Institution, Washington, D C , 1987

Nuclear Weapons Security and Control

Thomas A. Julian

This study of nuclear weapons security and control focuses on the protection of U S nuclear weapons after the Department of Energy has transferred them to military custody This transfer is effected in accordance with a biennial, presidentially approved Nuclear Weapons Deployment Plan that allocates the weapons to strategic and nonstrategic nuclear forces.[1] The weapons treated in this study are those covered by the plan The specific focus is their protection while being stored or transported by the military or when operationally deployed from peacetime storage worldwide Special attention is paid to issues involved in protecting U S Navy nuclear weapons

Definitions

Given the terrorist context of this study, *protection* is defined broadly It applies not just to the threat of actual physical seizure of a weapon by unauthorized people and its detonation—or, more probably, its threatened detonation. Moreover, *unauthorized people* encompasses not just terrorists[2] but also military personnel, both U S and allied, particularly from member nations of the North Atlantic Treaty Organization (NATO) with which the United States has concluded Programs of Cooperation (POCs).[3]

The terms of reference for the discussion here are the U S nuclear weapons employment policy. It is contained in successive (and evolutionary) presidential directives on the subject—National Security Decision Memorandum 242, Presidential Directive 59, and National Security Decision Directive 13—which lay down the policy for planning the possible employment of U S nuclear weapons in support of U S national objectives The purpose of this planning is to deter to the fullest extent possible any conflict with the Soviet Union and its surrogates

All the directives affirm the concept of extended deterrence (that is, the threat to employ U S nuclear weapons, including first use, on behalf of U S allies threatened by the Soviet Union or its client states) The United States has chosen to further the principle of extended deterrence in the NATO context by the forward deployment or storage of U S weapons during peacetime at locations within the integrated U S and allied military command called Allied Command, Europe (ACE) Geographically ACE covers all the continental members of the NATO alliance and the United Kingdom Within the context of NATO strategy and policy, the presence of these weapons in Europe in part meets the requirement that ACE military forces be capable of escalation to combat a Warsaw Pact attack Moreover and most significant, within the context of NATO's strategic concept of a flexible response, the storage of these weapons and their delivery systems in Europe is viewed as coupling the conventional forces of the alliance to the U S strategic deterrence forces based outside Europe

In view of the significance of these forward deployed weapons to NATO, it is possible that terrorist organizations might well view activities directed against these weapons, even if they did not actually result in the seizure of one or more, as successful The mere fact of an attack using mortars or rockets without actually entering or penetrating the storage site could, for example, generate substantial publicity and/or create anxiety about a nation's participation in the NATO integrated military structure, with its explicit emphasis on shared risk and responsibility At the extreme, these anxieties could generate domestic political pressures to remove U S nuclear weapons from national territories and to make them more secure by storing them in the United States

Some would argue that the removal of U S nuclear weapons is precisely what should be done, even without the stimulus of a terrorist attack At the same time, there is a well-documented concern on the part of Europeans that the perception of coupling be maintained, a stance that was painfully evident during the ground-launched cruise missile (GLCM) and Pershing II deployments (Another indication is the current concern with what Europe views as the potentially decoupling effect of the Strategic Defense Initiative) U.S and other alliance decision makers see the removal of U S nuclear weapons as a step that might irretrievably destroy NATO cohesion Even the most sanguine person could hardly be optimistic that the present consensus over security in each alliance nation could be maintained or, at the extreme, that a credible new deterrent strategy could be agreed to if forward deployment were abandoned. These forces militate against removal of the weapons

The point of this study is not, however, to argue the merits of forward deployment but rather to argue that the protection of U S nuclear weapons against terrorists must include protection against the loss of their functional utility to U S policy There is a range of plausible scenarios to suggest that

terrorist acts other than seizing a U S nuclear weapon (or acts short of detonation such as nuclear blackmail in the event a weapon is seized) could precipitate that loss Regardless of whether all the scenarios are equally credible, the fact remains that senior alliance officials are concerned about the possibilities

Within the spectrum of terrorist actions, the theft and detonation of a U S nuclear weapon by terrorists (or by other people) must be considered the extreme case The mere fact of an attack on a nuclear storage site or of access by unauthorized people to U S weapons could have negative effects on the weapons' functional utility in a number of direct ways For example, unauthorized people could damage the weapons so that they could not be used or could cause a nonnuclear detonation that would still scatter the plutonium Even a chalked message on a weapon container symbolizing the possibility of further action, whether actually carried out or not, might have a serious impact in a country where the public was particularly agitated by the presence of the weapons

Approach

Specific information about the means and processes through which the security and official control over U S nuclear weapons are maintained is generally classified. Therefore the approach taken here is to state a set of principles that should govern protection I then show how the application of these principles would serve to realize the fundamental U S (and NATO) objective of preventing unauthorized persons, including terrorists, from gaining possession of U S weapons or using them in any way Here, *use* like *protection,* is defined broadly to mean direct actions such as detonation or indirect actions such as the generation of publicity for the terrorists' cause

It is also important to define the protective task Clearly it is to maintain the security of U S nuclear weapons It is far from clear, however, how the United States or NATO can dissuade terrorists from attacking nuclear weapons storage sites Thus it appears that the task is also to find ways to prevent a decision to attack from being made From a terrorist's point of view, the attainment of publicity means success, whatever the undertaking Generally (though not always) a successful undertaking has involved a hijacking and seizure of hostages, assassination of an industrialist, or bombing of a government installation An inability to achieve these results can have a variety of adverse results for terrorists, such as demonstrating that the government is effective and can protect its citizens and facilities, the implication being that the terrorists' cause is associated with failure, or losing a trained cadre Measures that make nuclear weapons storage sites overtly more difficult

targets could well compel terrorists to seek softer targets that offer a higher probability of success

A secondary reason for developing a framework of protective principles is to avoid too specific a discussion about the potential vulnerabilities of U S nuclear weapons This approach should preclude possibly useful information from being made available to terrorist groups

The principles I have outlined are derived from a variety of unclassified sources on U S policy, interests, and national objectives They include the Atomic Energy Act of 1946, as amended, various congressional hearings and reports, other official documents and policy statements, and a small but significant number of published books and articles [4] Although these principles are broadly applicable to both the strategic and nonstrategic components of the U S nuclear stockpile, clearly both the circumstances of peacetime and wartime storage and the requirements for their movement vary sharply They therefore pose somewhat different issues or problems with regard to how the principles should be applied in specific terms For example, strategic weapons would be delivered by strategic nuclear delivery vehicles, including Titan, Minuteman, and Peacekeeper (MX) intercontinental ballistic missiles (ICBMs), submarine-launched ballistic missiles (SLBMs), and B-1 and B-52 bombers and cruise missile carriers In peacetime, these strategic weapons are located within the continental United States or at various places under the oceans, generally in one of three configurations or conditions mounted on their ICBMs and SLBMs, loaded aboard bombers standing alert at various Strategic Air Command bases, or stored at specially protected sites inside the general defenses of such bases, not too distant from the runways from which the bombers would take off

It would be imprudent to rule out the possibility of terrorist access to these strategic weapons, however, their location inherently limits the opportunities for successful access in comparison with the nonstrategic nuclear weapons that currently are or are planned to be deployed forward in potential theaters of operations outside the continental United States Because of the greater risk, the discussion here focuses on the nonstrategic nuclear weapons

Nonstrategic nuclear weapons employed by theater forces outside the United States would be delivered by systems whose range is less than intercontinental These systems vary between the so-called battlefield ones (nuclear-capable howitzers and Lance missile launchers) and the intermediate range GLCM and Pershing II missiles currently deployed in Europe The latter can strike targets just short of Moscow from bases in West Germany Deployment of these delivery systems and the storage of their warheads on the European continent is an integral element in NATO's strategic concept, which relies on the credible threat of their use to deter the Warsaw Pact

Peacetime forward deployment of U S nuclear weapons in Europe or in other locations outside the United States potentially places these weapons at

greater risk from terrorist actions The United States has acknowledged publicly not only that nuclear weapons are stored in Europe but also the quantity stored The location of the stored U S. weapons is dispersed but keyed to the peacetime positions of the national forces to which the weapons have been allocated The storage sites have also been chosen to further the principle of forward defense that is integral to NATO's strategic concept, as well as the General Defense Plan of the Supreme Allied Commander, Europe (SACEUR), that also supports forward defense

Although there has been a steady consolidation of storage sites to increase weapons security in recent years, some 4,600 U S nuclear weapons will still be located at various sites throughout Allied Command, Europe, in 1988, even after the 1,400 are withdrawn as directed by the alliance ministers of defense at Montebello, Canada, in October 1983 Operational requirements dictate that many of these sites be in the Federal Republic of Germany or nearby in other countries of NATO's Central Region These are the same locations where the German Red Army Faction and other terrorist groups have been active The Southern Region countries—Italy, Greece, and Turkey—have experienced similar problems, and the operational imperatives governing the peacetime storage of nuclear weapons there also apply In short, weapons storage in Europe must be responsive to the operational requirements that flow from NATO's military strategy In turn, these requirements constrain where peacetime storage sites can be located and require that they be dispersed to some degree The result is the creation of a set of potential targets that coincide with areas where terrorists, who are usually stridently anti-American, have been or are operating

U.S nuclear weapons stored during peacetime are not the only concern when it comes to terrorism or other acts by unauthorized people to seize, damage, or detonate the devices In times of crisis or international tension whose severity the alliance nations all recognize, NATO would probably implement its Formal Alert System This system, which applies to the NATO integrated military structure, comprises a set of actions, generally sequential, that the forces assigned to SACEUR commanders (that is, the Supreme Commander, Atlantic, and Commander-in-Chief, Channel) are to take as prudent preparations for possible conflict In view of the forward defense concept and given that in peacetime the national military ground forces that come under SACEUR's command are located rearward, one step in the Formal Alert System is to deploy U S nuclear weapons forward to their General Defense Plan positions, except for nuclear bombs, which must remain at or near the airbases from which NATO's aircraft operate Movement of the weapons to those locations means that they will be more dispersed, a situation that helps their survivability by increasing the number of targets that must be attacked

Once U S nuclear weapons are dispersed, they become more vulnerable to terrorist actions Because the weapons need to be reasonably near the

national military units that might be authorized to employ them, there would be more field storage sites (FSLs) than peacetime storage sites and therefore more potential targets to choose from Based on inferences drawn from current unclassified discussions, FSLs do not have elaborate protective structures Thus, dispersal combined with the conditions of field-type storage could present greater opportunities for terrorist action

The extent of the opportunities would depend on the degree to which civilian movement in the forward areas was controlled by West German territorial forces or inhibited by the presence of the defensive forces themselves On balance, it must be concluded that the threat of terrorism posed by dispersed U S weapons is slight In this circumstance, the greater threat is from Soviet special forces (SPETZNAZ) or U S or allied military personnel assigned to fulfill custodial, guard, or other protective functions but who might decide to act in an unauthorized manner These possibilities must also be considered when formulating principles of protection

Principles of Protection

Each of the principles is stated and then explored briefly The discussion contains information from unclassified sources regarding current practices that illustrate how each principle has been derived in light of the context described earlier

Principle 1: *The protection accorded U S nuclear weapons against terrorists or other people with similar intent should be provided by means of a multilayered system that encompasses technical means (equipment and other direct applications of technology to protect weapons physically or provide warning), procedures, personnel and structures, and other physical facilities.*

A multilayered protective system tends to create a synergistic effect whereby the protection provided by the whole is greater than the sum of its parts For example, technology that prevents physical access to weapons in peacetime storage for a specified period, when coupled with a guard force required and trained to respond within that period, provides greater protection than either a delay system or guards alone can provide Layers of protection also tend to ensure against the failure of one element and, presumably for a terrorist group, raise the level of uncertainty of a successful action against a peacetime storage site There are several U S -sponsored, alliance-funded NATO programs involving protective infrastructure that are either in the process of completion or have just been completed They do or will provide extra layers of protection

These programs were generated by concern over the security of weapons after the 1972 Munich Olympics and in the face of continuing terrorist activities These infrastructure programs include the Long-Range Security Program, by which the physical facilities at storage sites for U S nuclear weapons in Europe are upgraded (for example, through new fencing, buildings, and lighting that meet higher standards of security); the Weapons Access Delay System Program, under which physical barriers were erected that delay the access of unauthorized people to certain types of U S weapons, should the outer defenses protecting the actual storage igloos be breached; and the Intrusion Detection System Program, which provides sensors to warn custodians and guards of unauthorized activity directed against stored U S weapons

The newest layer or element of the system of protection will be the air force weapon storage vault, which provides for storage of air force nuclear bombs in such a way as to increase their survivability, security, and safety With respect to the problem of personnel contemplating unauthorized acts (insiders), whether U.S or allied, there is a two-man-rule that requires joint performance of certain key functions, as well as a system of overlapping elements—that is, one that includes different groups of personnel who may be either exclusively U S or multinational (U S personnel will always be present because of their custodial responsibilities) These measures also tend to lessen the threat from insiders The actual deterrence of insiders will depend on successful interaction among the different elements of the protective system Those elements include, at one extreme, protective features designed into the weapon itself or perhaps into its protective container

Principle 2: Protection should be an integral part of weapons design.

The core of the protection system should be the security features built into the weapon itself These can provide yet another layer of protection (and synergy) Of even greater importance, they can provide the most direct prevention against an unauthorized detonation Government officials in testimony before the U S Congress have repeatedly pointed to ongoing programs designed to increase the safety and security of U S. nuclear weapons and have emphasized that the latest of technologies are incorporated into new weapons as they are fielded. This point has been reflected in the annual arms control impact statements, and both the Congress and the executive branch have been lending important momentum to these programs since the early 1960s

The most significant technological development has been the permissive action link (PAL) systems integral to each weapon PAL systems are designed to preclude unauthorized detonation of a weapon by requiring the insertion of a proper digital code before the warhead can be armed The earliest PAL systems were mechanical combination locks, found on the older 8 inch and 155 mm nuclear artillery projectiles (designated, respectively, W33 and W48 by the Departments of Energy and Defense) still in the U.S. inventory and

currently deployed in Europe The PALs have now evolved into the electronically controlled category D and F PAL systems, with switches that can be individually coded so that only selected weapons can be unlocked These category D and F PAL systems also incorporate command disable systems that allow a nuclear weapon to be rendered incapable of a nuclear detonation through nonviolent means (that is, without using externally applied explosive devices) built into the weapon itself or its container. The new 8 inch (W79) and 155 mm (W82) weapons have category D PAL systems with this command disable feature

The command disable systems, at least those associated with the newer PAL systems, also incorporate the principle of automaticity After a limited number of attempts to unlock the weapon with an inaccurate code, the weapon automatically becomes incapable of nuclear detonation Clearly automaticity is preferable to other means that require action by U S custodial personnel (such as activating a switch or lever or, at the extreme, the actual physical destruction of the mechanism in the weapon that permits generation of the nuclear explosion), given that the worst case possibility is the incapacitation or death of U S custodians The combination of PAL and command disable systems is a powerful tool with which to prevent the unauthorized nuclear detonation of a U S weapon

The PAL systems alone, particularly the category D and F systems with their multiple code, coded switches, are also a powerful tool for helping ensure positive control of U S weapons Their status is regulated continuously and effectively, changing only as directed by authorized higher personnel Systems such as the PAL exemplify how technological means can provide an additional degree of certainty over that provided by the routine complex set of procedures, training, evaluation, and scrutiny by military personnel, all supported by basic military discipline, which are and will continue to be the primary means of ensuring positive control

A variety of other features that provide either greater safety or security (or both) to U S nuclear weapons also serve as obstacles to terrorists (The concept of overlapping protective measures is exemplified by the military's use of the term *nuclear surety* to mean nuclear security and safety) These other features include the use of insensitive high explosives (IHE) in modern weapons to make them resistant to chemical detonation that would produce a plutonium scatter One-point safe is another characteristic of the weapons. It ensures that in the event of a detonation initiated at any one point in the high explosive system, the probability of achieving a nuclear yield greater than the equivalent of 4 pounds of TNT will not exceed one in a million Weapons designed to function only when an insertible nuclear component (INC) is placed inside also inhibit terrorists or other unauthorized personnel from generating a nuclear detonation The degree of security here, however, depends on where and under what conditions the INCs themselves are stored,

arrangements that will have to reflect the operational requirements for employment of the weapon

Principle 3: *Protection systems must not be so cumbersome in either a figurative or literal sense (such as use of equipment or storage facilities that are deliberately designed to make rapid removal of U S nuclear weapons from peacetime storage impossible) that the weapons do not meet the operational requirements of military forces.*

Storage systems can be designed to impose deliberate time delays on either physical access to, or the removal of, U S nuclear weapons from peacetime storage The objective of the delays is to permit guards to respond to alarms or other indicators before the weapon can be damaged, stolen, or subjected to other unauthorized acts On the other hand, if authorized personnel have no way to circumvent the designed delay, the system will be biased toward physical security rather than operational responsiveness (for example, the capability to respond to directives to disperse the weapons for survivability or to move them forward that SACEUR might issue) General Bernard Rogers, the current SACEUR, has testified that weapons access delays, measured in minutes, are built into some current U S Army nuclear weapon storage sites in Europe through the weapons access delay system (WADS) and the new U S Air Force weapons storage vault for nuclear bombs Given the high degree of responsiveness required for forward deployed forces and the potentially short warning times of attack, given the proximity of the probable attackers, the delay times must be reasonably short and, it must be assumed, capable of being circumvented by authorized personnel This balance between security and operational responsiveness must be embodied in protection systems if U S nuclear weapons are to preserve their functional utility

This principle must also apply to elements of the protection system applied to U S weapons that have been removed from peacetime storage for dispersal and/or deployment forward Those elements should not inhibit the rapid transportation of U S weapons However, to the degree possible within the implicit limitations of space, weight, and size relative to the need for rapid movement, the elements of the protection system that pertain to weapons when they are moved should replicate those provided during peacetime storage While what might be construed as classic terrorism tends to be viewed as a peacetime phenomenon, recent indications relating to state-sponsored terrorist groups suggest that this presumption need not be true Given the greater range and size of resources available through governments, combined with the leverage this assistance gives terrorists in pursuing their objectives, conceivably terrorists with state sponsorship and guidance might seek to attack U S weapons during dispersal or even while located at some forward storage location. Admittedly this possibility seems remote because

of the difficulties that would constrain civilians from operating freely in a country mobilizing for defense In view of other threats (such as from SPETZNAZ) to U S weapons as they are going through the various phases of their operational deployment sequence (for example, in the case of ground-delivered weapons, removal from storage, transportation forward, establishment at field storage locations, and possible subsequent movement or employment of selected weapons), the need for such protection is conclusive, however

Principle 4: *Command and control elements and supporting communications systems must be incorporated into the weapons protection system to permit responsive action, including weapon movement, employment, and disablement by authorized personnel while precluding unauthorized personnel and terrorists the opportunity to detonate a weapon, should they acquire one Command and control elements or subsystems of the overall weapons protection system are seen as comprising military organizational structures, including all the appropriate authorities, technical means for supporting information flows among them, procedures, and other mechanisms, among them authentication systems and PALs and command disable or similar physical or technical systems that provide specific means of preventing the unauthorized detonation of a U S weapon.*

In military terms, the exercise of effective command and control over U S nuclear weapons by the National Command Authorities (the president and secretary of defense) and their subordinate military echelons is the mechanism through which positive control of U S nuclear weapons (including the maintenance of U S nuclear weapons in U S custody) is ensured, as required by U S law and the nature of the weapons themselves [5] Effective command and control must cover the possibility of hostile military forces overrunning locations where U S nuclear weapons are stored and employing them against U S or allied forces Terrorists and other people operating without authorization are the other principal threat to U S weapons with which the command and control elements or subsystems of the overall weapons protection systems must deal

In keeping with military organizational principles and as described in testimony and by various students of the subject, clear hierarchies and special channels exist through which directives regarding U S nuclear weapons are required to pass These directives start with the National Command Authorities and run down to the unified commander to whom nuclear-capable and conventional forces are allocated and then to the commanders of the nuclear-capable delivery forces through whatever intervening command levels have been established. These forces are the military means with which the unified commander executes the theater mission The command and control of the nuclear component of these forces are always handled separately and are

always dependent on authorizations and directives from the National Command Authorities

In Europe, SACEUR is the focal point of the command and control system for nuclear weapons deployed within (or specifically allocated to the support of) Allied Command, Europe, British as well as U S He identifies the levels at which requests for the release of nuclear weapons to be employed by his forces can originate and has the power to decide whether the requests (or requests originating at his level) are submitted to the National Command Authority or the British equivalent

For positive control, the flow of information among the elements of the hierarchy must be accurate, timely, and, most important, capable of validation as to the source cited in the message The familiar systems of message authentication employed by the U S military provide the last Typically these authentication systems require the inclusion in the message of special alphanumerics that can be compared to those designated for a given time and day as stated in the authentication tables distributed to the headquarters of the relevant commanders In the case of nuclear delivery units deployed forward and hence subject to the possibility of overrun, the potential acquisition of authentication tables by hostile forces poses the possibility that spurious messages could be generated, creating confusion and severe problems of positive control

The capability to validate directives from higher levels in the nuclear command and control structure, particularly at operational levels, is valuable chiefly in preventing hostile military forces from disrupting U S positive control In this regard, it is conceivable that terrorists or insiders might also seek to attain their objectives by generating messages containing valid authentication values but spurious directives intended to confuse or spoof the system The nuclear command and control structure, however, must be based on the far more serious potential for unauthorized persons securing the proper code with which to unlock and detonate U S nuclear weapons

U.S PAL systems are key elements in the exercise of effective command and control over U S weapons that are forward deployed on land in support of operational commanders Positive control requires that the code for unlocking U S nuclear weapons be provided to U S custodians of the weapons only at the time the president releases them for employment In operational terms, this requirement means that the code must be provided through messages directing the weapons' use For forward deployed weapons, logic suggests that these messages must originate at the unified or theater commander's level, since the forces deployed there are to support his mission and are under his command In Europe, the U S European Command supervises nuclear weapons storage and must provide the messages with the unlocking data to the custodians. During hostilities, the enemy, such as the Soviet Union, could conceivably intercept messages with sophisticated in-

tercept equipment and ascertain how to unlock the coding data with deencryption techniques In peacetime, however, terrorists and other unauthorized people would not have even this potential source of unlock codes to draw upon

An unauthorized person with access to a U S weapon with an operative PAL system but without the code to unlock it would try picking the lock That attempt would be foiled by the integral command disable systems A weapon in terrorist hands that required external activation (such as a switch thrown) that had been accomplished would still be useless If the system was of a limited-try type, a certain number of incorrect entries inserted in the PAL coded switch would automatically produce the same result This combination of an advanced PAL system with multiple code, coded switches, and an integral, non-violent command disable system that operates automatically appears to be the most effective means at present for both strict positive control of U S weapons and prevention of an unauthorized nuclear detonation

Navy nuclear weapons merit special discussion in the light of principles 2 and 4 Definitive unclassified data on the security systems associated with specific navy weapons are not available However, much testimony and other official information contained in the arms control impact statements provided by the executive branch to the Congress regarding various U S Navy nuclear weapons, together with information provided orally by former U S Navy officers, tend to confirm that navy nuclear weapons either have not been designed with integral PAL systems or, in the case of weapons used by the navy and other services that are known to incorporate PALs (such as most models of B-61 nuclear bombs), the weapons are stored unlocked, at least when on board ship Assuming this conclusion is true, the issue is whether principles 2 and 4 should be made applicable to U S Navy weapons [6] This issue is made all the more pointed by the fact that U S Air Force strategic nuclear missiles and air-delivered weapons are protected by PAL devices

Given the potential for terrorism or unauthorized acts by other people, including dissident U S Navy personnel, the issue must be considered from two perspectives (1) the possibility that such people could achieve their objectives by virtue of the possible presence of unlocked U S Navy weapons stored on land in the United States or its territories or on board U S Navy vessels in port anywhere in the world and (2) the possibility for unlocked weapons on board U S Navy vessels at sea being employed in unauthorized manner by the crew for whatever reason (such as the belief that the United States has been attacked on a massive scale and that nuclear retaliation is in order even without National Command Authority direction, a scenario that is the most salient concern of those who want U S Navy weapons to incorporate PAL systems)

As to the first possibility, it is generally analogous to the situation of forward deployed U S. Army and Air Force weapons in Europe In the absence

of PAL and associated command disable systems, the possibility that terrorists or other unauthorized people will achieve success—if success is measured by the potential to acquire a weapon that can be detonated and to produce the designed nuclear effects—is greater The ability of these people to gain access to a weapon in the first place will be determined largely by the effectiveness of the other elements of the multilayered protective system Conversely, whatever other use terrorists might be able to make of any weapon they acquire, at least an actual detonation would be precluded by a PAL and a command disable system

The potential for unlocked U S Navy weapons on board vessels at sea to be employed in unauthorized manner is the more serious concern, although it is a special case that, at least on the surface, has little to do with terrorism Fundamentally this possibility exists because of two factors the relatively greater difficulty of communicating with U S Navy vessels at sea, especially the submerged submarines (SSBNs) that carry the navy's strategic ballistic missiles, and the availability of unlocked nuclear weapons stored aboard essentially autonomous combat units that can only be communicated with via electronic means

With regard to the possible unauthorized launch of SLBMs, apparently authoritative U S Navy sources have described an intentionally complicated and (one must assume) lengthy process for launching these missiles The process can begin only upon specific National Command Authority direction and involves not only the two-man rule with respect to the authorizing message but also the performance of a large number of sequential actions by separate individuals (an unidentified senior navy official has estimated they number thirty) Ostensibly any participant in the launch process can stop it if he has reason to believe the launch is not truly authorized Thus the navy relies on the human factor rather than on physical and technical means (at least in the sense of a PAL system) to maintain the requisite positive control over its nuclear weapons, including SLBMs

Especially in the case of SLBMs, the navy obviously believes that it can ensure effective command and control by means of the extremely careful selection and monitoring procedures it has established for its submarine crews, their well-known discipline, and their frequent practice of procedures for launching (they include becoming familiar with the sound of the voices that would provide inputs to the launch procedure), particularly when this approach is coupled with the absolute requirement for a specific National Command Authority directive to launch

The navy's tactical nuclear weapons are subject to the same kinds of procedural checks and balances (or voting on a launch, as it has been described), although the human factor may be somewhat more problematical, since the crew of a surface vessel may not meet the standards required of submarine crews in entirety The implications of unauthorized employment

of tactical navy weapons are potentially somewhat less alarming, although the employment of any U S nuclear weapon must be viewed as producing a qualitative change in any ongoing hostilities, with consequences that are difficult to calculate Certainly the loss of a major Soviet fleet unit to a U.S Navy nuclear weapon, or even a Soviet SSBN, is hardly comparabale to the loss of a Soviet city from a U S bomber or ICBM attack However, the probability of a U S Navy commander's somehow employing a tactical nuclear weapon as a weapon of choice rather than a conventional weapon designed to perform the same mission (such as torpedoes or depth charges in antisubmarine warfare) seems low

In this regard, it is instructive to know that there appears to be a virtual lack of U S Navy doctrine on how to employ its tactical nuclear weapons, a situation that has been commented on critically by a number of national security analysts [7] These critics appear to have overlooked the fact that this gap implies a preference for conventional weapons with which to perform the same naval missions (for example, antisubmarine warfare, anti-air warfare, and antisurface warfare), for which carefully designed doctrine and tactics have been developed and are continuously exercised by U S. Navy vessels assigned these combat functions There is a concept, advanced recently by Desmond Ball, that a use-or-lose syndrome militates for use by the U.S Navy of tactical nuclear antisubmarine warfare weapons in a war at sea in which Soviet attacks were on the verge of destroying the navy's underwater sensor system for detecting Soviet submarines [8] The argument seems singularly unpersuasive when set in the context of tactical engagements at sea These events require extremely responsive weapons systems, and the uncertainty of securing timely NCA release of the navy's tactical nuclear weapons provides an additional reason why conventional weapons are indeed the navy's choice

This analysis of the potential for unauthorized employment of either strategic or tactical U S Navy nuclear weapons suggests that the trouble-free history of effective navy command and control can be extrapolated with confidence into possible future wartime situations However, integrating PAL systems into present and future U.S Navy nuclear weapons through retrofit or design has potential utility On balance, it may be desirable to put PAL systems with command disable features on these weapons PAL systems would provide the physical and technical means of raising to the maximum the already extremely high probability that effective command and control can be maintained over SLBMs in all situations, including during a communications loss Any cost in terms of time as a result of adding another step to the launch process, already deliberately designed to be complex, would be minimal and should have no significant impact on the responsiveness required of strategic weapons As to the tactical nuclear weapons carried on board a ship, PAL and command disable systems would provide another layer to their protection systems, an addition that would be particularly advantageous dur-

ing port visits anywhere in the world but especially in those areas where the visits are visible demonstrations of U S interest and power but where the potential for terrorist activities is high (as in the Middle East)

Principle 5: *Protection systems against terrorists or other persons with similar intent must be effective and reliable under a wide range of geographic and climatic conditions.*

The emphasis up to this point has been on U S nuclear weapons planned for or already forward deployed in Allied Command, Europe This focus is understandable because a great deal of unclassified information about U S weapons stored in various alliance countries is available It is important not to overlook the fact, however, that U S policy and worldwide force posture may require the forward deployment of U S nuclear weapons in other areas of the world where terrorist activities could be directed against U S weapons

The Republic of Korea is the one other geographic area in the world besides Europe that a U S secretary of defense has specifically discussed in the last ten years as a place where U S nuclear weapons might be employed in support of a U S. ally Thus it is possible that during a crisis U S. weapons might be deployed to the Korean peninsula, a place markedly different in many ways from Europe There are also other areas, notably the Middle East, where it is possible to conceive of U.S nuclear-capable forces being deployed

In the light of the differences of these areas, the various layers or elements of the multilayered protection system must be flexible enough to adapt to the specific conditions of each one, with the overall mix of layers providing the requisite level of protection For example, larger guard forces located at storage sites to respond to terrorist actions could conceivably be necessary for U S weapons stored in South Korea, given the rugged topography and potential for interdicting augmentation forces responding from other locations.

Principle 6: *Protection systems must include elements to facilitate the recovery of U.S. weapons that may have been removed successfully from peacetime storage by terrorists or other people with similar intent.*

One logical element in this regard should be specific additional bilateral agreements that address this contingency between the United States and those nations with which it has established programs of cooperation (POCs) covering U S. weapons forward deployed on their soil These agreements presumably would specify individual and mutual responsibilities for recovery actions, establish channels for bilateral and multilateral coordination of these efforts, and provide for external assistance as appropriate Given the relative propinquity of international borders in most of the known POC countries, the agreements might also cover hot pursuit and rules of engagement should the terrorists be brought to bay

The agreements would not be of direct assistance in locating a stolen U S nuclear weapon if original contact with the perpetrators of the theft was lost For this purpose, the U S has developed the Nuclear Emergency Search Team (NEST) The NEST was organized specifically as a means of dealing with possible nuclear terrorism It uses various sensors, including sensitive gamma ray detectors, to fulfill its functions, which include detecting stolen nuclear weapons, nuclear materials, or improvised nuclear devices, and it utilizes the technical skills, experience, and knowledge of senior scientific advisers, physicists, engineers, electronic specialists, computer analysts, and instrument specialists from the Los Alamos, Lawrence Livermore, and Sandia National Laboratories, as well as from supporting contractors

NEST's capabilities can be tailored to provide a graduated response appropriate to the nature of any incident, the number of people deemed necessary (which could range from 2 to 200), and the types of equipment required, whether airborne, handheld, or groundbased suitable for roadblock monitoring Given the basing of NEST in the continental United States, as currently structured it may not be entirely suitable for meeting the requirements of this protection principle It seems obvious that NEST capabilities would be most valuable in facilitating detection of a stolen U S nuclear weapon if its capabilities were applied within a very short time of the theft, ideally while the weapon was still being transported to its initial hiding place

Although NEST capabilities are configured to be moved by aircraft, the time necessary to traverse the distances between the United States and probable or known locations of forward deployed U S nuclear weapons throughout the world is still long It is certainly long enough to raise questions about how effectively NEST capabilities might be brought to bear upon a theft, particularly if it occurred in the highly urbanized areas of Western Europe where a variety of ways of shielding gamma radiation could be applied

Political and Cost Considerations

Political and cost considerations tend to merge in NATO, where common funding under the NATO infrastructure program is an intensely political issue The infrastructure program was created primarily to provide facilities and other special capabilities for the integrated military structure, with procurements subject to international competitive bidding in which national companies and multinational consortia drawn from the alliance nations participate The domestic political repercussions of infrastructure projects won or lost can sometimes have substantial impacts on the fortunes of alliance governments (including the United States) that usually work assiduously on behalf of their nationals' interests Moreover, alliance governments other than the United States have historically tried to keep the total NATO infrastructure

low in order to avoid domestic criticism of their budgets, which must include their proportionate share of the common NATO infrastructure annual budget

On the other hand, the U S government has generally sought to increase the level of infrastructure funding because of continuing concern about NATO's military posture and because of congressional pressure to get the other alliance members to bear at least part of the cost of improvements This congressional concern has also manifest itself in a general unwillingness to countenance U S prefinancing of infrastructure projects Prefinancing—that is, initial funding by a nation of a project thought to be eligible for NATO common funding—is an accepted way for a country to fund and procure items more quickly than is possible under standard infrastructure processes Prefinancing, however, involves a degree of risk, albeit generally slight, that the projects being prefinanced might not ultimately be accepted for common funding by the alliance as a whole There is also sometimes a substantial delay in recouping the funds expended by the prefinancing nation Historically, however, funding by NATO of projects related to improving the security of U S nuclear weapons has been relatively easy to obtain, and the U S Congress has tended to support prefinancing of these projects with less difficulty

This pattern does not mean that funding for new security improvements will be either timely or as easy in the future The three large security-related infrastructure projects—the Long-range Security Program, the Weapons Access Delay System, and the Intrusion Detection System Program—have involved substantial expenditures that are still ongoing It can be anticipated that U S initiatives for new infrastructure programs specifically designated to improve security will be scrutinized closely by U S allies The reason is that such initiatives tend to raise questions about the need and value of the earlier security programs that have not yet all been completed.

An additional factor on the NATO side that may well generate resistance to new security initiatives, at least in the near term, is the fact that the six-year NATO infrastructure program approved by the alliance ministers in December 1984 represented a substantial increase in funding over previous programs sought by the United States It was approved only after hard bargaining and considerable U S pressure On the U S side, in spite of a record of good congressional support for NATO security programs, including their prefinancing, the intense pressure to cut the defense budget stemming from the Gramm-Rudman-Hollings legislation may generate much weaker support than in the past Congress may also question why anything new is needed when large security programs for Europe have been funded already and partially executed

More purely political considerations with regard to improvements in security may arise from the nature of specific security improvement programs developed in accordance with the principles presented in this study For example, programs that seem to reflect a lesser emphasis on security in favor

of the operational utility of U S weapons might generate alliance opposition They might be construed as proof of a long-standing Soviet assertion that the United States would rather fight a nuclear war with theater weapons on European soil than deter a conflict through the threatened use of U S strategic systems Additionally, it is probably true that some European political opposition might be based on a fear that, in the absence of a clear terrorist threat to nuclear weapons that would militate for funding, overt attention to weapons security might actually precipitate terrorist activities against them

Recommendations

This study of U S nuclear weapons security and control has quite consciously not approached the subject from a rigorous analytical perspective To do so would have required the use of classified information that, even if it were available, would have been inappropriate A comprehensive data base would have been required, including descriptions of current facilities, procedures, and processes for protecting U S nuclear weapons against terrorists, and the status of the various upgrade programs. If this data base had been available, it might have been appropriate to make a basic recommendation that the principles presented in this study be used to assess the degree to which the baseline (including upgrade programs) adheres to these principles This assessment, in turn, could have provided a basis for recommended changes to ensure greater future consistency with the principles

Absent a detailed data base, the most appropriate basic recommendation is that the approach of this study—that is, the use of a broad set of protection principles—be considered by responsible U S government officials with access to the necessary classified information as a possible basis for evaluating the actual baseline U S unified commanders generate and submit to the Joint Chiefs of Staff documents called required operational capabilities that identify the additional capabilities (for example, survivable Command, Control and Communications systems) needed by the theater commander to perform his mission It appears that no parallel effort has been directed specifically at the subset of security relating to terrorism

Three specific recommendations flow from the discussion of the principles stated here

First, programmed modernization of U S nuclear weapons should be accelerated as a matter of the highest priority in order to ensure that these weapons, especially the ones that may be planned for forward deployment, incorporate the latest PAL and, as appropriate, command disable technology The latter should encompass the principle of automaticity to preclude the possibility of an unauthorized unlocking of a usable U S weapon Barring the possibility of retrofit, implementing this recommendation should involve, at

a minimum, the accelerated production and forward deployment of the new W79 and W82 weapons (presumably without their enhanced radiation capability) to replace the older W33 and W48 weapons

Second, U S. Navy nuclear weapons requirements should be reevaluated with regard to the technical, cost, and operational feasibility of incorporating modern PAL systems and, where appropriate, command disable systems into the weapons Although the various scenarios advanced by critics of U S Navy policy regarding PAL systems are not necessarily persuasive, the marginal increase in positive control that the systems might provide would remove a continuing source of criticism and might yield an additional element of stability of the perceived U S -Soviet strategic balance PAL and command disable systems could provide additional flexibility and better security for the deployments of certain U.S Navy tactical weapons This gain could be especially valuable for possible contingent deployments of air-delivered nuclear ASW weapons on foreign soil

Third, ongoing research and development programs must emphasize ways to prevent unauthorized access to U S nuclear weapons, as must the continual monitoring by officials of proposals to improve weapons security. The potential impact on alliance public opinion and governments that would result from a terrorist's merely gaining physical access to a U S weapon is such that finding ways to decrease the probability of that event is essential Assuming that weapons modernization with the objective of putting in place the most advanced PAL and command disable systems has taken place, these measures should provide sufficient guarantees against the possibility of an actual terrorist detonation of a stolen weapon

Notes

1 The term *nuclear weapons* is used throughout this report to denote nuclear bombs and nuclear warheads for missiles and artillery rounds, whether or not the warheads are mated with their associated missile bodies or artillery shells

2 The word *terrorist* as used here denotes individuals or groups such as the Red Army Faction, Red Brigades, and Fighting Communist Cells An interesting discussion of how else the term might be defined is contained in Thomas C Schelling, "Thinking about Nuclear Terrorism," *International Security* 6 (Spring 1982) 61–77

3 These POCs comprise a set of bilateral agreements concluded in accordance with the Atomic Energy Act of 1946 that establish the conditions and mutual and individual responsibilities of the signatory nations with regard to U S nuclear weapons provided for possible employment by allied military forces

4 These are listed in the chapter Bibliography They also constitute the sources for the data used in the discussions that follow These sources have not been footnoted in the text to avoid breaking the flow

5 As early as the August 1968 version, the governing Department of Defense directive, number 5210 41, "Security Criteria and Standards for Protecting Nuclear

Weapons," was explicit that "nuclear weapons require special protection because of their political and military importance, their destructiveness, and the attendant consequences of an unauthorized detonation" (August 14, 1968, p 3)

6 Principle 2 states that protective capabilities against terrorists or the acts of other unauthorized people should be an integral part of weapons design Principle 4 states that command and control systems for nuclear weapons should incorporate physical and technical systems to prevent the unauthorized detonation of U S nuclear weapons

7 The latest is Desmond Ball "Nuclear War at Sea," *International Security* 10 (Winter 1985–1986) 3–31

8 Ibid

Bibliography

"Cosmos Puts U S Teams to Test" *Los Angeles Times*, February 12, 1978, p 8

Ball, Desmond "Nuclear War at Sea" *International Security* 10 (Winter 1985–1986) 3–31

Cochran, Thomas B, William M Arkin, and Milton M Hoenig *Nuclear Weapons Databook* Vol 1 *U S Nuclear Forces and Capabilities* Cambridge, Mass Ballinger Publishing Company, 1984

Legge, J Michael *Theater Nuclear Weapons and the NATO Strategy of Flexible Response* Santa Monica RAND, 1983

Mayer, Lawrence "Failsafe and Subs Should We Trust the Navy to Trust Itself?" *Washington Post Magazine*, September 30, 1984, p 7

North Atlantic Assembly Special Committee on Nuclear Weapons in Europe *Nuclear Weapons in Europe* Brussels North Atlantic Assembly International Secretariat 1984

Schelling, Thomas C "Thinking about Terrorism" *International Security* 6(Spring 1982) 61–77

Stockholm International Peace Research Institute *Tactical Nuclear Weapons European Perspectives* New York Crane, Russak & Company, 1978

U S Congress House Committee on Appropriations *Military Construction Appropriations for 1985 Hearings before a Subcommittee of the Committee on Appropriations* 98th Cong, 2d sess, 1984

——— House Committee on Armed Services *Hearings on H R 2496 Department of Energy National Security and Military Applications of Nuclear Energy Authorization Act of 1984 before the Procurement and Nuclear Applications Subcommittee* 98th Cong, 1st sess, 1983

——— House Committee on Armed Services *Hearings on H R 5263 Department of Energy National Security and Military Applications of Nuclear Energy Act of 1985 before the Procurement and Military Nuclear Systems Subcommittee* 98th Cong, 2d sess, 1984

——— House Committee on Armed Services *Hearings on H R 1873 Department of Energy National Security Programs Authorization Act for Fiscal Years 1986*

and 1987 before the Procurement and Military Nuclear Systems Subcommittee. 99th Cong, 1st sess, 1985

——— House Committee on Armed Services *US Military Commitments to Europe Hearings before the Ad Hoc Subcommittee of the Committee on Armed Services* 93d Cong, 2d sess, 1974

——— House Committee on Foreign Affairs *The Modernization of NATO's Long-Range Theater Nuclear Forces* Report Prepared for the Subcommittee on Europe and the Middle East of the Committee on Foreign Affairs 96th Cong, 2d sess, 1981

——— House Committee on International Relations *First Use of Nuclear Weapons Preserving Responsible Control Hearings before the Subcommittee on International Security and Scientific Affairs of the Committee on International Relations* 94th Cong, 2d sess, 1976

——— House *Atomic Energy Act of 1946 and Amendments.* Washington, D C US Government Printing Office, 1975

——— Joint Committee on Atomic Energy *Development, Use and Control of Nuclear Energy for the Common Defense and Security and for Peaceful Purposes. First Annual Report to the United States Congress Pursuant to Section 202(b) of the Atomic Energy Act, as Amended.* 94th Cong, 1st sess, 1975

——— Joint Committee on Atomic Energy *Military Applications of Nuclear Technology Hearings before the Subcommittee on Military Applications of the Joint Committee on Atomic Energy* 93d Cong, 1st sess, pts 1–2, 1973

——— Joint Committee Print *Fiscal Year 1985 Arms Control Impact Statements* Statements Submitted to the Committees on Foreign Relations of the Senate and the House of Representatives 96th Cong, 1st sess, 1984

——— Joint Committee Print *Fiscal Year 1980 Arms Control Impact Statements* Statements Submitted to the Committee on Foreign Relations of the Senate and the House of Representatives 96th Cong, 1st session 1979

——— Senate Committee on Armed Services *Department of Defense Authorization for Appropriations for Fiscal Year 1985* Pt 7 *Strategic and Theater Nuclear Forces. Hearings before the Committee on Armed Services on S 2414* 98th Cong, 2d sess, 1984

——— Senate Committee on Armed Services *Department of Defense Authorization for Appropriations for Fiscal Year 1986* Pt 3 *Unified Commands Binary Chemicals, Hearings before the Committee on Armed Services on S 674* 99th Cong, 1st sess, 1985

——— Senate Committee on Foreign Relations *Nuclear War Strategy Hearing before the Committee on Foreign Relations* 96th Cong, 2d sess, 1981

——— Senate Committee on Foreign Relations *Nuclear Weapons and Foreign Policy Hearings before the Subcommittee on US Security Agreements and Commitments Abroad of the United States Senate* 93d Cong, 2d sess, 1974

——— Senate Committee on Foreign Relations *Post-Deployment Nuclear Arms Control in Europe* A Staff Report Prepared for the Committee on Foreign Relations 98th Cong, 2d sess, 1984

——— Senate Committee on Foreign Relations *US Security Issues in Europe Burden Sharing and Offset, MBFR and Nuclear Weapons* A Staff Report Prepared

for the Use of the Subcommittee on U S Security Agreements and Commitments Abroad 93d Cong , 1st sess , 1973

——— Senate Committee on Government Operations *The Atlantic Alliance Hearings before the Subcommittee on National Security and International Operations.* 89th Cong., 2d sess , pt 1, 1966

U S Department of Defense Secretary of Defense *The Theater Nuclear Force Posture in Europe* A Report to the United States Congress in compliance with Public Law 93-365 Washington, D C U S Government Printing Office, 1975

Wade, Troy E Statement "The Kinds of Responses It Is Prepared to Handle, and Examples of Some Recent Callouts " Before the Subcommittee on Crime of the House Committee on the Judiciary, November 12, 1981

Physical Security of Nuclear Facilities

Herbert Dixon

In the United States, the Department of Energy (DOE) and the Nuclear Regulatory Commission (NRC) are responsible for providing adequate protection to nuclear facilities, materials, and shipments under civilian control Of the two, DOE's task is somewhat more critical, since generally the nuclear materials it handles can more readily be converted into a nuclear weapon, and it is responsible for nuclear weapons prior to their transfer to military custody

A protection system should be able to deter attacks by making the price of entry too high for all but the most dedicated and determined likely adversaries in terms of personnel, equipment, and skills That security mission has several fundamental elements definition of the threat, design of a security philosophy, identification of the systems and processes to be used to deter, detect, and deny access to intruders, and decisions as to the required training and the tactics that will neutralize the threat.

Defining the Threat

The basis of the security system itself is the potential threat The definition of the threat must go well beyond numbers of adversaries to include detailed characteristics, such as method of attack, armaments, and speed of movement Although it is impossible to protect against all threats, the most likely ones need to be planned for

The intelligence agencies disagree to a considerable extent on whether a credible threat exists to nuclear materials facilities, and there has been little intelligence that provides any guidance In the absence of a clearly identifiable threat, both the DOE and the NRC have had to develop what are called design basis threats, within which context they have also prepared generic security standards that serve as guidelines for the design of security systems at specific

nuclear facilities The field offices, aided by security staff from the facilities, conduct site-specific threat analyses and are responsible for converting the generic standards into site-specific performance standards for the security system Implementation of the related security system is put out for competitive bid

The lack of a sufficiently detailed definition of the threat and the ambiguity over the interpretation and implementation of the headquarters' guidelines by the field offices have caused the DOE and the NRC many problems in developing their nuclear protection programs A common all-inclusive threat to all sites could be defined by headquarters, yet this step has not been taken Both the threat parameters and related standards have been vague, and as a result they have permitted different interpretations at the field level For that reason, actual security systems have varying capabilities that may or may not be equivalent to what headquarters intended

There is one comprehensive set of standards at the headquarters level the Inspection and Evaluation Section of the DOE recently completed (after some fourteen years) Draft Inspection Standards Documentation, which staff members use to evaluate security systems at nuclear facilities (In fairness to that unit, its status has been so uncertain over the years that it was unable to fulfill these types of fundamental functions in timely fashion) These standards are not policy, however, and hence cannot be used by plant licensees as the basis for requesting funds to adapt their systems to meet the inspection unit's standards Moreover, because there are conflicts between those standards and what has been put in place at the facilities, the inspection standards may engender controversy Finally, the standards appear in eight different volumes; the one on physical protection and operations alone is 400 pages long

In spite of this facility-based approach to designing security systems, there are some aspects of potential threats that seem to be universal Attackers are likely to be highly mobile, skilled in the operation of electronic security systems, and knowledgeable about security force routines These capabilities would apply to any nuclear facility It is interesting to note, then, that current guidelines call on each facility, in conjunction with law enforcement and intelligence agencies, to do a detailed local threat assessment These types of outside threats are similar across facilities and can be better assessed at the national level Local assessments should focus on what they are best suited to address· insider threats

Evaluating the insider threat requires an assessment of the impact of each employee at a facility in terms of the person's authority, access, job, and relationship within the organization and with the security program Positions that present the best opportunity for successful insider threats should be identified and security measures designed to minimize possible problems

Measures include the two-man rule, rotation of personnel, assignment of new work schedules, and perhaps interplant reassignments, along with more detailed checks on personnel background and strict enforcement of "need to know" and "need to be" regulations

Not enough attention has been paid to defining the insider threat Current specifications require the security system to detect an attempt by an insider to bring explosives or weapons into the plant or to remove nuclear materials illegally from the plant Some parts of the security system are designed to detect an attempt to approach certain critical elements of the nuclear process The problem is that these specifications do not adequately define the insider or certain characteristics of a potential threat, such as the range of speeds and time needed for electrical or mechanical detection, or the quantities and types of explosives an insider might have Yet this information is needed to design an effective and complete security system For example, depending on a sensor settling time after being triggered and its sensitivity, an intruder walking at the right speed could pass undetected through an area covered by a single sensor Adequate protection might require two sensors and a television monitor per zone

The outsider threat is even harder to design against Will the intruder use armor-piercing bullets, a shaped charge explosive, or something else? These questions should be addressed, although they can be unending, and a limit will have to be imposed In some cases, a capability will be considered unlikely enough that it will not be addressed or will be put aside for monetary or other reasons A good general basis for a security philosophy is the statement, "The security system must defeat the terrorist who will be armed with automatic weapons, possess explosives, and be highly trained and dedicated "

Once the fundamental threat parameters are established, more precise data can be developed, such as the speed of the intruder, different positions he or she may assume when moving, and minimum height and weight This type of information should be common to all facilities That is, the threat characteristics should not be site specific for the purpose of preparing system technical performance standards When local conditions are used to define a quantitative generic threat further, systems of varying performance capabilities among the facilities will result

Operational requirements and technical specifications should be defined for both the insider threat and some outsider ones The requirements and the specifications should address each segment of the detection and verification subsystems Only then can the security system designer provide the functional requirements to the producers of the hardware and software In addition, some common standard of security will be present at all nuclear facilities

Security Philosophies

The DOE and the NRC follow two basic security philosophies graded security and power block security Both philosophies are predicated on the idea that physical barriers, armed guards, and electronic devices will deter most would-be intruders Should deterrence fail, however, the objective is to provide means of detecting the intruder(s) and to aid the security forces in denying them access to the protected materials

The graded security philosophy is based on the premise that the security system should become more difficult to resist the nearer the intruder gets to the asset being protected Traditionally the first grade of defense has been perimeter fences with barbed wire on top; the second grade is a combination of electronic components to detect attempted intrusions and response forces to intercept the intruders Locks, vaults, steel doors, and concrete walls, along with inside and outside law enforcement personnel, are the last grade This philosophy is akin to DOD's "defense in depth" approach to protecting nuclear weapons storage sites

The power block security philosophy presumes that the intruder will be successful in arriving at the buildings that house the reactors and other power generation equipment Thus although the system includes perimeter security fences, they serve only as a barrier to keep out animals and casual passers-by and are not colocated with electronic detection and surveillance equipment The strategy is to deny attackers entry into the buildings through a circled wagon approach Vehicles and people are controlled by security guards ouside the power block areas, more sophisticated electronic equipment, including detection and verification devices, are found at the power block facilities.

Elements of a Security System

A discussion of the different segments of a security system is useful in understanding how the system as a whole deters, detects, and denies access The discussion also highlights the need for detailed operational requirements, technical specifications, and threat definitions so the system designers can select the best equipment and configurations of components and measures The elements of a security system addressed here are barriers, lighting, exterior sensors, interior sensors, alarm assessment equipment, and command and control devices Examples of some of the equipment standards published by the DOE are used to illustrate their weaknesses

Deterrence

Lighting and physical barriers such as fences, walls, and doors are used to deter and impede access to secure areas The barrier standards for civilian nuclear facilities cover such features as the height of wires and the thickness of doors The specifications yield some but not total uniformity of protection across all facilities Perhaps more important, neither the DOE nor the NRC standards address other important barrier problems, such as protecting against penetration by a high-speed land or aerial vehicle

As a further deterrent, entrance to protected areas by personnel and vehicles is controlled, for example, by steel turnstiles for people, as well as metal detectors and, in some instances, explosive and radiation detectors, and searches for vehicles, using mirrors to check underneath them Television cameras usually track all searches An elaborate system of badges ensures that only authorized people are admitted to a facility. Upon arrival at the actual plant, an individual turns in one badge and gets another that authorizes further specified access In some instances, access is possible only with a specially coded card inserted into an electronic card reader These readers are connected to a computer that can track individuals wherever they go in the facility

Other deterrents are the high visibility of the forces, loud sirens, and armaments When properly configured, these devices and measures can deter most thieves and vandals and protect the outermost perimeter and interior facilities of a nuclear facility against a low-level threat For better preparedness, security forces engage in mock responses to alarms

Detection

Should deterrence fail, the next element in the security system is detection, which relies on exterior sensors, interior sensors, and alarm assessment equipment

If a ground-based intrusion is attempted from outside the facility at other than an entrance, electronic detection sensors and a closed circuit television system at the exterior fence should pick it up There is also a possibility that the guards will detect intruders while still outside the fence, using standard military devices for nightsighting

At present, the only requirement at civilian facilities is for a human detection capability to sight adversaries before they reach the perimeter fence or within sight of a perimeter-viewing closed-circuit television camera When early detection is based on human capabilities, many factors must be considered· artificial and natural light levels, weather conditions, dress of the intruder, and the ability of the intruder to stop the human detector without alerting other security forces or the electronic and video systems The DOE,

NRC, and Department of Defense (DOD) have assessed the capabilities and accuracy of humans (and animals) as detectors extensively In all instances, they were found to be poor detectors The probability is therefore very high that an intruder at most civil nuclear facilities would not be detected by a human before reaching the perimeter fence, where there has to be an electronic security system

Exterior Detection Sensors. Most nuclear facilities use two sensors, each directed toward a different phenomenon, at the perimeters A fence detection sensor is usually mounted on the innermost fence A second sensor, which may consist of electric field fences, buried magnetic field metal detectors, buried seismic motion detectors, electric cable, or microwave or infrared beams, is installed between the two fences Because physical and environmental conditions can significantly affect exterior detection systems, their selection and installation are critical, particularly since each site is unique

All types of electric security sensors are subject to false and nuisance alarms, both of which have generally accepted definitions, although they may vary somewhat across agencies In general, a false alarm is system generated, a nuisance alarm is a response to a nonthreatening stimulus To deal with nuisance alarms, the sensitivity is adjusted while still maintaining an acceptable probability of detection. To permit a higher sensitivity setting, some nuclear facilities have integrated a form of combination logic into the system's software Selected sensors must activate in a prescribed sequence and within a preset time frame, or the system will conclude that a nuisance alarm has occurred The software must also allow for activation in reverse sequence and for overlapping zones, so that a person leaving the facility by climbing over the fence may be detected Clearly security of and access to the software and its documentation are critical with this type of system

In the absence of combination logic software, maintenance personnel tend to overadjust fence-mounted sensors, and console operators tend to become conditioned to repeated false alarms Another problem in designing adequate sensor systems is the absence of performance standards The threat must be defined in such terms as minimum weight and speed of the intruder, wind velocities, snow density, rainfall, and grass height Detailed specifications for all security equipment are especially important since each field office can approve substitute equipment Further, the DOE and NRC need to specify three performance probabilities that must be met or exceeded that the sensor will detect anomalies, that the sensor will work, and that the system will indicate what a sensor picks up

Present DOE standards do not address exterior intrusion detection systems, and what standards the DOE and NRC use for system probability are unclear At this time, the exterior (beyond the fence) detection capability at some nuclear facilities, because it relies on humans, does not provide suffi-

cient time for security forces to intercept intruders before they get through the perimeter fences

Other departments of the federal government have developed standards, specifications, and operational requirements for security sensors Unfortunately, there is inadequate sharing of information and R&D efforts For example, the DOD has foliage-penetrating infantry radars that might be applicable to civil nuclear facilities Greater sharing of equipment and other cooperation in security matters would produce greater efficiency and economy

Interior Sensors. Interior sensors are electronic devices that detect unauthorized personnel entering restricted areas such as desks, safes, and rooms Motion sensors such as infrared (passive or active), microwave, or ultrasonic (passive and active) can detect unauthorized personnel Proximity sensors relay an alarm if the protected item is touched In highly sensitive areas, a combination of volumetric detection and proximity sensors with video surveillance is appropriate Here, too, more detailed specifications are necessary, based on a clearly defined threat Without them, uniformity of security across facilities cannot be achieved

Alarm Assessment Capabilities

When a sensor generates an alarm, the cause must be determined Because human assessments are too slow against a fast-moving intruder, electro-optic devices that can view the area in question immediately are necessary Remote-controlled day and night television cameras are a very effective means of verifying alarms and determining the exact nature of the stimulus Each camera covers a particular section of the perimeter, usually 100 meters long

The capabilities of some video systems found at nuclear facilities are limited in some respects One constraint is their inadequate ability to handle multiple alarms in situations where an intruder must be viewed almost instantaneously—perhaps because the number of personnel available to monitor the cameras is insufficient and several cameras therefore have to be viewed through one monitor Although all the cameras tape what they see, this capacity does not help when immediate decisions have to be made

Standards and specifications relating to the performance of the television system are extremely important Lighting specifications in particular have a major impact on the performance of cameras The kinds of lights found at nuclear facilities are mercury vapor, sodium vapor, metal halide, and fluorescent

At present, the performance and technical specifications for video systems, as with electronic equipment, are determined by the field offices, an inefficient approach The final determination as to whether an alarm is real will be made by the system operator, and in most cases it will be based on

what the operator can see with the camera In turn, the camera will perform only up to the specifications prepared in the field offices

Command and Control

Command and control must interface with all sensors, assessment equipment, communications systems, and electronic displays Typically the consoles contain visual and audio alarms, panels for directly monitoring protected areas, and communications modes (radio, telephone, intercom, or public address) for contacting security forces and command officials The consoles may also contain switching controls and monitors for viewing information reported by closed circuit television assessment equipment and the electronic access control system The key point here is that the design of command and control equipment must emphasize human engineering and the needs of the security force commander

Several features of some command and control systems at nuclear facilities give cause for concern Some systems can manage only a limited number of alarm and video inputs, and the computers may be subject to failure, although the impact of that problem is greatly reduced by the use of redundant equipment physically separated from the primary system Two omissions in the command and control standards at nuclear facilities are noteworthy The security systems are supposed to protect against electronic devices that collect classified information illegally, such as by eavesdropping. Protection is provided by means of periodic electronic scanning of areas to be used for classified conferences Little attention is paid to eavesdropping on unclassified conversations of key officials in, for example, hallways, from which the best information may be obtained, stationary, fixed equipment is not used

To counter the threat of electronic eavesdropping, one U S government agency uses off-the-shelf surveillance equipment to measure line resistance and other factors that would indicate tapping This equipment alerts the operators to any anomalies and their location The same system also monitors a radio frequency analyzer that constantly samples radio frequency energy and calculates its point of origin, again alerting the operator to anomalies. This type of monitoring equipment is likely to be more effective and efficient than are traveling teams of individuals who periodically perform electronic sweeps of classified areas, the present system

A danger with clandestine listening devices is that they could cause the importance of a position to rise The potential security impact of a low-level employee who may be able to record conversations of key employees is certainly elevated

The second omission is the absence of a requirement that the security system software access other data bases at the facility where important personnel information may be stored. It is easy to determine job by job what

the impact would be if an employee were to collaborate with terrorists It is similarly easy to develop software to analyze events and personnel activities to detect suspicious patterns of behavior Information on security forces and technicians who maintain the system is especially important, because these two groups could do the most damage Variables to check are sick days taken, vacation patterns in relation to other employees, and pay advances

At the same time, it is important to be aware that the software used to analyze personnel information can itself be made the villain in the security system At present, the software is maintained by the contractor who installed the security system, in some cases, the nuclear facility does not even get a copy of the software source program There should be a clear requirement that the software be tested independently to ensure that it has not been subverted

Denial

The final step in either the graded or power block philosophy—barriers, walls, doors, and locks notwithstanding—is the use of the security force to deny access. The key to the security equation is denial, and that goal in turn lies almost exclusively with the capability of the on-site security force and the assistance it gets from off-site law enforcement agencies

On-site Security Forces. The quality of the security force is equivalent to the quality of each member in terms of character, training, and equipment The DOD is conducting studies of how people respond under stress in order to quantify the probability that a person will perform as trained, even in life-threatening situations A person's background and its potential influence on behavior are two points to be checked

The greatest point of vulnerability in any security system is the people who operate and repair it Some states, however, limit access to an employee's criminal record This restriction, which affects the NRC more than the DOE, is sufficiently troublesome that Congress passed a law requiring that the FBI help screen people who have access to nuclear facilities and materials and that the criminal records of employees be made available to facility licensees (Section 606 of the Omnibus Diplomatic Security and Antiterrorism Act of 1986, P L. 99-399)

With respect to those who operate or maintain the security system, DOE order 5632 4 of November 4, 1985, says that

> protective force personnel within exclusion areas are required to possess "Q" access authorizations and "L" access authorizations when a confidential matter is involved

> Maintenance personnel are to possess an access authorization equivalent to those levels of classified matter, and/or SNM [special nuclear materials] to which they will have access

The difference in the depth of the investigation for the "Q" and "L" clearances is substantial If their standards were followed to the letter, a portion of both the guard and maintenance crews would not get top security clearances, and the number of personnel with that access would be fewer, a positive change More important, a more stringent clearance requirement reduces the personnel base for rotating assignments, a measure that greatly assists in deterring collusion At the same time, it is prudent to clear all security and maintenance personnel to the highest level of access they may need In crises, an improperly cleared person may be granted access to sensitive material and information because of necessity; it is better to have foreseen this possibility and to have cleared the person in advance Finally, if supervisors are not fully confident of those under them because of a lack of information, their suspicion could be detrimental to the individual and the organization

A critical factor in security investigations is timing It is felt that more frequent reviews would, for example, have uncovered John Walker's spy activities One reason for periodic reviews is that people and the conditions of their lives change, sometimes to the detriment of job loyalty and performance. More frequent investigations should be required for all security and maintenance personnel. A related matter is the need to control the abuse of drugs Some facilities now require random urine samples and undertake routine searches of the premises

Training for the protective forces requires a minimum of eighty hours of introductory work and twenty-four hours of refresher courses each year The material should encompass the required procedures of the organization, individual skills training, and monthly exercises involving security responses to seizure, theft, or sabotage of the facility or materials Special response teams are also legislated, and their training is similar to that required of civilian SWAT teams One potential problem is that some training must sometimes take place during overtime, yet overtime funds are increasingly scarce

The DOE has improved the training of security managers and the readiness of its security forces through several programs They include the Central Training Academy at Albuquerque, New Mexico, and auxiliary protective force training That latter force, which is composed of nonsecurity guard contractor personnel, acts as a home guard The auxiliary force poses severe clearance problems, especially in terms of its being given access to classified material during an emergency

The size of the guard force, clearly an important consideration, must be determined on the basis of different attack scenarios. In general, the number of guards has been judged adequate in terms of the present design basis threat as defined for their facilities The problem is that the design basis threat may

not be appropriate As a result, the adequacy of the guard force may not be sufficient to protect nuclear facilities or materials

Another determinant of the size of the guard force is the amount of time required to place security forces in a position to intercept intruders Present guidelines state that "security inspector response time to alarms shall not be more than 5 minutes Alternately, response time shall be less than the delay time that can be demonstrated from alarm activation until intruder could complete their adverse actions"

Each field office decides what constitutes a proper response to an alarm, it can range from simply pushing an acknowledge alarm button to deploying the security forces Moreover, although a five-minute response time is called for, travel times during certain periods of the day at larger nuclear materials facilities can be unpredictable Generally a larger response time than that based simply on the travel time of the intruder is available because of the time it takes to penetrate doors, walls, and fences, given their deterrent characteristics For the most part, penetrability times have been calculated for different threats As long as the capabilities of the attacker do not exceed the parameters on which the calculations were based, it is possible to predict the penetration time quite accurately The preferred size of the guard force is that needed to cope with the worst case situation, but clearly that sort of standard is unrealistic The alternative is for facilities to improve on their early warning and detection capabilities

A key point in this discussion is the speed with which attackers can penetrate a perimeter fence and avoid the detection devices Tests show that it can be done in less than one to four minutes, depending on the distances to be covered, distance being the other determinant of force size The greater the amount of time there is to respond to an attack—and time is a function of the speed at which the attacker must move and the distance to be covered—the smaller the security force can be to protect against penetration of the outer barriers

Facilities that process nuclear materials, as well as the weapons assembly plant (PANTEX), equip their security forces with weapons that should be equal to the firepower that a terrorist group might have They also have night-sighting equipment State-of-the-art body armor and bullet-resistant helmets provide acceptable protection to individual guards against small caliber weapons and, to a lesser extent and depending on the distance, hand grenade fragments

The transportation for moving security forces and special response teams has not always proved reliable Moreover, armored vehicles have tires that are susceptible to light antitank weapons, to which most terrorist groups have access. Those weapons are also capable of destroying guard towers and the hardened portal cubicles Defenders rely on 50-caliber machineguns mounted on some of the armored vehicles as their principal air defense and

antivehicular (car or small truck) weapon These weapons are highly effective against a helicopter, hang glider, parachutist, or slow-flying fixed wing aircraft On the other hand, it is well documented that friendly fire from machineguns can exact a high toll on a facility's own forces Some security personnel do not realize the destructive capability of small arms and machinegun bullets With respect to the vehicles, they do provide the necessary high-speed transport capability

In the main, the conclusion reached on the basis of assessments of the type and quantity of weapons, equipment, and vehicles issued to security forces is that they are cost-effective against the quantified design basis threat being used. It has also been concluded that they would be used effectively in an attack On the other hand, these assessments do not assume any degradation of the systems, personnel, and equipment, as they should in order for realistic standards to be set

Off-Site Security Forces. The DOE and the NRC have entered into agreements with local, state, and federal law enforcement agencies for support of facility forces Field offices specify communications checks on assigned radio frequencies and local telephone systems, and the various forces engage in mock exercises annually With respect to the latter, however, funding is often so scarce that less than the full complement participates Moreover, it is unclear what would be the priority for local forces in the event of contemporaneous crises such as an attack on a facility and a natural disaster

Annual mock exercises do not provide sufficient experience to ensure a coordinated response in an actual emergency The movement and use of multiple security forces are a complex command and control matter, as evidenced by the problems encountered in the Grenada exercise Ideally more frequent and fully funded exercises involving both on- and off-site security forces are desirable

Denying access to a protected asset requires an integrated response by all elements of the protective system· equipment, facilities, and people At present, the subsystems and the required integrated response are based on the quantified threat prepared by headquarters, as interpreted, in terms of the detailed specifications and level of capability of the protective systems, by the engineers and security personnel at the field offices and facilities One result of this approach is that security system capabilities vary across facilities

Evaluation of Security Systems

The DOE evaluates security systems against the design basis threat, however, it is unclear what standards are to be used in evaluating capabilities because there are no predefined operational requirements or technical specifications

In the end, it is difficult to say with certainty what the capability of a protective system is with respect to threats of various levels of sophistication For example, the opening and closing of areas by operational personnel in the course of the regular activities is considered a valid test of access alarms However, a terrorist is likely to target the vulnerabilities of a system, not its normal operations Another example is that each field office is permitted to set the sensitivity test levels for sensors What is needed are uniform standards for all sensors and other segments of the total protection system

The inspection and evaluation section of the DOE has drafted its own performance criteria, which it uses to pass or fail the systems in place at facilities The problems with these standards have been outlined

Shipments of Nuclear Materials

Interfacility Shipments

The DOE transports nuclear materials and a portion of the nuclear weapons it manufactures for the DOD between its facilities Per year, it makes more than one hundred truck and rail shipments, with the percentage of weapons transfers by truck now increasing

DOE has developed special trucks and railcars for exclusive use in transporting threshold quantities of nuclear materials The trucks, modified tractor-trailers called safe-secure trailers, are armored and contain deterrent and denial devices All weapons-grade plutonium and enriched uranium are moved by truck. Similar safe-secure railcars are used for large-volume rail shipments Both types of vehicles have been tested extensively for their capability to withstand different kinds of terrorist attacks, with close attention to physical protection, communications, denial of access, armor, energy absorption in the event of impact, and personnel safety These vehicles are accompanied by escort and power buffer vehicles that are also specially equipped and protected

The communications system, which involves the transmission of voice and digital data, has been tested extensively as well For example, the feasibility of two-axis inertial attitude reference devices and laser radar and chemical beacon systems for relocating hijacked vehicles was analyzed The resulting communications system is capable of maintaining contact with the special vehicles anywhere in the continental United States

An access denial system for transport vehicles is designed to delay the attackers from reaching the nuclear weapons or materials until other forces arrive at the scene A variety of devices are used, including instant foam, maladorous substances, and some incapacitants It is believed that the various measures provide adequate protection against the defined terrorist threats

The guard forces that accompany the safe-secure vehicles are employees of DOE, they ride in escort vehicles for road transport and escort railcars for rail transport The trucks are also driven by armed couriers All these guards undergo security investigations and an eight-week training course, with refresher courses every three months They receive annual refresher training in radiation monitoring, firearms safety, security, and SWAT team techniques

More likely than a hijacking is an accident, particularly one involving an impact at high velocity It is widely believed that even in that circumstance, detonation of high explosives or plutonium dispersal is almost impossible

The greater danger to the viability of the interfacility transport program is complacency The system was designed to meet a specific terrorist and criminal threat The character of that threat is changing, however, in particular, terrorists seem willing to sacrifice even their lives New analysis of the design basis threat may be in order

Intrafacility Shipments

Special nuclear materials being moved between buildings are usually transported in a sealed, locked van or trailer A shipping custodian schedules authorized shipments with the nuclear materials custodian The shipping custodian also releases the materials from the storage vault to the uranium operations personnel for loading into the sealed van These procedures are all documented. At the destination, the van enters a vehicle trap that has doors at either end, only one of which may be open at any one time At this point, the two-person rule applies An exterior door is raised, and the material handlers back the van up to the loading dock A receiving custodian breaks the seal and inspects the material containers during unloading Both he and the guard verify the shipment and complete the necessary documentation Guards located in hardened cubicles oversee the loading and unloading process

Substantial effort has been expended to design a system that ensures the integrity of the cargo and that accounts for the materials during loading and unloading But the transport system is weak during the period of movement between the loading and unloading sites The current security system and procedures are geared to the skilled, covert, sneaky intruder. The recent helicopter snatch of prisoners from prisons in North Carolina and Paris and the truck bomb incident in Beirut suggest, however, that more violent, overt threats also need to be considered It is advisable to reassess the adequacy of the level of transport vehicle armament and security during the time of movement between buildings in the light of these types of threats Factors that should be addressed are the weight of the vehicle and the nature and number of weapons issued to the transport force

Conclusions and Recommendations

A serious problem with present security systems at nuclear facilities is that the threats and standards prepared by the NRC and DOE are general, and the field offices are required to develop their own local threats and, on that basis, to prepare detailed specifications for security systems at sites in their jurisdicton As a result, the capabilities of the systems vary across facilities

A further problem is that no testing is required beyond "alarm"/"no alarm" (which checks whether the sensors will activate the alarms), and there is no definition of what stimulus should set the alarm off Present standards accept the stimulus of routine personnel movements Such an approach to setting standards ignores the probable innovativeness and shrewdness of the likely adversary Another problem caused by the absence of defined performance standards is that there is no good basis for collecting empirical data on the true capability of the security system for any facility

For purposes of inspection and evaluation, the DOE unit in charge of that effort has had to develop its own standards Its standards do not, however, constitute policy to which all parties must adhere, and they differ from those being used in the field As a result, they are likely to engender conflict and controversy Nor can field or facility personnel use them as a basis for requesting funds to bring their systems up to that standard

Other agencies of the federal government have prepared their own security system requirements, standards, and specifications Sharing these data would be useful and cost-effective A new effort is needed to create an administrative process whereby the exchange of information, testing of equipment, and participation in R&D programs are facilitated among all federal agencies

As to the actual performance of systems, it is imperative that they be able to detect intruders sooner than is called for at present DOD has military personnel detecting radars and point sensors that meet the early warning requirements In addition, they reduce the number of human detectors needed Each nuclear facility should assess whether this equipment is cost-effective in terms of potential personnel reductions or possible reassignment to duties to increase overall security

Security guards and maintenance technicians are the potential weak link in the security chain against an insider threat Both groups have access to all parts of a facility and could be called on during an emergency to perform critical tasks Therefore their behavior and background are critical Present standards do not require that these two groups of personnel receive the highest security clearances, with their all-important comprehensive background check It is imperative that the relatively small amount of funds required to conduct background investigations of all security guards, maintenance technicians, and other critical personnel be made available In ad-

dition, it is important to conduct reinvestigations of key personnel frequently enough to identify adverse change in individuals and their circumstances

The vehicles used for intrafacility shipment of nuclear materials are vulnerable to small arms fire, are relatively light in weight, and can be entered easily using handguns or small explosive charges The entire physical arrangement of this transport system should be reviewed to determine its vulnerability to new types of threats, particularly a helicopter intrusion or a high-speed truck bomb, and other violent and overt attacks Physical security must be as thorough as that found at the loading and unloading stages

The physical protection systems of civilian nuclear facilities appear to approach the generic standards established by headquarters, however, the standards are vague and have left a lot of room for interpretation at lower levels Moreover, there is a serious question as to whether the defined design basis threats remain appropriate As to their implementation, the personnel security investigation stops short of a reasonable goal, and the lack of coordination among and use of equipment from all government agencies is economically wasteful When a security system at a nuclear facility is tested by a smart adversary, as it will be, his or her probability of success should be predefined and acceptable to headquarters, field offices, and facility managers. It should not be an unknown because the systems were designed around vague and incomplete standards.

Five steps in particular are strongly recommended at this time

First, those agencies responsible for civil nuclear facilities should jointly prepare detailed threat definitions, operational requirements, and equipment specifications to protect generic nuclear facilities, and these matters should be issued as policy The agencies should provide sufficient detail to guide the design of specific security systems and to identify candidate components

Second, the DOE, NRC, and DOD should explain to Congress why government-developed security and other military equipment are not used to upgrade existing security systems and to stock future ones

Third, each DOE and NRC facility should be assessed to determine the impact on the size of the guard force and on warning time when personnel-detecting radars and ground point sensors are installed

Fourth, all security guards and technicians should be investigated for the highest security clearance, with reinvestigations every four years

Finally, the processes and vehicles used in intrafacility transport of nuclear materials should be evaluated against a range of threats and attack scenarios, including violent air and vehicle assaults

All of these recommendations are feasible and cost-effective The appropriate congressional subcommittees should direct that they be implemented as soon as possible

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

International Safeguards and Nuclear Terrorism

Sidney Moglewer

This report provides a critical review of the effectiveness of International Atomic Energy Agency (IAEA) safeguards against potential acts of nuclear terrorism I argue that IAEA safeguards should be made applicable to deterring diversions of nuclear materials from civil to weapons purposes by subnational groups as well as by nations Both technical and institutional factors are considered, and suggestions for organizational restructuring and further technical development are made I hope to raise awareness of the necessity for effective preventive measures and to suggest possible directions for further effort

There are a variety of potential forms of nuclear terrorism nuclear material diversion, sabotage or destruction of material and facilities, on-site terrorist weapons fabrication, and theft or destruction of materials in transit Safeguards systems are needed to deter, prevent, detect, and provide timely warning of such terrorist activities, as well as diversions to national weapons programs IAEA safeguards are designed only to deter and give timely detection of national diversions The functional subsystems that characterize the total safeguards system—physical security, material control, and material accounting—will be discussed as they apply to international safeguards

The Nuclear Non-Proliferation Treaty (NPT) is the cornerstone of international efforts to prevent the further spread of nuclear weapons The nonnuclear weapons states agree to have the IAEA apply safeguards to verify that they are not diverting civilian nuclear materials to the production of such weapons In return, the nuclear weapon states preferentially share their civilian nuclear technology with the nonnuclear weapon states One hundred and thirty states are party to the NPT, with several more signatories awaiting ratification Since the inception of the NPT in 1970, both it and the IAEA have been praised for fulfilling the central undertaking of the treaty the agreement of nuclear weapons powers not to transfer nuclear weapons and of nonweapons states not to acquire them Only one nonweapons state, India,

which is not a party to the NPT, is known to have detonated a nuclear explosive device (in 1974), using material from an unsafeguarded facility

There is general agreement that the IAEA represents the most advanced system of international inspection of the internal activities of sovereign states that has ever operated, however, there is a fundamental question concerning IAEA effectiveness in a total safeguards sense, in particular with respect to the terrorist threat That issue is my focus here

IAEA Safeguards

Article III of the NPT requires each nonnuclear weapons state that is party to the treaty to accept safeguards on all nuclear activities as set forth in an agreement negotiated with the IAEA The purpose of IAEA safeguards is verification of the fulfillment of the obligations a state assumes under the treaty, with a view to preventing the diversion of nuclear material from peaceful uses to nuclear weapons or other explosive devices The basic approach used by the IAEA to determine the adequacy of safeguards is to evaluate and verify nuclear material accounting information developed by a country for specific facilities [1]

The IAEA is responsible for safeguard verification of approximately 1,000 facilities, which account for a significant portion of the world's nuclear activities The IAEA is required to judge in each situation whether the application of its nuclear material verification procedures in particular countries permits it to fulfill its safeguards responsibilities The agency also specifies the basis for project agreements, transfer agreements, and unilateral submission agreements under which equipment, facilities, nuclear material, and information are subject to safeguards [2] Further, the agency provides guidance on the physical security of host country material and facilities, as well as on the transportation of material, but clearly recognizes that this task is a responsibility of each nation and respects national sovereignty over these matters [3]

Subsidiary arrangements between the IAEA and a member state establish such measures as the following, based on a structure of material balance areas

1 A measurement system to determine the quantities of nuclear materials received, produced, shipped, lost, or otherwise removed from inventory and the quantities in inventory

2 Evaluation of the precision and accuracy of measurements and the estimation of measurement uncertainty

3 Procedures for identifying, reviewing, and evaluating differences in shipper and receiver measurements

4 Procedures for taking a physical inventory

5 Procedures for evaluating the accumulation of unmeasured inventory and unmeasured losses

6 A system of records and reports showing, for each material balance area, the inventory of nuclear material and the changes in that inventory, including receipts into and transfers out of the area

7 Provisions to ensure that the accounting procedures and arrangements are being carried out correctly

8 Procedures for the provision of certain reports to the agency

The objectives of IAEA safeguards are defined to be the "timely detection of the diversion of significant quantities of nuclear material from peaceful nuclear activities to the manufacture of nuclear weapons or other nuclear explosive devices or for purposes unknown, and deterrence of such diversion by the risk of early detection." A significant quantity of nuclear material is understood to be the approximate quantity of nuclear material—taking into account any conversion process involved—such that the possibility of manufacturing a nuclear explosive device cannot be excluded

Timeliness results primarily from the frequency of physical inventory taking, it is determined by the IAEA on the basis of conversion time Conversion time is the estimated minimum time required to produce the nuclear components of an explosive device For materials in direct weapons-usable form, such as the metallic state, conversion time is taken to be on the order of seven to ten days, conversion times of oxides or other pure compounds of plutonium or highly enriched uranium are taken to be on the order of one to three weeks The IAEA's timely warning criterion requires that the detection time (defined as the maximum elapsed time between an indicated diversion and its detection by IAEA safeguards) should correspond in order of magnitude to the conversion time Thus, the detection time could be perhaps several times larger than the conversion time and yet satisfy the IAEA timeliness criterion

Discrepancies in inventories are detected based upon the value of MUF, defined as the difference between book inventory and physical inventory At any given time, the book inventory of a material balance area is determined by adding the quantities of material transferred into the area to the initial inventory of record and subtracting from it the quantities transferred out of the area Periodically a physical inventory is taken to determine the total quantity of material in inventory The difference between the book inventory and the physical inventory at that time is the MUF for the period

Conversion plants, fuel fabrication plants, enrichment plants, and chemical reprocessing plants represent less than 10 percent of the facilities under IAEA safeguards, however, these facilities, known as bulk-handling facilities,

are the stage of the nuclear fuel cycle where civil material is in the form most suitable for nuclear weapons or other nuclear explosive devices These facilities are found in about two dozen countries

To verify the effectiveness of the material accounting system, the MUF calculations, and the other safeguards requirements, the IAEA deploys an inspection force to such facilities regularly Several weeks' notice must be given for planned inspections, although unannounced inspections may be held and are a major part of the inspections at gas centrifuge plants The IAEA negotiates with each country the allowable inspections per year, with three or four considered normal The actual number of inspections ranges from one a year for small reactors to continuous inspection at larger bulk-handling facilities Inspectors must be acceptable to the nation whose facilities are being inspected and usually are nationals of countries with which the host country has friendly relations The IAEA has about 250 inspectors from some 60 countries

The IAEA inspector's job is to verify that the declared material balance is correct The job is not to look for clandestine operations or ineffective physical security and/or material control Under NPT safeguards, an inspector does have the right to request access to an undeclared facility if he or she expects that it contains safeguarded materials, and if access is denied, the inspector may appeal to the director general and to the IAEA board of governors to negotiate entry No special inspection of this sort has ever been requested

The IAEA does not release data showing the MUF, plant throughput, measurement uncertainty, and inspection results or its judgment concerning the effectiveness of the safeguards for any facility or country All this information is classified "Safeguards Confidential" and is tightly held at IAEA headquarters in Vienna What the IAEA does provide is an annual report that states generally

> The Secretariat in carrying out the safeguards program of the Agency, did not detect any anomaly which would indicate the diversion of a significant amount of safeguarded nuclear material—or the misuse of facilities or equipment under certain agreements—for the manufacture of any nuclear weapon, or to further any other military purpose, it is reasonable to conclude again that nuclear material under IAEA safeguards remained in peaceful nuclear activities or was otherwise adequately accounted for

MUF as a Safeguards Measure

The key element of the IAEA safeguards system for determining inventory discrepancies and assessing possible diversion is the MUF Because of mea-

surement system errors, biases of unknown magnitude, human mistakes, unmeasured inventory, and unmeasured losses, the observed MUF contains terms of a random nature as well as unknown biases and is generally not zero Consequently procedures and techniques of statistical inference must be applied to interpret MUF properly It is also important to understand that MUF does not represent a physical quantity—actual kilograms of missing material—but rather is a statistical variable that, to some level of significance, provides a measure from which to infer the actual amount of material that may be missing or unaccounted for

In the case of medium to large bulk-handling facilities, the IAEA really does not know, with any reasonable degree of assurance, how much nuclear material may actually be missing MUF is an ineffective indicator of possible diversion because of deficiencies of both a statistical nature and a chemical processing nature (such as pipe holdup or stack losses) The ineffectiveness of current systems is attributable primarily to the assumption of a completely measured material balance and the failure of the classical statistical approach, which is derived from quality control considerations, to protect against the risk of an intelligent diverter who is out to take advantage of the system The entire framework of classical statistics does not take into account an interaction with a diverter and the options he or she has to foil the system [4] If the diverter knew the value of the alarm threshold of the system and the characteristics of the MUF statistical behavior, this person could use this information to mask his or her diversions

The IAEA system for obtaining MUF is derived directly from the methods and procedures developed in the United States by the Atomic Energy Commission and its successors, the NRC and DOE [5] The NRC has recognized that the current material accounting system contains serious deficiencies with respect to the statistical treatment of MUF [6] Consequently the NRC, unlike the IAEA, does not rely on MUF analysis for judgments concerning possible diversion Rather, the NRC's judgments are primarily based on evidence from the physical security system and material control records and procedures The NRC is preparing an upgrade rule to correct some of the statistical deficiencies for the material accounting system and to tighten the in-plant material control system by focusing on process monitoring

A further deficiency of the current material accounting system is the failure to consider the trade-off between the false alarm rate and the probability of undetected loss Under the current system, the setting of decision thresholds is dominated by false alarm considerations (type I error) That is, for a material balance to be investigated for possible diversion, the MUF reading has to be sufficiently large to reduce the possibility of a false alarm As a result, little or no consideration is given to the possibility of the diversion being contained within a small MUF reading (type II error) That is, although large diversions of materials over a relatively long period of time would

probably result in large MUF readings, the relatively small amounts of material in a medium to large throughput facility necessary to make a terrorist weapon could be masked within the results of a small number of material balances This further reduces the validity of MUF as an indicator of diversion, particularly diversion of a small but significant amount—enough for one or two bombs—as terrorists might do if successful in infiltrating the work force of a safeguarded bulk-handling facility

Tighter thresholds for protection against small but significant diversions of weapons-usable materials by terrorists are clearly needed For the establishment of a decision threshold for alarm and further investigation, the IAEA uses 8 kilograms of plutonium and 25 kilograms of highly enriched uranium By way of contrast, the United States uses 2 kilograms of plutonium and 5 kilograms of highly enriched uranium as trigger quantities

IAEA Effectiveness

The IAEA's safeguards activities are monitoring and auditing, not regulation These activities are subject to voluntary agreements between the IAEA with individual states Within the IAEA framework, little consideration has been given to the issue of whether nuclear materials are adequately monitored against potential diversions by terrorists

Support for the agency is based largely on assessments of the effectiveness of the monitoring of peaceful uses of nuclear energy involving agreements at a national level, the basic thesis of the NPT ~ David Fischer has stated

> The main political value of Non-Proliferation Treaty (NPT) safeguards was to provide a reasonable assurance that one's own country was *not* engaged in making nuclear explosives or nuclear weapons, in other words, to demonstrate one's own peaceful commitment and thereby contribute to international security [8]

In contrast, de Montmollin et al observed, "Protection against subnational adversaries and individuals rests with the sovereign authority of the nation, not the Agency "[9] Consequently, there should be genuine unease about the possible accumulation of diverted weapons-usable materials by terrorists

The technical deficiencies of IAEA safeguards, based on material accounting verification, are real and have been documented here and in the literature [10] Other safeguard deficiencies are the result of the IAEA's limited authority to oversee the adequacy of national material accounting and control systems and the physical security of safeguarded facilities By comparison, the NRC, which does have regulatory authority for domestic commercial nuclear facilities, requires the following from its licensees

1 A safeguard plan and program acceptable to the NRC

2 Physical security incorporating perimeter protection, intrusion detection, security forces, multiple barriers, personnel screening, and access controls

3 Material control and accounting systems and procedures

4 Security force training

5 Contingency response and public warning plans

6 Transportation safeguard regulations

7 Acceptance of routine NRC inspection and enforcement, as well as on-site reviews of safeguards effectiveness

8 A system of fines and penalties ranging up to a complete plant shutdown

Even with this more comprehensive safeguards approach, there are still serious questions as to the effectiveness of the domestic safeguards system and regulations of the NRC For example, the NRC has never justified in a consistent manner the design basis threat that guides the design of safeguard systems Another example is the failure of the current material control and accounting system to consider the trade-off between the false alarm rate and the probability of undetected loss

Given that the effectiveness of the domestic safeguards system of the United States is questionable in the face of a determined and intelligent threat, it follows that the incomplete and sparse safeguards system of the IAEA is even less of a deterrent to diversion of nuclear material by international terrorists Indeed, as de Montmollin et al. point out, the IAEA safeguards system is not necessarily intended to provide detection so timely that diverted material can be retrieved before the diverter is able to insert it into an explosive device According to de Montmollin et al , successful intervention before a single bomb could be assembled is more pertinent to the terrorist threat, which is the concern of the state [11]

That the IAEA has a deterrent effect against diversion at a national level cannot be denied It would appear, however, that the deterrence is based on political rather than technological factors (given the technological limitations of IAEA safeguards) Some defenders of the IAEA state that the reason for the success of the NPT and the IAEA is the confidence the parties have that signatories comply with IAEA safeguards. They further argue that loss of confidence will cause the whole structure of proliferation control to collapse These defenders thus oppose what they term "unfounded criticism on narrow technical grounds."[12]

If this argument is valid, the IAEA and NPT are weak reeds on which to lean for the prevention of nuclear terrorism as well as horizontal proliferation The world community needs a robust structure that can withstand such criticism and even benefit from it The defenders of the IAEA are acknowl-

edging the fragility of the current safeguards institutional structure and its inability to cope with the terrorist threat

The Third Review Conference on the NPT, which met in September 1985, reaffirmed the validity of the treaty and the commitment to its purposes and provisions The conference restated the belief of the attendees in the effectiveness of IAEA safeguards in preventing proliferation and noted that the verification system, by demonstrating compliance with the treaty, facilitates international nuclear trade

The conference should have focused greater attention on plugging the gaps in safeguards effectiveness The majority of the attendees were nonweapons states from the developing world; they were interested primarily in acquiring nuclear technology and facilities. There is a possibility that the structure of the NPT and compliance with IAEA safeguards could be considerably weakened once that goal is met

The primary concern of IAEA safeguards is diversion by a state on a national scale Diversion by terrorists is considered to be a concern of the state itself Consequently the IAEA does not regulate or evaluate the capability of the state to prevent or detect subnational diversions This major flaw in the concept and structure of the NPT and the international safeguards system is major This approach implicitly assumes that the objectives of terrorists and states are always in conflict It does not account for those cases where a state and terrorists may be cooperating or where a state engages in benign neglect of the operations of terrorists.

The IAEA facilitates the transfer of nuclear technology and material on an international level at the same time that the effectiveness of domestic safeguards varies widely among the nations Some nations could be attractive targets for diversion by well-organized terrorist groups, which, as has been amply demonstrated, operate worldwide Material stolen in one nation could be used for nuclear blackmail or destruction in another nation Do nations possessing nuclear technology have the right to transfer that technology to nations with questionable safeguards effectiveness? To do so is to expose all nations to future nuclear risk from terrorists The evaluation of total safeguards effectiveness—including physical security and material control, as well as material accounting—should be a major function of the IAEA

Alternative Safeguards Approaches

One alternative to IAEA safeguards has been the bilateral treaty or agreement This instrument is negotiated directly by two nations and usually includes provisions calling for the application of IAEA safeguards but can also contain mutually agreed safeguards arrangements exclusive of the IAEA These treaties or agreements often are temporary expedients that suit the interests of the

parties at the time the treaty was formulated. The problem with undue dependence on bilateral safeguards arrangements is that it probably would result in an uneven safeguards system worldwide, with no mechanism for independent assessment of effectiveness

Another form of international undertaking is a convention among states, almost equivalent to a multilateral treaty The Convention on the Physical Protection of Nuclear Material, ratified by the United States in September 1981, is a good example It addresses the physical protection of nuclear material international transport, domestic storage, and transport In addition, it sets levels of protection for international transport A principal weakness of the convention is that it does not provide for an international authority to regulate and/or evaluate the effectiveness of a state's adherence to the provisions of the convention or for any sanctions to be applied against nations for violations

Conclusions and Recommendations

The safeguards system of the IAEA is incomplete It was not designed for and is not effective against potential international nuclear terrorism The agency should be given authority to establish standards and to regulate safeguards Given the threat of potential terrorist diversions, the IAEA should have the responsibility to evaluate and assess the quality of the national material accounting, material control, and physical security programs of host nations and to bar those with ineffective systems from participating in world nuclear commerce The responsibility of the IAEA should be extended also to include the regulation of physical security, transportation, and material control

Modern technology offers the means to supplement the role of the IAEA inspectors and to improve the effectiveness of inspection and verification In particular, the implementation of a dedicated IAEA communications satellite system to help monitor nuclear materials in facilities and in transit is strongly recommended

The IAEA as an international body is the result of a cooperative agreement among sovereign nations These nations have formed a coalition to implement the NPT through the IAEA and to reap the potential benefits of safeguards and the technical benefits of nuclear cooperation through the IAEA There should be some concern as to the loyalty of some member nations to the coalition in the face of changing benefits of nuclear cooperation for these nations There should also be some concern as to the objectives of all the parties to the treaty and their consequent continued loyalty to the coalition These issues can be profitably studied and recommendations made for restructuring the IAEA based on insights derived from coalition theory [13] Increasing the authority of the IAEA would require agreement by a coalition

of nations Inasmuch as the world community has not yet suffered the consequences of nuclear terrorism, it is highly doubtful that the political will for such an agreement exists today

If nations are not prepared to sacrifice some national sovereignty to increase the authority and the effectiveness of the IAEA and if the improvement of IAEA safeguards is beyond foreseeable technological capability, then serious efforts should be made to curtail or eliminate altogether the use of plutonium and highly enriched uranium in civil programs Doing so would require a smaller coalition of nations—the major nuclear suppliers and owners of large bulk-handling facilities—and may be easier to structure than the large world community coalition essential for effective IAEA safeguards Again, insights from coalition theory might be useful in developing a stable institutional structure for such a coalition

Notes

1 International Atomic Energy Agency, *The Structure and Content of Agreements between the Agency and States Required in Connection with the Treaty on the Non-Proliferation of Nuclear Weapons,* INFCIRC/153 (corrected) (Vienna IAEA, 1972)

2 International Atomic Energy Agency, *The Agency's Safeguards System (1965, As Provisionally Extended in 1966 and 1968),* INFCIRC/66 Rev 2 (Vienna IAEA, September 16, 1968)

3 International Atomic Energy Agency, *The Physical Protection of Nuclear Material,* INFCIRC/225 Rev 1 (Vienna IAEA, June 1977)

4 Sidney Moglewer, "IAEA Safeguards and Non-Proliferation," *Bulletin of the Atomic Scientists* 37 (October 1981)

5 The system for the United States is specified in the *Code of Federal Regulations,* vol 10, pt 70 For the IAEA system, see International Atomic Energy Agency, *IAEA Safeguards Technical Manual,* IAEA-174 (Vienna IAEA, 1976)

6 U S Nuclear Regulatory Commission, "Report on the Statistical Treatment of Inventory Differences," Information Report from Executive Director for Operations to the Commissioners, SECY-80-514 (Washington, D C Government Printing Office, November 20, 1980)

7 J M de Montmollin et al , "Letter on IAEA Safeguards," *Bulletin of the Atomic Scientists* 38 (March 1982)

8 David A V Fischer, "Letter on IAEA Safeguards," *Bulletin of the Atomic Scientists* 38 (March 1982)

9 de Montmollin et al , "Letter "

10 Moglewer, "IAEA Safeguards", Roger Richter, "Testimony from a Former Safeguards Inspector," *Bulletin of the Atomic Scientists* 37 (October 1981)

11 de Montmollin et al , "Letter "

12 Ibid

13 Martin Shubick, *Game Theory in the Social Sciences* (Cambridge, Mass MIT

Press, 1981), and Steven J Brams, *Game Theory and Politics* (New York The Free Press, 1975)

A fundamental issue is the existence of a core for the coalition If a core exists, it provides an internal cement or inner stability that binds the coalition together If it does not, external, often transitory, constraints are necessary to keep the coalition intact, a generally unstable condition The core can be described intuitively as the set of imputations, or payoffs to the players, that leaves no possible coalition in a position to improve the payoffs of all its members In general, most political coalitions studied to date do not have a core However, the extreme destructive potential for nuclear weapons adds a new dimension to the problem There is a large incentive for all nations to eliminate the threat of nuclear terrorism It thus may be possible to restructure the IAEA so that a core exists, with consequent greater stability than is current today

European Nuclear Safeguards and Terrorism: A Personal Perspective

Enrico Jacchia

This analysis is divided into two parts that, in my view, deal with two fundamentally different types of terrorism national and state sponsored The information is drawn from my experience and recollections of data and events

National Terrorism

A fundamental fact has to be considered when dealing with the possible desire of national terrorist groups to acquire nuclear materials national groups, such as the Italian Red Brigades and the German Baader band, want to change or subvert the organization of the state in order to install a different regime They also need—and want to gain—the sympathy and support of at least a fraction of the nation They see killing a political leader or other terrorist actions that are directed at a specific target—a person, a building, and so on—as a way to get the approval of that fraction

Use of nuclear explosives would mean killing a large number of people and destroying a vast area That type of action would inevitably provoke a reaction of horror on the part of the population, the exact opposite effect of what the group wants Thus, it seems to me that the attractiveness to a national terrorist group of using nuclear material or devices is conspicuously low

That said, would it be difficult for a national terrorist organization to gain access to nuclear materials? This question is the old one of whether safeguards are safe It can hardly be said that safeguards are safe, even though many loopholes have been closed The first safeguards systems (EURATOM, IAEA) had two enormous loopholes transport and legal and administrative procedures These loopholes were all too evident in the well-known diversions recorded about two decades ago They were possible, it was concluded, because of the gaps in the safeguards system

The diversion of 200 tons of natural uranium in late 1968 was a chef d'oeuvre of adroitness, with the organizers making optimum use of the regulations The whole enterprise was planned and carried out in such a way that it was extremely difficult to prosecute the diverters under existing laws and regulations The nuclear material was being purchased by a West German firm from a well-known, respected Belgian company, Union Miniere West German and Belgian officials had authorized this transaction in full compliance with administrative rules The EURATOM Supply Agency had also given its authorization (the authorization of the Nuclear Security Control was not required by the safeguard system in this case) The material was destined for reprocessing at an Italian company in Milan that had requested and obtained the authorizations needed from Customs, the Ministry of Transport, and the Ministry of Industry

Once on the open sea, the ship transporting the nuclear material disappeared By the time it was located while on another merchant trip, the material had been unloaded and the crew, officers, and captain had changed To my recollection, nobody has been convicted, nor could they be This incident is an excellent example of how safeguards are not safe when the diverter is not a burglar acting for money but perhaps a nation with all the resources—technical, legal, and operational—it can command

The other famous case of suspected nuclear diversion occurred at the end of the 1960s Called the NUMEC case, it presents some analogies Based on my memory, the Nuclear Material and Equipment Corporation (NUMEC) of Apollo, Pennsylvania, had MUF of more than 400 pounds of uranium, 150 of which were uranium 235, a material almost directly usable as an explosive In this case, the suspected diversion was possible because of loopholes in the administrative rules and procedures, as well as the disastrously low level of accountability of the company and the poor performance of the controllers The case was prosecuted but was closed, administratively and judicially, for a fine of about $1 million. That penalty is inadequate given that 150 pounds of uranium 235 is enough to destroy several capital cities

Much has been done to close the gap in this area I imagine it would now be difficult to repeat successfully those operations and other similar ones that are less well known Moreover, it is believed that these diversions were masterminded by states A terrorist organization would need to have sophisticated leadership and advisers to replicate them, a condition that is possible but improbable

If a complex operation that seizes on the loopholes in the safeguards systems appears improbable now, a hypothesis that cannot be discarded is direct access to nuclear material by theft or something analogous However, if the materials accounting system works well, even a small MUF should appear within a matter of weeks at the latest A team of inspectors, dispatched immediately, should be able to clarify the situation or impose strict measures

of control until the MUF is explained satisfactorily In the case of EURATOM, the inspectors can request intervention by the police or armed services so as to impose effective control over the factory I am referring to prolonged theft of small quantities so that it would appear in the MUF Theft by assault cannot be protected against with safeguards, machineguns are needed instead

Accurate monitoring of material accounting and transfers is possible and is performed effectively in Europe It is probably less accurate and presents more obstacles of various types in other areas of the world However, it is precisely in European countries (and in the United States) that most nuclear material in its different forms is stored and processed As for the Eastern bloc countries and the Soviet Union, it is well known that the government in Moscow is a keen supporter of safeguards, which it enforces strictly on its own territory and that of its customers

Optimism is not justified, however It is known that the IAEA is permitted to safeguard only material, not facilities, unless they have been declared to be nuclear Although national terrorist groups would hardly be able to build their own facilities, they could try to gain access to facilities whose activities are ambiguous and that might not be subject to IAEA controls because they have not been declared nuclear IAEA safeguards inspectors have no authority to visit undeclared facilities that they suspect might be engaged in activities associated with nuclear material devices, even in states that have signed the NPT Further, the IAEA does not search for undeclared material Here is another wide loophole that affords a potential diverter fertile ground for operations In this case, however, the national services in charge of security matters should be able to fill the gap if they are aware that a diversion is being planned by terrorist groups

This discussion applies essentially to reactor sites or spent fuel storage facilities The situation is different with bulk-handling facilities involving substantial flows of nuclear materials, such as plutonium or uranium 235, that present a much higher risk Measures that would help in these cases are the ones that have been suggested frequently multinational fuel cycle centers, international spent fuel storage facilities, and others

Terrorist access to weapons-usable material is a tremendous risk It has to be emphasized, however, that weapons-usable materials in states other than the nuclear weapons ones are located at only a small and well-known number of sites Inspections of the so-called resident inspection type would reduce this threat of diversion They would probably not be enough, however This field is one where the intervention of the national services in charge of security and their collaboration with other states or international agencies are necessary

The intervention of these services has long-established precedents When foreign companies are engaged in research, testing, or production of sensitive military materials, the U S government requires that they sign contracts with

special clauses to protect secrecy This protection is ensured in general by personnel of the military intelligence services of the country concerned, they have exercised discreet, and satisfactory, surveillance within the plant

It is not advisable to say or write more on such a delicate subject. In any case, it would not be easy to extend these kinds of procedures and exercises to nuclear plants generally, although maybe that could be envisaged for the small number of installations that have or process weapons-usable materials If the terrorist threat extended to the nuclear field, such measures would have to be considered

State-Sponsored Terrorism

For more than two decades, the risk that terrorist groups will gain access to nuclear materials has been practically discarded by competent officials dealing with safeguards If, however, state-sponsored terrorist groups wanted to gain access to nuclear materials or highly toxic chemicals, the prospects would be totally different These groups operate in foreign countries amid a foreign population They do not have the same political constraints that the national groups referred to earlier do They are, or consider themselves to be, combatants, and they are fighting an enemy They may be fanatic or just imbued with a dramatic sense of combatting an adversary In their logic, there might be little difference between a grenade or a mass-destruction weapon Moved by a strong ideal or fanaticism, state-sponsored terrorist groups consider themselves at war, even at holy war

National groups would have difficulty getting access to nuclear materials With terrorist groups sponsored by states, however, it would be foolish to ignore the possibility that they could receive materials (nuclear or chemical) from their sponsor state(s) Nuclear weapons states have a long-established clean record in this field A number of nonnuclear weapon states are, however, considered threshold states, they are near to acquiring the capacity to produce nuclear explosive devices Nevertheless, there is no basis for thinking that they would establish a connection with terrorists

In terms of potential access to nuclear and chemical materials, the most dangerous possibility is the state-sponsored terrorist group, and it poses a difficult situation The sponsor state may or may not be a member of the NPT and may or may not have accepted IAEA safeguards Even if it had accepted them, given the technical and political limitations on the agency's activities, it is almost impossible for the IAEA to guarantee that illegal transfers do not occur

Chapter 4
Can Civil Uses of Weapons-Usable Nuclear Materials Be Minimized?

Intelligence and the Prevention of Nuclear Terrorism

John Despres

Nuclear terrorism is an exceptionally important problem for the United States and other Western countries that are both potential targets of and hosts for nuclear terrorists It is the most damaging possible variant of nuclear proliferation and general terrorism

Intelligence is the first line of defense against nuclear terrorism Western security policies should place a special premium on monitoring nuclear proliferation and international terrorism, not only to limit the separate threats they pose to Western security interests but also to prevent them from merging into the much more severe threat to Western societies nuclear terror

Here I address the role of intelligence in preventing nuclear terrorism I describe the problems and requirements facing national intelligence services in helping to prevent nuclear terrorism, including the difficulties of providing sufficiently timely, accurate, and reliable warnings to forestall actual threats, and I examine in some detail the problem of nuclear hoaxes that terrorists could use to intimidate people and coerce governments if intelligence cannot credibly expose their falsehood

I do not address the sources and methods that could be used to detect, monitor, and appraise nuclear terrorist threats, nor do I assess current intelligence resources and plans I focus instead on the intelligence policy implications of a long-term strategy to enforce a de facto ban on nuclear terrorism by averting any credible threat or actual use of nuclear violence by nonsovereign forces against national interests

The paper first defines intelligence and nuclear terrorism and analyzes the nature of the problem from both a specifically U S and a more generally Western viewpoint As used here, intelligence refers broadly to the collection and reporting of information, the production of assessments, and the presentation of judgments by intelligence specialists who work for public and national security authorities Intelligence encompasses the entire range of investigative and reporting activities at all levels of government—from local

police units to allied military commands—that could contribute to the discovery and disarming of nuclear terrorists Nuclear terrorism, in contrast, refers only to credible threats or acts of extreme violence by forces outside the direct control of any state through false threats or actual use of a nuclear bomb This definition excludes other highly menacing or damaging activities involving nuclear materials, facilities, weapons, or phobias such as poisoning the air or water supplies with radioactive substances; stealing nuclear materials, sabotaging nuclear powerplants, occupying a facility or seizing a vehicle with nuclear weapons, or inflaming public fears in the event of a nuclear accident These events can be extremely frightening, as in the case of public reactions throughout Europe to the nuclear accident at Chernobyl in the Ukraine However, their potential destructiveness and exploitability by terrorists do not match the threat of nuclear explosion

Problem of Nuclear Terrorism

It might seem that nuclear terrorism is not a clear and present danger because there have been no public signs that any terrorists have the ability and will to engage in it. Moreover, modern technology and society offer would-be terrorists ample means of threatening and killing large numbers of people in other ways. At the same time, nothing could have anything like the impact of a nuclear explosion, which could be more physically damaging, psychologically shocking, and politically disruptive than any event since World War II Aside from the lives lost and awesome destruction, nuclear violence would breach the postwar moratorium against the use of nuclear weapons, the most important, even if only tacit, arms control arrangement of the nuclear era Although the casualties from a single act of nuclear terrorism might not match those of nuclear war, they would still dwarf other forms of terrorism by many orders of magnitude and could easily exceed those of most conventional wars

Nuclear terrorism cannot be dismissed as technically impossible, and it is likely to become even more feasible with the continuing spread of the nuclear materials and know-how required to make fission weapons. Nor, clearly, can the interests of individual terrorists or state supporters of terrorism in acquiring a nuclear capability be discounted as contrary to any principles or scruples they may have. Italian terrorists have already shown active interest in locating the storage facilities for NATO's nuclear weapons, although their purpose was unclear Less ambiguously, Libya has openly sought a nuclear weapons capability, at the same time that it has sponsored and supported a variety of terrorist operations A number of other states that have been unstable or that have supported foreign terrorist operations are pursuing similar goals

At present, nuclear terrorism from abroad does not appear imminent, at least not on the basis of information in the public domain But it is likely to become more feasible and credible with the continuing diffusion of the materials and know-how needed to make nuclear weapons

Nuclear terrorism is a potential problem for almost all societies, especially for the United States, for several reasons Terrorists tend to regard the United States, particularly its armed forces, as an enemy Because it is the leading democratic power, the most active proponent of cooperative efforts to combat terrorism, and the best-equipped nation to avert the use of nuclear weapons, the United States is logically a main target of terrorist intimidation and violence It may also face threats from nuclear terrorists who want simultaneously to intimidate others into submission and to deter the United States from intervening by threatening it or its interests abroad with nuclear violence Nuclear terrorist organizations, like small states seeking to develop nuclear weapons, may envisage this offensive capability as a supplement to, rather than as a substitute for, more conventional means of armed violence and intimidation The United States could be vulnerable to just a single nuclear weapon if it could be placed and detonated near valuable U.S. facilities, residential areas, or other targets of terrorists So terrorists could regard the United States both as a threat to their own designs on others and as a target that may be highly susceptible to nuclear intimidation

The United States could also serve as an unwitting source of supplies and expertise for nuclear terrorists Indeed, many Western countries, including the United States, have inadvertently contributed to foreign nuclear research and development efforts that in turn may have helped in the production of nuclear weapons Terrorists could similarly seek gullible or sympathetic Americans who could provide them with the special materials, designs, or devices required for a nuclear weapon

Nuclear terrorism within the United States has been neither a clear nor a present danger The director of the FBI, William H Webster, testified before a U S Senate subcommittee that

> There has historically only been one instance of a bona fide nuclear threat in this country and it was not that much of a threat, but three barrels of low enriched uranium were stolen and the FBI was able to recover those three barrels and apprehend the person He was not, incidentally, trying to extort under threat of explosion [1]

At the same time, it must be recognized that the United States has already been both the host to and victim of domestic terrorist organizations pursuing a wide variety of causes—among them, supporters of anti-imperialist revolutions in the Third World, of Puerto Rican independence, and of white supremacy It also has an abundance of nuclear materials, facilities, and ex-

pertise Thus, although the possibility appears remote, the prospect that the United States could become a target of or host for domestic nuclear terrorists should not be dismissed

In sum, the possibility of nuclear terrorism within the United States is a growing problem for the future But international nuclear terrorism is a more likely and less remote threat to Western society, especially the United States

Intelligence and Nuclear Terrorism

The problem of preventing nuclear terrorism resembles that of limiting nuclear proliferation and international terrorism in some ways but differs in several important respects First, nuclear terrorism requires a policy of absolute prevention that allows for no exceptions In contrast, nuclear proliferation and other forms of terrorism may not be, and may not need to be, suppressed completely While desirable, absolutely preventing any further proliferation of terrorism may be impossible

Second, preventing nuclear terrorism requires dealing with the possibility of false alarms Nuclear terrorists need not possess a nuclear weapon, much less use it, to achieve their objectives because of the panic and other costs even the possibility could engender if perceived to be true The role of intelligence in preventing nuclear terrorism is particularly complicated by this simultaneous need to avoid succumbing to false alarms while ensuring prompt, accurate, and specific warnings about actual threats Western leaders are elected to protect national security, economic interests, and democratic values. This means that their intelligence advisers must be prepared to dispel convincingly any apparent but empty threats of nuclear terrorism that could precipitate public panic, costly mobilizations, spontaneous evacuations, extraordinary searches and surveillance measures, and other disruptive or restrictive reactions to false alarms

In the noncommunist world, where the public media are independent and skepticism is widespread, political authorities will be especially hard-pressed to prove that apparent threats are actually hoaxes A particular concern is how to establish that proof without jeopardizing the intelligence sources and means It is also possible that successive nuclear hoaxes will be more sophisticated and plausible and therefore increasingly difficult to verify

A final and alarming concern is that good intelligence capable of identifying hoaxes may inadvertently induce nuclear terrorists to detonate a nuclear explosive because the threats no longer work Even if that demonstration were intended only to authenticate future threats, not inflict casualties, it would generate widespread terror That result would hold even if the terrorists were discovered immediately and disarmed The requirements for high-quality intelligence on the plans, motivations, and organization of ter-

rorists are particularly stringent in the case of a sophisticated attempt to simulate a nuclear threat In the event of a well-designed one, there may be no good alternative to an inside informer

The task of intelligence against nuclear terrorists is made even more difficult by the nature of the enemy Penetrating a nuclear terrorist operation is likely to be even more difficult than penetrating the larger terrorist organization that may support it As the director of central intelligence wrote recently, "Terrorist groups are a very tough nut for intelligence to crack They are small and not easily penetrated Their operations are closely held and compartmented They move quickly and place a high premium on secrecy surprise "[2]

In the light of the difficulty and importance of preventing nuclear and other forms of terrorism, penetrations of terrorist organizations that could acquire a credible nuclear threat should be a high-priority effort Good intelligence is essential to limiting nuclear proliferation and other forms of terrorism, still better intelligence is needed to prevent nuclear terrorism

Roles of Intelligence

The roles required of intelligence to prevent nuclear terrorism are determined by national security policies They cover a spectrum of services that is comparable to those intelligence must also perform in limiting nuclear proliferation and nonnuclear terrorism basic assessments of key actors, timely indications of new dangers, clear warnings of specific threats, and direct support for diplomatic, police, politico-military, or other operations intended to disable or dissuade identifiable nuclear terrorists Intelligence is thus not only the first line of defense against nuclear terrorism, it is also an essential guide for effective action that keeps a threat from materializing or disarms it before exploding

Intelligence must also be prepared to address urgent questions about the precise nature of the operational problems that political authorities would confront when threatened by apparent nuclear terrorists such as who they are, what they can do, why they would do it, and how they could do it

Prevention

Intelligence can contribute to the prevention of nuclear terrorism in many ways Good intelligence can play a major peacetime role by helping statesmen to isolate and resolve the conflicts that animate political terrorism of all sorts, including potential threats or acts of nuclear violence By focusing policy makers on the costs and risks of recurrent or persistent belligerence and identifying mutual interests in settling conflicts, intelligence can help in iden-

tifying and pursuing opportunities for peace and not just in warning against threats of war or terrorism

This peacetime role for intelligence, however, is likely to be overshadowed by several others. In the case of nuclear terrorism, a more active and important role of intelligence is to deny terrorists access to the elements needed for a credible nuclear explosive capability and to nuclear materials, explosive devices, and technical know-how Indeed intelligence assessments based on information from all sources related to prospective threats provide general direction and sometimes even specific guidance for nuclear and security programs, export controls, and law enforcement efforts intended to minimize the spread of nuclear explosive capabilities

Technical assessments of foreign research, development, and acquisition activities that could relate to nuclear weapons and politico-military assessments of the operational intentions and capabilities of terrorists are the most important contributors of intelligence to the prevention of nuclear terrorism Technical assessment also furthers nonproliferation policies aimed at restricting the undue spread of nuclear weapons and the capability to produce them The latter helps to ensure that nuclear weapons, explosive designs, and materials are secure against possible terrorist plans to steal, seize, buy, or simulate a nuclear bomb

In the case of the United States, in implementing nuclear export controls, decision makers have been sensitive to current estimates and new information on the paths that individual states are pursuing toward the acquisition of nuclear weapons or the development of a capability to produce them Possible early warning signs—an intent to enrich uranium as the fuel for a nuclear power reactor, research reactor, or explosive, to use centrifuges or nozzles in a processing plant to concentrate the isotopes of uranium, or to use particular types of power inverters or pumps to help generate the pressures required—have led the United States and other suppliers to tighten their nuclear export controls Stringently focused but adaptable export controls, well guided by intelligence, can be useful in keeping nuclear weapons beyond the reach of unreliable or unstable states, especially those that might provide nuclear materials, know-how, or weapons to a terrorist organization or that might lose control of their nuclear assets to terrorists during power struggles, military coups, or civil wars

An obvious role of intelligence is to develop basic knowledge about potential nuclear terrorists before any well-defined threats begin to emerge. For the most part, the information and evaluations are those that are most useful in planning to counter nonnuclear operations by terrorist organizations Potential nuclear terrorists merit extra attention In particular, it is important to close in while they are in the earliest phase of planning and organizing the operations. This task is difficult The security measures and

compartmentation of terrorist activities approach the sophistication of the intelligence operations or nuclear weapons programs of small states

For the United States and other Western nations, the long-term problem of nuclear terrorism is likely to be aggravated by nuclear and political developments in the Third World Some states that have supported terrorist groups (such as Libya, Iran, and Iraq) have also pursued nuclear research programs that could yield the components of a nuclear weapons capability One or more of them could eventually succeed in obtaining nuclear weapons These and other states in the Third World with a capacity to build small nuclear arsenals could be subject to violent and disorderly national political crises in which nuclear weapons could be used as a threat by those controlling the weapons. The threat might be aimed at both foreign backers and domestic rivals. In short, new sources of potential nuclear terrorism could emerge not only in states that support other forms of terrorism and acquire nuclear means but also in nuclear-armed states that disintegrate politically

In sum, there are a variety of more or less plausible ways in which terrorists could acquire credible nuclear threats, including stealing weapons, fabricating them, simulating a nuclear explosive device, or receiving one from a sponsoring state None of these paths to nuclear terrorism should be ignored

Crisis Response

If a nuclear terrorist crisis occurs, with or without prior warning, the intelligence services would be expected to advise the political authorities on whether the threat is a hoax or real They would have to present their evaluations persuasively enough either to dispel false alarms or to motivate appropriate emergency measures, precautions, and counteraction In the event of a genuine threat, intelligence must offer its best estimate of who and where the terrorists are, what they want, how they plan to act, whether they are susceptible to restraints of any sort, if and why they would execute their threat, and the prospective effects of alternative courses of action

In an emergency, the quality and reliability of those critical judgments depend heavily on prior knowledge of plans and intentions, as well as on the capabilities, of the terrorists One difficulty is that, in contrast to nuclear-armed states, nuclear terrorists are more likely to be anonymous, at an unknown location, without assets whose potential seizure or destruction is likely to deter violent behavior, and beyond the influence of others besides their sponsor By hiding, arming, and shielding their nuclear weapons in a major metropolitan area and dispersing themselves elsewhere, as in the story *The Fifth Horseman,* the fictional account of a Libyan-sponsored threat to New York, nuclear terrorists and their threat can be expected to remain invulnerable to most conventional countermeasures

Preventing nuclear terrorism after their weapons have been deployed and armed requires prompt and reliable information on location or on procedures for remotely countermanding orders to fire them automatically This sort of information terrorists are likely to guard most closely and is the most difficult to acquire on short notice, unless special measures had been taken in anticipation of a crisis

Policy Implications

The policy implications of these views are simple in principle but complex in practice To prevent nuclear terrorism, good intelligence on the intentions and capabilities of potential nuclear terrorists is indispensable It is vital to the detection of possible acts, to dealing with threats, and to identifying and dispelling false alarms States that support terrorists and gain access to nuclear materials, know-how, or weapons and unstable states that have nuclear weapons or their components merit special attention

To persuade other countries concerned about nuclear proliferation to limit their inadvertent contributions to the spread of nuclear weapons, the United States must be able to share its assessments of how those countries' export controls are subject to circumvention by potential nuclear weapons states or to violations by their suppliers Good intelligence based on multiple, independent, and reliable sources of information and thorough analysis is invaluable in facilitating the adoption of more effective export controls by all prospective suppliers Moreover, intelligence is an essential adjunct to active security measures and law enforcement activities aimed at preventing the emergence of a black market in the special nuclear materials required to make an explosive device

The common interests of Western nations are likely to offer new opportunities for cooperation in anticipating and countering potential nuclear terrorism One approach will be cooperative monitoring of international terrorist organizations, as well as joint assessments of particular international terrorists, state supporters of terrorism, and their nuclear capabilities These strategies may be essential to ensuring that Western political authorities are ready to act together rapidly and effectively Exchanges of information among Western intelligence and security services can contribute to common assessments and to prompt detection, identification, location, and even interdiction of terrorists and their state supporters before they initiate operations

The United States and the Soviet Union share a great interest in identifying and controlling terrorists who are trying to raise tensions or catalyze nuclear conflict They presumably also continue to share a strong interest in perpetuating the de facto moratorium since 1945 on the use of nuclear weapons On the other hand, Soviet and U S interests could diverge and conflict in

situations where terrorist operations are directed primarily against the United States and its allies and friends

The extent to which the interests of the United States and the Soviet Union converge or conflict is often unclear The case of the Soviet allegations to Western governments that South Africa was undertaking nuclear test preparations in August 1977 is an example In this instance, both countries presumably had a common interest in limiting nuclear proliferation At the time, however, the Soviets were interested in discrediting the United States in black African eyes by linking it with the nuclear ambitions of South Africa's apartheid leadership As a result, rather than just privately advising the United States and other potentially influential states of its concerns, the Soviet leadership launched a public campaign denouncing the United States and others for their ties to South Africa This propaganda raised doubts about the reliability of Soviet allegations and made it unclear whether the Soviets were more interested in arousing and exploiting fears of a South African bomb or in helping the West prevent one In turn, this publicity also limited the range of actions that Western countries could take to counter actual developments

If the Soviets alert Western countries to apparent nuclear terrorists in a similarly sensational and self-serving way in the future, they may generate far more damaging false alarms, whether they intend to or not The problem is that in a case of nuclear terrorism, there might be little time to resolve the usual and inevitable uncertainties, let alone any fresh doubts raised by Soviet propaganda

Common understandings between the United States and the Soviet Union on the sharing of information in case of a threat or act of nuclear terrorism would be invaluable in countering the possibility through the deterrence of nuclear-capable states from supporting international terrorists with nuclear means in the first place

Thus, common assessments and cooperative exchanges of information and assistance can improve the world's political and operational readiness for effective action The unique vulnerabilities, capabilities, and responsibilities of the United States confer a premium on its knowledge and leadership in fostering international consensus and cooperation At the same time, the United States has an obligation to protect the sources and methods of its intelligence-gathering against damaging disclosures This obligation includes protecting the identity of cooperative foreign intelligence services whose contributions to U S intelligence are potentially valuable

Finally, nuclear terrorism warrants special recognition by the U S intelligence community as the most damaging possible variant of nuclear proliferation and general terrorism Fortunately, it is probably not too late, despite the long lead time, for investment in the monitoring of nuclear terrorist threats that might emerge in the 1990s

Mobilizing Intelligence against Nuclear Terrorism: A Personal Perspective

Yuval Ne'eman

The acquisition of intelligence is best achieved when the following sequence of logical steps controls the process

1 *Definition of essential information.* This step consists of identifying the most important items of required information and will be closely tied to the issue under consideration, such as a specific event, evolution, or deployment It is also important to determine how much warning time is needed prior to an event's occurring

2 *Identification of indicators* This step involves the determination of observable facts or actions that are indicators of the essential information Sometimes they may be indirect and worth noting but not sufficient in themselves—for example, an interesting characteristic of an envisaged evolution that may be emerging.

3 *Intelligence acquisition program.* This step can be thought of as a matrix in which the columns list the indicators, and the rows list the various means of acquiring information about them

4. *Ongoing review of the basic premises.* Step 1 always involves a set of assumptions Once the process of intelligence acquisition is underway, it is important to check and recheck whether the basic premises still hold or need to be modified on the basis of new intelligence This process should be ongoing. Often, however, it is forgotten, albeit at heavy expense

Here the discussion centers mainly on steps 1 and 2 Much of what would come under step 3 relates to the specific operations of intelligence services and thus cannot be discussed However, some aspects of step 3 are in the public domain

The Essential Information

A basic assumption made here is that the danger we believe we need to defend against (through warning, deterrence, and prevention) is possible actions by terrorists and not possible nuclear sabotage by a nuclear power (including the Soviet Union and China) as part of its own direct covert operations This assumption is plausible in terms of our present thinking, but it should be rechecked periodically in the light of new information

What we are after in this step centers around three main threats [1]

1 The acquisition of a nuclear device by a terrorist organization through procurement, theft, or forcible action
2 The acquisition of nuclear materials by a terrorist organization in order to manufacture a nuclear device
3 Terrorist action against a nuclear reactor or base

The third threat can be part of 1 or 2 if the aim is to obtain a nuclear device or fissile material, but it should also be treated as a separate topic because the aim might be to cause harm by generating nuclear fallout by directing conventional explosives against nuclear materials or devices

The Indicators

The conditions that create the possibility of acquisition of a manufactured nuclear device and that therefore serve as indicators include the availability of nuclear devices in countries in which there are terrorist groups with a sufficient level of organization This condition is true throughout Western Europe and the Mediterranean, Japan, the Republic of Korea, and Okinawa, and for U S or other naval forces, some regions in Latin America, and the Southern Hemisphere

Nuclear devices are generally supplied with mechanisms designed to preclude a nuclear explosion if detonated by unauthorized personnel. However, the nuclear device could still serve as a source of fissile material for manufacturing a new one (threat 2) Even if one weapon did not contain enough fissile material for a more primitive bomb, it must be remembered that bombs often come in clusters

Concerted action by different terrorist organizations is an indicator of the high degree of organization and planning capability needed to realize this threat The assistance rendered by the Japanese Red Army to the Popular Front for the Liberation of Palestine in the attack on Ben Gurion airport in 1969 implied liaison, briefings, supply of intelligence and other resources,

and capabilities on the part of the terrorists The notorious Carlos, a Latin American in the service of the Palestine Liberation Organization (PLO) and working out of Beirut, is another case in point Such collaboration might help resolve various difficulties facing European terrorists preparing to move against a U.S base, given that European terrorist groups have very limited membership—some twenty active participants per organization To mount a serious assault, they would need reinforcements, which could come from Latin America or Japan Reinforcements from Japan or the Middle East also raise the possibility of suicide squad personnel, who could be an important element in such an assault Preparations by European terrorists (such as reconnaissance activities around U S bases) and interregional movements (bringing in key personnel from Latin America, the Middle East, or Japan) are thus possible indicators

Terrorists planning a theft or assault would need precise information on the location and protection of the nuclear device within the base Thus, any internal reconnoitering and attempts to infiltrate personnel on the base could be considered as very high probability indicators Identifying a terrorist, even one posing as a waiter in the base kitchen, should be regarded as a serious warning, considering that the acquisition of a nuclear device could be the most valuable prize and thus the first possible motivation for an infiltration effort, where bombs are available

Vulnerability is maximized during transport and movement, such as the transfer of a base or the replacement of old devices Should a terrorist group be strengthened by reinforcements, theft when the devices are between bases is a serious possibility Evidence of the monitoring of military movements by terrorist groups is another strong indicator and calls for a higher state of readiness

Should the terrrorists succeed in obtaining a nuclear device, they will have to hide it while preparing to use it It is possible that just as these devices are protected against unauthorized detonation, they could be equipped with hidden emitters or responders that would help in locating them In many cases, these devices might hurt the strategic security and capabilities of the weapons by making it easier for the enemy to strike at them in war For tactical weapons, however, this possibility might be less important

Regarding the manufacture of a nuclear device, fissile material is generally less protected than a bomb Vulnerability is greater when the material is on the move—for example, in transit for reprocessing The French ship that sank recently in a Belgian port after being loaded with uranium hexafluoride, which was to be shipped to the Soviet Union for enrichment, proved that vulnerability

Generally, handling fissile material requires radiation protection equipment—for example, hot cells The purchase of that type of equipment is thus an indicator However, Kamikaze-type Japanese or Middle Eastern Shiites

might be persuaded to handle fissile material without personal protection. It should also be noted that manufacturing is a major operation that would be liable to detection The possibility that this stage might be performed in a state sponsoring the terrorists is of greater concern here

Lists of the specific elements needed for the transformation of a quantity of fissile material into a weapon or at least into a static device should be prepared The purchase of any of these items, or perhaps the appearance of several of them in conjunction, could be an indicator Of course, the purchase might have nothing to do with weapons, but it should be possible to check the reasons in each case

Manufacturing requires specialists The recruitment of physicists and chemists by a terrorist organization should be regarded as an important indicator

Fissile material originates in reactors or in isotope separation plants If fast breeders do enter the industry, the danger will be multiplied It should be considered as highly advantageous that as yet nuclear energy, even conventional reactors, has not made any inroads in the Middle East At present, there are no nuclear power stations from Afghanistan to Morocco Considering the volatility of the region and the high level of terrorist activity, Middle Eastern countries should be persuaded to postpone indefinitely any plans they might have for nuclear energy I would be willing to place a moratorium on nuclear energy in Israel as long as the other countries in the region did likewise. At the same time, the introduction of nuclear power in unstable countries should be considered as a prime indicator, creating conditions that might develop into a threat Brazil and Argentina do have nuclear reactors Given the level of regional terrorism in Latin America, a special effort at surveillance is justified

As a consequence of the rising traffic in narcotics, most countries (including those of the Middle East) now have tight border controls These should be strengthened and adapted to deal with the new danger through the erection of well-camouflaged detection devices at all entrance points to a country Such detection devices should be capable of discovering both nuclear fuel and closed nuclear devices There is room for a research and development program, and any equipment that might be developed should be offered to any country wanting to protect itself

Intelligence regarding conventional attacks on nuclear facilities is largely similar to any situation where an essential facility has to be protected In particular, it is important to be on the alert for a major means of attack falling into the hands of terrorists a bomber, an artillery piece, or a mortar that might later be hidden near a facility

Intelligence Acquisition

There is now a greater awareness in the United States of the dangers of terrorism The Task Force on Combatting Terrorism, headed by Vice-Presi-

dent George Bush, has recommended the creation of a "center to routinely analyze intelligence on terrorism." It would consist of a "cadre of experts from various government departments and agencies." Another recommendation is the "enhancement of intelligence exchanges with like-minded foreign governments, with international law enforcement agencies and national police organizations."[2]

Establishing a group with specific responsibility for intelligence on terrorism is a good way to ensure that the subject receives appropriate attention at intelligence agencies. The center should include a unit (perhaps a committee of experts) that focuses specifically on prospective nuclear terrorism.

Once the United States starts to treat the study of terrorism in general and of nuclear terrorism in particular as an important strategic issue, the same will happen in Europe and Japan. Exchanges with friendly intelligence services should cover all these issues, with special care and attention paid to them.

It is conceivable that on the issue of nuclear terrorism, an agreement can be reached with the Soviet Union. Although much international terrorism is boosted by or directed from the Soviet Union, the dangers of nuclear terrorism specifically should be clear to the Russians. An agreement about mutual warnings on these matters should be in the realm of the possible, however, such sharing involves a fine line. The West cannot engage in a general sharing of intelligence on terrorist groups, which are often supported by the Soviet Union. Rather, cooperation is called for when there is a danger of a group's going nuclear.

International organizations reveal ambivalence when it comes to terrorism. The PLO, for example, enjoys observer status at the International Atomic Energy Agency (IAEA). In this case, a terrorist organization is in a position to monitor in detail directly or indirectly through friendly nations every set of precautions the IAEA might initiate or sponsor. States sponsoring terrorism such as Libya or Syria are also actively participating in these types of organizations. Their position might be instrumental in setting up sabotage or theft of materials in conjunction with a terrorist organization. On the other hand, the IAEA could have an extremely useful role to play, provided it is depoliticized. It could monitor movements of every kilogram of fissile material all over the world, notice disappearances, and notify intelligence and police bodies. This role could be particularly important with respect to monitoring the large quantities involved in fuel reprocessing.

Summary

Aside from the search for indicators, I have several auxiliary recommendations.

1 Easy-to-handle, highly sensitive detectors capable of registering the presence of nuclear explosives, even when the packaging is designed to avoid detection, need to be developed

2 Camouflaged attachments to existing nuclear weapons, especially tactical, and to stocks of fissile materials, need to be designed to help trace their movement and location, should they fall into illegal hands

3 In the long run, the organization of an apolitical centralized control system capable of accounting for every kilogram of nuclear fuel throughout the noncommunist world (and hopefully everywhere in the future) needs to be established

4 The spread of nuclear power stations to the more volatile regions of the world needs to be postponed

5 The United States and the Soviet Union should negotiate an agreement to provide mutual warnings on items relating to the potential threats of nuclear terrorism

Notes

1 I focus on action rather than intent, since it is the action that needs to be forestalled Knowledge about intent is academic and it can be assumed that every terrorist organization would like to possess nuclear weapons

2 *Public Report of the Vice President's Task Force on Combatting Terrorism* (Washington, D C U S Government Printing Office, February 1986)

Chapter 6
What International Measures Can Be Taken?

U.S.-Soviet Cooperation in Countering Nuclear Terrorism: The Role of Risk Reduction Centers

Sam Nunn
John W. Warner

We live in a world bristling with nuclear technology, ever growing in complexity and danger In the last decade, there has been a relentless dispersion of the know-how, equipment, and materials necessary to build nuclear devices In addition to the five declared nuclear powers, two more nations—India and Israel—are assumed to be capable of quickly fabricating a weapon By the mid-1990s, perhaps as many as twenty nations will have the industrial capability to build nuclear weapons

We live also in a world of terrorism, ever growing in its influence and virulence The number of terrorist incidents worldwide has steadily risen from 500 in 1983 to 700 in 1984 to an estimated 1,000 in 1985 However, the destructiveness of contemporary terrorism has increased qualitatively in proportion to its quantitative rise Suicidal truck bombers can obliterate entire embassies Car bombs level densely habitated city blocks Previously unknown groups claim credit for destroying crowded, wide-bodied jets in mid-air There seems to be no limit to their madness

Accompanying these trends has been an even more ominous development. the emergence of state-sponsored terrorism. Terrorists are no longer necessarily solitary free agents pursuing individual ends or grievances Increasingly terrorists are supported, directed, or employed by governments that see them as weapons of choice in advancing national interests through means short of declared conventional war With the active support and backing of hostile regimes, terrorists have benefited immeasurably in terms of their weaponry, mobility, logistics, and intelligence resources

Should these alarming trends in terrorism and nuclear proliferation ever converge, the world would clearly face a menace of unprecedented dimensions As devastating as the prospect is, the threat posed by nuclear terrorism

is not limited to the almost unimaginable loss of life and damage that could be inflicted on a single city or area should a nuclear-armed terrorist detonate a device through design or inadvertence Rather, the threat of nuclear terrorism has the potential of plunging much of the world into accidental or unintentional nuclear devastation

Far-fetched? Consider these all too plausible scenarios, outlined in a 1984 RAND Corporation study [1]

Scenario 1. Terrorists attack a U S nuclear weapons storage depot in West Germany and capture a nuclear device The United States suspects that the attack may have been instigated by the Soviet Union or that the terrorists may try to escape with the weapon to East Germany How does the United States determine whether the Soviets played a role in the theft? Assuming the Soviets were not involved, how does the United States enlist Soviet assistance in blocking escape routes across the border? If the nuclear weapon has a short-range launch capability, how does the United States cooperate with the Soviets to ensure that the terrorists do not try to blackmail the Federal Republic of Germany by threatening to destroy its cities from a sanctuary east of the border? Assuming that the terrorists are neofascists intent on derailing West German détente initiatives, how does the United States assure the Soviet Union that the terrorists will not threaten East German cities from launch sites west of the border?

Scenario 2. A radical PLO faction claims to possess a nuclear device, which it threatens to detonate in Israel unless the Israeli government withdraws from East Jerusalem and the West Bank The threat message is accompanied by a diagram of the device and a small amount of highly enriched uranium Israel announces that any detonation will be followed by prompt, massive, and, implicitly, nuclear retaliation against states suspected of supplying the terrorists with the nuclear material and/or know-how (Libya, Iraq, or Syria) The Soviet Union announces that any such attack on one of its regional allies will be responded to in kind Israel reminds the United States of its security commitments Since neither superpower wants to get dragged into a nuclear war, how do they cooperate in determining whether the terrorist threat is real, and, if so, in nullifying the terrorists?

Scenario 3. A nuclear explosion occurs at a nuclear facility in Iraq, with a massive loss of life Iraq blames Israel A new Middle East war seems imminent, raising the specter of a superpower crisis that neither side wants How do the United States and the Soviet Union cooperate in determining what actually caused the detonation and in defusing the crisis? Was the explosion caused by another Israeli aerial bombing of the facility? Was there an accident caused by the Iraqi operators of the facility? Was the facility attacked by Iranian saboteurs? Or was the detonation set off by Arab terrorists confident that Israel would be implicated?

Another nuclear terrorism scenario comprises the plot of a recent best-seller, *The Fifth Horseman.* Radical terrorists, supplied and trained by Libyan leader Muammar Qaddafi, hide a nuclear device in New York City and threaten to detonate it unless the United States forces Israel to withdraw from the occupied territories How might the United States determine if the threat is real? How could the United States enlist Soviet cooperation in persuading Qaddafi to back down? How could the United States ensure that any U S military action against Libya would not escalate into a superpower confrontation?

We believe that scenarios such as these are more than just hypothetically credible We believe the danger of nuclear terrorism is clear and present and as such demands concrete preparations by the United States and the Soviet Union These two countries have an overriding mutual interest in preventing such contingencies from ever unfolding or, failing that, in minimizing the possibility that a nuclear terrorism incident could provoke a nuclear exchange between the two As Vice-President George A Bush said at a colloquium on nonproliferation in Geneva in 1985, "Although we have so far been spared the terrible specter of nuclear terrorism, that doesn't mean that we don't need to begin addressing this problem "[2]

Indeed, it is the specter of nuclear terrorism, more than any other factor, that originally prompted and has subsequently sustained our deep interest in promoting U S.-Soviet agreements on the establishment of U S -Soviet Nuclear Risk Reduction Centers and other important risk reduction measures

Emergence of a Concept

The origins of the Nuclear Risk Reduction Center initiative date back to 1981, when Senator Sam Nunn (D-Ga) wrote the commander of the Strategic Air Command (SAC), General Richard Ellis, and asked SAC, as the premier defense command in nuclear matters, to analyze the potential for an accidental nuclear exchange between the superpowers and to recommend some initiatives for dealing with the problem Ellis, now retired from the air force, is serving as the U S representative on the U S -Soviet Standing Consultative Commission (SCC) and is one of the most thoroughly knowledgeable military men in the area of arms control, as well as an expert in nuclear policies and weapons

Ellis established a group that studied this issue extensively, and their conclusions are as relevant today as they were five years ago The SAC analysis showed that both the United States and the Soviet Union needed to improve dramatically their warning and attack characterization capabilities to deal with the use of a nuclear device by a terrorist or other third party in either peacetime or a crisis Under several possible scenarios, SAC concluded that neither superpower could likely determine the party responsible for such an attack The analysis identified many unconventional methods of nuclear de-

livery other than such normally discussed platforms as fighter planes or missiles that could be utilized by third parties to explode a device on U S or Soviet soil

Joined by our late colleague, Senator Henry Jackson (D –Wash), we responded to Ellis's analysis and recommendations by introducing legislation in 1982 that required the Defense Department to evaluate a number of suggested measures that addressed this and other accidental nuclear war scenarios That legislation resulted in an April 1983 report by Secretary Caspar W Weinberger to the Congress outlining four specific risk reduction measures, all of which were eventually proposed to the Soviet Union

1 Adding a high-speed facsimile capability to the hot line
2. Creating a joint military communications link (JMCL) between the Pentagon and the Soviet military command
3 Installing high-rate data links between the United States and the Soviet Union and their embassies in the capital of the other country
4 Promulgating a multilateral agreement for nations to consult in the event of a nuclear incident involving terrorists

Although the Soviets demonstrated no interest in either the JMCL proposal or the improved embassy data link, agreements were reached with respect to improving the hot line and consultations about nuclear terrorism

In July 1984, the United States and the Soviet Union signed an accord governing the upgrade of the hot line Pursuant to this agreement, a facsimile capability is being added to the hot line that will enable each country to transmit and receive graphic materials In addition, the planned improvements will allow the U S and Soviet heads of government to exchange messages more rapidly than they can with the existing teletype The increase in the speed of communication and the ability to send pictures and maps could be especially critical in future crises, including possible nuclear terrorism incidents This capability has been long overdue

The U S -Soviet direct communication link will now consist of three circuits (two satellite circuits plus one wire telegraph circuit), one earth station in each country for each satellite circuit, and terminals in each country linked to the three circuits and equipped with teletype and facsimile equipment

The 1984 agreement specifies that the U S government will sell the Soviet Union at cost the equipment necessary to install and maintain the improved hot line This transaction will include facsimile equipment, personal computer equipment, modem equipment, and microprocessor systems to ensure the privacy of these sensitive communications Most of this transaction will be completed in the initial sale of the specified equipment to the Soviet Union However, sales of services and additional equipment, including consumable items, will recur periodically over the life of the hot line Congressional

authority for the secretary of defense to execute these sales, on a reimbursable basis with the Soviet Union, was provided by Senate Joint Resolution 108, which we introduced and which both Houses passed in 1985

With respect to consultations concerning nuclear terrorism incidents, discussions with the Soviet Union on this subject bore fruit in June 1985 when the SCC announced that the two nations had concluded the Common Understanding to the Agreement on Measures to Reduce the Risk of Outbreak of Nuclear War between the United States of America and the Union of Soviet Socialist Republics of September 30, 1971 (the so-called Accidents Measures Agreements)

The 1971 Accidents Measures Agreement was a spin-off of the SALT I negotiations It covers three main areas.[3]

1 A pledge by both sides to take measures each considers necessary to maintain and improve its organizational and technical safeguards against accidental or unauthorized use of nuclear weapons
2 Arrangements for immediate notification should a risk of nuclear war arise from such incidents, from detection of unidentified objects on early warning systems, or from any accidental, unauthorized, or other unexplained incident involving a possible detonation of nuclear weapons
3. Advance notification of any planned missile launches beyond the territory of the launching party and in the direction of the other party

The 1971 agreement specifies that the parties shall utilize the hot line "for transmission of urgent information, notifications and requests for information in situations requiring prompt clarification"

Because of Soviet insistence on strict confidentiality, the June 14, 1985, SCC announcement on the new common understanding was extremely circumspect It noted only that the understanding dealt with "the use of immediate notifications in connection with the Agreement on Measures" and "in no way changes or expands the Agreement on Measures, it merely records the parties' understanding of their obligations under it" However, at an international conference later that month, Vice-President Bush revealed that the agreement concerned "measures to combat nuclear terrorism" Administration officials subsequently provided the press with a few details on the new understanding, confirming that it clarified U S and Soviet responsibilities in the case of a nuclear explosion by a "third party," including terrorists The officials indicated that although there was a mutual obligation to consult, there was no advance agreement on joint action

Nuclear Risk Reduction Centers

One important risk reduction measure that has been included in our amendment to the fiscal year 1983 defense authorization act but that was not acted on by the administration was the establishment of Nuclear Risk Reduction

Centers The administration took the position at that time that although these centers might represent a useful long-term goal, it preferred to pursue its own package of proposals before taking on what it regarded as the more ambitious step of negotiating the establishment of the centers

Seeking expert help in fleshing out the center concept and in sharpening our arguments for proceeding with formal negotiations with the Soviet Union on this idea, we formed a working group in 1983 whose members included such experts in national security as former Secretary of Defense James R Schlesinger, former CIA Deputy Director Admiral Bobby Inman, Lieutenant General Brent Scowcroft (USAF-Ret), General Richard Ellis, former Under Secretary of Defense William Perry, *Foreign Affairs* editor William Hyland, Georgetown University senior fellow Barry Blechman, and RAND Corporation president Donald Rice

In its report, released in November 1983, the Nunn-Warner Working Group on Nuclear Risk Reduction noted a "rising danger of nuclear terrorism " Although the group conceded that the specific risk in any one year of a terrorist group's acquiring a nuclear device was "no doubt a low probability," it stated that the "cumulative risk covering all such groups over ten or twenty years may be very great indeed " In its view, this sobering assessment underscored the "necessity of the two great powers initiating discussions aimed at establishing an explicit and comprehensive system for the prevention and containment of nuclear crises "

The group applauded President Ronald Reagan for proposing the four risk reduction measures that grew out of our 1982 legislation, however, it disagreed with the administration's decision not to embrace the Nuclear Risk Reduction Center concept, saying that there are "crucial political aspects" to preventing crises that can be addressed only through the "designation of particular representatives and facilities in both nations that would be assigned specific responsibilities for preventing a nuclear crisis "

In February 1984, we introduced Senate Resolution 329, which incorporated the recommendations of the working group and urged the president to propose the establishment of the centers The legislation identified five possible functions for the centers, three of which related directly to nuclear terrorism

1 Discussing procedures to be followed in the event of possible incidents involving the use of nuclear weapons by third parties
2 Maintaining close contact during nuclear threats or incidents precipitated by third parties
3 Exchanging information on a voluntary basis concerning events that might lead to the acquisition of nuclear weapons, materials, or equipment by subnational groups

4 Exchanging information about U S -Soviet military activities that might be misunderstood by the other party during periods of mounting tensions

5 Establishing a dialogue about nuclear doctrines, forces, and activities

In June 1984, the Senate voted 82-0 to approve an amendment to the FY 1985 defense authorization bill paralleling the language of Senate Resolution 329 This provision was subsequently approved in conference with the House and enacted into law (P L 98-525, Sec 1108)

Negotiations with the Administration

Despite the overwhelming show of congressional support for the risk reduction center concept, the administration did not focus on the proposal in any depth until spring 1985 At that time, a number of factors—including the Soviet Union's return to the Geneva negotiating table, a moderation in the administration's pronouncements on U S -Soviet relations, and the increasing prospect of a Reagan-Gorbachev summit—created a more favorable climate for careful consideration of our 1984 legislation

At a meeting we hosted in March 1985 attended by members of the Nunn-Warner Working Group and key administration officials in the risk reduction area, we outlined a specific concept for the organization and operation of the centers Our presentation included a number of optional functions for the centers that we believed warranted consideration By discussing specific options with the administration, we hoped to identify areas where common ground existed between us and thereby to overcome the administration's past coolness to this concept A central premise of our approach was that it would be best to suggest some rather modest tasks that the centers could be assigned in their initial phase of operations, recognizing that a more ambitious set of responsibilities would have to evolve over time as the centers demonstrated their worth

The concept we presented built on the 1971 Accidents Measures Agreement, the 1963, 1971, and 1974 hot line accords, and the provisions of the Antiballistic Missile Treaty dealing with the responsibilities of the SCC This approach reflected our sense that the Soviets would be more likely to respond favorably to the Nuclear Risk Reduction Center concept if it were presented in the context of an incremental expansion of existing agreements rather than as a new proposal

Under our concept, the centers would be separate facilities in Moscow and Washington, linked by modern communications equipment, they would keep a twenty-four-hour watch on events that could lead to nuclear incidents The U S center would be directed by an ambassador-level official who would report directly to the National Security Council throught the president's national security adviser The permanent staff would include diplomatic,

military, and intelligence personnel We left open the question of whether each center would be jointly staffed by U S and Soviet personnel

At the March meeting, we outlined five options for the functions to be assigned the centers The first involved a function that has traditionally been associated with the risk reduction center concept that of serving as the primary point of contact for the exchange of all military information required under U S -Soviet agreements (for example, about accidental detonations of nuclear weapons and advance notification of intercontinental ballistic missile test flights) This option corresponded to the function cited in our 1984 legislation concerning the exchange of information about military activities that otherwise might be misunderstood during periods of mounting tensions

The second option was to have the SCC meet on a rotating basis at the Washington and Moscow centers The agreements establishing the SCC do not require that the body meet only in Geneva By associating the risk reducion center concept with the SCC (whose charter specifically assigns it responsibility for the implementation of the 1971 Accident Measures Agreement), we hoped to promote two goals an expansion and revitalization of the role of the SCC and the incorporation of the center concept within the existing framework of the Accidents Measures Agreement

Option 3 related to the ongoing bilateral discussions regarding nonproliferation between the United States and the Soviet Union We suggested that these semiannual discussions led on the U S side by Ambassador Richard Kennedy, be held at the centers If progress so warranted, we also suggested that the two delegations might authorize the establishment of a standing working group on nuclear terrorism that could conduct discussions at the centers more frequently This option corresponded to another of the functions cited in our 1984 legislation the exchange of information concerning events that might lead to the acquisition of nuclear weapons by terrorists

The fourth option was drawn from a proposal by President Reagan in his September 1984 UN speech regular, institutionalized ministerial or cabinet-level meetings between the two countries The president suggested that these meetings, which we proposed be held in the centers, could include the exchange of five-year military plans We also proposed that such meetings discuss the procedures to be followed by both nations in the event of nuclear terrorism incidents

The last option also related to a proposal that President Reagan had endorsed, although it had been put forward by many others, including a former chairman of the Joint Chiefs of Staff, General John W Vessey, as well as Senators Carl M Levin and Sam Nunn, and fifty-three other senators in a letter to the president in 1983 regular, high-level meetings between U S and Soviet military officials These meetings could promote a dialogue on nuclear doctrines, forces, and activities, as recommended in our 1984 legislation We

indicated that we thought the centers would be an ideal facility for these exchanges

The March meeting was followed by five months of intensive consultations with the administration, during which the participating agencies reached a firm consensus on what was, and was not, viable from their perspective In many instances, the administration accepted key elements in our proposal In the course of our discussions, however, four strongly felt administration concerns became evident

First, to avoid compromising security, the administration was adamant that the centers should not be jointly staffed by U S and Soviet teams Second, doubts about the value and effectiveness of the SCC were so pronounced in some quarters of the administration that any role for this body in the centers was effectively vetoed Third, the agencies were extremely leery of giving the centers any specific responsibility for joint U S -Soviet planning for nuclear terrorism incidents Notifications and consultations were endorsed, but joint contingency planning was ruled out

Last, the administration felt strongly that the principal role of the centers should be crisis prevention, not crisis management Were the superpowers to find themselves in a dangerous confrontation, the administration insisted that existing mechanisms, including the hot line and the crisis control team headed by the Vice-President, would come into play Thus, the administration stressed that the mandate for the centers should be to help prevent a crisis from occurring by relaying information and facilitating discussions intended to reduce the risk that a tragic misunderstanding ould precipitate a crisis In this context, however, the centers could perform a vital role by ensuring that the United States and the Soviet Union would be making decisions based on an identical data base in Washington and Moscow

Outcome of the Negotiations

We concurred with some of these reservations On others, we disagreed, suspending for the time being any further efforts to resolve conflicting perspectives Within this framework, we were able to reach final agreement with the administration on a specific concept for the initial establishment and functioning of the centers At an August 26 meeting at the White House with Robert McFarlane, the president's national security adviser, we agreed that the centers initially should be structured along the following lines

> They would be established in Washington and Moscow and maintain a twenty-four-hour watch on any events with the potential to lead to nuclear incidents
>
> They would be linked by communications equipment equivalent to that accepted in the 1984 hot line upgrade agreement

The U S center would be manned by U S diplomatic and military personnel, and vice-versa Designated liaison officers from each embassy would be given access to the other party's center under controlled escort on a periodic basis

The centers would serve as communications links for all required military and arms control notifications They would also function as a meeting place for ministerial-level visits and other diplomatic discussions relating to risk reduction and confidence-building measures and as a meeting place for Incidents at Sea sessions, high-level military exchanges, National War College exchanges, and other discussions designed to promote a dialogue on nuclear doctrines, forces, and activities

Joint annual reviews of the functioning of the centers would be conducted at the centers This approach has proved especially helpful in maintaining the effectiveness of the Incidents at Sea agreement, signed on behalf of the U S Navy in 1972 by Senator Warner, who in his capacity as secretary of the navy headed the U S delegation during the two years of rigorous negotiations

In our discussions with McFarlane, we made it clear that we continued to believe (and would state so publicly) that, as our experience in operating the centers grew, we envisioned expanding their role into more ambitious areas, including joint planning for responses to incidents involving the use or threatened use of nuclear weapons by terrorists or other unauthorized parties Other evolutionary refinements might include joint staffing of each center and upgraded communications, such as teleconferencing systems

Negotiations with the Soviet Union

At a meeting with General Secretary Mikhail Gorbachev at the Kremlin on September 3, 1985, we had the occasion to present our concept for the centers directly to the Soviet leader We were in Moscow as part of a delegation led by Senators Robert Byrd (D–W Va) and Strom Thurmond (R – S.C) At the meeting, we handed Gorbachev a set of materials that explained the background of this initiative and summarized the points of agreement we had reached with the administration with respect to the initial organization and functioning of the centers We also outlined our view of the expanded roles the centers might take on in time Gorbachev responded positively, stating that the proposal "demanded attention " During our visit to Moscow, we also had an opportunity to discuss the risk reduction center concept with top Soviet Ministry of Defense officials

Building on this foundation, the United States was able to raise the risk reduction center issue at the November 1985 summit without having to start

from scratch in explaining the concept to Gorbachev During the summit discussions, the Soviets took a somewhat reserved stance, indicating interest but emphasizing that it was a U S initiative (perhaps in the hope of getting us to give up something to gain their assent)

The summit discussion focused more on the question of where the center question should be negotiated than on how the centers would operate The Soviet delegation indicated a strong preference for using the Nuclear and Space Arms Talks (NST) in Geneva as the negotiating forum The U S delegation, however, feared having the risk reduction center proposal linked, and thus possibly held hostage, to resolution in the NST negotiations of such difficult issues as the Strategic Defense Initiative (SDI) and offensive arms reductions Instead, it advocated independent negotiating teams

The two sides reconciled their conflicting points of view by adopting a deliberately vague sentence in the U S -Soviet summit communiqué "The two sides agreed to study the question at the expert level of centers to reduce nuclear risk taking into account the issues and developments in the Geneva negotiations" The United States took satisfaction from the words "at the expert level," a diplomatic phraseology normally used to denote separate teams. The Soviets stressed the words "taking into account," which suggested at least an indirect linkage to the NST negotiations

Notwithstanding this procedural dispute, it is important to emphasize that the two nations did agree in principle to begin negotiating the establishment of the centers As President Reagan said in his postsummit address to a joint session of Congress "We agreed to begin work on risk reduction centers"

Future of the Centers

The immediate task is to resolve the issue of the negotiating forum Here it is worth asking what the implications would be of acceding to the Soviet position that the center question be addressed in Geneva

First, there are precedents for establishing a risk reduction working group as a formal part of the NST negotiations In the original START negotiations, the two sides discussed confidence-building measures (CBMs) in a special subgroup prior to the Soviet walk-out in 1983 This approach was also successfully employed in SALT I to produce the 1971 Accidents Measures Agreement

The principal U S concern is that the centers could be held hostage not only to U S concessions on such major negotiating issues as SDI but, more narrowly, to selective Soviet goals in the CBM area, such as a ban on close approaches to either side's territory by aircraft carriers of the other side On the other hand, using the Geneva talks would at least ensure that the Soviet

team negotiating the centers include political as well as military representatives One source of U S frustration during the 1983–1984 talks on the hot line upgrade was that the Soviets restricted their negotiating delegation to technical-level personnel, a move that blunted efforts by the United States to use the talks to promote a broader political dialogue about risk reduction

The main advantage of using the alternative approach of negotiating teams is that the centers would be isolated from the vicissitudes of the Geneva talks, at least directly It is important to recall that the hot line upgrade negotiations were carried to a successful conclusion after the Soviets walked out of the INF (Intermediate-Range Nuclear Forces) and START negotiations

If the United States can persuade the Soviets to appoint a full range of political, military, and technical specialists to their team, the main hurdle the United States would have to overcome would be the delicate bureaucratic question of who to put in charge of the U S delegation There are compelling arguments for putting the U S center under National Security Council (NSC) auspices rather than assigning this responsibility to the Pentagon or State Department If a Pentagon or State Department official were put in charge of negotiations, it could prejudice the decision as to where the center is located. Moreover, we are particularly skeptical that the Soviets would continue to show interest in this concept if it appeared to them that the centers were an initiative of the Pentagon The more the centers are associated with the Defense Department, the greater will be Soviet suspicions that the centers are seen by the United States essentially as an intelligence-gathering device Since the Defense Department would probably contest putting the State Department in charge of negotiations, we believe the talks should be run out of the NSC, with appropriate Defense, State, and CIA personnel detailed to the delegation

Conclusion

Strategic arms control efforts have for some time concentrated almost exclusively on the number of launchers and warheads each side has and the possibility of a premeditated strategic strike With few exceptions, arms control negotiations in recent years have tended to focus on ways to reduce the size or alter the characteristics of U S and Soviet nuclear arsenals In short, nuclear arms control negotiations have been attempting primarily to reduce the risk of nuclear war indirectly by concentrating on the capabilities of the two superpowers to wage one

We earnestly hope that the Geneva negotiations will be crowned with success and that the two sides can indeed cut their respective offensive arsenals by 50 percent But even if these talks succeed, there will still be far more than enough nuclear weapons to destroy both countries This realization

places an extraordinary premium on thinking seriously about catalysts more likely to lead to a nuclear war than the prospect of a premeditated first strike As Ambassador James Goodby has perceptively observed "Arms control experts have tended to think of risk reduction as not central to present-day security needs, and therefore not worthy of the intense interest and the lobbying efforts given to those more traditional negotiations, particular nuclear arms reduction This is a mistaken attitude"

Preventing nuclear terrorism should be high on the agenda of U S -Soviet relations In this regard, Nuclear Risk Reduction Centers can play an invaluable role in facilitating discussions aimed at forestalling possible contingencies and in providing a mechanism for dampening escalatory dangers that might otherwise result from any future nuclear terrorism incident In addition to these crucial substantive functions, the centers could serve to reassure anxious publics that the governments they have entrusted with command authority over tens of thousands of nuclear devices are giving the highest priority to reducing the risk that any of them will ever be used, whether by design or by accident

Nuclear Risk Reduction Centers are an idea whose time has come The challenge confronting the United States and the Soviet Union is to transcend the deep-rooted differences and competing interests that complicate so many aspects of their relationship and to act decisively in this area where their common interests are so clearly manifest

Notes

1 "Improving the Means for Intergovernmental Communications in Crisis" (Santa Monica RAND, Report R-3157-FF June 1984)

2 Transcript of Vice-President Bush's remarks to the Groupe de Bellerive colloquium on nuclear proliferation, June 29, 1985

3 U S Arms Control and Disarmament Agency, *Arms Control and Disarmament Agreements, 1982 Edition* (New Brunswick, N J Transaction Books, 1984)

The Nuclear Emergency Search Team

Mahlon E. Gates

Need for Remote, Mobile Radiation Detection

In the early days of the Manhattan Project, there was a need to be able to detect radiation so as to protect workers from exposure to nuclear radiation, and a number of detection devices were developed For the most part, they were hand-held units for examining workers' hands and feet or for searching limited local areas Some were affixed to doors and walls within the manufacturing plants where radioactive materials were being processed Subsequently, radiation detection instruments were used abundantly in the program to develop and test nuclear weapons.

Two events occurred that caused the national weapons laboratories and selected contractors to develop radiation detection instruments for mounting on moving and air vehicles the aircraft-weapons accidents in Palomares, Spain, January 17, 1966, and Thule, Greenland, January 21, 1968 At the time, it was perceived that the principal application of the new detection capability would be to define the extent of the radioactivity dispersed by accidents involving moving vehicles (aircraft or trucks) transporting nuclear weapons This purpose was to be accomplished by patroling the accident site with instruments mounted on aircraft or land vehicles That instrumentation was available in the early 1970s

A third event precipitated the establishment of the Nuclear Emergency Search Team (NEST) In May 1974, the FBI alerted the Atomic Energy Commission (AEC) to a reported terrorist threat in Boston The assistant general manager of the AEC for military application directed the manager of the Nevada Operations Office (NV) of the AEC to assemble appropriate personnel and instrumentation from the national laboratories and to transfer them to Boston via Rome, New York [1] Their purpose was to conduct a search for an alleged improvised nuclear device (IND)

At the time, the NV actually received a number of calls from Washington, D C , from several different sources Frequently the instructions given by one party were nearly the opposite of those given by another Amid this confusion, a group consisting of personnel with instrumentation from the Los Alamos and Livermore National laboratories and from the EG&G Company in Las Vegas, all under leadership of an official from the NV, was dispatched via commercial airline to Rome Air Force Base It took the group twelve to fifteen hours to assemble and travel to Boston Once there, the group was advised that the threat was a hoax and was instructed to return to Las Vegas

Birth of NEST

Based on the problems that emerged in dealing with the Boston incident (such as the conflicting instructions and the time required to pull a team together), late in 1974, the NV manager requested that the assistant general manager for military application assign him the mission, with appropriate authority, to organize a team of experts under his control to carry out future operations involving the search, identification, and rendering safe of any nuclear or radiation dispersal devices involved in a terrorist threat NEST was born early in 1975, initially with no publicity A nucleus for NEST-related activity was established within EG&G, which was assigned responsibility for overall development of the NEST logistics capability, including communications and technical support Specific volunteer personnel were identified at the three weapons laboratories (Los Alamos, Livermore, and Sandia), and an R&D program was instituted for the further development of NEST equipment Arrangements were made with the Military Airlift Command of the U S Air Force to transport the NEST team from Las Vegas to wherever deployment might be directed Training of the team and affiliated agencies became an important consideration

Presidential Authority for NEST

The establishment of NEST was acknowledged and authorized by executive order (EO) 11490 (amended by EO 11953), which assigned the AEC and succeeding agencies up to the current Department of Energy (DOE) the following emergency preparedness functions

Security of special nuclear material, fissionable material, nuclear weapons, or nuclear devices in the agency's custody

Coordination of search and recovery operations for nuclear materials, weapons, or devices

Assistance in the identification and deactivation of an IND

Provision of scientific and technical advice on radiation problems in the event of the detonation of an IND

Responsibility for the following tasks was given to the principal operating official of NEST, the NV manager deployment plans and procedures, on-scene command of the operation, logistic and communication support base, and scientific and technical support to agency headquarters, the Department of Defense, and other relevant groups These responsibilities are now under the ultimate authority of DOE

Modus Operandi and Responsibilities

A threat message, oral or written, normally flows through police channels to FBI headquarters in Washington, D C , where, in concert with the DOE and affiliated laboratories and contractors, the message is evaluated as to validity This is known as the threat assessment phase [2] If the evaluation is positive, the NEST team is deployed on instructions from the DOE

A NEST operation involves several phases after the team has arrived on-site

1 *Search* Conducted, as appropriate, with fixed or rotary wing aircraft, unmarked vans, or personnel on foot seeking an unknown source of ionizing radiation

2 *Identification* Identifying the source of radiation, the outcome of a positive search

3 *Access* The ability to approach the object (IND) emitting the radiation This task might require the neutralization of booby traps or other devices that delay the team's approach to the IND

4 *Diagnostics* Determining the make-up of the IND, its component parts, the fissionable material contained in it, and the means to render it safe

5 *Render safe* Measures taken to preclude or limit the severity of a nuclear explosion

6 *Damage mitigation* Measures taken to minimize the damage and contamination should there be an explosion

7 *Clean-up* Action taken to clean up the debris if the IND detonates

In addition to the DOE, both the FBI and the U S Army Explosive Ordnance Disposal (EOD) teams have certain responsibilities during a NEST operation The FBI is to investigate threats or misuse of special nuclear material, provide for public health and safety, and handle public information

The army's EOD teams are to provide access for diagnostics and perform the render safe It is likely that the Federal Emergency Management Agency (FEMA) has also been assigned responsibilities during a NEST operation

The First Training Exercise

To test the ability of the team to conduct a search for a radioactive device in a public place and to do so surreptitiously so as to avoid public awareness and undue anxiety, as well as to test the detection capability of the team's newly devised equipment, which is housed inconspicuously in standard-looking briefcases, a field training exercise was held in the San Francisco International Airport in the summer of 1975 Three radioactive sources were hidden in luggage lockers at dispersed locations All were found within three hours, and the exercise was considered successful in accomplishing the objectives

Strengthening NEST's Capability

In November 1975, the NEST team was deployed from Las Vegas and from the laboratories to Los Angeles in response to an FBI request for assistance in locating a possible IND allegedly placed in one of Union Oil Company's facilities in Los Angeles The threat message, evaluated as positive, stated that a 20 kiloton device would be detonated unless a large sum of money (I believe it was $14 million) was placed at a specified location The team spent over forty-eight hours searching all possible locations, including refinery areas, storage tanks, shore-to-ship oil transfer locations, a large office building, and the home of Union Oil's chairman, but to no avail Subsequently the FBI arrested the perpetrator of the threat, who was tried and sentenced to six months in jail, the only such case to date

In June 1976, a month before the celebration in Washington, D C , of the bicentennial anniversary of the United States, concern arose over the possibility of terrorist activity during the celebration One response was the establishment of a limited capability for conducting NEST-type operations at Andrews Air Force Base, Maryland In December 1976, a decision was made to maintain NEST EAST on a permanent basis as a hedge against the time required for deployment of a full NEST team from Nevada (and the three weapons laboratories) in response to a terrorist threat in the eastern United States Although NEST EAST had only a limited radiation detection capability, it was considered to be a valuable asset, since it could effect a rapid response in the East while awaiting the full strength of NEST from the West

The Threat in Spokane, Washington

Almost one year after the threat against Union Oil Company, in late November 1976, the second principal nuclear terrorist threat arose in Spokane, Washington [3] This threat, as in the case of Union Oil, turned out to be a hoax, although this time a radiation dispersal device rather than an IND was cited in the threat message

Between 1977 and 1982, large sums of money were expended to upgrade the sophistication, sensitivity, and/or miniaturization of NEST radiation detection, communication, transport, and logistics support equipment and instrumentation The two major incidents for NEST had been hoaxes, no IND had ever been found Consequently, only phases 1 and 2 of NEST's operations (threat assessment and search) had ever been practiced [4] To make up for this lack of experience for the personnel involved in identification, access, and diagnostics, three additional training exercises were carried out using mock nuclear devices at Idaho Falls in 1977, at White Sands, New Mexico, in 1979, and at Los Angeles, with its police department, in 1981 A major command post exercise involving most of the cabinet agencies was conducted in Washington, D C , in 1982 The NEST group has also provided considerable training for FBI agents and members of the EOD teams and other elements of the Department of Defense

As more became known about the threat of nuclear terrorism, the need for extensive intelligence gathering to assist in responding to a threat became evident To that end, the then Energy and Research Administration (ERDA) entered into negotiations with the FBI and the CIA that resulted in agreements concerning cooperation in the intelligence arena for both domestic and foreign situations

General Assessment of NEST Capability

NEST provides the United States with a valuable asset in containing nuclear terrorism through its ability to respond rapidly to threats and to discover devices There are, however, limitations to NEST's capability to find hidden and well-shielded sources of radiation For example, if an improvised nuclear device were hidden in a large metropolitan city such as New York or Chicago, with no further information on its location, it would be next to impossible for NEST to find it within a limited period If the IND were known to be in a specific area—say, vicinity of Times Square—the probability of its being discovered increases considerably

One of the stumbling blocks to a total discovery capability is the existence of background radiation, which exists to some degree nearly everywhere Thus, one goal of the R&D in radiation detection technology is to increase

the sensitivity of NEST equipment and thus overcome that problem In addition, the NEST research group inaugurated a program some years ago to establish the levels of background radiation in several U S cities and federal buildings This information is maintained in NEST's data base

Suggestions for Consideration by the Task Force

The task force should consider several points First, is the current NEST configuration (with teams in Las Vegas and Andrews Air Force Base) sufficient? Should consideration be given to additional NEST organizations in other geographic locations in the United States, Europe, or the Pacific Ocean area? Second, is it feasible to establish a NEST team(s) on an international basis? Third, is there a mechanism other than NEST for searching for and identifying lost or stolen weapons, nuclear materials, or INDs? Finally, can the responsibilities of the International Atomic Energy Agency be augmented and complemented with authority to impose fines or sanctions when inspections disclose lax security?

Notes

1 The Nevada Operations Office manages the underground nuclear testing program at the Nevada test site and is intimately associated with the three national weapons laboratories and with technical contractors involved in nuclear testing activities

2 In actual practice, the FBI would no doubt immediately evaluate the message as to credibility, and the NEST team would be placed on alert Between 1974 and 1980, a great number of threat messages were received, of which only eighty (approximately) were determined to be credible, of these, only two were given a positive assessment that resulted in the deployment of NEST

3 At least, during the period July 1972 through December 1982 when I was manager of NV

4 A major portion of the NEST team was deployed to the Northwest Territory to assist Canadian Forces in searching for the fallen Soviet satellite in January 1978 (Operation Morning Light) This effort provided the team with an incomparable training exercise from both the scientific and logistics aspects of its mission

Civil Liberties and Nuclear Terrorism

Steven Goldberg

This study would not be necessary if we were willing to fight terrorism at all costs. We do not, however, live in that type of society. Indeed, as the President's Commission on Law Enforcement wrote in 1967,

> What most significantly distinguishes the system of one country from that of another is the extent and the form of the protections it offers individuals in the process of determining guilt and imposing punishment. Our system of justice deliberately sacrifices much in efficiency and even in effectiveness in order to preserve local autonomy and to protect the individual.[1]

The importance of preventing nuclear terrorism is so great that it is easy to believe that the usual concern with civil liberties must take a back seat. But it is precisely when emergencies are invoked that we must not forget the importance of freedoms. Emergency powers are easily abused, and, even in the absence of abuse, mistakes can be made. It is hard to understand why we care about civil liberties if every suspect is guilty, every wiretap is necessary, and every search is justified. But sometimes suspects are innocent, wiretaps are used for political ends, and searches disrupt lives to no end.

Civil liberties do not exist in a vacuum. If society is destroyed, civil liberties are likely to be destroyed as well. Virtually every legal doctrine this study addresses involves a recognition that individual rights must be balanced against valid social needs.

The civil liberties I focus on here fall under the general headings of freedom of speech and association, privacy, due process rights for suspects, and freedom from unreasonable searches and seizures. One essential point applies to all these areas: although a counterterrorist activity is legal, that does not mean the activity has no impact on civil liberties. It may be legal, for example, to have a massive federal police force that provides hundreds of guards for every shipment of plutonium. Even so, that procedure still raises

civil liberties concerns, since many Americans would feel less free in a society of that type

Thus, although I consider whether a particular counterterrorist activity is valid under current law, I do not stop there I consider as well whether a valid activity may nonetheless have important costs for civil liberties One of those costs may be that in the context of a terrorist emergency, the courts will uphold peremptory government actions and thus create a dangerous precedent that could be used in less drastic situations in the future As Justice Robert H Jackson wrote in his opinion dissenting from the exclusion of Japanese-Americans from the West coast during World War II

> Once a judicial opinion rationalizes such [an illegal military] order to show that it conforms to the Constitution, or rather rationalizes the Constitution to show that the Constitution sanctions such an order, the Court for all time has validated the principle The principle then lies about like a loaded weapon ready for the hand of any authority that can bring forward a plausible claim of an urgent need (*Korematsu* v *United States*, 323 U S 242, 246 [Jackson, J , dissenting])

None of these thoughts are meant to suggest that civil liberties must prevail over all other concerns Rather, the point is that we cannot escape hard choices by simple reference to whether a procedure is legal Those who fight terrorism have an important responsibility to weigh carefully the civil liberties implications of what they do

Intelligence Gathering

Gathering information on those who might engage in nuclear terrorism raises several civil liberties concerns The existence of government surveillance programs discourages some people from engaging in legal political activity since they fear that, despite their innocence of wrongdoing, information might still be gathered and misused Moreover, all those subject to surveillance suffer a diminution of privacy Because different legal doctrines govern the various types of intelligence gathering, I look in turn at infiltration, wiretapping, and the maintenance of centralized computer files Finally, I look at whether the Freedom of Information Act undercuts the government's ability to gather intelligence

Infiltration

The use of informers to infiltrate suspected terrorist groups is a well-established method of intelligence gathering The Supreme Court has often upheld the use of informers Indeed, the Court has held that no warrant is necessary prior to an informer's beginning work, since, in the Court's view, individuals

have no justifiable expectation that the person to whom they are speaking will not repeat what they have said (*Hoffa* v *United States,* 385 U S 293 [1966]) Moreover, the Court, using the same theory, has allowed informants, without warrants, to carry concealed electronic devices to monitor what the suspect is saying (*United States* v *White,* 401 U S 745 [1971])

The use of informers is a classic example where the legality of a procedure does not mean it is uncontroversial When plutonium recycling was under consideration by the Nuclear Regulatory Commission, several legal authorities regarded the possibility of increased surveillance of citizens as a major threat to civil liberties [2] Critics of nuclear energy in Great Britain have similarly stressed the danger of spying on one's fellow citizens that they believe such energy use entails [3] The source of these concerns is not hard to understand Someone who believes the government is always watching him or her will find that the surveillance inhibits freedom of speech and association, as well as a sense of privacy It is imperative, even in fighting terrorism, that infiltration be undertaken only when necessary and that the information obtained be used only for proper law enforcement purposes

Wiretapping

When the government wiretaps telephones, there is somewhat greater judicial protection, although executive self-restraint is vital When the government sought to use warrantless wiretaps to gather information on domestic organizations said to be seeking to subvert it, the Supreme Court found the practice unconstitutional (*United States* v *United States District Court,* 407 U.S 297 [1972]) The Court rejected giving an exception to the warrant requirement of the Fourth Amendment on national security grounds in this case However, the Court left open the possibility that warrantless wiretaps on national security grounds could be upheld in cases involving foreign powers The matter remained uncertain until passage of the Foreign Intelligence Surveillance Act of 1978 (50 U S C 1801–1811) Although the Supreme Court has not yet ruled on the matter, the lower federal courts have upheld the constitutionality of this act (See, e g , *United States* v *Duggan,* 743 F 2d 59 [2d Cir , 1984] and *United States* v *Falvey,* 540 F. Supp 1306 [E D N Y , 1982])

Under the Foreign Intelligence Surveillance Act, warrants are generally required but under somewhat relaxed standards Although generally warrants are issued when there is probable cause to believe that a crime has been or is about to be committed, it is possible under the act to get a warrant on a showing of probable cause to believe that the target of the electronic surveillance is an agent of a foreign power (50 U S C 1805[a][3][A]) A foreign power can include a "group engaged in international terrorism or activities in preparation therefor [*sic*]" (50 U S C 1801[a][4]). Among other things, the

act creates a special federal court to hear warrant requests and makes provisions for warrantless wiretaps in emergencies (See, generally, *United States* v *Falvey*)

The Foreign Intelligence Surveillance Act, because it generally requires warrants, may provide more protection for individuals than the Fourth Amendment to the Constitution requires since it is possible that the Supreme Court would have upheld warrantless searches in the context of foreign threats to national security (See, for example, *United States* v *Duggan.*) This is a case, therefore, where Congress has balanced civil liberties concerns against terrorist threats, and the courts have approved Obtaining a warrant from a judge is not foolproof protection, but it has gone a long way toward allaying fears about wiretapping, and it does not appear to have hindered government surveillance Of course, the warrant requirement does not afford complete protection, since the government could still conduct a warrantless and illegal wiretap, and the only likely sanction is that any information obtained from the wiretap, directly or indirectly, could not be used in a later prosecution However, given the civil liberties costs of unsupervised wiretapping, the executive should resist any temptation to evade the limited restrictions of the Foreign Intelligence Surveillance Act

Centralized Computer Files

Once intelligence is gathered, it is typically organized into large computer files so that it can be cross-referenced and easily accessed These files pose a civil liberties concern in that unauthorized access to them could subject individuals to a loss of privacy, as well as job sanctions and the like The Supreme Court has recognized that the constitutional right to privacy may require that computerized files be kept private and that they be used only for proper purposes In the case of *Whalen* v *Roe* (429 U S 589 [1977]), which concerned a New York State computer file of records about drug prescriptions, the Court held that the right to assemble computer files for public purposes, including enforcement of the criminal laws, is "typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures " The Court went on to say that "duty arguably has its roots in the Constitution" (429 U S at 605) In *Whalen* itself, the Court found that New York had provided adequate statutory protection and upheld its record-gathering system Under that system, the computer files were kept in secure rooms, and when the computer was in use to look at secure files, it was run off-line (that is, no terminal outside the computer room could gain access to the information)

Here is a case where civil liberties concerns and the effort to fight terrorism point in the same direction Ensuring that the information in computer

files is accurate and up to date and ensuring that it is available to no one without proper authorization both protects civil rights and helps fight terrorism

Freedom of Information Act

The final aspect of intelligence gathering that raises civil liberties concerns is the relationship of the federal Freedom of Information Act (FOIA) (5 U S C 552), to efforts to fight terrorism That act enables individuals to obtain certain federal government documents (There are comparable state statutes concerning access to state government documents in virtually every jurisdiction) The FOIA reflects a concern for open government and thus, in part, the desire of civil libertarians and others to control government abuse However, the FOIA has been identified by some as a hindrance in the fight against terrorism For example, at a 1978 Department of State conference, some foreign participants argued that concern over the possible release of information through the FOIA made them nervous about sharing sensitive intelligence information [4]

The FOIA is a statute, not part of the Constitution, and thus could be changed relatively easily if there were a broad societal consensus that it was hampering efforts against nuclear terrorism Recent developments in FOIA law make such changes unnecessary, however First, the FOIA has always exempted properly classified material from disclosure In addition, the FOIA exempts from disclosure information "specifically exempted from disclosure by [another] statute" (5 U S C 552[b][3][A]) In 1985, the Supreme Court held that the National Security Act of 1947 was another such statute In particular, the Court held that because of the 1947 enactment, FOIA requests that would reveal Central Intelligence Agency intelligence sources could be turned down (*Central Intelligence Agency* v *Sims,* 105 S Ct 1881 [1985]) In addition, Congress recently enacted the Central Intelligence Agency Information Act, Public Law 98-477 (98 Stat 2209 [1984]), which exempts the CIA's operational files from the FOIA As a consequence, any broad attack on the FOIA would be unnecessary and misguided

Open government is an important value in a democracy and one that must be weighed carefully against allegations of national security concerns There is understandable suspicion, particularly since Watergate, that secrecy in government may be designed not to further national security but for personal or political gain

Background Checks and Terms of Employment

One way to combat nuclear terrorism is to attempt to ensure that potential terrorists do not have access to strategic nuclear materials through their jobs Thus, the screening of potential and current employees in sensitive jobs to

see if they pose a security risk is a common feature of antiterrorist programs The civil liberties problem arises because an individual could be denied employment for activities that pose no real threat to security but rather represent the exercise of the basic rights of free speech and association

The first legal check on the misuse of screening programs was imposed by the courts, which insisted that such programs not be undertaken unless explicitly authorized by Congress In a leading case, *Schneider* v *Smith* (390 U S 17 [1968]), the Supreme Court held that the U S Coast Guard could not deny employment on merchant vessels for security reasons because it lacked the statutory authority The Court emphasized that it was insisting on this explicit authority because of the First Amendment speech and association rights involved

Partly in response to *Schneider,* the Atomic Energy Act was amended to give authority to the AEC (now the Nuclear Regulatory Commission) to restrict access to special nuclear materials to those persons "whose character, associations, and loyalty shall have been investigated and as to whom the Commission shall have determined that permitting each such person to conduct the activity will not be inimical to the common defense and security" (Public Law 93-377, sec 7 [1974], now codified at 42 U S C 2201 [i][2])

Concern has arisen in recent years as to whether further authority is needed to screen employees at nuclear powerplants adequately These employees typically work for utilities, and screening is generally limited to state and local police files To allow the screening to include a check of the FBI's criminal records, recently the U S Congress considered S 274, introduced by Senator Jeremiah Denton (R–Ala) This bill would require that reactor employees be fingerprinted and their FBI records checked In response to privacy and other concerns raised primarily by the Nuclear Regulatory Commission, the bill was amended to authorize the commission to promulgate regulations to ensure that individuals be given the opportunity to correct the information contained in the FBI file, information from the FBI file be used only to determine suitability for the job at the nuclear facility, and old and incomplete data in the FBI file not be given undue weight in employment decisions (S 274 was added to H R 4151, the Omnibus Diplomatic Security and Antiterrorism Act of 1986, which was enacted into P L August 27, 1986)

The amendments to the Denton bill represent a careful balancing of civil liberties and security concerns It is certainly in everyone's interest to get up-to-date, accurate information, to be used only for its intended purpose Even when that is done, however, a fundamental First Amendment problem remains For what type of activity can a security clearance be denied? The courts will impose limits here because some of the most fundamental values are at stake

The leading case of *United States* v *Robel* (389 U S 258 [1967]) is instructive Robel, a member of the Communist party, was prosecuted for

having worked in a shipyard designated as a defense facility, employment deemed illegal under the Subversive Activities Control Act The Supreme Court found the relevant portion of the act unconstitutional since it was so broad that it punished people simply for their association with a group, without showing whether the individual agreed or disagreed with the group's unlawful aims The Court emphasized that Congress could "keep from sensitive positions in defense facilities those who would use their positions to disrupt the Nation's production facilities" (398 U S at 267) In *Robel,* however, the Court found that Congress had swept into its security program too many people who posed no threat

The message is clear efforts to improve security through employment screening must be relevant and carefully tailored because of the enormous possibilities for abuse During the debate over plutonium recycling in the mid-1970s, it was alleged that employees at the Kerr-McGee nuclear fuel processing plant had been asked, as part of a security program, "whether they had ever talked to newspaper reporters, whether they belonged to the union, whether they had ever been involved in 'anti-nuclear activities,' and whether they had ever had an affair with another plant employee "[5] This type of overly broad, poorly conceived employment screening has the potential to chill individual freedoms and to erode public support for valid antiterrorist measures

Physical Protection of Nuclear Materials and Prevention of Theft

The actual guarding of nuclear materials poses two major civil liberties concerns the use of deadly force and the possible growth of a federal police establishment

Although the legal standards are ill defined, the ability of guards to use deadly force probably increases gradually along the continuum from private guards to police to the military [6] In all cases, guards can use deadly force in self-defense That power is important, since guards can be positioned to force any thief to pose a threat to the guards The more difficult question is when guards can use deadly force to shoot an escaping felon, such as one who has stolen nuclear material In a recent case involving police officers, the Supreme Court held that it was unconstitutional to use deadly force to prevent the escape of all felony suspects The Court said that such force could be used only when the police officer "has probable cause to believe that the suspect poses a threat of serious physical harm, either to the officer or to others" (*Tennessee* v *Garner,* 105 S Ct 1694, at 1701 [1985]) Clearly someone escaping with strategic nuclear material fits that definition The only caveat, therefore, is to be sure the guard is not shooting at, for example, a harmless

individual who has wandered into a sensitive area by mistake Thorough training, careful positioning of guards, and vigorous security at sensitive areas can greatly increase the odds that deadly force will be used only when appropriate

The matter of a federal police force poses a somewhat more fundamental question Opponents of plutonium recycling often argued that the only way to secure plutonium fuel was to have a massive police presence during its shipment and use It was then contended that that presence would inevitably lead to the growth of federal involvement, either through the military or some type of federal police

It is important to emphasize that the civil liberties concern here is not that the government will act illegally There is nothing illegal about having a lot of guards around a truck carrying nuclear material, and there would be nothing illegal about legislation creating a federal police force to guard the material The concern is simply that the United States would be much less pleasant if there were police on every corner; indeed, it might eventually result in the erosion of fundamental liberties

The British experience provides some support for the view that a federal police presence might increase opposition to antiterrorist activities Since 1954, the British have had special Atomic Energy Authority police to guard against nuclear sabotage The powers of these police were extended by legislation in 1976 to give them the power to carry firearms, not a routine with regular British police [7] There has been some opposition in Britain to these police and their powers [8]

In the United States, there is a strong tradition of local control of police and a longstanding fear by many liberals and conservatives that the centralization of police power in Washington, D C , might be dangerous Under the circumstances, direct federal involvement in guarding civilian nuclear facilities might be costly in terms of public support

Search and Recovery of Nuclear Materials

From the public's perspective, the most dramatic event in the fight against terrorism would be the theft of dangerous nuclear materials, which would result in a large-scale search Three civil liberties concerns stand out in this situation· the legality of the search, the ability to detain and question suspects, and the legality of efforts to control the media reporting on the crisis

Legality of the Search

The search for nuclear weapons controlled by terrorists has received considerable attention in both factual and fictional accounts In fact, the legal

restraints in this area are not great Of course, one cost of terrorism is the loss of privacy that comes about when massive search operations are necessary, however, the loss of privacy is one the courts would likely accept under a variety of doctrines

The central legal questions here revolve around the Fourth Amendment's protection against unreasonable searches and seizures The general presumption under the Fourth Amendment is that a warrant is necessary to conduct a search However, it should be noted that even if a search were illegal under the Fourth Amendment, the most important remedy would generally be that any evidence obtained directly or indirectly from the search would not be admissible in court In the case of a search for a concealed nuclear weapon, this deterrent would not be important The priority of the government would be to find and disarm the weapon, with later court proceedings a secondary concern at best

More important, it is unlikely that any responsible search, undertaken in a good faith effort to find dangerous nuclear materials, would be found wanting by the courts First, judges will be quite willing to grant warrants promptly on a serious showing that nuclear materials might be found In fact, it would be possible to get numerous warrants to cover the various dwellings in a search area since at least some of the occupants might not consent to a search without a warrant It is even possible that the courts might grant a broader warrant to search a well-defined region that includes many dwellings, analogous to the regulatory searches carried out by administrative agencies under warrants that do not show probable cause to find a violation in any particular business (See, e g , *Marshall* v *Barlow's, Inc*, 436 U S 307, 320 [1978])

Even if a warrant cannot be obtained, because, for example, time is of the essence lest a nuclear weapon be detonated, the search is likely to be upheld Under the doctrine of exigent circumstances (see, e g , *Michigan* v *Tyler,* 436 U S 499, 509 [1978]), courts have upheld the warrantless search of a house where dynamite was believed to be located (*United States* v *Perez,* 440 F. Supp 272 [N D Ohio, 1977]) and of a hotel room where a shotgun was believed to be (*United States* v *McKinney,* 477 F 2d 1184 [D C Cir 1973]) As a general proposition, the American Law Institute's Model Code of Pre-Arraignment Procedure has approved warrantless searches upon reasonable cause to believe that the premises contain "things imminently likely to burn, explode, or otherwise cause death, serious bodily harm, or substantial destruction of property," and leading scholars have approved of this formulation [9] The Supreme Court, which has approved public safety exceptions in other settings (see, e g , *New York* v *Quarles,* 104 S Ct 2626 [1984]), is likely to approve this one as well

There is no denying that a broad-scale search is disruptive and invasive, nor is there any denying that such a search undertaken in error would be highly costly to the public and to an antiterrorism program However, the

fact remains that Fourth Amendment law is sufficiently flexible that a good faith search taken on reasonable grounds is likely to be upheld in court

Detention of Suspects

The legal precedent protecting civil liberties is likely to come into sharper conflict with antiterrorism in the area of detention of suspects Under numerous strands of U S law, individuals detained by the police must be told of their right to remain silent and their right to a lawyer, and they must be brought promptly before a magistrate who can determine under what charge they are being held (See, e g , *Miranda* v. *Arizona,* 384 U S 436 [1966]) The U S Constitution does provide for these protections to be undercut through suspension of the writ of habeas corpus but only "in cases of rebellion or invasion" (U S Constitution, Art I, sec 9, cl 2) In a crisis, it might be tempting to hold suspects for interrogation for hours or days without letting them see anyone, a situation that poses tremendous possibilities for abuse and that represents an extension of police authority not approved by current U S law

This possibility of court approval of expanded police powers may pose the gravest threat to civil liberties If a terrorist threat were genuine, there would be tremendous pressure on the courts to approve irregular procedures, particularly if doing so could lead to the punishment of an unpopular defendant In turn, these newly approved procedures might later be employed in less dramatic circumstances This is the sort of situation Justice Jackson warned about when he dissented from the Supreme Court opinion upholding the exclusion of Japanese-Americans from the West Coast during World War II (See *Korematsu* v *United States,* 323 U S 214, 246 [1944]) Moreover, experience in other countries indicates that the detention of suspects in a terrorist situation is not unlikely Current British law allows for detaining terrorism suspects up to seven days [10] In Italy there have been allegations, hotly denied, that terrorist suspects have been tortured [11] This is clearly an area in which an absence of self-restraint on the part of the executive is likely to be costly in the long run for the civil liberties of everyone

Role of the Press

The final source of conflict between civil liberties and the search and recovery of nuclear materials involves a free press It may sometimes be in the interests of those seeking to recover nuclear materials to keep their efforts secret, both to avoid public panic and to increase the odds of success There are two distinct First Amendment issues involved here press access to government information and press freedom to publish whatever information it obtains

On the first issue, there is no general requirement that the government inform the media of what it is doing Although the press has been given access to information in certain highly specialized settings, such as criminal trials (see *Richmond Newspapers, Inc.* v *Virginia*, 448 U S 555 [1980]), there is no general First Amendment right to government information As former Chief Justice Earl Warren wrote for the Supreme Court,

> The prohibition of unauthorized entry into the White House diminishes the citizen's opportunities to gather information he might find relevant to his opinion of the way the country is being run, but that does not make entry into the White House a First Amendment right The right to speak and publish does not carry with it the unrestrained right to gather information (*Zemel* v *Rusk*, 381 U S 1, 17 [1965])

The second question remains, however If word of counterterrorist activities gets out, can the media be stopped from printing or broadcasting what they know? The answer is almost surely no The unwillingness of the courts to issue prior restraints against speech is well documented, the fundamental role of a free press in a democracy makes any such restraints highly suspect As the Supreme Court has said in tracing the history of the First Amendment, "The chief purpose of the [amendment is] to prevent previous restraints upon publication The struggle in England, directed against the legislative power of the licenser, resulted in renunciation of the censorship of the press" (*Near* v *Minnesota*, 283 U S 697, 713 [1931])

It is true that one lower court enjoined publication of a magazine article that supposedly revealed secrets concerning construction of the hydrogen bomb (although another journal subsequently published the same article) (See *United States* v *The Progressive, Inc*, 467 F Supp 990 [1979]) However, restraining information about terrorist activities would be much harder to justify because the public's interest in knowing would be much higher It must be recalled that in the Pentagon papers case, the U S Supreme Court refused to enjoin publication of a classified study of U S policy making in Vietnam, despite allegations that U S security interests would be damaged (See *New York Times Co* v *United States*, 403 U S 713 [1971]) Some commentators have suggested that media self-restraint is the best hope for minimizing harmful coverage in a terrorist situation [12]

Conclusions and Recommendations

As a starting point, it is useful to summarize the legal status of various counterterrorist activities Certain of them are unlikely to be challenged successfully in the courts The use of informers, the use of wiretaps pursuant to current statutes such as the Foreign Intelligence Surveillance Act, the use of

properly trained armed guards, and the conduct of searches for dangerous materials are in this category

Certain other activities are more likely to be successfully challenged. If computer files are poorly maintained and improperly disseminated, if employees are fired for exercising their First Amendment rights, if suspects are detained with no statement of charges, or if efforts are made to censor the press, legal actions may well hinder executive actions Moreover, if court challenges in these areas fail, the result may be the creation of judicial doctrines that will come back to haunt us in areas far removed from counterterrorism

The distinction between these two categories of counterterrorist activities can be overstated A legal activity can still impose a cost on civil liberties Indeed, in the debate about plutonium recycling, it was precisely the areas of use of informers and of armed guards that led to the greatest protests Since the courts are unlikely to stop these activities, many citizens regard them as particularly dangerous

I do not recommend any change in our society's fundamental balance between civil liberties and public order as reflected in current judicial decisions What I am struck by is that in every category covered in this study, there is an important role for executive self-restraint Whether it is a matter of meeting legal requirements, such as in discharging employees only on proper grounds, or a matter where the courts impose few requirements, such as the use of informers, those fighting terrorism can make a vital contribution to civil liberties I recommend that counterterrorists consider the civil liberties implications of what they are doing and, when choosing among workable alternatives, opt for the approach that poses the least threat to those liberties This notion of the least restrictive alternative will avoid conflict with the courts and build public support for counterterrorism

A free society can successfully fight terrorism We need not turn into a dictatorship overnight to address this problem, and I do not believe we are about to do so The greater danger is that we will gradually erode some important freedoms in the long struggle with terrorism However, even that danger can be minimized, particularly if counterterrorists take it upon themselves to weigh the civil liberties implications of their actions

Notes

1 President's Commission on Law Enforcement and the Administration of Justice, *The Challenge of Crime in a Free Society* (Washington, D C U S Government Printing Office, 1967), p 7

2 John H Barton, "The Civil Liberties Implications of a Nuclear Emergency," *New York University Review of Law and Social Change* 10 (1980) 299, 317 Professor

Barton refers in this article to his 1975 study on intensified nuclear safeguards and civil liberties See also Russell W Ayres, "Policing Plutonium The Civil Liberties Fallout," *Harvard Civil Rights–Civil Liberties Law Review* 10 (1975) 369, 403

3 Robert Jungk, *The New Tyranny* (New York F Jordan Books/Gosset & Dunlap, 1979), p 159

4 John F Murphy, *Legal Aspects of International Terrorism Summary Report of an International Conference* (St Paul, Minn West Publishing Co , 1980) p 16

4 Ayres, "Policing Plutonium," p 397

5 Barton, "Civil Liberties Implications," pp 308–309

6 J C Woodcliffe, "Nuclear Power Does It Threaten Civil Liberties?" *Public Law* (Autumn 1983) 440, 456–457

7 Ibid , pp 456–457, Jungk, *New Tyranny,* p 158

8 Wayne R LaFave, *Search and Seizure A Treatise on the Fourth Amendment* (St Paul, Minn West Publishing Co 1978), 2 456

9 Alec Samuels, "Terrorism and English Law," *Kingston Law Review* 10 (April 1980) 3, 21

10 Antonio Cassese, "Terrorism and Human Rights," *American University Law Review* 31 (1982) 945, 953

11 See, generally, Abraham H Miller, *Terrorism, the Media and the Law* (Dobbs Ferry, N Y Transnational Publisher, 1982)

About the Task Force Members

Harold Agnew is the former director of the Los Alamos Scientific Laboratory and former president of GA (General Atomic) Technologies, Inc He worked in the group that achieved the first self-sustaining nuclear reaction, and he helped to develop the atomic bomb He was scientific adviser at NATO headquarters and served as head of the Weapons Physics Division at Los Alamos before becoming director of the laboratory

Yonah Alexander, see *About the Editors.*

George Bunn holds the Stockton Chair in International Law at the U S Naval War College As general counsel of the Arms Control and Disarmament Agency, he was one of the drafters of the Nuclear Non-Proliferation Treaty of 1968 He has been dean of the University of Wisconsin School of Law and professor of strategy at the Naval War College He has also worked for the Atomic Energy Commission and the Nuclear Regulatory Commission, serving the latter as chairman of a special panel on civil use of plutonium fuel, the Generic Environmental Statement on the Mixed Oxide program (GESMO)

Rear Admiral Thomas Davies retired from the U S Navy to become assistant director of the Arms Control and Disarmament Agency He headed the Nuclear Non-Proliferation Bureau and chaired the U S delegation in treaty negotiations with the Soviet Union on a comprehensive test ban and on environmental warfare In the navy he was an aviator and aeronautical engineer and served as chief of naval development and as commander of North Atlantic surveillance operations during the Cuban missile crisis

Donald DeVito is director of the New York State Emergency Management Office and president of the National Emergency Management Association Previously he was county administrator of New York's Montgomery County He also served in the U S Air Force, where he received the Distinguished Flying Cross and the Air Medal

Bernard Feld is professor of physics at the Massachusetts Institute of Technology He participated in the creation of the first nuclear chain reaction and in the formation of the Atomic Energy Commission He has published extensively in technical journals and is a consultant to the Brookhaven National Laboratory He is former editor-in-chief of the *Bulletin of the Atomic Scientists.*

David Fischer is the former assistant director general for external relations of the International Atomic Energy Agency He led the IAEA's negotiation of the main safeguards agreement under which the agency operates He is the author of several works on safeguards and nonproliferation, including the recently published *Safeguarding the Atom A Critical Appraisal* (with Paul Szasz)

Victor Gilinsky is an independent consultant on nuclear energy issues He is a former two-term member of the Nuclear Regulatory Commission Before his appointment to the NRC, he was head of the Physical Science Department at RAND and assistant director of policy and program review for the Atomic Energy Commission

Reinosuke Hara is executive vice-president of Seiko Instrument and Electronics, Ltd in Japan Previously he was the company's managing director He has also served on the executive staff of the International Atomic Energy Agency and as a researcher with the Japan Atomic Energy Research Institute

Enrico Jacchia is the former director of EURATOM Safeguards for the European Community He retired from the European Community after twenty-five years of service with the title of honorary director-general and is now director of the Institute for Defense Studies in Rome, where he writes on nuclear, political, and military issues

Paul Leventhal, see *About the Editors*

Harald Muller is a senior fellow at the Center for European Policy Studies and executive director of the CEPS project New Approaches to Non-Proliferation A European Approach He is also a research fellow and a member of the Foundation Council of the Peace Research Institute in Frankfurt and a visiting professor at the Johns Hopkins University Center for International Relations in Bologna

Yuval Ne'eman is professor of physics at Tel Aviv University and codirector of the Center for Particle Theory at the University of Texas He is the former Israeli minister of science and development and chairman of the Cabinet Committee for Science and Technology He is a member of the Knesset and

has also served as vice-chairman of the Israeli Atomic Energy Commission and senior adviser to the minister of defense

Bernard O'Keefe became chairman of the executive committee of EG&G, Inc , after serving as the company's chairman of the board and chief executive officer He was a principal developer of the firing circuits for the first nuclear weapons and participated in the assembly and delivery of those weapons He worked in the Engineering Department of the Massachusetts Institute of Technology and, with an MIT colleague, formed Radiation Instruments Co before joining the three principals of EG&G in founding that company

Jerrold Post is director of behavioral sciences for Defense Systems, Inc , which conducts policy analysis research for the federal government Prior to joining DSI, he was responsible for developing and leading the Center for the Analysis of Personality and Political Behavior An associate professor of psychology at George Washington University, he is a founding member of the International Society of Political Psychology

John Redick, a specialist on nuclear development and nonproliferation in Latin America, is a program officer with the W Alton Jones Foundation, Inc , of Charlottesville, Virginia He is a lecturer at the University of Virginia and the former research director of the Stanley Foundation

Mohamed Shaker is the deputy permanent representative of Egypt to the United Nations Before that he was the representative of the director general of the International Atomic Energy Agency to the United Nations He was president of the Third Review Conference of the Nuclear Non-Proliferation Treaty in 1985 and is the author of *The Nuclear Non-Proliferation Treaty Origin and Implementation, 1959–1979*

Claire Sterling is an American foreign correspondent who has been based in Italy since 1951 She has reported on European, African, Middle Eastern, and Southeast Asian affairs for the *New York Times,* the *Atlantic, Reader's Digest, Harper's,* and *The New Republic.* She is the author of *The Masaryk Case, The Terror Network,* and *The Time of the Assassins.*

Shuzaburo Takeda is professor of engineering at Tokai University in Japan He holds a master's degree in engineering from Keio University, a Ph D in physics from Ohio State, and has done research in chemistry at the University of North Carolina He is active in nuclear energy activities and serves on a number of committees of the Japanese Atomic Industrial Forum

Kenneth Taylor was a career diplomat in the Canadian Foreign Service from 1959 to 1984 before becoming senior vice-president, government affairs, for Nabisco Brands, Inc From 1977 to 1980, he served as the Canadian ambassador to Iran He received recognition for the Canadian embassy's sheltering of six U S diplomats during the Iranian hostage crisis

Theodore Taylor is chairman of the board of Nova, Inc , which specializes in solar energy applications He is a nuclear physicist who once designed the United States' smallest and largest atomic (fission) bombs He also designed nuclear research reactors He has served as deputy director (Scientific) of the Defense Atomic Support Agency and as an independent consultant to the U S Atomic Energy Commission He is coauthor (with Mason Willrich) of *Nuclear Theft Risks and Safeguards* and is the subject of John McPhee's *The Curve of Binding Energy*

Inga Thorsson is the former under secretary of state for disarmament in Sweden's Ministry for Foreign Affairs She was president of the 1975 Review Conference of the Nuclear Non-Proliferation Treaty She also has served as a member of Parliament, as ambassador to Israel, and as chairman of several United Nations committees

Admiral Stansfield Turner was the U S director of central intelligence from 1977 to 1981 Prior to that appointment, he served as president of the Naval War College, commander of the U S Second Fleet and NATO Striking Fleet Atlantic, and commander in chief of NATO's Southern Flank He is the author of *Secrecy and Democracy* (1985)

Merrill Walters is director of the Nuclear Planning Group for NATO Previously he was deputy director and acting director of theater nuclear forces in the Department of Defense He also has served as chief of the Strategy and Doctrine Department of the Air War College at Maxwell Air Force Base and as chief of the Nuclear and Chemical Section of the Supreme Headquarters of the Allied Powers, Europe (SHAPE)

Mason Willrich is senior vice-president of Pacific Gas and Electric Company Previously he was John C Stennis Professor of Law at the University of Virginia and director of the university's Center for the Study of Science, Technology, and Public Policy He has also served as assistant general counsel of the Arms Control and Disarmament Agency and wrote *Nuclear Theft Risks and Safeguards* (with Theodore Taylor)

Bertram Wolfe is vice-president of General Electric and general manager of the company's Nuclear Technologies and Fuel Division He is president of the American Nuclear Society, as well as a member of the board of directors of the Atomic Industrial Forum and the American Nuclear Energy Council He holds a number of patents in the nuclear field and is the author of several dozen publications concerning nuclear energy

About the Authors

David Albright is a physicist who is a consultant for Princeton University's Center for Energy and Environmental Studies. A specialist in nuclear fuel cycle issues, he is also a consultant for the Federation of American Scientists and writes for such publications as *Scientific American* and *Bulletin of the Atomic Scientists*.

Louis René Beres is professor of political science and international law at Purdue University and the author of numerous works on nuclear issues. His most recent book is *Security or Armageddon: Israel's Nuclear Strategy*. He is also the author of *Nuclear Catastrophe in World Politics*, an exploration of possible routes to nuclear confrontation and the means to prevent them.

George Bunn, see *About the Task Force Members*.

John Despres is special assistant for national intelligence strategy on the staff of the Senate Select Committee on Intelligence. He also has served as director of the Institute for National Strategic Studies at the National Defense University and as national intelligence officer for nuclear proliferation in the U.S. intelligence community.

Donald DeVito, see *About the Task Force Members*.

Herbert Dixon is president of National and International Business Systems Corporation, which specializes in security analyses to detect white-collar crime. He has served as chairman of the Defense Department's Physical Security Equipment Action Group and, in June 1980, as the first industry representative on the Department of Energy's Physical Security and Safeguards Assessment Team for nuclear materials processing facilities.

Eugene Eyster is a former leader of Los Alamos National Laboratories' WX Division, which is responsible for the explosive components of nuclear weap-

ons A specialist in chemical explosives, he participated in the Manhattan Project

Mahlon E. Gates is senior vice-president of the Southwest Research Institute, San Antonio, Texas Following retirement from the U S Army in 1972, he served as manager of the Nevada Operations Office of the Atomic Energy Commission, in which capacity he supervised the underground nuclear testing program and, in 1974, organized the Nuclear Emergency Search Team (NEST) He was awarded the Bronze Star for leading a combat battalion in Burma during World War II and then served in the Manhattan Project He received the Distinguished Service Medal for service in Vietnam

Steven Goldberg is associate professor of law and science at Georgetown University Law Center He previously served in the Office of the General Counsel of the U S Nuclear Regulatory Commission, where his duties included environmental law and civil liberties aspects of a special panel on civil use of plutonium fuel, the Generic Environmental Statement on the Mixed Oxide program (GESMO) He is the coauthor of *Law, Science, and Medicine.*

Eldon V. C. Greenberg, a specialist in nuclear export and marine law, is a partner in the Washington, D C , law firm of Galloway & Greenberg He is counsel to the Nuclear Control Institute He has served as general counsel for the National Oceanic and Atmospheric Administration, deputy general counsel for the Agency for International Development, and staff attorney for the Center for Law and Social Policy

Daniel Hirsch is director of the Stevenson Program on Nuclear Policy at the University of California, Santa Cruz, and chair of the program's nuclear terrorism research group

Milton M. Hoenig, a nuclear physicist, is technical adviser to the task force project He is coauthor of volume 1 of the *Nuclear Weapons Databook,* for the Natural Resources Defense Council In 1979 and 1980 he was in the Non-Proliferation Bureau of the U S Arms Control and Disarmament Agency, where he worked on technical and economic issues related to the nuclear fuel cycle

Enrico Jacchia, see *About the Task Force Members*

Burton F. Judson is manager of advanced engineering for high-level radwaste services of General Electric's Nuclear Energy Operations He has thirty-seven years of experience in process engineering and technical management in the nuclear industry, including spent fuel storage, reprocessing of com-

mercial and defense irradiated fuel, and conversion and fabrication of plutonium fuels

Thomas A. Julian is senior analyst at Science Applications International Corporation, where he has produced several reports on NATO's weaponry and command structure Previously he was a senior analyst with the BDM Corporation He also has served as special assistant for NATO and nuclear matters to the deputy director for plans and policy at U S Air Force headquarters A graduate of the U S Naval Academy, he was in the air force for twenty-six years and taught at the Air Force Academy He retired with the rank of colonel

Konrad Kellen, a member of the senior staff of the Behavioral Sciences Department of the RAND Corporation since 1965, is the author of numerous RAND reports on terrorism, including nuclear terrorism He has worked on studies on protecting nuclear facilities and programs against terrorist attack, including a study he led for the Nuclear Regulatory Commission on guard forces for nuclear installations

William Maraman, a specialist in chemical and metallurgical processing of plutonium and uranium, is director of TRU Engineering Co , which does consulting work on transuranic elements He was at Los Alamos National Laboratories for thirty-seven years, where he was leader of the Plutonium, Chemistry and Metallurgy Group and of the Material Sciences Division

J. Carson Mark is a member of the Nuclear Regulatory Commission's Advisory Committee on Reactor Safeguards and of the Foreign Weapons Evaluation Group of the U S Air Force He is a former division leader of Los Alamos National Laboratories' Theoretical Division and serves as a consultant to Los Alamos and a number of governmental agencies

Eugene Mastrangelo is a senior analyst at Risks International Inc and editor of the company's publications on terrorist operations throughout the world From 1959 to 1983, he was a member of the U S Air Force Office of Special Investigations and was responsible for all counterintelligence collection, analysis, and dissemination within the air force

Sidney Moglewer is doing classified military operations research for a major aerospace company From 1975 to 1982, he was senior operations research analyst for the U S Nuclear Regulatory Commission, where he concentrated on international safeguards and on NRC regulations and procedures on accounting for special nuclear material to protect against unauthorized diversions

Robert K. Mullen is an independent consultant who has been engaged in assessing the threat of subnational groups to various potential targets He has served as chairman of the U S Atomic Energy Commission's Working Group on the Ecological Effects of Plutonium at the Nevada Test Site He also has consulted for a number of government agencies on matters dealing with nuclear safeguards and nuclear event consequence effects

John F. Murphy, professor of law at Villanova University, is a specialist in the application of international law to terrorists and criminals He is author of *Punishing International Terrorists The Legal Framework for Policy Initiatives* He also has written *The United Nations and the Control of International Violence* and coedited *Legal Aspects of International Terrorism.*

Yuval Ne'eman, see *About the Task Force Members.*

Sam Nunn, U S senator from Georgia, is the ranking Democrat on the Armed Services Committee With Senator John Warner (R–Va), he cochaired a working group that proposed establishment of Nuclear Risk Reduction Centers by the United States and the Soviet Union

Gerald L. Pollack is professor of physics at Michigan State University He has served as a consultant to the Nuclear Regulatory Commission, the National Bureau of Standards, and the Illinois Department of Nuclear Safety He is the author of numerous articles in scientific publications

Jerrold M. Post, see *About the Task Force Members*

Alexander Rossnagel is a professor of law at the Sachhochschule in Darmstadt, the Federal Republic of Germany, who specializes in issues of nuclear power and constitutional rights His published books include *Bedroht de Kernenergie unsere Frieheit* (Does nuclear energy threaten our freedom?) and *Radioaktiver Zerfull der Grundrechte* (Radioactive decay of constitutional rights)

Leonard S. Spector is a senior associate at the Carnegie Endowment for International Peace and author of the endowment's annuals on the spread of nuclear weapons, *Nuclear Proliferation Today* and *The New Nuclear Nations.* He has served as legislative counsel to Senator John Glenn (D –Ohio), as well as chief counsel to the Senate Energy and Nuclear Proliferation Subcommittee He was also special counsel to Commissioner Victor Gilinsky at the Nuclear Regulatory Commission

Claire Sterling, see *About the Task Force Members*

Lacy Suiter is the state director of the Tennessee Emergency Management Agency He also has served as deputy director and operational readiness officer at the agency He is a past president of the National Emergency Management Association and chairman of the Central United States Earthquake Consortium

Theodore Taylor, see *About the Task Force Members.*

John Warner, Republican U S Senator from Virginia, is second-ranking majority member of the Armed Services Committee and chairman of its Subcommittee on Strategic and Theater Nuclear Forces With Senator Sam Nunn (D–Ga), he cochaired a working group that proposed establishment of Nuclear Risk Reduction Centers by the United States and the Soviet Union

Jacob Wechsler is a physicist specializing in nuclear explosives He was a member of the Manhattan Project and was leader of Los Alamos National Laboratories' WX Division, which is responsible for the explosive components of nuclear weapons

Bertram Wolfe, see *About the Task Force Members*