Workshop Report

Communicating Nuclear Risk: Informing the Public about the Risks and Realities of Nuclear Terrorism

May 20, 2002

Tonya L. Putnam

October 2002

About the Author

Tonya Putnam has a J.D. from Harvard Law School and an A.M from Harvard University. She is a Ph.D. candidate in the Department of Political Science at Stanford University and a MacArthur Affiliate at CISAC. Her dissertation explores the extraterritorial reach of U.S. federal courts and regulatory institutions, and implications for the development of de facto international regulatory frameworks.

Preface

This report presents the highlights of a workshop entitled "Communicating Nuclear Risk: Informing the Public about the Risks and Realities of Nuclear Terrorism" held at the Center for International Security and Cooperation (CISAC) of the Institute of International Studies at Stanford University on May 20, 2002.

In the wake of the September 11, 2001 attacks, many members of the media and the public became aware that further acts of terrorism against U.S. targets were possible, and that such attacks could involve chemical, biological, or nuclear weapons. Although accurate basic information about the effects of nuclear and radiological weapons is available, mainly through specialized sources, it is not widespread, and it can be difficult to separate from misinformation about the sources, characteristics, and effects of radioactivity. In short, there was a clear appetite for more and better information. At the same time, concerns exist on the part of scientists and first responders about how best to meet the public's need for information about these types of threats in order to avert panic and save lives—without simultaneously helping terrorist groups to stage more effective attacks. The workshop was intended as a first step toward meeting these needs and concerns. It brought together local representatives of the media (newspaper, radio, and television); local first responders, including local representatives of federal and state agencies; scientists; and risk analysts for an informal, daylong meeting.

The meeting had two main purposes. One purpose was to present and discuss the effects that various kinds of nuclear and radiological terrorist attacks might have on targeted communities, as well as those nearby. Some effort was made to discriminate between risks that, though they might involve serious damage to life and property, were within the range of public experience, and those risks that would constitute an unprecedented catastrophe. The second purpose was to identify and explore the concerns that each category of participants had regarding such an attack.

Because of time limitations, the workshop focused solely on risks associated with nuclear and radiological terrorist attacks. However, many of the points made and concerns raised would apply to preparing the public and the media for other kinds of terrorism. In order not to give terrorists new information, workshop participants restricted their observations in several ways. First, discussion of the details of attack scenarios was limited to those that have

already been widely discussed in the press and in nonclassified sources. Another self-imposed limitation was restricting discussion of the probable consequences to basic facts regarding effects and remedies, without incorporating "how to" information. And finally, the information contained in all formal presentations was vetted by appropriate authorities prior to the workshop.

Of particular benefit in the view of workshop participants was the opportunity to better understand the demands and constraints under which individuals and organizations engaged in various roles are required to work. Examples include the pressure on journalists to generate reliable information under strict deadlines; the requirement of scientists and experts to make judgments and issue opinions only when based upon adequate evidence; and the demands placed upon public officials, fire, police, and medical personnel to respond to a wide variety of emergencies.

Participants in the workshop stressed the need for follow-up activities. Several concrete suggestions that were put forward by workshop participants are included at the end of this report. At the time of this writing, at least one of these suggestions, the drafting of nuclear terrorism fact sheets for journalists, has been completed. More local workshops and media briefings would be helpful, and some are indeed taking place under local and federal sponsorship. This report is published in the hope that it may be useful to groups planning similar activities elsewhere.

We would like to thank the workshop participants for contributing their knowledge and experience to this experiment, and we are grateful to Carnegie Corporation of New York for its generous support.

MICHAEL MAY
September 2002

Introduction

Achieving adequate preparedness for a terrorist attack against the United States involving a nuclear or radiological weapon is simultaneously a technical problem, a public-policy challenge, and a public-education mission. Response to terrorist attacks differs in important ways from response to more familiar nuclear emergencies arising from reactor accidents, and also from response to conventional and chemical and biological terrorist attacks. The complications of risk communication in the realm of nuclear terrorism include overcoming misinformation about the nature of the threats posed by terrorist attacks involving nuclear and radiological weapons as well as mistrust of experts, the government, and the media.

The key issues are what to communicate, when, how, to whom, and with what degree of certainty. Those issues specifically discussed include:

- When communicating the range of possibilities to the public between best and worst-case scenarios, how can the range of risks be effectively conveyed, and where along that range of risk should attention focus?
- How should the balance be struck between informing the public about particular dangers and vulnerabilities and suppressing such information in order to avoid providing terrorists with guidance for carrying out more effective attacks?
- How should "standard" emergency response and emergency preparedness differ when facing a "thinking enemy" as opposed to an accident or a natural disaster?
- In a low-exposure radiological terrorist event, how can first responders[1] and other public officials effectively communicate the level of risk in appropriate perspective?

The projected consequences of nuclear and radiological terrorism have received increased attention, both among experts and in the media, as consideration of potential domestic terrorist threats has broadened following the attacks on September 11, 2001. Experts predict that, contrary to popular perceptions, in the most likely class of nuclear terrorist attacks—those involving attempts to disperse relatively small amounts of radioactive material by means of conventional explosives—the loss of life from the dispersal blast will be greater than from

radiation exposure. Although the health risks associated with radiation exposure from this type of terrorist attack tend to be the focus of public concern, other predicted costs of a nuclear terrorist attack including economic disruption and cleanup (decontamination) are likely to have a greater overall impact.

I. Dimensions of the Terrorist Threat

The threat posed by nuclear terrorism can be analyzed along several related dimensions.[2] First, threats can be evaluated according to the *means of attack*, which can range from various types of nuclear devices and conventional explosive devices to attacks on fixed installations and covert releases of radiation. A second dimension is the *probability* of occurrence for each type of attack. Estimates regarding the likelihood of any particular type of terrorist attack are viewed as a function of three elements: the quantity and quality of materials required to construct a terrorist device, the difficulty of acquiring these materials (or a ready-made device), and the degree of technical sophistication required to carry out an attack with each type of device. A third dimension along which nuclear and radiological terrorist threats can be evaluated is the *severity of the consequences* likely to follow from a "successful" attack.

A. Technical Issues

The focus of the workshop on broad issues of threat communication and response coordination precluded consideration of detailed threat scenarios. However, the following four general threat scenarios, described in descending order of severity, communicate the range of possibility that informed the workshop discussion.

1. Detonation of an improvised (or stolen) nuclear device

The first general scenario for nuclear terrorist attack considered is a "worst case" set of events involving a Hiroshima-type 10 or 12 kiloton nuclear bomb detonated in a densely populated urban area such as San Francisco or Los Angeles. A nuclear detonation of this magnitude would have catastrophic results, producing an expected 100,000 immediate deaths and 200,000 or more casualties of various kinds, including roughly 48,000 burn victims and a large incidence of "flash blindness" within a seven-mile radius.[3] Buildings would be destroyed, together with highways, bridges, power grids, and other infrastructure. Massive fires would be ignited around the periphery of the blast area that would continue to produce damage and casualties. Additional deaths and casualties would result from radioactive fallout (or "rainout")[4] for several miles from the blast site, with specific fallout patterns depending heavily on local wind and weather conditions.[5]

This "high-consequence" scenario has a low probability of occurrence for two reasons. First, the primary challenge associated with building an improvised nuclear device is the difficulty of acquiring the materials needed for construction. Nuclear devices require either plutonium or highly enriched uranium (HEU) to achieve an explosive fission chain reaction.[6] In the construction of a nuclear device, these materials cannot be substituted with other, more readily available materials. Non-weapons-grade plutonium, which, theoretically, can be used in a weapon, is more prevalent, but generally also controlled (at least in the United States). Nevertheless, these materials may be more easily acquired elsewhere, for example in South Asia and

1,000 rem in hour to 5 miles
1,000 rem in day to 10 miles
1,000 rem in week to 15 miles

Figure 1. Fallout from 10 KT Nuclear Explosion

in the Soviet successor states, where vast quantities remain under conditions that are considerably less secure.

A second barrier to carrying out a major nuclear terrorist attack is the difficulty of constructing an effective nuclear device. Opinions differ within the technical community regarding whether a terrorist group could construct an effective multiple kiloton nuclear device. Although the technical information required to construct a nuclear device is acknowledged to be publicly available, many workshop participants emphasized the difficulties of achieving an effective nuclear detonation. In the opinion of many experts, the most likely outcome of a

terrorist attempt to detonate an improvised nuclear device would be a "fizzle"—an explosion with minimal nuclear yield resulting in no ground vaporization and no mushroom cloud.[7] To achieve even this level of effect would be relatively unlikely, even assuming access to materials of a reasonable quality, in the absence of equipment and expertise requiring the resources of a nation-state or groups supported by a nation-state. Again, however, these estimates involve probabilities and not certainties.

A related scenario posits that terrorists acquire an existing nuclear device by diverting it in transit or by stealing or purchasing a device illicitly from a storage site. The United States government has attempted to forge a cooperative relationship with the Russian government to improve the security surrounding transportation and storage of nuclear weapons and materials through enhanced physical security and accountability structures for weapons facilities and radiological source sites. Included in these efforts is a program to reduce available stockpiles by bringing materials to the United States for conversion from weapons-useable forms to fuel for nuclear reactors.[8] Although international efforts to improve the security of nuclear stockpiles have concentrated on Russia and the other nuclear successor states to the former Soviet Union, the new nuclear states in South Asia have more recently become a focus of concern.[9] The United States has had considerably less success in encouraging the new members of the "nuclear club," such as Pakistan, to adopt strict measures for control. This illustrates that the political hurdles to achieving nuclear security may in some cases be more challenging than the technical issues.

2. Attacks on "civilian" sources of nuclear and radiological material

A few categories of fixed installations are a source of particular concern for potential terrorist attack, either as an act of direct sabotage or for the purpose of acquiring materials from which to build nuclear bombs or radiological dispersal devices (RDDs). Most attention has been focused on nuclear power reactors (active and inactive) and spent fuel storage sites, but there is also concern that other installations, such as research reactors, waste sites, hospitals, and food irradiation facilities could be attractive targets for nuclear terrorists.[10] The sites of these facilities are not secret. However, following the September 11, 2001, terrorist attacks, detailed information about these sites has become more difficult to acquire from public sources such as the Internet.

a. Nuclear power reactors[11]

An attack against a nuclear power reactor is a scenario treated with varying degrees of plausibility by experts. Reactors are hard targets, but they are also obvious targets. Modern reactors are constructed with safety and security as an objective and are designed to endure a variety of accidents, natural disasters, and acts of sabotage. The critical part of most reactors, including the core and much of the cooling system, is contained inside thick concrete and steel structures, often located below ground level.[12] Reactor "design envelopes" include safeguards against damage to fuel assemblies, as well as mechanisms to control releases of gaseous radiation.[13] They are also generally capable of withstanding extensive damage to containment buildings and secondary equipment without critical damage to the reactor core or its coolant systems.

An attacker attempting to target a reactor from the air (e.g., with an airplane or missile) would need knowledge of the reactor's construction and the technical ability to reach the target (which is considerably greater than that required to guide a jet into an office tower).[14] Large aircraft attacks targeting power reactors were not part of Nuclear Regulatory Commission (NRC) threat scenarios before September 2001. However, plans to forestall and minimize

the impact of terrorist attacks against nuclear power reactors from the ground, for example, using a truck or boat filled with conventional explosives have been included in security planning for nuclear power facilities since the mid-1990s. Due to specific technical and design features common to all reactors currently in operation in the United States, a ground-based attack from outside a reactor facility would be unlikely to penetrate the primary containment structures surrounding the reactor core or to cause a simultaneous "common mode" failure of layered safety systems.

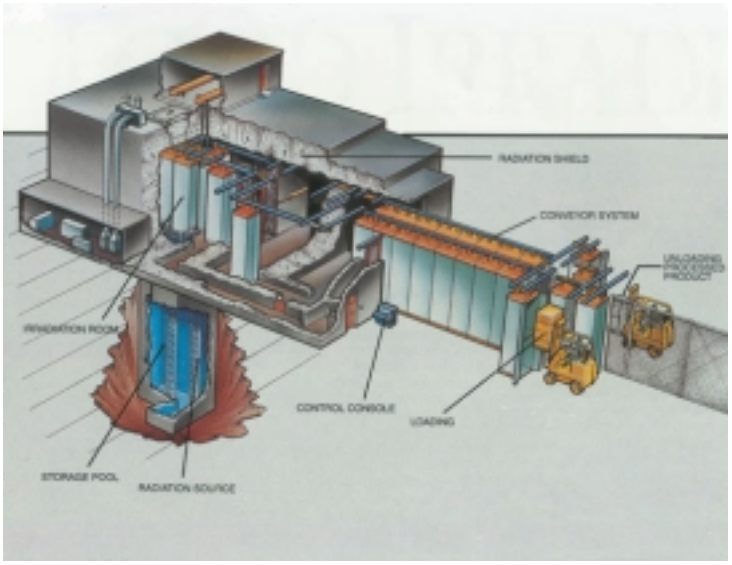
Another possibility discussed is the threat posed by attacks against nuclear power facilities by (or with the complicity of) facility insiders, including, for example, incidents arising from a forced seizure of a plant control room. Even before the September 11, 2001, terrorist attacks, critics censured NRC policies and practices regarding the security of nuclear power facilities. However, much of this criticism was viewed by those technical experts among the workshop participants as excessively harsh and to a degree unfair.[15] Indeed, many experts believe it is highly unlikely that any ground-based terrorist attack against a nuclear power reactor, with or without the aid of insiders, could succeed in penetrating or damaging the reactor core, thereby triggering a Chernobyl-type emergency. Evolving factors of structural design and security planning, although not a guarantee, mitigate against the already low plausibility of this type of attack succeeding.

A further issue raised is the comparative vulnerability of onsite facilities for storage of spent nuclear fuel. Spent fuel, which is highly radioactive, is stored under tens of feet of water in cooling ponds until cool enough for placement in dry-casks for transportation and long-term storage. Spent-fuel storage facilities are a source of concern, both as possible primary targets of a terrorist attack and as sources of materials for offsite attacks.[16] First, many of the buildings that house spent-fuel pools are standard steel industrial-type structures, and are less well protected than reactor containment buildings. This makes them more vulnerable to attack both from the ground and from the air. A highly successful primary attack against a spent-fuel storage facility could result in potentially widespread dispersal of highly radioactive material through fallout. Second, fuel-storage facilities are potential sources for radioactive material for use in RDDs and for plutonium that (with great effort) could be reprocessed into a nuclear weapons-usable state. However, the difficulties of approaching and handling spent nuclear fuel are enormous and should not be underestimated.[17] Furthermore, the equipment and processes required to separate plutonium from spent nuclear fuel are currently within the capacity of only a handful of nation-states. Enhanced physical security for spent-fuel facilities in the United States was completed in 1998 and has been coupled with additional security procedures for plant personnel. Nevertheless, these sites remain a source of concern for potential terrorist attack.

b. Medical, industrial, and research sources of radioactive material

Small research reactors located in laboratories and universities constitute a further set of targets, together with irradiation sources found in hospitals and at industrial radiation facilities.[18] Industrial and agricultural uses of radioactive sources include industrial radiography and facilities for the irradiation (sterilization) of food and medical products.[19] Common medical uses of radioactive materials include radiotherapy for the treatment of tumors and radiographic diagnostics.[20]

• Heavily walled labyrinth structures
• Sources stored in deep pools or inside massive shielding
• Designed for remote operations
• Most radionuclides likely remain within the building in event of an explosion.



Typical large cesium source:
9,000 Ci Cs-137
3 tons
Theft likely to be promptly detected

Figure 2. Large Irradiation Facilities Are Hard Targets

The consequences of an attack on a research reactor are likely to be less serious than those associated with an attack on a large power reactor.[21] The spent fuel from research facilities typically has lower burn-up and fewer fission products than that contained in power reactors, which means that the potential harm from exposure is reduced proportionately. Moreover, research reactors operate with much less radioactive and fuel material and in the event of a successful terrorist attack are unlikely to suffer a catastrophic fuel failure or "melting," which further reduces the potential for a major radiation release. However, research reactors and industrial and medical sources are softer targets than nuclear power facilities—a factor that heightens the potential for a successful attack against, or the theft of materials from, these

sites.[22] Experts agree that a massive explosive device from *inside* a research reactor or industrial facility would be required to achieve any appreciable radiological effect outside the facility. Because industrial, medical, and research facilities are foreseeable specific targets, protective measures can be taken to "harden" potential attack positions and to institute procedures to limit access to vulnerable areas.

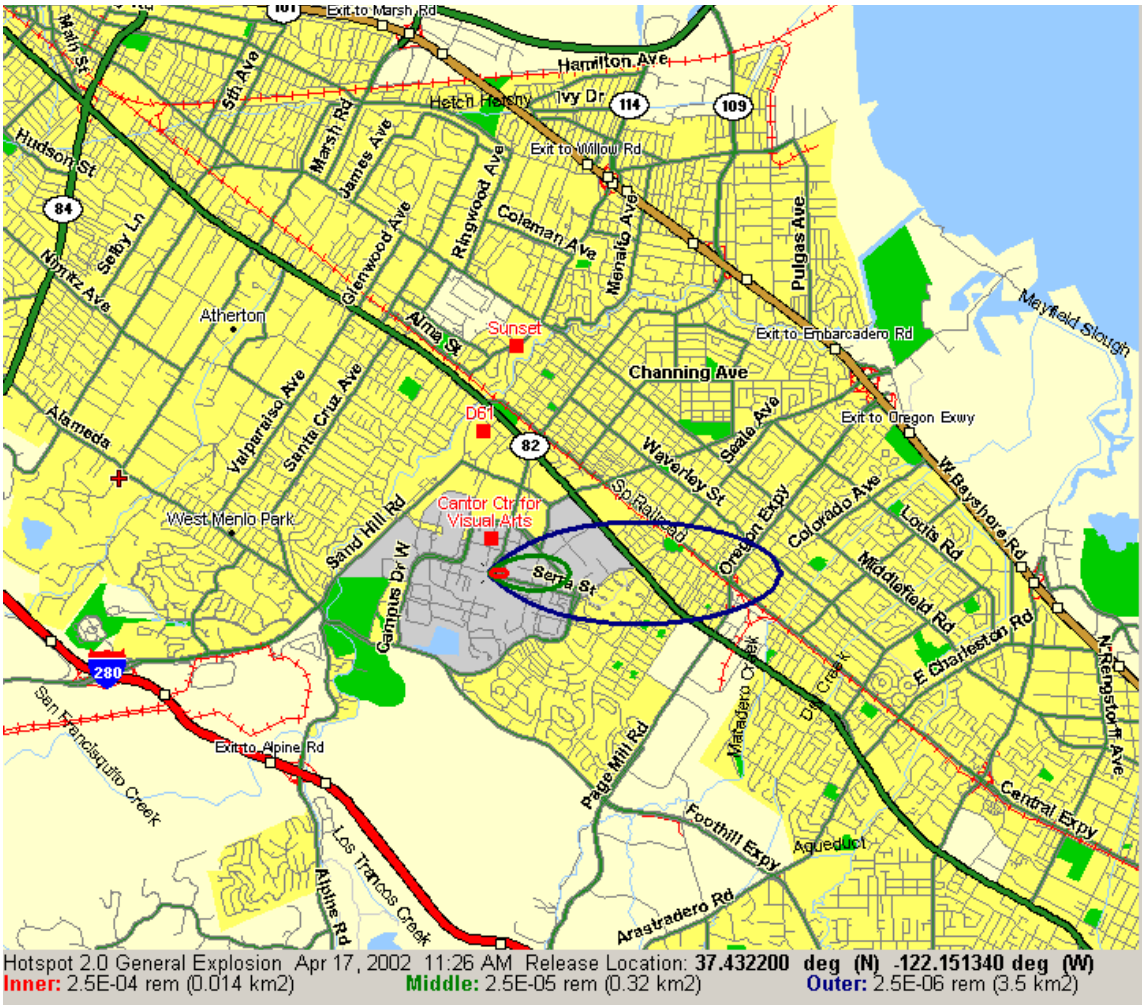
A somewhat different set of issues is presented by the potential for attack against a medical or industrial facility to obtain radiological materials for use in an RDD. To stage an attack against a commercial or research facility for the purpose of obtaining radioactive material, a terrorist would need, at a minimum, to (a) gain access to a radiological containment area, (b) transport the container from the secure facility, and (c) remove the source from its shielding. The technical difficulties at each stage are considerable, and, in addition, the probability of detection is high.[23] The amount of radioactive material contained in medical and industrial facilities is small in comparison to power reactors, although some research reactors have significant amounts of fuel located at or near the reactor. Radioactive sources are typically housed inside layers of protective metal shielding that are designed to be operated remotely, making them difficult to access and difficult to transport covertly.[24] Removal of the radiation source from its protective shield would make these sources still easier to locate and would expose handlers to potentially lethal doses of radiation.[25]

3. Radiological dispersal devices ("dirty bombs")

A terrorist attack using a crude explosive device for radiological dispersal would require considerably less in the way of technical expertise than either a successful detonation of a nuclear device or a dedicated attack against a nuclear reactor or an industrial facility. Furthermore, an attack using an RDD, or "dirty bomb," is achievable using a far wider range of radiological materials that are more readily available than materials used in nuclear explosive devices.[26] At the same time, RDDs pose a substantially smaller risk of fatalities, or even negative health effects, than detonation of a nuclear device.

RDDs are far less effective at dispersing radioactive material than a nuclear explosion. A low-level Cs-137 dirty bomb incident would produce little significant short-term physical damage to individuals or the blast environment. For example, an RDD containing a ten-curie Cs-137 source exploded on the roof of a building on a clear day with a light breeze could be expected, assuming no additional extraordinary circumstances, to have the following exposure results.[27] The radiation dose in the immediate blast area would be roughly 250 mrem with harmful effects diminishing with distance—or 100 mrem *less* than an average annual dose of background radiation.[28] Further than a few blocks from the detonation site, the blast exposure dose would not exceed the level of everyday environmental background exposure. However, this is not to say that an RDD attack would have no radiological impact. Cleanup and decontamination of the immediate blast area would be required in order to mitigate future longer-term effects from radiation exposure to those living or working at the site.[29] Another type of consequence that should be factored into cost estimates of an RDD terrorist attack is the potential for significant social and economic disruption following from an attack, independent of actual levels of physical damage. Emergency-management experts predict that even a crude RDD capable of producing few casualties (or none at all) could generate potentially severe social and economic disruption because of the radioactive character of the materials used.

"Portable" sources of radioactive material used for industrial purposes, such as those for field inspection of x-ray welds in ship-building and pipeline construction, create considerably



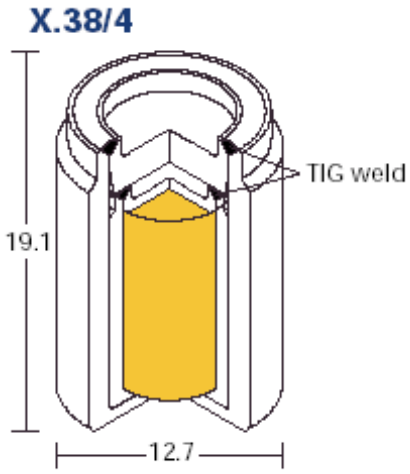
Inner contour (Red)	250 microrems (equivalent to less than 1 cigarette)
Middle contour (Green)	25 microrems (equivalent to 2 bananas)
Outer contour (Blue)	2.5 microrems

Figure 3. Fallout from RDD Explosion - 2 Ci Cesium-137

less concern as potential sources of radioactive material for terrorists than many of the sources mentioned. Portable sources are designed for transport from site to site and are therefore relatively light and mobile. They range in weight from roughly 50 pounds to several hundred pounds, most of which is protective shielding.[30] Despite their ease of transport, portable sources do not generate great concern among experts, since each source contains relatively little radio-active material. To achieve a significant radiological impact using a portable source would require significantly more than simply wrapping it in dynamite and detonating it.[31] Radioactive material from several such sources would likely be necessary in order to construct an RDD capable of producing radiological effects beyond a conventional blast range.

Portable sources have limited activity:
- <100 mCi Co-60
- 40–50 lbs
- 30–40 lbs DU

A typical capsule:
- 10 Ci Cs-137
- 1/2 inch diameter
- 3/4 inch long
- Ceramic matrix
- Welded double SS
- Tested to 25,000 psi



Larger sources are much heavier:
- 10–20 Ci
- 340 lbs total
- 225 lbs DU

Figure 4. Typical Portable Sources Are Weaker

In sum, the larger range of radiation sources suitable for use in RDDs, combined with their widespread use, indicates that efforts to maintain control over materials alone are unlikely to be sufficient to prevent RDD attacks. The United States has nearly two million licensed sources of radiological materials. Although these materials are strictly regulated, each year approximately 200 sources (most of which are low-grade) end up "lost" or "stolen." As of October 2001, official tallies included some five thousand "orphaned" sources.[32] Viewed internationally, achieving security by means of achieving control over nuclear materials alone is a nearly impossible task, despite commendable International Atomic Energy Agency (IAEA) efforts to institute controls on the sources and movement of such materials internationally.

4. Covert release of radioactive material

The final general scenario discussed is one involving the covert release of radioactive material (i.e., without the aid of an explosive device). A small (in terms of dimensions) radioactive source placed in a nondescript container in a public place where members of the public are likely to loiter for several minutes at a time could potentially kill several dozen individuals though acute exposure and expose many others to heightened long-term cancer risks.[33] In the post–September 11, 2001, emergency response environment, emergency-room physicians are more likely to suspect exotic sources of illness, including radiation sickness. However, the ability to detect radiation exposure as a cause of illness depends heavily on the size and severity of the immediate doses, since radiation sickness occurs only from acute high doses of radiation. A small (in terms of physical dimensions) "silent" source of radioactivity could deliver exposures at a sufficiently low level to avoid radiation sickness and could take weeks to detect.

As a rule, effective dispersal of radioactive material is difficult to achieve without an explosion or a fire. The most serious dangers associated with exposure to "silent" sources of radioactivity stem from the difficulty of detection and the economic and social disruption that could potentially follow from public reaction to such an attack.[34] However, there is little motivation for a terrorist to contaminate at an entirely covert level—particularly where, unlike the case with many types of chemical and biological terrorism, the consequences of an attack may not be discovered until decades later. It follows that placement of a radioactive source too small or too weak to generate radiation sickness would likely be accompanied by a subsequent announcement by the individual or organization responsible, at which point site decontamination and treatment of potential exposures could begin. This raises the possibility—if not the likelihood—of disinformation regard the site and quantity of release in order to provoke public apprehension.

B. Health Risks Associated with Nuclear and Radiological Attacks

The individual and societal health risks associated with exposure to nuclear and radiological materials range from utter catastrophe (nuclear explosion) to small effects that would go unnoticed if not for the modifier "radioactive." Numerous hypothesized terrorist scenarios involving attacks with nuclear or radiological devices predict relatively low radiation exposures. Indeed, a radiation source in the range of 1,000s of curies would be needed before concerns about the health effects of radiation exposure would outweigh damage likely to be caused by the explosion itself. However, in projecting the overall health effect and social

impact of a nuclear or radiological attack, a focus on blast effects versus radiation effects may be overly narrow. The principal impact of a nuclear or radiological terrorist event may be public panic, or, at a minimum, an erosion in public trust in the ability of the federal government to provide security to American citizens. It follows that a terrorist could produce a highly "successful" bomb that incurred no direct casualties. At the same time, accurate, timely information coupled with good leadership have been shown time and again to be effective tools against panic and disaffection.

Radiation from detonation of the 10-kiloton nuclear device hypothesized above would have initial lethal and non-lethal effects within approximately one mile of the site of explosion. The lethal effect would be compounded by associated blast and burn injuries within a somewhat wider area. Delayed radiation would emanate outward from the blast site, with almost all harm occurring downwind of the site. On a clear day with a light wind, populations located within five miles downwind of a 10-kiloton blast could be expected to receive radiation doses of approximately 1,000 rem within an hour. Similarly lethal doses could be expected as far as ten miles downwind within one day and up to fifteen miles within a week. Of course, these areas would be identified and evacuated as quickly as possible, thereby minimizing the population that would actually receive these doses.

A smaller, non-nuclear dispersal device ("dirty bomb") is likely to achieve little dispersion of radioactive material beyond the immediate blast site, and result in little fallout. Most of the initial radiation dose will be from radioactive material finely dispersed by the explosive blast. How much is dispersed will vary, with the proportions varying with the type and amount of radioactive material and with the size of the blast. Within the range of a few city blocks to a few miles, radiation doses delivered by the RDD explosion would fall rapidly to almost "background" levels. Longer-term doses might result from residual materials that "fall out" and are absorbed into the soil and various types of organic matter, thereby resulting in radiation "contamination."[35] The probable health effects following from a covert release of radiation are even more difficult to predict, depending upon the isotope, its quantity, the area of its dispersion, the population exposed, and other factors. Moreover the effects may not come to light until decades later in the form of higher than average rates of cancer.[36]

Estimates of the likely effects of low-dose exposures to radioactivity are generally inferred from higher dose data using "dose-effect curves."[37] The biological impact of a radiation dose depends not only on the level of contamination but on the type of radiation involved.[38] The short-term negative effects of exposure result either from absorption of radiation from external sources or from ingesting vaporized radioactive material, resulting in a "committed dose."[39] The biological half-life of an exposure (the length of time required for the body to rid itself of the radioactivity)[40] varies significantly among sources.[41]

The absence of clear data regarding the health risks associated with the type of low-dose exposures likely to follow from an RDD-type terrorist attack complicates the task of emergency responders and public officials charged with informing the public about the risks and consequences of various types of terrorist attack. The message that the public has less to fear than is commonly supposed from conventional radiological attacks is rendered less credible by the inability of experts to project with precision the likely public health consequences of such attacks. The best estimates use a linear, no-threshold hypothesis for low-dose exposure inferred from study of radiation sources encountered in everyday life, and from a very large array of experimental data in animal and cellular research. These estimates suggest that a 2.5 rem exposure leads to a .01 percent increased chance of dying from cancer—a risk which,

even at the upper bounds of uncertainty about the dangers of low-dose exposures, is considerably lower than is routinely assumed.

* * *

Worldwide 70 to 80 percent of all terrorist attacks involve explosives. Detonation of a nuclear device in a densely populated area would have catastrophic consequences, but is relatively unlikely for the reasons described. Nevertheless, experts agree that, due to the extreme nature of the consequences that would follow from a successful terrorist attack using a nuclear weapon, efforts that may help to reduce this likelihood still further are warranted. It is far simpler to acquire materials for and to construct a conventional RDD, but such devices entail few risks of severe radiation exposure beyond the immediate range of the blast. Although an ineffective means of killing large numbers of people, RDDs are nevertheless likely to result in severe short-term economic and social disruption, with potentially high clean-up costs over the longer term. Effective control over materials, together with early detection and response, is essential to prevent or to mitigate the harms from nuclear and radiological attacks.

II. Communicating the Risk of Nuclear Terrorism to the Public

A great deal of general information about to how to communicate risk is currently available and much of this can be applied to the task of informing the public about the risks and consequences of various types of nuclear and radiological terrorist attacks.[42] There is a high degree of public apprehension and misinformation about radioactivity and radiological risks that make explaining the risks posed by nuclear and radiological terrorism to members of the general public particularly challenging. Overcoming these barriers to effective communication is made more difficult by the perceived lack of credibility of those with authority and expertise on the subject among the general public. An additional impediment is the reticence of many experts in the field of nuclear science to discuss risk and consequence issues in public forums or with members of the media. This hesitancy is a function of scientific uncertainty about the issues involved, legitimate security concerns, and apprehension among individual scientists that their statements will be misunderstood or that the information will be used out of context.

Clearly, members of the scientific community, policymakers, and the media share the overall objective of saving lives and minimizing the impact of a terrorist attack involving an RDD or a nuclear weapon. In practice, however, more immediate parochial incentives within each profession create tension between these roles, as does the need to account to different audiences with varying levels of sophistication about the issues. These tensions need to be acknowledged and factored into practical strategies for coordinating emergency response to nuclear terrorism. With this level of complexity in mind, the following issues were identified at the workshop as particularly important to achieving effective communication about the risks and probable consequences of a terrorist attack involving nuclear or radiological devices:

- How should public officials strike a balance between creating public apprehension about the risk of nuclear terrorist attack and the need for a public informed about these issues?

• How can current, reliable information about risks and consequences be kept in the public consciousness, particularly when the hope is that it will never be needed?

• Which roles and which organizations can serve as credible sources of public information about nuclear and radiological issues?

• In what ways can experts help to educate the public about the technical challenges of such attacks and calm fears without providing terrorists with an "instruction book" to improve the effectiveness of their attacks?

a. Public perceptions of radiation and radiological consequences

A distinguishing hallmark of terrorist attacks using nuclear or radiological weapons is the issue of radiation and its consequences, and the broad incidence of public fear of anything labeled as radioactive. However, this fear is in most cases greatly out of sync with the actual degree of biological threat. The concern among emergency response planners is that in a terrorist incident involving an RDD (the most likely class of radiological terrorist attacks), public reactions driven by blind fear of radiation may produce as much physical and economic damage as the attack itself. The more information disseminated to first responders and the general public in advance of a nuclear or radiological terrorist incident, the greater the likelihood of achieving measured results if an attack occurs. Indeed, experience has shown that panic during disasters is actually quite rare: with leadership and information, people can, on the whole, be expected to behave calmly and reasonably.[43]

Shaping public perceptions regarding the threats posed by nuclear and radiological terrorism is not a matter of working from a blank slate. Indeed, one of the steepest challenges to effective risk communication on this topic is to reeducate members of the public about issues they think they understand, and to teach them to distinguish fact from fiction on the subject of radiological risks.[44] In the absence of reliable information, most people make intuitive risk judgments on the basis of memorable images and events within their own direct and indirect experience. Information feeding into intuitive risk perceptions comes principally from the news media, which tends to document mainly injuries and mishaps, and from images gleaned from the entertainment media.[45] Consequently, a substantial proportion of the public is willing to believe that radiological exposure is by definition harmful, even at very low levels, even though the data to support that hypothesis is highly equivocal. This fear is not, however, unbounded. The American public has for decades traded off the risks associated with maintaining an arsenal of nuclear weapons for safety and security from external threats.

The terrorist attacks of September 11, 2001, were signal events. The post–September 11 American public is more attentive to information about terrorism and terrorist threats, and more inclined to take steps, and accept inconveniences, to reduce those threats. The downside of this new ability of the public to imagine further and greater threats is that virtually all threat scenarios now have a greater plausibility among the public. Consequently, the need exists to actively manage public perceptions—some of which may be accurate, and some not—that feed into public fear.

The primary obstacle to increasing public understanding of the probable consequences associated with nuclear terrorism is not a lack of information, since information about radioactivity and other effects of nuclear weapons has been available in the public domain for decades. Rather, the problem is finding ways to persuade the public of the importance of paying attention to this information without causing panic, and to maintain public interest in plans and programs that will hopefully never be needed. The media has considerable power to create and maintain—or alternatively to correct and replace—public misperceptions about the

nature and extent of the threats at issue.[46] In contrast, public officials have limited resources for conveying information about nuclear and radiological risks and consequences directly to the broad cross-section of the public for whom it may become relevant. Many journalists (and certainly the best among them) view their role as intermediaries between experts, policymakers, and the public in which they are called upon to translate complicated, often technical information into comprehensible terms.[47] Consequently, the most promising channel for disseminating such information widely is sources of television, radio, print, and electronic media at the local level.

Communication about the probable consequences of a terrorist attack should be tailored to the community being addressed. An important factor in effective communication is to identify those individuals who are likely to be most interested and most affected. Where possible, "articulate elites" (scientists, experts, policymakers, and activists) at the community level should be enlisted to help generate public meetings and articles in local newspapers and to participate in interviews on local radio and television. The message should take into account demographic factors such as a community's average age and education level, as well as existing levels of familiarity with information about nuclear and radiological threats. Communication may need to occur on two (or more) levels to inform both those among the previously interested public and those beginning with little or no knowledge of the issues. For example, those who live near a nuclear power plant are more likely to have encountered information about nuclear risk than those who do not, and may require a different approach or a different level of explanation.

Workshop participants from the emergency preparedness sector and the media emphasized the need for honesty and candor in dealing with the public. Consequences and probabilities need to be explained and honestly discussed for members of the public to be able to draw meaningful distinctions between the dangers posed by various types of attack. A nuclear explosion would be an event of catastrophic proportions and, therefore, clearly deserves attention. At the same time, discussion of the consequences of an RDD attack is equally necessary, given the far higher likelihood of an occurrence and the widespread overestimation of the consequences for public health and safety.

Public communication about the terrorist threat should also include concrete steps the public can take to prepare for or mitigate harm from a terrorist attack, including information about segments of the population who are particularly vulnerable (e.g., young children). One lesson from the "civil defense era" of the 1950s and 1960s is that members of the public welcome opportunities to control risk within their immediate environments. Activities to protect against a nuclear exchange between the United States and the Soviet Union, such as holding duck-and-cover exercises and retention drills, building basement bomb shelters, and stockpiling food, although somewhat naive in retrospect, gave people a sense of participation and agency in the face of a serious threat. Moreover, there is a natural coupling between public education about individual-level risk-control measures and educating the public about more general risks and dangers, as well as the emergency response measures in place at the local, state, and national level to help manage those risks and dangers.

At the community level, information should be unambiguous and tailored to the locality. Evacuation areas and procedures should be identified and publicized. If public shelters are provided, people need to be advised where they are, how they can be accessed, and which services and provisions will be available. People residing within evacuation intake areas need to be told what to expect and be encouraged to participate in emergency response and evacuation drills to increase the general level of familiarity with the procedures and to help identify

unforeseen complications.[48] When responding to a particular, ongoing emergency, communication should start early and be continuous. Initial messages need to be specific, clear, and simple. Information about who should evacuate, where to, and why is extremely important.[49] Once people scatter, it may be impossible to ensure that important information reaches those for whom it is intended.[50]

b. Credibility

A threshold condition of effective risk communication is finding a "credible communicator"—an organization (or individual) with appropriate expertise that will be believed and trusted by the public. The public stigma associated with anything "nuclear" is difficult to overcome in many contexts, as is skepticism toward experts who argue that radioactive substances may less dangerous than is commonly supposed.[51] From the perspective of a nonspecialist member of the public, it is difficult to know whom to trust, particularly where opinions differ among trained specialists within and between the government and the private sector.[52] Both business and government agencies have frequently adopted the "DAD" (decide, announce, and defend) approach to public communication about nuclear and radiological issues. Where public discussion is suppressed and evidence of flawed decision-making later emerges, as unfortunately has been the case in several instances related to nuclear safety, the damage to the future credibility of the organizations involved can be enormous and of long duration. An unfortunate consequence of this history is that, at present, those entities and individuals most centrally involved in and therefore most knowledgeable about nuclear issues frequently are perceived as having little credibility among the general public.

In the opinion of several workshop participants, neither the Department of Energy nor the Nuclear Regulatory Commission is likely to be perceived as a credible source of information due to their presumed "pro-nuclear" interest—especially information that downplays the threats posed by nuclear and radiological terrorism. The National Research Council, the National Academy of Sciences, and the Institute of Medicine were viewed as more credible candidates for delivering the message that RDD attacks involve little or no danger of widespread radiation dispersion. At present, first responders and especially firefighters have a high store of credibility among the public. During an unfolding emergency, when firemen, police, and medical emergency responders are all "singing from same page of music," the public tends to be reassured. However, first responders themselves need to have reliable information to maintain their public credibility. The many professional demands on the time and attention of first responders requires focused efforts for ensuring adequate pre-crisis training and preparation for a nuclear or radiological terrorist incident.

A source of unease among experts who do regularly engage in public education and lobbying is that, in attempting to address the concerns of different audiences, the message will become confused, and this will in turn reflect negatively upon their own authority and the credibility of their organizations. Even with identical data, different-sounding messages may be required to address varying levels of understanding and different types of fears and concerns. However, concerns about credibility vis-à-vis the public are not limited to experts and policymakers. Building and maintaining credibility is likewise an issue for those engaged in the gathering and publication of information, namely media outlets and individual journalists.

The representatives from the media at the workshop pointed out that the U.S. government and scientific experts frequently have an unworkable approach to communication about strategically sensitive issues. Experts want journalists to write stories with the message that the risks associated with nuclear terrorism are largely overstated. However, these same experts are

often unwilling to provide enough background information and detail to make that message convincing. Nuclear scientists are typically highly conscious of their roles as gatekeepers of information. When scientists transmit detailed information to decision-makers, emergency responders, the media, and the general public about the severity (or non-severity) of various threats in this sphere, the concern is that they are at the same time educating terrorists about how to conduct attacks more effectively. Hence the conundrum of the credibility deficit: where insufficient information is provided to allow for independent evaluation of a conclusion, how the message is received depends wholly upon the credibility of the source. And, as pointed out above, when the topic is nuclear and radiological issues, the government's credibility is often questioned.

However, where particular media sources are themselves considered credible, the willingness to publicize information can itself lend credibility to the underlying story. The workshop consensus was that, where journalists are knowledgeable (or at least conscientious), a useful partnership can be forged with scientific experts. It follows that developing relationships between experts and individual journalists at trustworthy media organizations would benefit those in both roles. For the expert, a relationship of trust with individual journalists willing to take the time to get the story right will create channels for more open communication, including collaboration on how to present information accurately without creating additional security risks. Journalists can benefit from "deep background" briefings on important stories from experts prior to their becoming front-page news. And, having an authoritative and accessible source of information when an attack does occur can be invaluable to a journalist working under extreme time pressures.

c. Communication under conditions of uncertainty

When a crisis occurs, policymakers and the media—unlike scientific experts—do not have the option of remaining silent. Timely responses to scientific inquiries from policymakers are important: decisions will be made early on in a crisis with or without the input of experts. However, scientific and technical experts are uncomfortable with pressure to go beyond what they know in offering authoritative opinions on an evolving situation.[53] Several workshop participants voiced the opinion that the scientific and technical community needs to be more responsive to the need for information during crises and more willing to give "best estimates" with appropriate caveats. During crises, information is inevitably incomplete and subject to change. Where personnel working in all aspects of emergency response accept this premise, communication will be facilitated and trust can be preserved.

In advance of a crisis, a tension exists between the concerns and priorities of scientists capable of recognizing the full range of technical consequences from attacks using crude and not-so-crude dispersal devices and the policymakers and first responders who must make decisions about specific resource allocations and policies. A standard source of tension between scientific experts and members of the policy and emergency response communities is that scientists operate in a world defined by estimates and probabilities. Policymakers and first responders, by contrast, are on the front line in dealing with the immediate social and political consequences of terrorist activity, and, moreover, are actively called upon to justify the choices they make.

Similarly, journalists and other members of the media are driven by deadlines. At the same time, good journalists, like good scientists, value research and accuracy. The media representatives at the workshop emphasized the importance of receiving straight talk from scientists and technicians. When experts don't have an answer, it is preferable for experts to define the

parameters of their uncertainty rather than to refuse to comment; incomplete information is helpful as long as it is placed in a constructive context that allows people to take sensible actions and to avoid panic. While acknowledging that not all members of the press adhere to the highest standards, the media representatives at the workshop underlined that the impulse at most media organizations is not to "hype," but rather to be responsible providers of information.

The view was also expressed that technical people should themselves be more skeptical about the quality of available technical data, particularly when trying to get up to speed on complex issues in the context of an emergency. For example, during the anthrax scare, off-the-shelf AMA statistics regarding anthrax exposure were relied upon to evaluate exposure risks. Upon closer examination, these data turned out to be very weak, having been derived solely from a series of small-N studies on laboratory animals. In the literature on organizations, knowledge of the range of possible outcomes (even if the particular outcome is unknown) is a standard element in the definition of "risk." By contrast, "uncertainty" means not being able to define with confidence even the range of possible outcomes. "Experts" can easily delude themselves into thinking they are operating in the realm of "risk" when they are actually in the realm of "uncertainty." Where this occurs, the danger is that experts may create "fantasy documents," lending a veneer of rationality to situations that are, in fact, not well understood.

With regard to official government sources of information, it was suggested that an appropriate goal should be to prompt the U.S. government to be as professional in communicating information about homeland security and terrorist attacks as it is in the context of war fighting. U.S. government spokespersons have become adept at giving quality briefings with a great deal of credibility while at the same time separating out information appropriate for release and information that should be withheld in order to ensure the safety and security of U.S. military personnel. And finally, the public impact of uncoordinated actions also should be taken seriously in the context of deciding upon localized responses. For example, on September 11, 2001, evacuations of government officials from New York City resulted in widespread questions about the safety of remaining in the area, contrary to public reassurances.[54]

III. Emergency Response to Nuclear or Radiological Terrorist Attack

Information about the plans and resources in place at the local, state, and national level to respond to terrorist attack involving nuclear or radiological weapons is an important component of informing the public about the probable risks and consequences of this type of attack. In the realm of response to, and recovery from, a terrorist attack, three sets of issues dominate the agenda. First, there is a need to ensure the integrity of essential systems infrastructure, including transportation systems; energy production, transmission, and distribution systems; vital utilities; and telecommunications. The second set of tasks concerns direct emergency assistance at the attack location and surrounding areas. It encompasses coordinating law enforcement, medical, and fire personnel, including temporary personnel and volunteers, and providing for their protection, as well as ensuring an adequate supply of necessary materials and facilities. A third set of issues more specific to nuclear and radiological incidents concerns the job of containment and removal of radioactive materials.[55]

Emergency response to any significant natural or manmade disaster involves multiple agencies and actors at many levels of government. Ensuring communication and coordination

among these various spheres of activity is essential to an effective response, particularly where standard emergency-response routines must mesh with more specialized activities. The following issues and ideas concerning this aspect of the response to terrorist incidents were central to the workshop discussion:

- What plans are in place at the local, state, and national levels for immediate response to a terrorist attack (or threatened attack) involving nuclear or radiological weapons?
- What kinds of special equipment and training do first responders require in order to deal with a terrorist attack using nuclear or radiological weapons in order to minimize risk to themselves and their communities?
- How can information be most effectively managed during a terrorist crisis to ensure appropriate coordination among responding agencies, and to reassure the public?

A comprehensive approach to informing the public about emergency-response plans for a nuclear terrorist attack requires attention to at least four distinct threat contexts: an actual terrorist attack, an emergency of possible terrorist origin, a specific threat of terrorist action, and a generalized threat of terrorist activities involving nuclear or radiological weapons. These four contexts vary according to the certainty and specificity of the threat and the time horizons in which action must be taken. In each of these four contexts the key question is: what do first responders and the public need to know, and how will that information be communicated?

The first, and most extreme, situation is a terrorist attack using nuclear or radiological weapons that occurs with no advanced warning. Under these conditions, information about the attack and its probable consequences is likely to be largely reactive. Broadcast and electronic media outlets are expected to be the primary initial purveyors of information, the quality and effectiveness of which will depend heavily upon the degree of advanced training and preparation received by spokespeople, journalists, and the public at large. The ability of first responders, officials, and their spokespeople to accurately assess—and credibly communicate—the *actual* level of threat will be key to avoiding public panic.

Moving down the scale, the second general context is an actual catastrophic incident where there is uncertainty about whether the cause is a terrorist attack or merely an accident (e.g., a plane crash or an incident at a nuclear power facility).[56] Knowing whether the incident is an attack, an accident, or a natural disaster is essential to determining the proper response repertoires for law enforcement and first responders at all levels. The need for accurate assessment is particularly acute with nuclear, chemical, or biological attacks where specialized equipment may be required to enter the affected site safely. An accident or a disaster caused by natural means has a small probability of prompt reoccurrence. However, in an incident caused by a calculating enemy, the possibility exists of "layered" attacks, or that "booby traps" may have been set for emergency responders. First responders are not, in general, trained to take such factors into account. The time frame for determining what types of information to communicate to the public is similarly compressed in this context.

The third context is where authorities have received specific threat information or uncovered specific plans for a terrorist attack. In this situation, issues of misinformation, credibility, and decision pressures under time constraints and incomplete information collide forcefully in the debate over the propriety of releasing warnings of specific threats of attack to the public. In making this determination, policymakers, experts, first responders, and members of the

media must balance the credibility of the threat to public security with the costs of the anticipated public reaction. Issuing a specific threat warning, particularly concerning a possible nuclear or radiological terrorist attack, is certain to result in some level of significant economic and social disruption. Consequently, policymakers and experts who go public with such warnings may set themselves up for intense criticism if the threat does not materialize. Moreover, too many false alarms will heighten the level of security risk insofar as public attention and patience are resources that can be depleted by a perceived lack of credibility or a scarcity of information about the threats being communicated. At the same time, the hazards of *not* communicating specific threat warnings to the public are considerable: a forgone opportunity to evacuate a specific threat target site, thereby preventing loss of life and property, is a public official's nightmare.

The fourth and least time-sensitive context is a "general threat" situation in which risk analysts and other experts estimate that an attack of some kind is probable, but no specific targets, timetables, or attackers have been identified. As underlined in the previous section, the main challenge in this area is to find ways to focus public attention on the real dimensions of the threat and to prepare communities for the full range of probabilities—without simultaneously educating terrorists about technical issues or pointing out vulnerabilities in security provisions and response plans.

A. Plans for Coordinated Response

The U.S. federal government has developed a comprehensive Concept of Operations (CONPLAN) for responding to potential and actual terrorist threats and acts on United States territory, including nuclear and radiological terrorism.[57] The purpose of the plan is to provide guidance to local, state, and federal agencies regarding how the federal government "would respond to a potential or actual terrorist threat or incident" on U.S. territory, and in particular those involving weapons of mass destruction. The plan sets up a structure for "systematic, coordinated, and effective national response to acts of terrorism in the United States."[58] The CONPLAN defines procedures for state and local officials to access and use a broad range of federal agencies and sources of funding to supplement their own emergency response resources, and, where necessary, provides specialized services and support operations available only at the federal level.

The CONPLAN is intended to facilitate effective coordination between the "crisis management" and "consequence management" functions of response to a terrorist incident, without superseding existing plans and procedures in the various departments and agencies of the federal government. Crisis management involves primarily law enforcement tasks—identification of the source and means of attack in order to anticipate, prevent, or resolve further threats or acts of terrorism.[59] By contrast, consequence management is geared toward protecting public health and safety, restoring essential government services, and providing emergency relief to governments, businesses, and individuals affected by the consequences of terrorism.[60] Both crisis management and consequence management operate simultaneously within the plan, with consequence management initially subordinated to the tasks of crisis management. As the emergency subsides crisis management is gradually phased out and consequence management assumes the lead coordinating role.

1. Crisis Management

Crisis management encompasses not only traditional law enforcement tasks, including intelligence, surveillance, investigation, tactical operations, negotiations, and forensics, but also more specialized techniques for identification, neutralization, and disposal of the hardware employed in the attack or threatened attack. The FBI is specified as the lead federal agency in the "crisis management" phase pursuant to the federal government's responsibility under U.S. law to respond to and prevent terrorist activities against the United States. As the lead agency during the initial phase of response, the FBI assumes primary responsibility for determining what steps are needed to best ensure public health and safety.

The crisis management phase of response to a terrorist incident involving a weapon of mass destruction (WMD) is triggered by notification of a problem from officials at the local level. The FBI first verifies the information and conducts an initial threat credibility assessment. At the same time, state and federal agencies, including the national laboratories, are placed on notice of the situation for the purpose of "triage"—detailed analysis and feedback between local first responders and specialists to determine the scope and character of the threat or attack. The Federal Emergency Management Agency (FEMA) is also notified immediately in order to begin coordination of consequence management.

Following an initial determination that a reported incident or threat of nuclear or radiological terrorism is credible, the FBI will establish a Joint Operations Center (JOC) in the nearest field office to coordinate further activities and to provide ongoing assessment of the threat's credibility. The JOC will coordinate with the Strategic Information and Operations Center (SIOC), which is located at FBI headquarters in Washington, D.C. If required, the FBI may request the support of the Department of Defense or the Department of Energy through the attorney general and the president. In situations of extreme emergency, the secretary of defense may also be given direct tactical response authority from the president for use of force to destroy or neutralize an immediate threat. Once the threat is neutralized, the Department of Energy and the National Nuclear Security Administration (NNSA) are tasked with making the device safe for transportation and disposal and coordinating recovery and cleanup. As part of this phase, a Special Operations Task Force will be created to control the physical space surrounding the site of the threat or attack until the threat is resolved and control is passed to the agencies involved in consequence management.

The federal government offers a range of scientific and technical capacities in a terrorist crisis involving nuclear or radiological weapons. The NNSA through its three laboratories, production facilities, and test sites has a sophisticated scientific and technological base for analyzing risks associated with radiological incidents.[61] The agency is attempting to define its role in plans for counterterrorism and homeland defense and to increase the availability of scientific, technological, and laboratory expertise for operational support during crises. For example, the atmospheric release analysis capability at the Lawrence Livermore National Laboratory can identify and track radioactive plumes, predict their paths and how they will fall out, and also seek out hot spots by combining sophisticated models with real-time on-scene data. These resources can be used to direct responses in real time, even at the city level.[62] This agency has also developed highly specialized resources for emergency response to nuclear or radiological incidents, including the Nuclear Emergency Search Team (NEST). The NRC and the U.S. military are also active in this area.

During the crisis management phase, first responders are required to treat the site of the incident as a crime scene. This means they must coordinate their actions with appropriate law enforcement and conduct all consequence management activities with care toward preserving

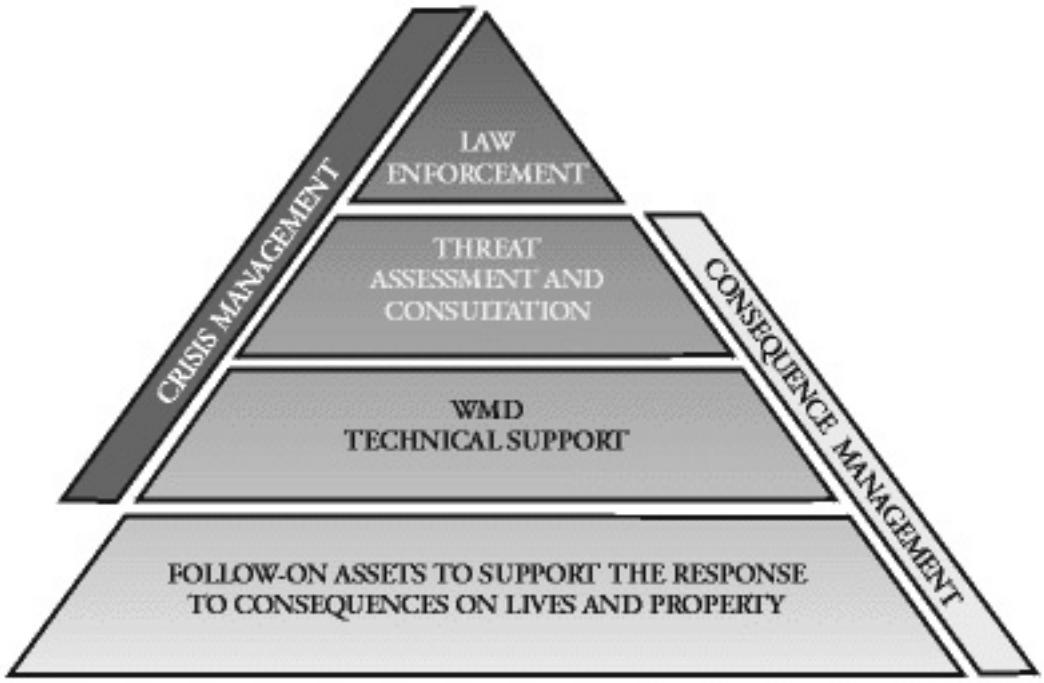


Figure 5. Relationship between Crisis Management and Consequence Management[63]

evidence.[64] Where there is uncertainty as to whether an incident is an accident or the result of a terrorist or criminal act, the standard procedure is to undertake tasks according to the more restrictive procedures until a determination is made.

2. Consequence Management

The consequence-management phase of response to a terrorist attack against U.S. territory using nuclear or radiological weapons would proceed according to the general Federal Response Plan for managing emergencies and disasters of all kinds. The Federal Response Plan currently includes twelve basic emergency support functions for terrorism and natural disasters. Under the CONPLAN, FEMA serves as the lead agency for the consequence-management phase, in coordination and consultation with state and local authorities.[65] In the event of a terrorist attack, FEMA would immediately dispatch a "Forward Command Team" to provide direct and timely federal expertise to the onsite incident commander regarding available federal resources.[66] Each Forward Command Team comprises a state official and a federal official knowledgeable about resources for the given emergency who are granted authority to expedite access to those resources throughout the federal system. In addition, a lead federal agency is designated for each of the twelve emergency support functions. For example, the EPA is the lead agency for emergencies involving hazardous materials, with other federal agencies tasked in supporting roles. FEMA may also assist with media coordination, together with local and state officials and the FBI.[67]

Planning for emergency response to a nuclear or radiological terrorist attack is also ongoing in California at the level of counties and operational areas as part of SEMS, the Standardized Emergency Management System. This system includes procedures for requesting assistance and resources at the local level from state and national sources (e.g., FEMA or National Guard assistance), and for requesting that the governor declare a "state of emergency" in the affected areas. The plan for the city of San Jose, for example, provides for a citywide emergency response center to be immediately activated in the event of an attack to be staffed by law enforcement, fire, medical, and public works personnel. Requests for resources will be coordinated through the County/Operational Area Emergency Operations Center.

In the event of a major nuclear terrorist incident, the probability is high that local government and administrative functions at the attack location would cease to function. Consequently, California emergency response plans include provisions for the county or state to step in to provide continuity of governance. Similarly, contingency plans include backups for key federal programs (such as FEMA) from other regions, in the event an attack destroys the ability of the local office to perform its functions. Even if being managed from another geographic location, local actors will still be able to quickly plug into the coordinated nationwide response system in a familiar way.

B. Local Responders: Police, Fire, and Emergency Medical Personnel

In 2001 the U.S. federal government spent $11.7 billion on homeland defense. Another 33.7 billion dollars have been proposed for the 2003 budget.[68] Of this amount, $3.5 billion is earmarked for the training and equipping of first response and emergency personnel. One issue of immense importance for effective response to acts of nuclear and radiological terrorism is to ensure that the necessary safety and detection equipment is available when and where it is needed, and that police, fire, and medical personnel are trained to use it. Without tools to accurately assess a situation and decide upon an appropriate response, first responders risk exposing themselves and others to unnecessary danger. Where first responders use radiation detection equipment in responding to emergencies, there is a strong probability of discovering the presence of abnormally high radiation levels early on.[69] One means for increasing the prospect for this equipment to become part of standard emergency-response routines (instead of gathering dust in an equipment closet) is to design "dual-use" equipment that will be brought along to incidents and used as a matter of course.

A difficult aspect of training for response to a terrorist attack in which a nuclear device is successfully detonated is impressing upon first responders the reality that most of the victims close to the event will die. First responders need to be able to differentiate between those who are savable and those who are not, and to refrain from taking undue risks on behalf of individual victims. It is well documented that most of the direct victims of radiation disasters, for example the 1986 incident at the Chernobyl nuclear power plant in Ukraine, have been the emergency responders who were first on the scene.

Emergency medical response is an important aspect of consequence management. Under plans currently in place in California cities, triage and treatment of attack victims could begin almost immediately following an attack at a safe, but relatively proximate, location. A mutual aid system for medical response has been developed for fire departments across California to provide resources and assistance to affected jurisdictions. EMS resources and hospitals across the state are similarly coordinated in order to send patients to available beds in undamaged communities. At the federal level, the National Disaster Medical System coordinates resources

and patient placement in available beds throughout the United States. Finally, FEMA also coordinates Disaster Medical Assistance Teams, which include mobile surgical units for transport to disaster areas.

Safety and communications are the two primary concerns of emergency medical personnel during the implementation of disaster-response plans. Emergency medical personnel need to be informed about the character of the risks that victims have been exposed to—both to treat victims effectively and to ensure their own safety and the safety of other patients.[70] To ensure that medical personnel remain focused on delivering needed care in a nuclear or radiological event, they need active assurance that proper decontamination has occurred in the field before patients are transported to, or allowed to enter, treatment facilities. Accidental emergency-room contamination from "walk-in" patients can force the closure of hospital facilities and disrupt the care and transport of other patients.

Emergency medical personnel require input from local, state, and federal authorities about how the situation is developing in order to be able to allocate staff and resources effectively. Mechanisms for communications between medical personnel and the families of the victims seeking treatment is important, as is any information regarding the well-being of the families of medical staff who are otherwise fully engaged in care of victims. And finally, to the degree that emergency physicians will be required to communicate to the press, they need to be kept informed by others in the field to be able to make appropriate statements and to communicate information necessary for public safety.

It follows that proper training of first responders and medical personnel *in advance* of a nuclear or radiological emergency is essential.[71] Most training of first-responders, particularly at the local level, is based upon past experiences with natural disasters, and does not include planning for a "thinking" enemy that may intentionally attempt to disable or disrupt emergency-response services. In anticipation of this possibility, cities have started planning for multiple backups, including locations for an emergency-operations center, and placing renewed emphasis on training emergency personnel to anticipate booby traps and "secondary devices." To expect that all first responders at the local level be fluent in the character of threat posed by all possible manners of terrorist attack is clearly too great a demand, given the relatively small likelihood of attack in most locations. Far more realistic is the goal of making available to the first responder community up-to-date, authoritative information that can be easily accessed when a particular type of incident does arise. The workshop consensus was that it is important not only to generate the necessary information, but also to periodically remind first responders and the public that this information is available.

C. Information Management

Managing information during a terrorist emergency is an enormous challenge commensurate with the more technical tasks of emergency response.[72] All comprehensive emergency-response plans include elements for passing information on to members of the print and electronic media. As noted above, a symbiotic relationship exists between public officials and the media during emergencies. Public officials have an interest in supporting the media—to help journalists get good stories and pictures, and to facilitate transmission of accurate information. But, public officials are also fearful of media where coverage focuses on the mistakes of competent, well-intentioned people without proportionate coverage of systems and procedures that function as planned. This fear can, in turn, be interpreted as official secretiveness, or even dishonesty.

During a crisis stemming from a terrorist attack, governments typically wish to communicate a message reassuring the public about what is being done to respond to and alleviate the threat. At the same time, terrorists have an agenda for which they are seeking exposure, and the media can unwittingly play a role in fulfilling that agenda to the detriment of their own and the government's credibility. In seeking explanations for why an attack has occurred, members of the local and national media publicize the aims and objectives of an attack. The media can unintentionally assist terrorist organizations in other ways as well. Terrorists seek information from the media for use in planning better attacks. They can, for example, glean information on the movement of radioactive plumes, the exposure of weak points in response systems, and how much public pressure is being placed on public officials. Consequently, governments dealing with an unfolding emergency will frequently attempt to seek cooperation and restraint from members of the media.[73]

Standard emergency-response procedures in the United States call for establishment of a Joint Operations Center (JOC) among local government, FBI, and FEMA to facilitate the authoritative transmission of information and the coordination of emergency response between state and local officials and federal agencies.[74] Within the JOC, a Joint Information Center (JIC) is specially tasked with managing communications with the media and the public.[75] JICs begin life as city-level emergency-information centers. Typically, the mayor's public information officer (PIO) and the city PIO will be the initial spokespeople, backed by a team trained in marketing and public-information production whose job it is to work with the public and the media. Information is collected in coordination with field public-information officers (fire, police) who are also specially trained in public disaster communications. The group monitors the media to determine what information is needed when, to control rumors, and to troubleshoot for unbalanced or incomplete reporting. JICs also coordinate press information, arrange press conferences, and, where necessary, disseminate information and materials directly to residents.

Local emergency response coordinators at the workshop expressed frustration over the perceived lack of respect for the purpose and value of JICs and the tendency of some reporters to avoid coordinated media centers altogether in favor of "independent sources." From the perspective of officials attempting to manage the public response to a terrorist incident, a single, authoritative message regarding the scope and status of the threat is necessary to avoid widespread disinformation and panic. However, the media representatives at the workshop emphasized that when journalists operate outside the JIC, it is not always to seek flashier headlines. Rather the objective is frequently to seek more specialized information, or to verify independently the message being communicated from the top down in order to maintain credibility among the public. One concrete step proposed at the workshop for increasing the level of independent media participation in JICs was to institute more interactive briefing sessions where journalists are able to ask questions of spokespersons and officials, rather than relying upon a standard press-release format.

The possibility that terrorists could launch a concerted media campaign of disinformation as part of a terrorist attack should be anticipated as part of an information-management strategy. Deliberate disinformation, like well-intentioned conflicting information (or misinformation), can disrupt emergency-response activities and undermine the sense among the public that the situation is being well managed, irrespective of the actual performance of public officials and first responders. Establishing mechanisms for journalists to verify information specific to nuclear and radiological terrorist threats with scientific experts and public officials before it is publicized will minimize the chance that members of the media will unwittingly

contribute to a climate of chaos and disruption. For example, mechanisms need to be in place for journalists to verify source information—e.g., to ensure that the phone call from "the FBI" is really from the FBI, or the press release faxed on Department of Energy stationery is really from the DOE.

Educating the public about the risks and realities of nuclear terrorism in advance of an attack is an important component of crisis management. Giving members of the public sound, accurate information for response to terrorist attacks before they occur will reduce the need to rely on information generated in the immediate aftermath of an attack, which may be unreliable and contradictory. Decreasing the incidence of overreaction among members of the public will, in turn, serve to minimize the longer-term economic and societal impact of a nuclear or radiological terrorist attack.

IV. Future Steps

The workshop on Communicating Nuclear Risk generated concrete proposals for beginning immediately to correct for known gaps in public information on nuclear and radiological issues of importance in responding to a nuclear or radiological terrorist attack. Other proposals were generated for beginning to resolve some of the tensions identified in the workshop discussion between various roles, and in particular between the media and scientific experts.

- Briefings for newspaper editorial boards and media umbrella organizations, such as the California Newspaper Publishes Association, the Associated Press Managing Editors Association, and the American Association for the Advancement of Science, on issues of nuclear and radiological terrorism. These briefings could take place at individual media outlets and at annual national media conferences.

- Media participation in field training exercises and scenarios for nuclear and radiological emergency-response organizations on "background only" terms. This participation can both impart information regarding the details of specialized emergency-response procedures and provide an opportunity for scientific experts and members of the media to forge cooperative relationships at an individual level.

- Compilation of a comprehensive fact sheet for journalists reporting on nuclear and radiological terrorist incidents encompassing information such as critical dose levels, combined with a list of experts in relevant fields to call on for information.

- Advance preparation of media graphics concerning particular types of nuclear or radiological terrorist incidents that can be fine-tuned for actual crises. Each media outlet can then supplement the format with more specific local information about what individual members of the public should do and whom they should call.

The Center for International Security and Cooperation (CISAC) at Stanford University has already undertaken the task of preparing the proposed media fact sheet in consultation with local emergency response coordinators and experts at Livermore National Laboratory.

Notes

[1] First responders include police, fire, medical, and other emergency personnel who would be involved in the immediate response to a terrorist incident.

[2] For the purpose of this discussion, "terrorism" is defined as any conduct by a non-state actor or organization that intentionally targets civilians (noncombatants).

[3] Currently, Los Angeles and San Francisco have approximately 250 beds each for burn victims.

[4] Fallout is the dispersion of radioactive downwind of radioactive materials following a nuclear explosion. Rainout is rain washing radioactive materials from the atmosphere onto the ground.

[5] A nuclear explosion creates quantities of "fission products" that are much more radioactive than the plutonium and uranium from which nuclear weapons are constructed. "Radioactivity" refers to the rate at which a given material emits radioactive particles and is inversely proportional to the "half-life" of the material (the period required for a material's radioactivity to decrease by half through decay). Weapons-grade plutonium (Pu-239) has a 25,000-year half-life and U-235, the main component of HEU used in nuclear weapons, has a half-life of hundreds of thousands of years. By contrast the fission products from a nuclear blast have half-lives ranging from fractions of seconds to several years.

[6] Nuclear fission occurs when the nucleus of an atom is split, thereby releasing energy and emitting additional neutrons. A "chain reaction" occurs when the neutrons produced from the initial splitting cause other, nearby nuclei to split and to sustain the reaction until the fissionable material is consumed or dispersed.

[7] Note that a nuclear "fizzle" would still be a potentially serious event with local catastrophic effects. People in the immediate blast area would die, and fallout could be a factor within a 1–2 mile radius.

[8] Unfortunately, neither program has proceeded as quickly as envisioned, and each would benefit from added priority and funding. The members of the G-8 recently pledged several billion dollars to initiatives to reduce the chance that nuclear weapons materials (or nuclear weapons) could be acquired for terrorist uses. Fulfilling this pledge would greatly assist ongoing U.S. efforts in this area.

[9] Established nuclear weapons states equip their weapons with layered security devices designed to protect against unauthorized use (e.g., coded electronic locking devices called "permissive action links," or PALS). The possible absence of these types of safeguards in other nuclear states is a source of concern from the standpoint of proliferation.

[10] Note that linear accelerators are an alternative to cobalt-60 sources; these contain very little radioactive material and, like x-ray machines, are radioactive only when in use.

[11] In the United States, there are 103 operative nuclear power plants licensed by the NRC. There are also between 15 and 20 nonoperative nuclear power plans in various stages of decommissioning. A small number of these facilities still contain radioactive material. See Nuclear Regulatory Commission *Information Digest* 2000.

[12] Damage to a reactor's cooling system is a point of concern since draining the pools would cause the temperature to rise and the zirconium cladding to melt, resulting in dispersal of highly radioactive substances, such as Cs-137.

[13] Most modern reactors would likely withstand the impact of a medium-sized commercial jet (or its explosive equivalent), but the impact of a large modern jet has not at this point been fully evaluated.

[14] See Bill Keller, "Nuclear Nightmares," *New York Times Magazine*, May 26, 2002, p. 57; Douglas M. Chapin, Karl P. Cohen, W. Kenneth Davis, Edwin E. Kintner, Leonard J. Koch, John W. Landis, Milton Levenson, I. Harry Mandil, Zack T. Pate, Theodore Rockwell, Alan Schriesheim, John W. Simpson, Alexander Squire, Chauncey Starr, Henry E. Stone, John J. Taylor, Neil E. Todreas, Bertram Wolfe, and Edwin L. Zebroski, "Nuclear Safety: Nuclear Power Plants and Their Fuel As Terrorist Targets," *Science*, 20 September 2002, 1997–1999.

[15] For example, critics frequently cite low performance in force-on-force security tests carried out as part of each plant's ongoing security appraisal as evidence of an unacceptable level of vulnerability. However, this line of criticism fails to take into account that force-on-force tests are training exercises for personnel as much as assessments of plant security, and therefore also occasions for improving plant security.

[16] The United States alone stores roughly 40,000 tons of highly radioactive spent nuclear fuel. See *International Energy Outlook* 2002, http://www.eia.doe.gov/oiaf/ieo/pdf/nuclear.pdf.

[17] Even leaving aside the difficulties of attaining access, stealing spent fuel would require highly specialized equipment, including large, heavily shielded trucks for transport, and the participation of a crew of experienced people in order to avoid lethal exposures and offsite detection.

[18] These sources are typically located in massive buildings; the material to be irradiated enters into a labyrinth on a conveyor to avoid direct radiation paths to the outside. Radiation sources are housed under massive shielding (often under water pools). Exposure is often achieved remotely by raising the source out of the pool and resubmerging.

[19] See Abel J. Gonzalez, "Security of Radioactive Sources: The Evolving New International Dimensions," *IAEA Bulletin* 43, no. 4 (2001).

[20] Radiotherapy for the irradiation of tumors includes both teletherapy (exposure from a source beamed from outside the body) and brachytheraphy (actual contact between the radioactive source and the affected tissue). In the United States, most external radiation therapy is undertaken with medical linear accelerators that contain no radioactive material. In much of the rest of the world, however, cobalt-60 sources are still regularly used in radiation oncology.

[21] The IAEA reports that, as of 1997, there were 53 research reactors operative at universities and other sites around the United States. See "Research Reactors in the World" on the organization's website, www.iaea.org/worldatom/rrdb.

[22] For example, NRC regulations do not ask that research reactors be protected against attack by truck bombers as is the case with power reactors.

[23] Most sources of radioactivity that might be attractive to terrorists (e.g., x-ray sources) have penetrating radiation and are readily detectable where appropriate detection instruments are available.

[24] A typical large 9,000-curie cesium-137 source is contained within a protective drum weighing approximately three tons.

[25] Radiation safety issues are generally not assumed to pose an insurmountable obstacle to terrorist groups, since individuals involved in such activities may be willing to expose themselves to levels of radiation that would be unacceptable to technicians and researchers work-

ing in laboratories in the United States. However, there are limits to the "effectiveness" of an individual's willingness to sacrifice his own life, and to his ability to function while ill in order to handle these materials. Many highly radioactive materials (such as those used in the most dangerous class of RDD devices) would deliver lethal doses of radiation to handlers before the device could be deployed.

[26] Neither plutonium nor uranium (including weapons-grade plutonium and HEU) would be effective if used in an RDD due to their low radioactivity. Uranium-238, the main component of natural and depleted uranium, has a half-life measured in billions of years, making this material only mildly radioactive. In fact, depleted uranium is commonly used as shielding material for other radiation sources. Uranium-235, the main component of HEU, has a similarly long half-life, and plutonium–239 has a half-life of 20,000 years. Many radiation sources used for medical and industrial purposes have considerably smaller half-lives, and therefore present far greater dangers for short-term exposure and contamination. The most likely materials for use in "dirty bombs" have half-lives in the range of tens to hundreds of years. Other materials with medical and industrial uses are still more radioactive, such as iodine-131 with a half-life of one week, but are less likely to be employed in a terrorist attack precisely because of the short duration of their usability.

[27] In general terms, a "dose" of radiation is the energy (measured in ergs or joules) that is absorbed from radiation per unit mass of tissue. A "biologically effective dose" or "dose equivalent" (measured in "rem" or "sieverts") refers to "the biological damage to living tissue from radiation exposure." Radiation exposure (or dose) can result from either external sources (being near a source of radiation) or from contamination (from ingesting radioactive material, or surface contamination). The probable health consequences likely to follow from a terrorist attack using an RDD are frequently discussed in terms of a "committed dose," which is the lifetime dose expected to result from intake (e.g., by means of ingestion or inhalation) of radioactive material (see discussion in section I(B) below). See "Glossary," Low Dose Radiation Research Program, http://lowdose.tricity.wsu.edu/glossary.htm and the "IAEA Glossary" available at http://www.iaea.or.at/ns/CoordiNet/safetypubs/iaeaglossary/glossarypages/glossaryindex.htm.

[28] Stated differently, the increased cancer risk associated with this quick, low dose would be approximately the same as that from smoking a single cigarette.

[29] Decontamination of buildings and other structures is more complicated and more costly than for open spaces. Cleanup costs and the standards applied are likely to vary with the terrain of the contaminated region and its intended future use. Studies conducted by several agencies have found a "kink" in the cost-benefit curve at approximately the 15–25 mrem per year, beyond which the incremental costs for cleanup begin to rise steeply. In all cases, the level of proposed standards on the table for discussion involve small doses—lower than the U.S. average annual background exposure (roughly on the order of getting a dental x-ray once a year).

[30] A typical source for testing welds contains a 100 mCi cobalt-60 source roughly one-half inch in diameter and less than an inch high weighing 40 to 50 pounds, most of which is shielding. A typical large source containing 10–20 curies weighs over 300 pounds, again mostly shielding.

[31] The radiation sources contained in these devices are typically housed in double-welded, double-sealed, stainless steel canisters capable of withstanding a considerable blast.

[32] The Environmental Protection Agency defines an orphaned source·as a discrete source of radioactive material that falls into one of four categories. A radioactive source is considered orphaned·if it is in the possession of an unlicensed entity, a licensee not authorized for the material, or a licensee with doubtful abilities to maintain the necessary security over the source (e.g., a bankrupt licensee). A fourth category comprises radioactive sources that have been abandoned or for which there is no legal disposal option. See Neil Naraine and John M. Karhnak, *The New Orphaned Radioactive Sources Program in the United States*,·at http://www.epa.gov/radiation/cleanmetals/docs/dijon_pa.pdf.

[33] A "safe" stand-off distance for radiological exposure will vary according the type of source, but is generally on the order of tens of meters.

[34] The symptoms associated with radiation sickness may be evoked by a multitude of bacterial, viral, and toxic agents. Their nonspecificity suggests that such symptoms may be erroneously attributed to radiation exposure where none has occurred.

[35] Rain-out and other factors change doses considerably with respect to migration, soil absorption, and drainage.

[36] Note, however, that researchers tracking the health effects caused by the Chernobyl reactor incident have found "no consistent attributable increase" in the rate of leukemia or in the occurrence of tumors among members of the general population in the areas surrounding the site. One exception to this trend was a marked increase in thyroid cancer among children who were under 5 years old at the time of the accident. Frances E. Winslow, "WMD/NBC: Lessons Learned from Three Mile Island and Chernobyl Reactor Incidents," citing Malcolm J. Crick, "The International Conference One Decade after Chernobyl: Summing Up the Consequences of the Accident," see http://www.iaea.or.at/worldatom/Periodicals/Bulletin/Bull383/box1.html.

[37] Flight attendants and other airline workers may be an interesting research group for the study of low-dose radiation effects. They constitute a fixed population, their times of exposure are meticulously recorded in flight records, and the average dosage per hour of flight is known. Naturally, risks for flight personnel may also be complicated by other risk sources, such as smoking.

[38] Radiation is part of everyday life. The average annual cumulative individual exposure from all sources is 300 mrem per year, including an average U.S. "background dose" of radiation ranging from 50 mrem to 90 mrem per year. The difference between background exposure and total exposure is attributable mainly to medical exposures, as well as air travel and exposure to radon from building materials.

[39] See explanation in footnote 26 above.

[40] The biological half-life of the material ingested is calculated, together with the amount, to yield a total expected dose.

[41] Alpha sources, for example those contained in sources such as smoke detectors, can travel only a few inches in the air and are dangerous only if inhaled into the lungs. Most alpha emitters are not biologically active, meaning they are quickly expelled from the body. By contrast, "gamma" sources, those contained in weapons and reactor materials, are far more penetrating than either alpha or beta sources, and, moreover, are biologically active and may require decades to expel.

[42] Universities and private organizations have issued helpful material regarding, for example, communicating earthquake risks. The Public Entity Risk Institute has a website with useful materials available, including "Risk Identification and Analysis: A Guide for Small Public

Entities" and "Community Response to the Threat of Terrorism." Materials are widely available to help local communities be good partners in any response. See http://www.riskinstitute.org/ptr.asp#.

[43] Panic is different from fear, which is a rational response that may lead to unreasoned actions. People with little understanding of scientific or technical matters are more inclined to panic, given lack of basis for a reasoned response. There was no mass panic in New York City on September 11, 2001, none in California following the 1989 Loma Prieta earthquake, and none in London during the World War II blitz.

[44] Among the general public, there is little understanding of probability. For example, the U.S. Geological Survey has long predicted a 70 percent chance of a 6.7 magnitude earthquake within the next thirty years in the San Francisco Bay Area. To many readers, however, this information is interpreted as meaning such a quake *won't happen for 30 years.*

[45] For example, the topic of radiological events frequently triggers associations with the accident at Chernobyl.

[46] One suggestion as to how to keep information in front of the public in a meaningful way is through relationships with credible news organizations that are able to delve more deeply into a story and to pursue stories over time in order to document progress and changes in technology and response plans.

[47] When a significant story breaks, the radio news is usually first on the scene, followed closely by information on the Internet. The next wave of exposure is typically television coverage from cable news sources (CNN, MSNBC) and the local news. Finally, in events of significance, many of the most talented journalists from the print media also will converge to cover the story in more depth.

[48] Plans save lives. One reason so few people died in transit areas of the World Trade Center is a plan in place that directed transit authority personnel to shove everybody onto a train and send them uptown in the event something went wrong on the surface.

[49] The 1979 reactor incident at Three-Mile Island serves today as a lesson in how *not* to manage a nuclear emergency. The individuals chosen as spokespeople had little understanding of the scope of the event or how to frame appropriate public directives. As a result, there were unnecessary evacuations in areas as far-flung as Maryland and New York, galvanized by a general sense of panic.

[50] For example, in the aftermath of an attack, medical experts will issue guidance regarding which health symptoms to monitor closely and what steps should be taken to minimize harm to those affected. Police and fire personnel need to be able to notify evacuated residents when it is safe to return to their homes.

[51] Plutonium, while certainly not benign, is far less toxic and far less available than many other substances, yet the public fear associated with plutonium is enormous.

[52] Since the 1960s, public trust in scientific expertise has eroded, particularly with regard to government sources. Replacing the presumption of trustworthiness among nuclear scientists is a presumption of incompetence and hidden agendas. Risk analysis is frequently associated with efforts to lend a scientific veneer to corporate efforts to roll back environmental and safety standards. In policy-making roles, the tendency is to use scientists as "intellectual mercenaries" employed to legitimize particular policy proposals.

[53] Many people in the technology world mistrust the media and are reluctant to talk to journalists out of fear that their opinions will be misrepresented or that by offering an opinion they open themselves to future criticism.

[54] Similarly, in Washington, D.C., the Department of Energy placed cement barriers in front of a road running underneath the Forrestal Building. This act sent a tremendous signal around the city and led to a confrontation with the mayor.

[55] In this sphere, state and local governments exercise *primary authority* to respond to the consequences of terrorism, and the federal government acts in support of state and local efforts as required.

[56] For its part, the federal government, and some local governments, already have experience with low-level radiological dispersal incidents—including reactor accidents and B-52s that have crashed with nuclear weapons on board—although none of these incidents have involved RDDs.

[57] The federal "CONPLAN" plan is the implementation of PDD 39, which commits the federal government to support local actors in their response to such emergencies. See http://www.fema.gov/rrr/conplan/conpln4.shtm.

[58] CONPLAN, January 2001, II(C).

[59] The federal government exercises primary authority for prosecuting offenders. State and local governments provide assistance as required.

[60] CONPLAN II(D)(2).

[61] The NNSA mission encompasses oversight of the U.S. nuclear weapons complex, together with developing and safeguarding the U.S. stockpile of weapons. The NNSA is also charged with handling nonproliferation issues and control over materials.

[62] These resources are becoming web-based so that cities may work with the laboratories to develop models tailored to local meteorological conditions, the designs of buildings, and other relevant factors.

[63] Figure TI-1 from Federal Response Plan Terrorism Incident Annex, http://www.fema.gov/rrr/frp/frpfigt1.shtm. Permission to reproduce granted by FEMA Public Affairs Office.

[64] The exact response to a given incident depends to a degree on the likelihood the event is benign. For example, explosions have a high probability of turning out to be accidents; by contrast, an outbreak of smallpox is probably not benign. Similarly, reported detection of abnormally high levels of radiation is evaluated initially to determine whether it is "out of context."

[65] FEMA is not a first-responding organization, but rather it comes in to support local jurisdictions in their first response upon a request from the appropriate local officials. On May 5, 2002, FEMA field offices were tasked with helping to ensure national preparedness through building local capacity for up-front response. To this end, FEMA oversees grants to state and local emergency-management agencies to enhance and reinforce state and local capacities for emergency management, particularly among first responders who are likely to deal with chemical, biological, radiological, nuclear, and explosive terrorist incidents.

[66] Following the terrorist attacks on September 11, 2001, FEMA reevaluated its procedures to improve flexibility and response time to requests for assistance. During that emergency the traditional local-state-federal chain of request proved overly cumbersome, and FEMA was quickly overwhelmed with requests for assistance at Ground Zero for search and rescue.

[67] Such information is likely to be particularly helpful in responding to a radiological event, since local responders are highly unlikely to be familiar with the range of federal resources in this specialized area.

[68] As recently as 1995, the U.S. federal government had no budget allocation whatsoever for homeland defense.

[69] Since the September 11, 2001, attacks, first responders going into incidents involving explosions are far more likely to look for radiological signs than previously, although there is little response infrastructure in place for nonexplosive events.

[70] For example, an anthrax patient does not require the type of decontamination required for radiation exposure.

[71] The reaction of local, state, and federal authorities to the anthrax scare in October 2001 demonstrates the consequences of uncoordinated response to a specific type of ongoing terrorist threat. Despite the availability of accurate information among the first-responder community on how to identify and treat anthrax exposure, this information was frequently overlooked and more extreme measures were taken than were necessary.

[72] In attempting to coordinate contributions from various types of agencies and departments, differences in protocol, terminology, and equipment must be overcome and institutional cultures blended. For example, in one incident when the Marines were called in during the 1992 Los Angeles riots, police were moving in on what they thought was a drug house. They asked the Marines to provide "cover"—at which point the Marines started firing.

[73] In the United Kingdom, efforts to manage the media exposure given to terrorist organizations have taken the form of "voluntary" guidelines for media outlets, such as those promulgated by the BBC, for reportage of terrorist events.

[74] California also has a Standardized Emergency Management System to give responders continuity from the field through the emergency operations center for managing contacts with the press and outside agencies. Important components of this plan include the designation and training of public information field officers and pre-made general-application public information messages for the first critical hours of an emergency, with blanks to be filled in for real-time adaptation to the specific situation.

[75] FEMA supports the JIC concept and accommodates it within the Federal Response Plan.

Participants in the Workshop on Communicating Nuclear Risk: Informing the Public about the Risks and Realities of Nuclear Terrorism, held at CISAC, Stanford University

Herb Abrams, CISAC
John Ahearne, Sigma Xi
Chaim Braun, CISAC
George Bunn, CISAC
Jor-Shan Choi, Lawrence Livermore National Laboratory
Chris Chyba, CISAC
Laura Donohue, CISAC
Sonni Efron, Los Angeles Times
Ruben Grijalva, Palo Alto Fire Department
Jim Hassberger, Lawrence Livermore National Laboratory
Siegfried Hecker, Los Alamos National Laboratory
Jack Hubbard, Stanford Communications
Neil Johnson, FEMA
Ty Kim, KPIX-TV
Robert Kuckuck, NNSA
Michael Levi, Federation of American Scientists
Dawn Levy, Stanford Communications
John Lightfoot, FBI
Michael May, CISAC (Chair)
Robert Nelson, Princeton University
Robert L. Norris, Stanford Medical Center
David Perlman, San Francisco Chronicle
Jessica Priselac, CISAC
Donald Prosnitz, Department of Justice
Tonya Putnam, CISAC
Thomas Ridgeway, FEMA
Scott Sagan, CISAC
Dan Sneider, San Jose Mercury News
Doug Sovern, KCBS All-News Radio
Ronald Stolz, Sandia National Laboratory
Bill Sutcliffe, Lawrence Livermore National Laboratory
Benjamin Tong, California Governor's Office of Emergency Services
Harry Vantine, Lawrence Livermore National Laboratory
Dean Wilkening, CISAC
Frances Winslow, San Jose Office of Emergency Services
Lyudmila Zaitseva, CISAC