

Protecting The Homeland

***Report of the
Defense Science Board Task Force***

on

**UNCONVENTIONAL NUCLEAR
WARFARE DEFENSE**

***2000 Summer Study
Volume III***



July 2001

**Office of the Under Secretary of Defense
For Acquisition, Technology, and Logistics
Washington, D.C. 20301-3140**

This report is a product of the Defense Science Board (DSB). The DSB is a Federal Advisory Committee established to provide independent advice to the Secretary of Defense. Statements, opinions, conclusions, and recommendations in this report do not necessarily represent the official position of the Department of Defense.

This report is unclassified.

Distribution authorized to U.S. government agencies and their contractors. Other requests for this document shall be referred to the Defense Science Board.



DEFENSE SCIENCE
BOARD

OFFICE OF THE SECRETARY OF DEFENSE
3140 DEFENSE PENTAGON
WASHINGTON, DC 20301-3140

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE (ACQUISITION,
TECHNOLOGY & LOGISTICS)

SUBJECT: Defense Science Board Task Force Report on Unconventional Nuclear Warfare
Defense

I am forwarding the final report of the DSB Task Force on Unconventional Nuclear Warfare Defense. This study, chaired by Dr. Roger Hagengruber, was established to review and evaluate DoD's current state of detection, identification, response, and prevention to terrorist subnational, or other unconventional nuclear attacks to the U.S.

The Task Force found that a substantial base of capabilities exists within the DoD and the Department of Energy to handle the Unconventional Nuclear Threat (UNT) but these resources are not optimized. The Task Force has outlined a strategy for improving the DoD's ability to defend against and better deter the changing UNT. The strategy presented here does not require significant increases in funding; however, it will require adjustments within existing programs for intelligence collection, research and development for advanced nuclear material detection, nuclear forensics, and nuclear security programs with the Former Soviet Union. The recommendations of the Task Force form the basis for a coherent strategy and would not only increase military security, but also provide for broader protection to the homeland.

I endorse all the recommendations and propose you review the Chairman's letter and final report.

A handwritten signature in black ink that reads "William Schneider, Jr." with a stylized flourish at the end.

William Schneider, Jr.
Chairman



DEFENSE SCIENCE
BOARD

OFFICE OF THE SECRETARY OF DEFENSE

3140 DEFENSE PENTAGON
WASHINGTON, DC 20301-3140

Dr. William Schneider Jr.
Chairman, Defense Science Board
3140 Defense Pentagon, Room 3D865
Washington, D.C. 20301-3140

Dear Dr. Schneider:

Subject: Final Report of the Defense Science Board -- Task Force on Unconventional Nuclear Warfare Defense.

Attached you will find the report of the Defense Science Board Task Force on Unconventional Nuclear Warfare Defense.

The Task Force Terms-of-Reference asked the Task Force to:

- 1) Determine the adequacy of the DoD's current ability to support detection, identification, response, and prevention of unconventional nuclear attack.
- 2) Determine appropriate role(s) and needed capabilities (with a specific emphasis on technical capabilities) for the DoD in support of homeland defense against unconventional nuclear attacks.

In response to (1) we found that there is a substantial existing framework of capabilities, process, and experienced people within the DoD and DOE for dealing with the unconventional nuclear threat. However, these capabilities and activities are not optimized for the emerging unconventional nuclear threat nor are they part of a coherent strategy. In response to (2) we believe the appropriate DoD role is to focus on protection of key military and national security facilities. Protection of these assets fall within the broad responsibility of the DoD.

Our principal recommendation is the deployment of protection systems built from existing technologies to key military facilities. Such systems would also provide a capability to deploy to a wider variety of facilities upon warning. Additional supporting recommendations can be found in the body of the attached report. These recommendations form the basis of a coherent strategy that will make possible the further extension of protection to a broader range of homeland assets at a later date.

Mr. William Schneider Jr.

- 2 -

The task force would like to express its appreciation to the members and government advisors of the task force and for the extensive support of the OSD staff.

Sincerely,

A handwritten signature in cursive script that reads "R. Hagenruber". The signature is written in black ink and is positioned above the typed name.

Roger I. Hagenruber
Task Force Chair

I.C:9815:ggh

Attachment:
Report of the Defense Science Board Task Force on
Unconventional Nuclear Warfare Defense.

EXECUTIVE SUMMARY

The Terms of Reference (TOR)

Unconventional Nuclear Threat (UNT) pertains to a nuclear attack on the United States via unconventional delivery methods, e.g. delivery other than by missile or military aircraft. The possible perpetrators of such an attack can range from small terrorist groups, subnational groups, transnational groups, state-sponsored/supported terrorist groups, to nation-states. The nuclear devices also cover a spectrum from crude radiation dispersal devices and improvised nuclear explosive devices, to stolen nuclear weapons. The Task Force focused on two main objectives as laid out in the Terms of Reference (TOR):

- (1) Determine the adequacy of DoD's current ability to support detection, identification, response, and prevention of unconventional nuclear attacks,
- (2) Determine appropriate role(s) and needed capabilities (with a specific emphasis on technical capabilities) for the DoD in support of homeland defense against unconventional nuclear attacks.

In pursuit of these tasks, the UNT task force (a) reviewed the history and the present status of the UNT threat, (b) examined the current technical capabilities for nuclear material detection and identification, and (c) met with members of the principal DoD organizations, as well as other government agencies either directly or tangentially involved with the UNT threat.

History of the Unconventional Nuclear Threat

The UNT threat has changed and evolved over the decades since the end of WWII. Concerns over the UNT were high in the U.S. for years over the fear that the Soviet Union might attempt to smuggle nuclear devices into the U.S. to create a threat against critical assets or leadership. The fear of covert delivery of a nuclear weapon was and remains a valid security consideration, but for most of the past four decades this threat has been overshadowed by the threat of nuclear conflict via missiles and bombs.

In the 1960s and 1970s, there was also a backdrop of concern in the U.S. over proliferation and the growing global plutonium stockpiles from reprocessing and recycling nuclear reactor fuel. Another factor in the collective psychology of the period was the persistent enigmatic fear of things nuclear that was exacerbated by nuclear accidents at Three Mile Island and in the USSR. These various nuclear concerns were strong in the public mind amid a period of airplane hijacking and worry over terrorism.

It was in this context then that the response to the unconventional threat became focused primarily on nuclear terrorism. In response, the government created the Nuclear Emergency Search Team (NEST). NEST is a DOE managed activity with well-established interagency relationships including significant DoD collaboration. NEST is focused on responding to an act-in-progress, where a nuclear device has already been smuggled into the country or has been stolen from a U.S. facility. Among the various terrorist threats involving weapons of mass destruction, the nuclear response structure and capabilities are, through the long standing NEST program, the most mature and competent for the threat often serving as a model for threats like chemical and biological terrorism.

The World Has Changed and The Threat Has Increased

One of the most profound shifts in nuclear safety and security since the end of WW II has accompanied the end of the Cold War with the fall of Communism and the breakup of the USSR. Hundreds of tons of special nuclear material - half the world's stockpile - had its security status dramatically reduced. The potential for nuclear terrorism and proliferation increased with unprecedented quickness. While the view that terrorism is on the increase would dictate increased attention to nuclear terrorism, it appears that equating the potential for an UNT to the homeland to nuclear terrorism alone would underestimate the true UNT.

The simple fact of increased accessibility to nuclear material and knowledge unquestionably increases the potential for nuclear terrorism. And, there are persistent indications of interest in nuclear explosives by terrorist and sub-national groups. Yet, it would appear that the national security community perceives the threat of terrorism from conventional explosives, chemical and biological agents, or disruption of critical information infrastructure as much more probable. In this study, we conclude that nuclear terrorism is a relatively unlikely form of terrorism even though the situation in Russia has increased the threat. Perhaps the more likely form of true nuclear terrorism (e.g. terrorist actions undertaken by individuals or groups acting on their own) in the future will be nuclear events (sabotage, dispersal) as a form of protest against renewed or expanded nuclear energy activities.

On the other hand, shifts in U.S. military strategies may be providing an impetus to a different type of UNT. Increased regional presence, greater dependency on a limited set of power projection overseas bases and carrier battle groups, a slimmer and more Just In Time (JIT) military force structure, and an emphasis on missile defense are all strong stimuli to a different class of nuclear proliferation and/or use of nuclear weapons. In fact, it is the increased availability of nuclear materials accompanied by the increasing attractiveness of the U.S. military as a military target that makes the UNT an emergent and serious issue for DoD and an untraditional problem for the homeland.

As a nuclear target, the U.S. homeland is likely most threatened by direct and indirect attack on the effectiveness of U.S. force projection. Direct attacks on military bases or supporting infrastructure overseas or in the continental United States (CONUS) constitute an asymmetric and potentially effective threat with benefits that could be worthy of nuclear use. In our judgment, the likelihood of such use has increased much more than the likelihood of terrorist use against our cities. This is a threat that would be executed either directly or indirectly by another country, quite likely a regional state and not a major nuclear weapon state.

Complete Protection of the Homeland: Not Feasible at This Time

The NEST activity is intended to operate after an alert or warning, and to detect, localize, secure, and render safe a nuclear explosive weapon or improvised device. It is a competent capability that can be very effective given warning and time. However, for nearly 50 years, there has been a desire to extend detection, hence interdiction, to the borders and entry ports of the U.S. Substantial amounts of money have been spent to this end, and a substantial body of technology exists. Yet, today, it is still not possible to provide an assured detection and protection perimeter against clandestine entry of nuclear materials into the U.S.

Part of the reason that complete protection is problematic lies in the scope of the potential access. The U.S. has thousands of miles of open borders and hundreds of legal entry points through which millions of shipping containers enter each year. Detecting the presence of a few kilograms of weapons-capable nuclear material hidden in all of the diverse variety of containers, vehicles, aircraft, and ships that enter the U.S, while technically feasible, is impractical. Further, the more capable threats will find a way to elude the technologies that are affordable and the deployments that are most predictable. In effect, a sophisticated UNT cannot be consistently defeated at any time and target of their choosing. On the other hand, it is possible to increase the deterrent effect for unsophisticated threats by deployment of low cost detectors or for more competent threats by random sampling with more sophisticated systems at attractive entry portals.

In the end, the limit of protection is more tightly associated with the quality of intelligence indications and warning, and to the psychology of deterrence, than to any achievable technology. There is no amount of funding or restructuring of approach that is capable of reducing the probability of an UNT to zero. But, with a modest investment and some limited changes, it is possible to significantly reduce the UNT to the homeland. Most importantly, there are initiatives that will better match technology to the quality of intelligence information, and better match the intelligence to the threat. A key element is to narrow the set to targets where significant investment will be needed and such a narrowing is consistent with the more rational threat that we find most probable than for the terrorist psychology.

Strategy and Approach

While complete protection of the U.S. appears impractical, we do believe that an effective technical detection system can be developed to protect key point-targets. The most important point targets appear to be of high military value such as bases overseas. Many of the technologies that show the highest promise are or could be made modular and portable. We also see operational changes that can cause significant improvement in protection at certain key point targets such as military facilities and key logistics nodes. Combined with existing and some new technology, a hierarchy of increased operational controls based on alert status can dramatically increase the effective protection of potential targets.

The best strategy for enhanced protection is to adapt the technology and operational procedures to a few classes of scenarios. For fixed high value targets such as military facilities, some fixed sensors should be combined with deployable or extendable arrays of sensors that would be activated on warning or at an increased alert status. For logistic nodes, some deployable and fixed sensors should be combined with changes in operational procedures such as those that would increase inspection and vetting of vehicles or ships before they are allowed entry into a controlled area. In the case of the more general threat (e.g. that which would include terrorism), rapidly deployable systems that are matched to the intelligence and warning capabilities (such as the current NEST equipment), but that could be utilized to screen large objects rapidly and/or configured as a network would be most useful.

Any program of increased levels of protection or broader deployment will suffer from the issues associated with rare, but serious threats. Namely, there will always be a difficulty in achieving and maintaining a high level of diligence and competence for contingency that has a low probability of occurrence. Since we believe that the most likely UNT to the homeland is one directed against the U.S. military by or on behalf of another country, the best deployment of enhanced protection would be a key overseas military facility. At such a facility, there is also the benefit of a military structure accustomed to discipline in the application of operational procedures and technology against a relatively low probability event (in peacetime). Selecting the military for developing and deploying more effective protection serves a number of purposes. First, it would be an appropriate response to the evolving threat and completely consistent with the DoD emphasis on force protection. Additionally, it would allow the development of technologies and protocols that could be more effectively extended to support field operations in CONUS by agencies such as the FBI, and eventually to supply a base for deployment to better protect civilian sites. This strategy would also represent a prudent approach to civilian support that does not confuse mission with capabilities.

Another important area related to more comprehensive protection is associated with the observation that the increase in importance of the UNT has a strong correlation to the security of nuclear materials in Russia. DoD and DOE are both involved in programs to assist the Russians in reducing the likelihood of loss of materials or weapons. Clearly,

this work is one of the few activities that could be seen as having a comprehensive relationship to the various ways an UNT can affect the U.S.

Our overall strategy was, in recognition of the substantial existing base of technology and programs, to seek to adapt current systems, programs, and technology to the emergent UNT. The nuclear response capability has benefited from a persistent concern and a good coupling to technology for 50 years. We would choose to take advantage of this without allowing the stereotypical terrorist threat to be the primary driver, or the primary path to solution to be technology development alone.

Recommendations

In regards to DoD's current capabilities, we believe there is a substantial, existing base of capabilities residing within the DoD and DOE for dealing with the UNT threat. However, these capabilities are not currently optimized for the emerging threat as we see it. We have mapped out a strategy for improving the DoD's ability to defend against and better deter the changing UNT threat. This strategy does not require significant increases in funding, but does involve an adjustment in existing programs for intelligence collection, nuclear security programs with the Former Soviet Union (e.g. within DoD and DOE such as Nunn-Lugar), nuclear forensics, and R&D for advanced nuclear materials detection. This strategy is presented as six recommendations for making the current programs and approaches more effective.

1. Deploy sensor technologies and systems to protect critical DoD installations.

In this context, establish a test-bed military facility to rapidly adapt technology and procedures into deployable systems, and to test and demonstrate such systems to base commanders. This recommendation involves modest cost (some \$5M per year and \$2M-\$10M per base), but will only be possible if the services and DoD give some priority to the UNT as a strategic and force protection issue. We are convinced that they should.

2. Change the structure for processing and analyzing of intelligence collections to increase the sensitivity of detection of nuclear indicators.

The subtlety of indicators associated with the changing UNT requires an enhanced detection and evaluation system. To achieve this enhancement would require relatively modest resources (perhaps a few \$M per year), but will need an enhanced connectivity between the intelligence and technical communities. Such a change is fairly simple and long overdue in the post-Cold War period.

3. Improve nuclear forensics capabilities to achieve accurate and fast identification and attribution.

One of the strongest elements of protection is deterrence through the threat of reprisal, but to accomplish this objective a more rapid and authoritative attribution system is needed. Laboratory capabilities in this area exist to support the nuclear stewardship program. Some technology developments will be needed to adapt for rapid forensic assessment.

4. Rebalance (perhaps enhance) resources to re-establish a strong research and development base in NEST and related programs.

There are fruitful areas of R&D that would assist in developing a more effective response to the UNT and it would be appropriate to shift the investment focus of existing programs somewhat from the current operational emphasis towards R&D thus responding to the changing nature of the threat.

5. Continue investment in Russian nuclear security but create a strategy and systems approach to investment and deployment better matched to the UNT threat.

Clearly, this is one of the most effective ways to attack the threat at its source, but given the limit of resources available, there should be a more effective focus and approach where protection of the U.S. is a more explicit factor in the allocation of resources than is currently the case.

6. Develop a body of studies and analysis to better characterize the variety of unconventional nuclear threats.

Compared to the environment of the Cold War, the capability and body of work associated with studies and analysis related to the changing threat is surprisingly shallow and clearly inadequate. Done well, such analytical work can be very effective in identifying threat dynamics and response options at low cost. Some work of this type was done in the course of our study, but that analytical product is a poor substitute for the level of analysis appropriate to this threat.

Accompanying many of the recommendations is the strongest encouragement to the Defense Threat Reduction Agency (DTRA) and the National Nuclear Security Administration (NNSA) to develop an effective Memorandum of Understanding (MOU) relating to their programs and capabilities. It is relatively rare in the government to see an area of such constructive potential strategic alignment and collaboration.

All of the recommendations made in this report are within the authority of existing agencies and individuals, and many could be accomplished within current budget categories. Some recommendations will need additional resources. Some can be accomplished by the shifting of strategies within existing resources. Not all of the needed resources are the responsibility of the DoD. The cost of the proposed response is modest by virtually any standard.

The emphasis in this report and in the recommendations naturally fits the responsibilities of the DoD, and does not require expansion or adaptation of the traditional military missions. Taken together, the set of 6 recommendations form the basis for a coherent strategy. When executed they would not only enhance military security, but they would provide a foundation for extending broader protection to the homeland. In our judgment, this approach is a cost-effective and executable approach to the UNT to the homeland as it is emerging in the 21st century.

Report of the Task Force on Unconventional Nuclear Warfare Defense

Defense Science Board

August 18, 2000

Roger Hagengruber

Emery Chase
Don Cobb
Len Connell
Steve Dupree
Julie Evans
Tyra Flynn
Stan Fraley

Dave Havlik

John Immele
Don Kerr
Richard Kerr
Frank Martin
Scott McPheeters
Edward "Shy" Meyer
Cathy Montie
Gordon Negus

Sid Niemeyer

Art Payne
Vic Reis
Wayne Shotts
Brad Smith
Chip Smith
Frank Sullivan
Rich Wagner

*Briefings from: DOE, DOE/DP labs, DTRA, DIA, JTF, CIA,
OSD/CS/SOLIC, NSC, OSTP, TSWG, FBI, Border Patrol, AFTAC*

Figure 1.

This is the report of the Task Force on Unconventional Nuclear Warfare Defense. Figure 1 lists the members of the task force and support personnel from the various organizations who participated on the task force. The task force also received briefings from a broad variety of government organizations, including the Department of Defense, the Department of Energy, the FBI, and others - including individuals who go about the day-to-day task of trying to intercept contraband, smuggled devices, or information at our borders.

Task Force Terms of Reference

- Determine the adequacy of DoD's ability to support detection, identification, response, and prevention of unconventional nuclear attacks by national, sub-national, and terrorist entities
 - ❖ Develop general characteristics for classes of unconventional threat (estimate feasibility and cost)

- Determine appropriate role(s) and needed capabilities (with a specific emphasis on technical capabilities) for the DoD in support of homeland defense against unconventional nuclear attacks
 - ❖ Review current detection and response capabilities
 - Define technical and operational elements needed for complete response
 - Identify deficiencies

Figure 2.

The unconventional nuclear threat is a broadly defined nuclear threat not delivered by ICBM (Intercontinental Ballistic Missiles), SLBM (Submarine Launched Ballistic Missiles), bomber, or cruise missile but by some other, unconventional method of delivery by either nation-states or terrorists). The Terms of Reference for the task force established two major focus elements for this threat, as shown in Figure 2.

First, the task force was asked to examine the adequacy of the United States capability to cope with the range of problems that unconventional nuclear attacks might pose. This capability encompasses all the possible activities that might be used to deter threats and to detect, intercept, render safe, and mitigate threats that are not deterred. Our current capabilities - while substantially addressing this threat in some areas - can clearly be improved. Evaluating the adequacy of our capabilities required that we assess the variety of threats that might be posed to the United States under the general term "unconventional nuclear threat." Capabilities could then be assessed in terms of their effectiveness against the possible threats.

Second, the task force was asked to determine appropriate roles and needed capabilities for the Department of Defense, with specific emphasis on technical areas. Based on the threats identified in the first element of the Terms of Reference, we determined what the appropriate DoD roles might be for the

various activities identified above, determined which of these roles the DoD was currently performing, determined what technologies or other capabilities were needed to fulfill or support those roles, and evaluated the adequacy of current technology to meet the requirements.

The Nuclear Explosive Threat is Unique

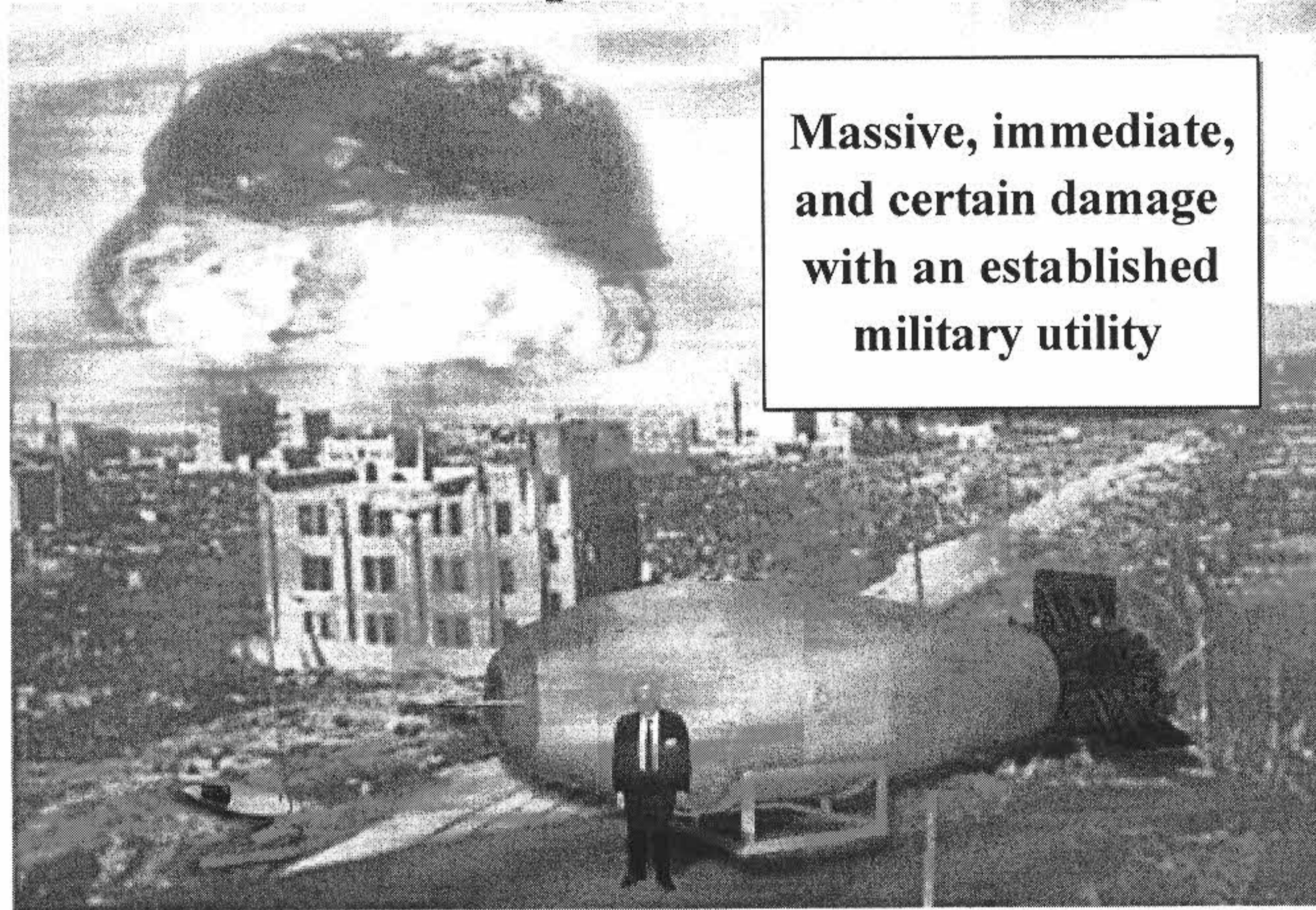


Figure 3.

The nuclear explosives threat is a unique one. The effects, as we all understand, are massive, immediate, and certain. In addition to killing people, nuclear explosions destroy buildings, docks, ships, and other military equipment and facilities. Because of these characteristics, nuclear explosives are well suited to achieving quick, decisive, and predictable effects against military or other targets or, in general, to be used in situations involving rational objectives. Were an adversary near defeat, the immediate effect produced by use of nuclear weapons would be especially attractive.

The backdrop in Figure 3 shows the destruction area at Hiroshima in the aftermath of the detonation of the approximately 15-kiloton "Little Boy" nuclear weapon on 6 August 1945. The images in the foreground illustrate that the size of nuclear packages can, in fact, be quite varied. Two weapon types are shown in the figure. In the lower right is an example of a very large nuclear device - a 60 megaton-class weapon developed by the former Soviet Union, with an individual shown alongside for scale. Conversely, at the lower-left of the chart is shown a rather small nuclear artillery round. Nuclear weapons can, therefore, be packaged as small as a backpack or can be as large as a truck or a transport container, depending on the crudeness or purpose of the device.

We note that the effects of nuclear explosive devices are almost unfathomable, even for individuals who work day-to-day with nuclear weapons and nuclear weapons maintenance in the national laboratories and in the military. Nuclear

weapons effects cannot be "measured" only in terms of numbers of people killed. Characterizing the effects of such a device in terms of "prompt deaths" - while a technically accurate metric - may not be at all adequate in measuring the net impact of its use.

*The Unconventional Nuclear Threat Includes
Everything from Radiological Dispersal Device
to Unconventional Delivery of a Nuclear Weapon*

- Availability of nuclear materials
 - ❖ More than 1500 tons of weapons-capable nuclear material in Russia
 - Bomb requires ~10 kg nuclear material
 - ❖ 20,000-50,000 nuclear weapons in Russia
 - ❖ Globally: ~5000 tons of weapons-capable material
- A nuclear explosive device requires amounts of material
 - ❖ Small weapon (approx. 1 kt) could fit in a backpack
 - ❖ Gun assembly (approx. 10 kt) could fit in a truck
- An RDD can produce severe economic damage (clean-up, loss-of-use) and psychological effects

Figure 4.

The focus of the task force is on the “unconventional nuclear threat,” and we use the terminology to describe a wide variety of threats against the United States.

Perhaps the most singular and important difference that exists in this threat today, compared to about 10 years ago, is the *availability* of nuclear materials in the world. And the availability of this material is dominated by the breakup of the Soviet Union and the change in the process of control of Russian material. Currently, over 1500 metric tons of weapons-capable fissile material exists in Russia, *i.e.*, Highly Enriched Uranium (HEU) or relatively pure plutonium, the core material for nuclear weapons. “Weapons-capable” means sufficiently enriched to make a nuclear weapon through an explosive assembly without any additional expensive and complicated enrichment or purification processes.

Approximately 10 kg of weapons-capable nuclear material is required to produce a weapon, depending on the actual material used and the weapon design. A complete assembly could weigh approximately 50 kg (for a demolition munition or an artillery round) to over a 1000 kg (for a fairly crude device). A major weapons program capability would not be required to fabricate a single crude nuclear explosive provided that weapons-capable nuclear material was available.

In addition to the raw material, there are approximately 20,000 to 50,000 existing nuclear weapons in Russia. We use the range of these numbers purposefully to indicate our uncertainty regarding how many weapons the Russians actually

have. We are confident that the Russians know the number of their weapons exactly. However, the level of security attached to all of those weapons, while higher than the security given the raw materials, appears to have dropped considerably since the breakup of the Soviet Union.

On a global basis, the quantity of all types of nuclear material is increasing at a fairly rapid rate due to the presence of nuclear reactors around the world. Currently, about 5,000 metric tons of weapons-capable material is available, globally, that could be used in some type of weapon configuration. In addition, one needs to consider both the higher-quality waste material that could be used as feed for further reprocessing, thereby simplifying the production of weapons-capable material, and other radioactive materials that could be used for Radiological Dispersal Devices. The amount of these materials is substantially more than 5,000 metrics tons. There's a lot of it, and it's everywhere.

Since even a less-sophisticated nuclear nation-state might develop a crude gun-type assembly (a very simple approach to a nuclear device, similar to the device configuration used at Hiroshima), which could easily fit in a truck. Therefore the key to preventing implementation of such designs is restricting the availability of nuclear materials, because the challenge of actually designing and building the weapon is, in fact, fairly low.

Finally, we raise the issue of Radiological Dispersal Devices (RDDs). Weapons-capable nuclear materials and, in fact, the larger class of nuclear materials that includes those that cannot be used in a weapon, represent a threat that has some analogs to the contamination issues of chemical and biological threats. Radiological material (*i.e.*, radioactive material of any type) can be widely dispersed by mixing it with explosives or by creating an aerosol and dispersing the material in the atmosphere. Some classes of material, *e.g.*, Strontium-90, and certain plutonium compounds, when dispersed, present extremely difficult cleanup challenges. If dispersed in a city, for example, these materials would produce very serious economic and psychological damage. RDDs are not likely to kill a lot of people, but the costs of restoring the environment to an acceptable condition could be staggering.

An Old Problem

- Concern about terrorist nuclear threat has existed for decades, but never has been accompanied by evidence of a real threat
 - ❖ The Nuclear Emergency Search Team (NEST) program is a reflection of concern, with real sustained action and integration with DoD over decades
- Unconventional military use of nuclear weapons was a tacitly acceptable vulnerability with an assumed very low relative probability
 - ❖ Periodic DoD concern about unconventional military use of nuclear weapons in periods of conflict or tension*, but largely lost in Strategic Deterrence
 - ❖ Emerging/candidate states for nuclear possession slowly growing

**The Unconventional Nuclear Threat - A Preliminary Survey (U),
ARPA Order No. 1141, ARPA, May 1969*

Figure 5.

The concern about the misuse of nuclear materials - or their use against the United States - is an old problem. Such concerns, including those about the terrorist threat, have been raised since the Manhattan project.

The Nuclear Emergency Search Team (NEST) is a result of this concern. The program is long-standing - it is many decades old - and it is a program with real, sustained action. The involvement of the Department of Defense and the Department of Energy has stood the test of the past 30-40 years.

Unconventional military use of nuclear weapons in a non-terrorist way, *e.g.*, the unconventional delivery of a nuclear weapon by a country such as Russia, has been a perceived vulnerability for many years. However, the probability of (or even the interest in) such use was assumed to be very low, given the mutually large inventory of strategic weapons and aircraft. There has been periodic concern, and reports have been written about various scenarios. However, that vulnerability was not thought to be important relative to the strategic deterrence that dominated the relationship between the United States and the Soviet Union during the Cold War.

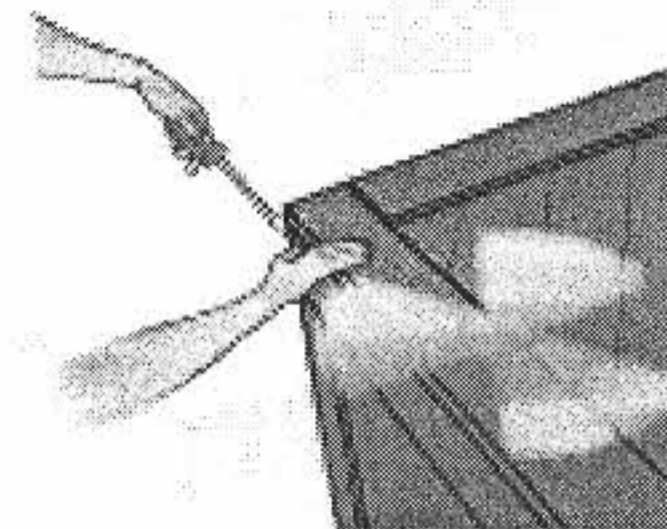
The proliferation of nuclear weapons, or the emergence of additional candidate nation-states that might possess nuclear weapons, has been, a slow-developing and persistent problem. It continues today, as exemplified by recent developments in India and Pakistan.

There is a History of Investigation

Project Screwdriver -- 1950-52

How do we prevent clandestine entry of nuclear weapons into the U.S?

- Cannot cover all borders
- Use available technology
- Shielding presents a problem



"The only instrument that would enable an inspector to find out if a packing crate contained an atomic bomb is a screwdriver."
- J. R. Oppenheimer

Project Doorstop (1953-70)

Implement the recommendations of Project Screwdriver

- Detect 1 kg or larger quantity
- Monitor designated choke points
- Use passive Pu detection
- Use active U detection

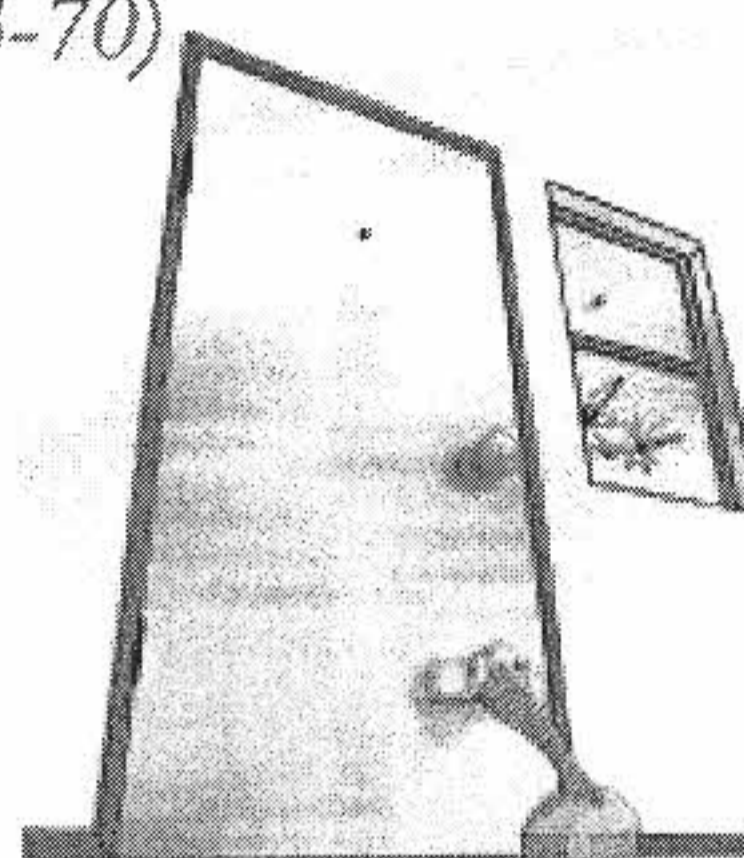


Figure 6.

The concerns over the unconventional use of nuclear weapons and devices – and the importance of trying to deal with them – is a long-standing and crucially important area of investigation that has involved both Department of Energy and the Department of Defense. As early as 1950, there was an urgent concern over the clandestine entry of nuclear weapons into the United States. A study of the problem was hurriedly undertaken, and a report summarizing the findings was written. The title of the report, *Screwdriver*, was taken from a comment made by J. Robert Oppenheimer during his Congressional testimony (cf. Figure 6) in which he addressed the complexity of dealing with shielding and trying to detect a nuclear device hidden within a packing crate. “The only instrument that would enable an inspector to find out if a packing crate contained an atomic bomb,” he said, “is a screwdriver.” The *Screwdriver* report concluded that wide-area detection of nuclear weapons and materials smuggling was not technically feasible. However, the report also concluded that reasonably good point detection could be provided at key ports of entry against kilogram-quantities of lightly-shielded nuclear material (uranium and plutonium).

Project Doorstop implemented the *Screwdriver* report’s recommendations. Key U.S. ports-of-entry used by foreign diplomats from Iron Curtain countries were instrumented for nuclear material detection. It was a multi-agency effort involving the Department of Defense, the Department of Energy (then the

Atomic Energy Commission), and others. The effort to rigorously consider the question of interception was taken very seriously over a multi-year period. Passive radiation sensors were used for detecting the intrinsic radiation (neutrons and gammas) emitted by plutonium and uranium. The project ended in 1970 due to the effects of the changing strategic deterrence strategy (i.e., mutual assured destruction). The project never detected a significant attempt to smuggle nuclear weapon material into the U.S. However, it is interesting to note that the DoD took an early and active role against the unconventional nuclear threat.

Doorstop resulted in an extensive, two-volume set of reviews about how to address the problem. A fair amount of useful research and development was performed in support of the project, including research on active detection of uranium by causing fissioning in the material with an "interrogating" beam of neutrons. Active detection was never deployed due to the concerns associated with radiation exposure to the general population.

Project Doorstop

1960s technology was slow and cumbersome but generally competent

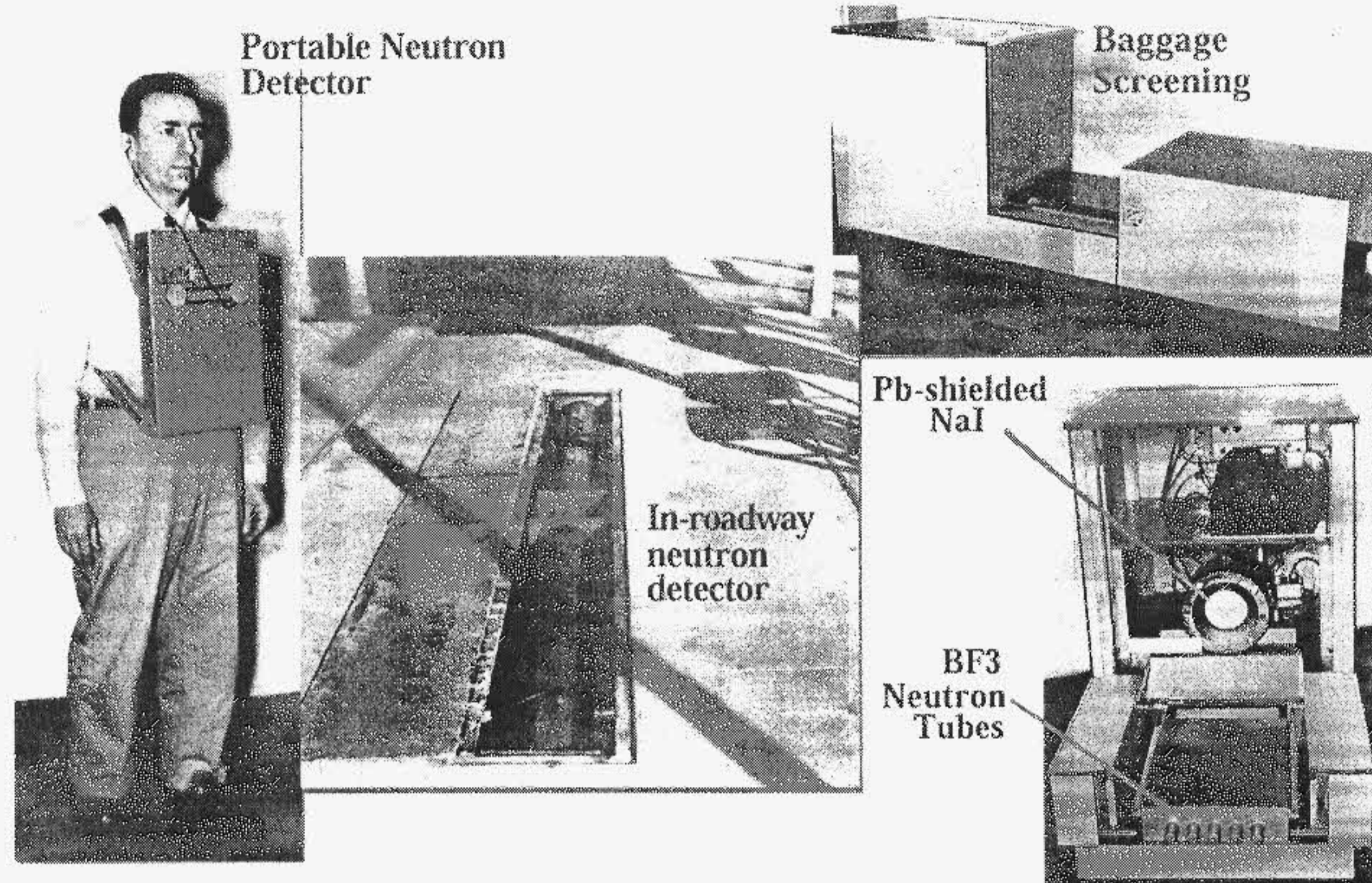


Figure 7.

The *Project Doorstop* technologies were deployed at key ports-of-entry such as international airports and at key border crossing points authorized for use by communist country diplomats. The border crossings employed detectors embedded in the roadway, while airport detectors were hidden within baggage screening equipment.

Figure 7 shows the types and variety of technology that were either considered or developed under the *Doorstop* program, including the technology that was installed, for example, at border crossing points to monitor foreign diplomats entering the United States. (One of the scenarios considered in *Doorstop* was the possibility that these individuals might attempt to clandestinely bring a nuclear weapon into the United States, *e.g.*, for the purpose of attacking the nation's leadership in Washington, D.C.) Figure 7 depicts a variety of instrumentation that is old and reasonably out-of-date. However, the basic technology was generally competent and could be used today to interdict nuclear materials at our borders.

THIS PAGE INTENTIONALLY BLANK

Nuclear Material Has a Fingerprint that can be Detected but Shielding and Distance Work Against Us

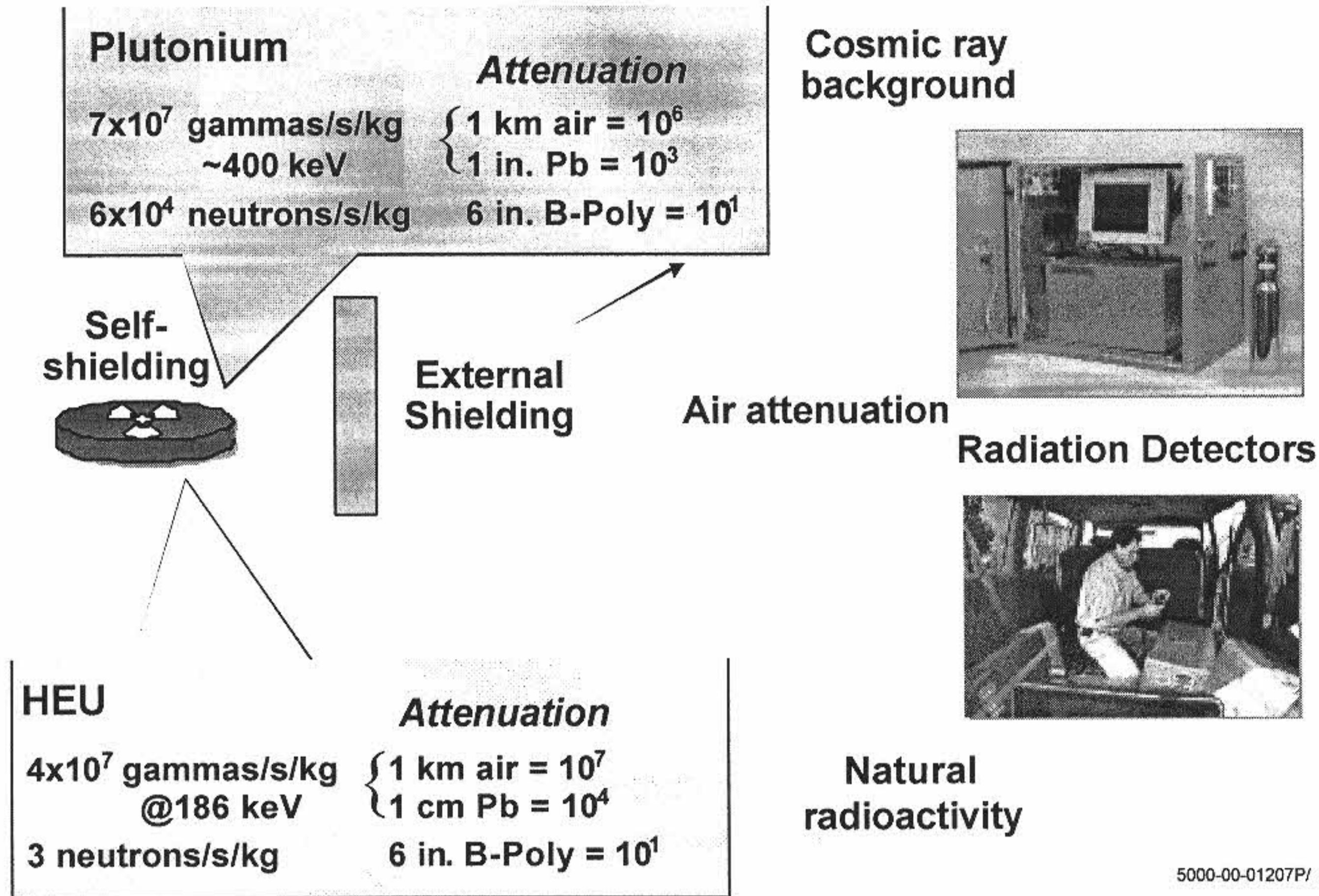


Figure 8.

Let us briefly consider the technical features of the problem of interception of nuclear weapons or devices.

The fortunate characteristic of nuclear materials, *e.g.*, plutonium and Highly-Enriched Uranium, is that they have a "fingerprint." That fingerprint is manifested as radiation that can be detected at a distance from the material. The plutonium fingerprint is more pronounced and easier to detect because it emits a higher energy gamma ray (400 keV vs. 186 keV for HEU) and a much larger number of neutrons. Over short distances, *e.g.*, about 100 ft, it is possible to detect and measure the fingerprint and measure it with instrumentation that can identify the material.

Unfortunately, as shown in Figure 8, air attenuates the signal and also scatters it. The same is true with shielding materials, such as, lead - but almost any material will scatter and change the characteristics. So, very much like a fingerprint being covered with dust, the imposition of shielding material or of an air gap tends to blur the "nuclear fingerprint" we wish to detect and identify. This is the classic signal-to-noise problem. The actual signal emitted by the source nuclear material is both (i) hard to "hear" amongst the "loud" background radiation coming from the natural radioactivity of the earth and from cosmic rays and (ii) difficult to distinguish uniquely, even if detected, due to "smearing" of the signal.

These factors conspire to make detection-at-a-distance extremely problematic. Today's best detectors would be extremely hard-pressed to detect a moderately shielded significant quantity of nuclear material (enough to make a nuclear explosive device) at distances beyond a few meters.

Background Also Obscures the Radiation Fingerprint

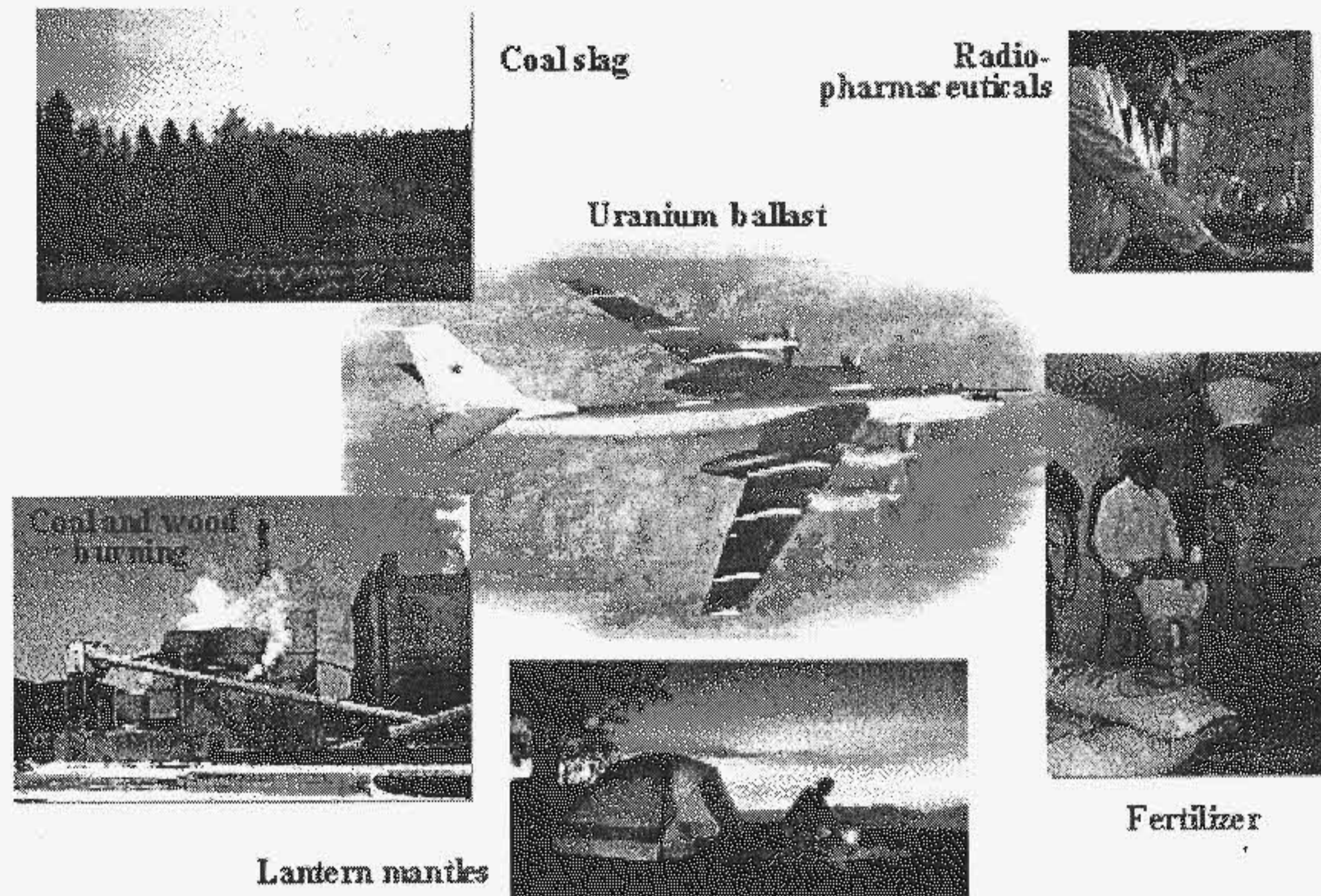


Figure 9.

The world is awash in radioactivity, both natural and from the many man-made radioactive materials some of which greatly benefit society. As mentioned previously, this background complicates the problem of detecting or "reading" the signature of the characteristic radiation from weapons-capable material or material that could be used in an RDD device.

Coal, fossil fuels, oil, petroleum, and raw crude oil all produce significant nuclear signals because of the concentration of uranium and thorium in those materials. Wood- and coal-burning plants emit a significant amount of radioactive material in the fly ash: in some cases, coal-burning plants emit several 100 kgs of uranium in the fly ash per year. Fertilizers contain a radioactive potassium isotope that can be detected at a distance. Manufactured products such as radio-pharmaceuticals are frequently present in airports and other locations as they are shipped from one point to another. Moreover, increasing numbers of people are undergoing medical procedures involving radioactive materials (~30,000 per day in the United States alone), and these individuals, *themselves*, are sources of radiation. This trait is now so prevalent that a radiation detector installed at an airport to monitor daily personnel traffic would constantly be detecting individuals undergoing medical treatment whose bodies are emitting nuclear radiation. Even camping lantern mantles are relatively high in radioactivity from the thorium they contain. Uranium, which is a very dense material, is also used for tail ballast in aircraft such as Russia's Bear bomber.

"Legitimate" radiation sources such as these can make it difficult to detect nuclear fissile material or isotopes that could be used for RDD devices at ports-of-entry or other choke points. The quality of detectors has been improved over the past 30-50 years to give them greater spectroscopic capabilities and otherwise make them more capable of looking at the "nuclear fingerprint" (instead of only measuring the gross ionizing radiation count). It is possible, therefore, to remove some of the effects of the background radiation and the problem of false positives.

The NEST Program (Nuclear Emergency Search Team)

- | | |
|---|---|
| <ul style="list-style-type: none"> ▪ Organizations ❖ LANL ❖ LLNL ❖ SNL ❖ RSL ❖ Pantex ❖ DOE/AL ❖ DOE/NV | <p>Additional, as-needed organizations</p> <p>DOD</p> <p>DOJ</p> <p>DOS</p> <p>Budget</p> <p>About \$35M/year</p> <p>Steady for last several years</p> |
|---|---|



HE Sniffer

The program has produced a significant inventory of equipment, experienced personnel and operational plans

Figure 10.

Nuclear Emergency Search Team (NEST) is an example of a long-standing activity that addresses the Terms of Reference of this task force, *i.e.*, an unconventional attack on the homeland utilizing nuclear material. Figure 10 indicates that many organizations are involved in NEST, and, generally, they are associated with the Department of Energy. However, the Department of Defense, the Department of Justice, the Department of State, and others have also been involved. The involvement of the Department of Defense is regular and consequential, and it involves DoD operational elements.

At ~\$35M/year, NEST's annual budget is fairly significant and has been reasonably constant in recent times. NEST has produced a host of equipment, experienced personnel, and operational plans comprising a capability to accomplish the mission of search and interdiction of nuclear material or weapons that either enter the United States from abroad or have been stolen from the United States Government.

While *Screwdriver* and *Doorstop* examined and deployed the technology for detecting covert nuclear material crossing into the U.S., NEST established an operating system for responding to a nuclear threat. In the early 1970's, concern had arisen in the nuclear weapon community that the projected growth in worldwide nuclear power reactor numbers would generate large quantities of plutonium, which might not be properly safeguarded. Various actions were taken to improve nuclear material safeguards and protect design information,

but it became clear that measures were needed to prepare for the possibility of "loose nukes."

In 1974, Dr. Theodore Taylor published *The Curve of Binding Energy* in which he expressed his concerns about the probability (and ease) of construction of improvised nuclear devices by terrorist groups. A credible scenario was reviewed in the *New Yorker* magazine and received wide attention. Subsequently, a large number of hoax nuclear extortion threats were received by various government agencies. Accordingly, in late 1974 the Atomic Energy Commission (AEC) Director for Military Applications sent a letter to the Directors of Lawrence Livermore, Los Alamos, and Sandia National Laboratories and to the Manager of the AEC Nevada Operations Office tasking them to establish and support what became known as the Nuclear Emergency Search Team (NEST).

The AEC/ERDA(Energy Research Development Administration)/DOE NEST program evolved over the next several years into a multi-agency national capability with operational skills going far beyond the "search" designated in its name. 1976 marked the first exercise covertly searching a public facility with law enforcement help at the San Francisco International Airport. The first full field exercise with U.S. Army Explosive Ordnance Disposal (EOD) participation was held at the Idaho National Engineering Laboratory in 1977, which was also the same year that the team was deployed to a real threat (later determined to be a hoax) at the Union Oil facilities in Long Beach, CA. A formalized methodology to evaluate communicated threat messages was established in 1977 to assess credibility and obtain tactical intelligence from their content. This project has significantly reduced the incidence of deployments, even though threat messages continue to be received.

An important milestone occurred in January 1978, when the team deployed to Canada to aid in locating nuclear reactor debris from the Soviet satellite, COSMOS 954. This successful operation generated worldwide attention and exposed the team to operations in very difficult environmental conditions. It also provided experience in rapid deployment and had a significant impact on field organization and logistics planning.

Even today the formation of a Nuclear Emergency Response capability stands not only as a sound decision but also as a good example on which to build capabilities for unconventional attacks using chemical and biological devices, or even attacks on the military and civilian information infrastructures.

Regular NEST Program Exercises are Held

- National/International - 1 or 2 per year
 - ❖ More than 100 people involved
 - ❖ Sometimes many more than 100 involved
 - ❖ Involves Defense, law enforcement, State, as needed
- Drills - 5 or 6 per year
 - ❖ Subset of total capability
 - ❖ 10-50 people involved
- Events (Olympics, Tall Ships, etc.)
 - ❖ Subset of total capability
 - ❖ As needed - 1 to 2 per year
 - ❖ Preparedness staff at Operations Center

Figure 11.

The NEST capability is exercised regularly, on both a national and on an international basis. Drills involve a substantial number of people, including individuals from the Department of Defense.

NEST has been activated at the Atlanta Olympics and other public events in order to exercise them in actual, real-life environments.

Exercises continue with various military and/or civil organizations. The first NEST field exercise with major FBI participation was held in 1983 in Albuquerque, NM. While this operation provided an opportunity to explore FBI/DoD/DOE field organizational issues, it also tested the concept of conducting searches with local emergency personnel who are trained for the task on-the-spot. The original concept did not work very well, so the concept has evolved through training a cadre of approximately 200 "reserve searchers" to the development of search equipment with built-in intelligence to avoid the expense of having large numbers of personnel on-call.

Many exercises have been held dealing with different military organizations both within the continental United States (CONUS) and outside the continental United States (OCONUS) scenarios, different technical issues, and different physical locations. The emphasis since the mid-90s has been on OCONUS scenarios.

Training for Emergency Ordnance Disposal personnel has included application and use of DOE-developed equipment for diagnostic, disablement, and containment use, in conjunction with DOE scientific personnel.

Throughout its history, NEST personnel have worked to improve their technical capability. However, they still lack tools to deal with various threats that have been defined. There are limitations caused by the laws of physics and by insufficient information about specific threats with which they must deal. Some of these deficiencies are being addressed by numerous forward-looking ideas that have been proposed for search, diagnostics, and disablement use.

The Situation Has Changed to Increase the Nuclear Threat

- Increased accessibility to nuclear material and expertise
 - ❖ Security of Russian weapons, materials, and expertise has decreased
 - ❖ Dispersal of nuclear materials around the globe, in general, has increased
- Proliferation and regional security issues
- U.S. Military Strategy (e.g., overseas bases, carriers, NMD)
 - ❖ Could our 21st Century National Security Strategy increase the military and/or strategic value of unconventional nuclear attack?
- Unconventional National Use
- Sub-national use
- Terrorism
 - ❖ Trend to larger scale incidents?
 - ❖ Increased technical sophistication and dissemination of knowledge?
 - ❖ Low public tolerance of risk?

Figure 12.

As discussed previously, the NEST program was designed around the nuclear threat, the importance of which has been recognized for over 50 years. But the situation has, in fact, changed, and we think that the nuclear threat has increased. There is increasing accessibility to nuclear materials and expertise. There has been a persistent pattern among nation-states and terrorist groups seeking, or at least probing to determine whether they could possibly buy, nuclear material or expertise. The security of Russian weapons materials and expertise has decreased. While we had a global standard of protection that was high and reasonably uniform during the Cold War, that standard has been significantly lowered in the one nation where a large fraction of the nuclear materials in the world is currently held.

Proliferation has been persistent, and we continue to see interest on the part of countries like Iran and Iraq (and many others) in the area of nuclear weapons. This proliferation is enabled - and exacerbated - by the global spread of relevant knowledge and technology (and possibly by increasing accessibility of nuclear materials). The dominant military capability of the United States creates incentive for potential adversaries to attempt to compensate by exploiting potent (and "asymmetric") capabilities such as Weapons of Mass Destruction and information operations. Nuclear weapons may be favored by some adversaries because of their immediate and certain (and, of course, massive) effects. This inclination may be enhanced by U.S. military strategy itself, which has been to

reduce the number of overseas bases and focus on aircraft carriers as the heavy support to Marine forces overseas. Even the National Missile Defense - a light defense against a few weapons - could create some motivation for parties to consider, if they have nuclear weapons or choose to procure them, delivering them via unconventional attack.

The term "Sub-national use" in Figure 12 refers to organizations such as Al'Qaeda lead by Osama Bin Laden, or Aum Shinrikyo lead by Shoko Asahara. These two organizations have expressed an interest in weapons of mass destruction. Groups such as this may have substantial resources well beyond those of typical terrorist organizations in the past. They can be composed of a small or large number of people, they may have direct access to chemical processing and manufacturing facilities of the highest quality (i.e., investments of hundreds of millions of dollars), and their participants may include highly educated people.

Terrorism continues to be a problem, and we have noted in Figure 12 the trends toward larger scale incidents, increased technical sophistication and knowledge, and low public tolerance of risk that people tend to believe are currently associated with terrorism. We pose these as questions because they are somewhat controversial. But for many years, a bellwether indicator for the nuclear community has been a terrorist groups' level of technical sophistication and ability to perform complex technical activities. As that level and ability increase, the likelihood that terrorist groups will use nuclear weapons or materials increases apace. There may also be a trend in terrorism and its motives and methods toward less inhibition against - or, indeed, increased desire for - creating large numbers of fatalities. The intentions of those who attempted to destroy the World Trade Center exemplifies this trend.

Also, global nuclear materials inventories continue to grow and spread, affording opportunities for theft, illegal sale, or national diversion of these materials for the purposes of nuclear explosive development. (Of course, in some cases these materials require significant processing before they can be used in nuclear weapons.)

The Problem As We See It Has a High Overlap with DOD

- DoD's explicit responsibilities
 - ❖ Military operations in war
 - ❖ Preparedness in periods of tension
 - ❖ Force and capabilities protection
- DoD's shared responsibilities
 - ❖ Shared domestic infrastructure (e.g., communications, transportation)
 - ❖ Protection of overseas citizens, companies, and
 - ❖ Allies and international
- DoD's unique capabilities (ref. ATSD/CS, JTF, JSOTF) (e.g., aircraft, ships, material, manpower, expertise)

Figure 13.

We tried to look at the whole problem of protecting the United States and its assets at home and overseas, from the unconventional nuclear threat and we started by looking at the problem's association with the Department of Defense. Clearly, if we consider the unconventional nuclear threat as not being limited to terrorism but, in fact, being broadly-defined (*i.e.*, a nuclear threat not delivered by ICBM (Intercontinental Ballistic Missiles), SLBM (Submarine Launched Ballistic Missiles), bomber, or cruise missile but by some other, unconventional method of delivery by either nation-states or terrorists), we see a high degree of overlap with some major responsibilities of the Department of Defense: successfully prosecuting war, preparedness in times of tension (perhaps leading to conflict), and force and capabilities protection.

DoD also shares a number of other relevant responsibilities with agencies of the federal government. For instance, the domestic infrastructure (*e.g.*, communications, energy, and transportation) could provide rich targets for attack by an enemy. This infrastructure is also a key capability required and used by Department of Defense and military operations during conflict. DoD and other agencies share responsibility for protecting this infrastructure. DoD also shares responsibility for protection of overseas citizens, companies, and assets, and for U.S. allies and international infrastructure.

As noted in Figure 13, there is no question that the DoD has unique and valuable capabilities to address the larger domestic problem of the unconventional threat. These include consequence management activities under the Civil Support

functions reporting to the Assistant to the Secretary of Defense for Civil Support (ATSD/CS) and the crisis management activities under the Assistant Secretary of Defense for Special Operations and Low Intensity Conflict (ASD/SOLIC), which include the Special Forces capabilities. In addition, DoD's aircraft, ships, materiel, manpower, and expertise are clearly of value in addressing this threat problem.

Unconventional delivery of nuclear explosives against U.S. warfighting capability (especially U.S. military bases in CONUS and overseas) may be a particularly attractive option for an adversary in times of crisis or war. Unconventional delivery offers less potential for attribution, does not require a missile delivery capability (which would be ineffective were the United States to deploy missile defenses), and results in the massive, immediate, and certain effects of nuclear explosions that are well suited to achieving desired military effects. DoD unequivocally has the prime responsibility for dealing with such possibilities.

DoD also has increasing responsibilities for support to civil authorities in homeland defense. The Department's ability to carry out large operations under highly stressing conditions is unmatched for both protection of military assets and support to civil authorities.

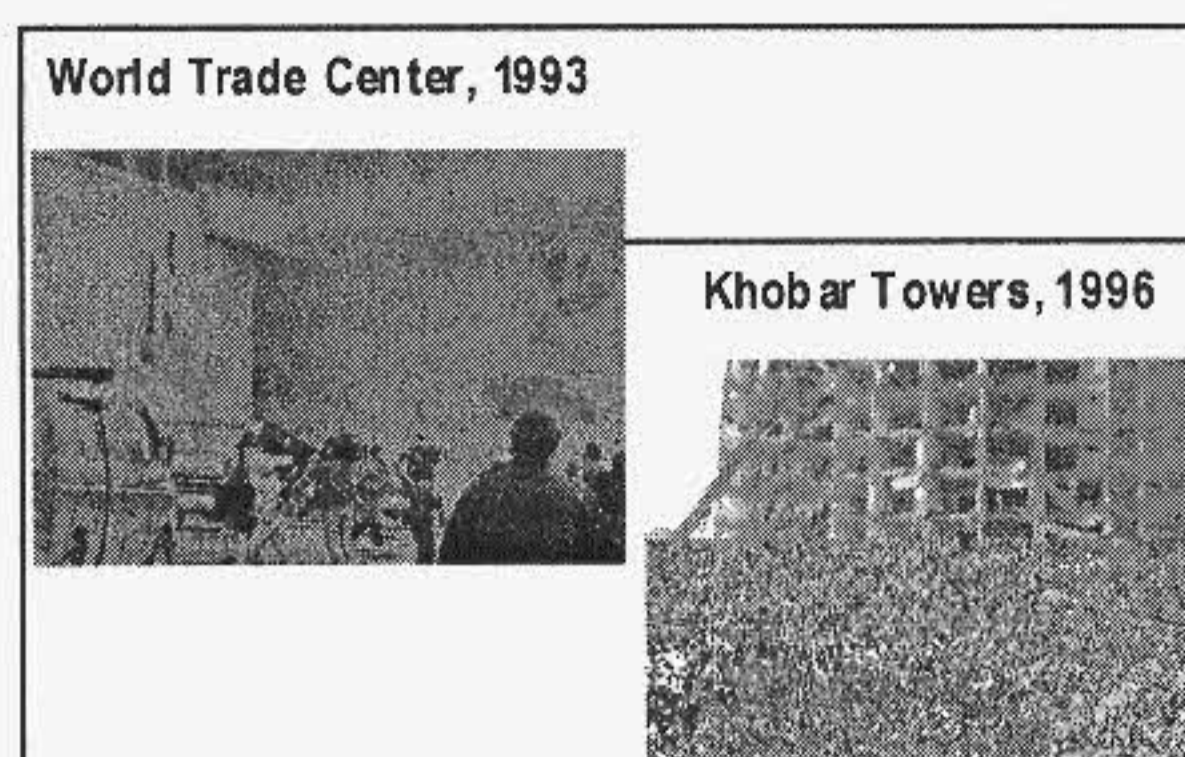
Therefore, the long-term potential of the capabilities that we recommend developing is not limited to missions that are solely the DoD's responsibility. These near-term DoD (and DOE) developments will be effective stepping-stones toward long-term capabilities for effective, widespread homeland defense.

The "Homeland" Faces a Diversity of Potential Unconventional Nuclear Threats

State-Directed Attack



Terrorism



- Most likely unconventional nuclear threat to the homeland is an attack executed or supported by another country
- Most credible targets will be rational (military, policy, economic) that fall within the broad responsibility of the DoD

Figure 14.

The homeland faces a diversity of threats. Terrorism, illustrated by two notorious examples on the right side of Figure 14, continues to be an important issue. We believe special attention should be paid to nation-state-directed or nation-state-complicit attacks on military assets, in times of tension or war, as elements of revenge, or as attacks in response to a U.S. policy.

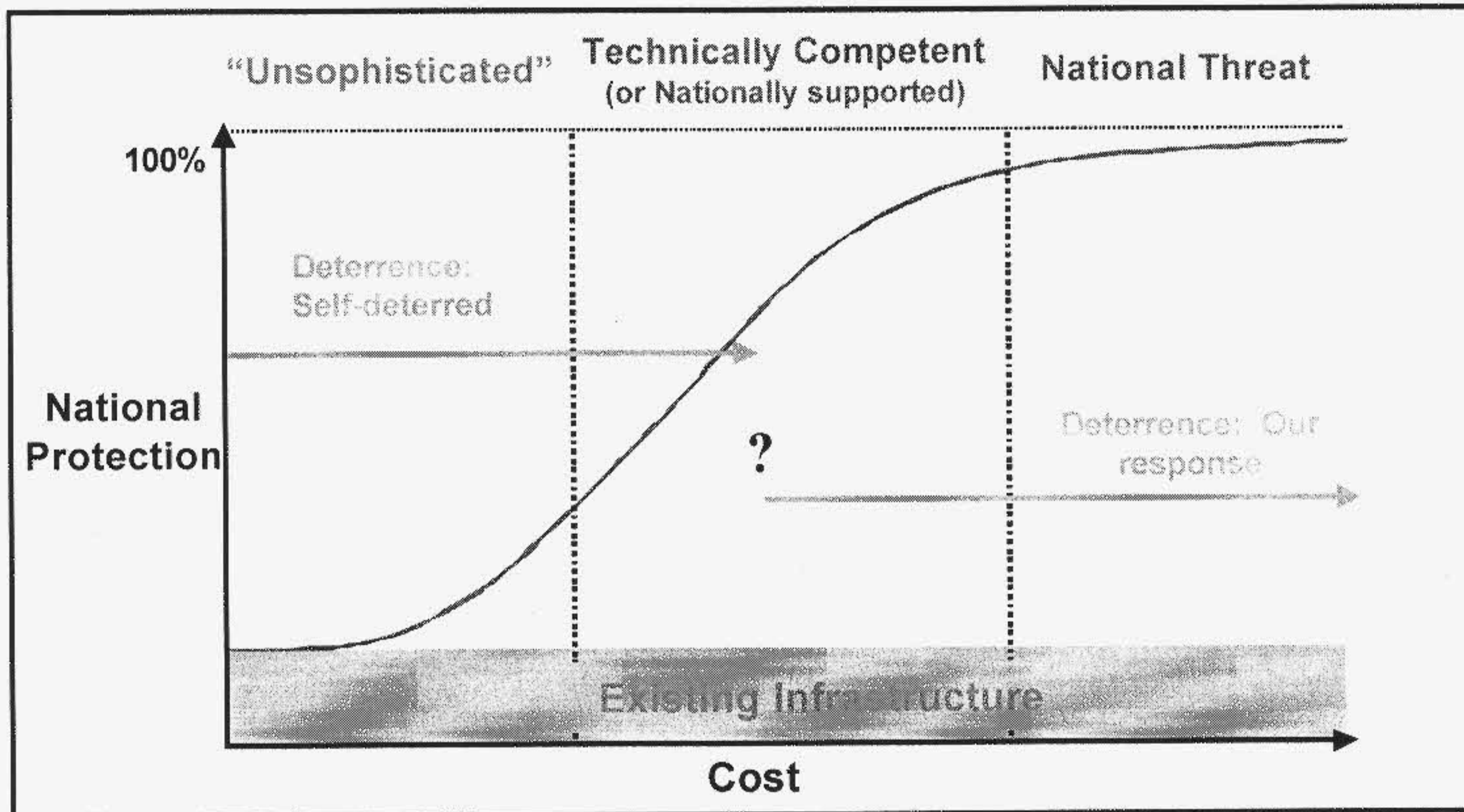
The most likely unconventional nuclear threat to the homeland may be, in fact, an attack executed or supported by another country, as opposed to a collection of people classically perceived as a "terrorist group."

For some time now, the predominant assumption has been that clandestine emplacement of a nuclear explosive in the United States or against its interests would be the work of terrorists. But the task force believes that unconventional delivery of nuclear explosives by nation-states, or by groups sponsored by nation-states to achieve state-related objectives, should receive considerably more attention than this class of scenario has received in the past.

The task force believes that nation-states are more likely to have the capabilities needed to carry out an unconventional nuclear attack. The immediacy and certainty of the massive effects produced by nuclear weapons may be more

suiting to the needs of a nation-state, including its military objectives in war. If this proves to be true, then the most credible targets of unconventional nuclear attacks by nation-states will be rational, *i.e.*, they will involve military, policy, or economic targets that fall within the broad responsibility of the Department of Defense.

Allocation of Resources to Achieve Protection Against Unconventional Threats is a Complex Function Without an Absolute Assurance



The psychological dimension is an essential consideration, but not subject to confident quantification.

Figure 15.

Allocating resources to achieve protection against unconventional threats is very complex because the variety of threats is so broad - ranging from a terrorist threat, such as a malcontent gaining access to nuclear material and dispersing it, all the way up to a country using a nuclear weapon in war in an unconventional fashion.

Figure 15 schematically depicts the fraction of "National Protection" against unconventional threats as a function of cost. The curve depicts the fact that attempting to obtain 100% protection against this broad range of threats is simply not possible - the function is asymptotic. As a nation, we can pour money into this endeavor. However, at some point, regardless of what is done, an enemy with comparable assets, given as much (or more) time than we have, will find a way to beat us - especially since *he* picks the target(s), time(s), and circumstances.

The task force believes that there is a base level of national protection provided by 1) the preexisting infrastructure of national protection provided by border protection capabilities, intelligence activities, and nuclear and criminal forensics capabilities and 2) by the technical complexity of constructing or obtaining a nuclear device. This implies that any additional efforts will result in increased protection and indeed, the cost axis reflects increases in spending above this baseline.

On the left-side of the chart, we see that there are many things we can do regarding the unsophisticated nuclear threat. In fact, one agency has deployed a variety of "beepers" containing nuclear detectors, and security and customs people carry these at airports and other locations. The fact that they have done this, and the fact that the beepers are widely dispersed, provides a reasonably significant level of deterrence against individuals who might start contemplating the use of nuclear devices - but then are dissuaded, believing such precautions have made the problem "too hard."

Low-cost methods that are widely dispersed have a very strong psychological effect and are a deterrent against a class of threats that are, perhaps, less sophisticated and less persistent than one might find in a nation-state-based threat. Hence, we can achieve a level of deterrence against this class of threat that is based either on the fear of detection before carrying out the threat or the perception that the technical requirements required to carry out the threat successfully are overwhelming.

How far we can extend that to technically competent groups (or groups that are nationally supported, *e.g.*, an unconventional threat by a country) is an interesting question for which we do not have a clear-cut answer. However, the deployment of equipment, the advertising of our deterrent capabilities, and the advertising of our national concern do not, in many respects, attract more threats but, rather, diminishes the threat. This is not an obvious conclusion since one might argue that, in some cases, knowledge of our systems might encourage certain groups to try to develop countermeasures against them. Thus the level and type of knowledge that one might want to disseminate would need to be quite selective and play into the psychological dimension of this problem.

At the other end of the cost spectrum, it is very hard to prevent national threats, *i.e.*, countries that might launch an unconventional attack against a U.S. base overseas or against U.S. forces (*e.g.*, against an aircraft carrier). However, the certainty of reprisal and the absolute certainty that, through intelligence and forensics, the perpetrators will not be able to escape attribution together act as a deterrent.

There is no question that we must consider the psychological dimension of how we actually achieve deterrence on these two ends of the spectrum - and how it overlaps into the central region of the curve in Figure 15. So there are elements

that figure into this that are psychological, and elements that are technical in their nature. These elements, however, are not subject to confident quantification, and the task force was unable to probe the relationship between the psychological and technical elements well enough to make substantive recommendations at this time (see Recommendation #6 below, where a systems analysis of this issue is proposed).

The central region in Figure 15 is where our strategy is focused. This allows decisions of investment that move us far enough up the "knee" of the curve that we still obtain quantifiable improvements in protection while making reasonable investments. Such improvements could occur by increasing the protection of the sources of nuclear materials that are still less-than-well-protected in Russia. Improvements could also be realized by designing deployable capabilities that could be used to protect key high-value assets during times of tension or upon being cued by intelligence assets. Finally, improvements can be made in intelligence and forensics. These include the ability to attribute actions in order to bolster deterrence, and increased intelligence to support detection, interdiction and attribution.

THIS PAGE INTENTIONALLY BLANK

We Support the Conclusion of the 1997 DSB Summer Study: It is Possible, Over the Long Term, to Adequately Deal With the Unconventional Nuclear Threat

- It is possible to protect nuclear materials/weapons very well
- Most nuclear threat operations are likely to be large enough to have significant observable signatures
- Networks of advanced correlated sensors have the potential to detect presence/transit of nuclear materials over base- or city-sized areas
 - ❖ A wider range of threats can be approached by scaling up on mobile deployment
- Forensics and intelligence can provide attribution and thus deterrence
- Synergies in a layered defense help us:
 - ❖ Better protection forces more observable threat operations
 - ❖ Both protection and attribution deter (esp. state-complicit threats)

“Very little implementation”

Figure 16.

The problem of the sub-national threat to the United States was addressed in the 1997 Defense Science Board Summer Study. The findings of that study, and its recommendations, are hard to dispute, *e.g.*, better protection of nuclear materials at the source; improved intelligence to detect threats before they can be executed; the focus and emphasis on NEST and rendering safe the nuclear devices the NEST team finds; improved ability to attribute nuclear explosions or operations by intelligence and forensics; and strong recommendations in research and development. Our task force is comfortable with all of these recommendations.

On the other hand, except for an increased investment in the protection of Russian materials through Department of Defense and Department of Energy activities, there has been very little implementation of these recommendations. Essentially no real, meaningful progress has been made on most of the other recommendations from the 1997 Summer Study.

THIS PAGE INTENTIONALLY BLANK

Complete Protection May Be Unrealistic



- Ports of Entry: 427 total
 - ❖ 158 border crossings
 - ❖ 170 seaports
 - ❖ 99 airports
- Commerce: 12M containers a year, only 3% inspected
- Major Cities: 201 cities >100,000 population
- Nodal points: many important transportation nodes

Figure 17.

The problem of "complete protection" is a difficult one if we look at protection of the United States as a whole. The 1997 DSB Summer Study addressed, in a rational and thoughtful way, the question of how one would start to approach this problem, including preparing for surge capabilities and deployable capabilities instead of trying to protect everything.

We can see, from Figure 17 that the problem that was evident during projects *Screwdriver* and *Doorstop* was also evident in 1997, and it continues to be an important problem today: there is an enormous number of legal ports-of-entry into the United States and a large amount of commerce passing through these ports. For example, 12 million containers enter the United States annually, and only 3% of them are inspected; furthermore, that "inspection" is mainly an examination of paperwork, rather than an actual opening of the container. A small fraction of these containers is then subjected to more detailed inspection, including x-ray inspection. This level of surveillance is partly a manifestation of the fact that the load and the burden of interrupting commercial traffic is still felt to be extremely high when balanced against the actual likelihood of the threat. We find that this same percentage, 3%, applies to containers, cars, and vehicles that are inspected by the U.S. Border Patrol searching for illegal aliens and contraband. So "3%" may, in fact, represent the limit of the ability of Customs and Border Patrol, as currently staffed and funded, to actually perform a more detailed interrogation.

Of course, we must add to this all of the other possible illegal pathways into CONUS. Many government agencies claim responsibility for protecting our borders from the illegal entry of contraband, including the U.S. Customs Service at the ports-of-entry, the U.S. Border Patrol for our land borders with Canada and Mexico, and the U.S. Coast Guard for our coastal borders. These agencies are not well coordinated and do not apply equal emphasis to contraband interdiction. The U.S. Coast Guard, for example, considers its principal mission to be search-and-rescue. The other two agencies appear to be overwhelmed by the massive flow of material crossing the borders.

To illustrate some of the other difficulties associated with nationwide protection, a very large amount of shipping enters the Great Lakes through the St. Lawrence Seaway, and large numbers of ships enter ports such as Galveston and other locations to deliver oil to the United States. None of these ships are actually inspected until they have reached their ports. Although the Coast Guard is empowered to stop, board, and inspect a ship prior to entering a U.S. port, this power is rarely used, and not without probable cause. Therefore, ships are generally allowed access to U.S. ports, including inland ports, without being inspected before entering the port.

Therefore, because of the large numbers of border crossings and because many of the border crossings, *e.g.*, the Mississippi River, have no inspection points until the inbound traffic reaches its destination interior to the United States, there is an enormous challenge regarding the vulnerability of the country. It is difficult and daunting to approach the level at which the 1997 Summer Study recommended this problem be addressed.

There is a synergy, however, between the problems of attacks by weapons of mass destruction of all kinds and criminal activities such as the smuggling of drugs and illegal aliens. All of these involve illegal transportation of materials and people across our borders. Efforts to suppress international crime of all sorts remove resources from terrorist or other groups. Hence, suppressing terrorism and criminal activity in *all* forms - not just terrorists who want to use weapons of mass destruction against the United States - removes potential sources of recruits and resources for such activities. This makes it more difficult for these groups to sustain a program to develop and/or use weapons of mass destruction.

Approach to Recommendations

- There is a substantial, existing base of capabilities, processes, experienced people, and roles/responsibilities framework for the unconventional nuclear threat
- It is not optimized for the nuclear threat as it is emerging. It is not part of a coherent strategy
- Our principal recommendation is the deployment of protection systems built from existing technology to key military targets. Such systems would also provide a capability to deploy to a wider variety of targets upon warning
- Other recommendations are made that would lower the threat by limiting the availability of nuclear materials and by strengthening deterrence
- We recommend reestablishing a vigorous and creative R&D program to address cost and effectiveness
- A stronger base of analysis accompanied by these recommendations would lay the basis for a coherent strategy

Figure 18.

There is a substantial base of capabilities, processes, experienced people, and a roles-and-responsibilities framework for the unconventional nuclear threat. This base is not, however, optimized for the threat that we see emerging. Not only do we have an emerging threat across-the-board, but also, the unconventional *military* threat to the United States seems to be the one that needs to be addressed – and these systems are not really optimized to deal with it.

We offer six recommendations all of which are directed at the unconventional nuclear threat to military assets. These recommendations are all within the current programmatic structure and the authority of the agencies involved, and they entail modest cost. They do not require new Congressional legislation or creation of a new position or office. If these recommendations were implemented, they would form the “approach ramp” to the larger National problem.

THIS PAGE INTENTIONALLY BLANK

1. Deployment Recommendation

Finding: Military installations, especially OCONUS, are particularly attractive targets to adversaries in peacetime, during political disputes, as well as in military conflicts.

Recommendation: Deploy technology and systems to protect critical military installations.

- Conduct a Joint DTRA/NNSA ACTD-like program to test an integrated sensor network (\$30M)
- Deploy vetted technology to critical OCONUS/CONUS bases (\$2-10M per base)
- Establish a permanent technology integration testbed (\$5M per year)
- Deploy improved technology and networks to response organizations (e.g., Special Forces, FBI, NEST)

Time frame: Operational deployment (one base) by 2003

Figure 19.

The task force's first and principle recommendation, shown in Figure 19, deals with deployment. It involves an advanced concept technology demonstration (ACTD)-like project. This recommendation is a reaction to the 1997 Summer Study.

As mentioned above, the 1997 Study was rigorous, and it addressed a number of issues with recommendations that were very difficult to implement. As a result, there was no real community-organized forward movement to try to test and investigate the implications and meanings of the 1997 Study's recommendations. This is a mistake we do not wish to repeat as we frame our recommendations.

There are many recommendations we could make that would be *institutionally* very important. However, from the point-of-view of action, we think it is absolutely essential that we have an ACTD-like project that tries to integrate our capabilities, our resources, and our experience to address targets over which we can have some control. The specific objectives of the ACTD are: (i) to provide an integrated sensor test-bed for base/force protection; (ii) to leverage law enforcement, DoD force protection, and DOE technology; and (iii) to integrate, if/where possible, other types of sensors (chemical/biological/explosives) into the network.

Our finding is that U.S. military installations are particularly attractive targets to our adversaries in both peacetime and during times of military conflict. We offer two examples:

- The United States has nuclear weapons stored at a limited number of military facilities. In some cases, their continuing presence at these facilities is a very complex policy and political question, as opposed to being a technical issue. Any kind of a nuclear incident in a nearby region could, in time, be easily attributed to something other than U.S. nuclear operations. However, any event that would raise the public dialog or discussion about these policy issues, in fact, begins to force the policy dimension of discussions in a direction that's not as controlled. Therefore, groups could use a nuclear incident at one of these sites to create tremendous problems for the United States.
- The U.S. military maintains key bases for the forward deployment of air- and land-forces during periods of conflict. These key bases may be very attractive targets in terms of interdicting the forward flow of materiel, manpower, and air assets. There are other military installations overseas that have symbolic or political meaning or association with policy - as well as having a practical relationship to military operations - that would make them very attractive targets for unconventional attacks. Some of these attacks could involve radiological dispersal systems, which are easily accessed by various groups.

We think that a systems demonstration project can stimulate the development of a coherent strategy and investigate the relationships between and capabilities of current sensor technologies and can also produce a tangible product, as is really required.

The task force recommends that there be a joint Defense Threat Reduction Agency-National Nuclear Security Administration (DTRA-NNSA) program with one of the military services (*e.g.*, the Air Force) to develop and test an integrated sensor network. We are not proposing the development of a whole set of sensors. Instead, we are recommending taking the inventory of existing sensors, experience, and capabilities already on-hand, integrating them into a security perimeter, and testing the deployable or extendable network on Red Team and Intelligence data. If executed correctly, we will gain experience with operating integrated sensor systems, their interface with law enforcement and DoD protection forces, and the cost of deployment or ownership of such a system at a military base. This demonstration would also provide a framework for the integration of other sensors (*e.g.*, existing or developmental chemical, biological, or explosive sensors) into a network for force protection at a military base.

A Systems Test-Bed of Correlated-Sensor Networks Around Kirtland AFB

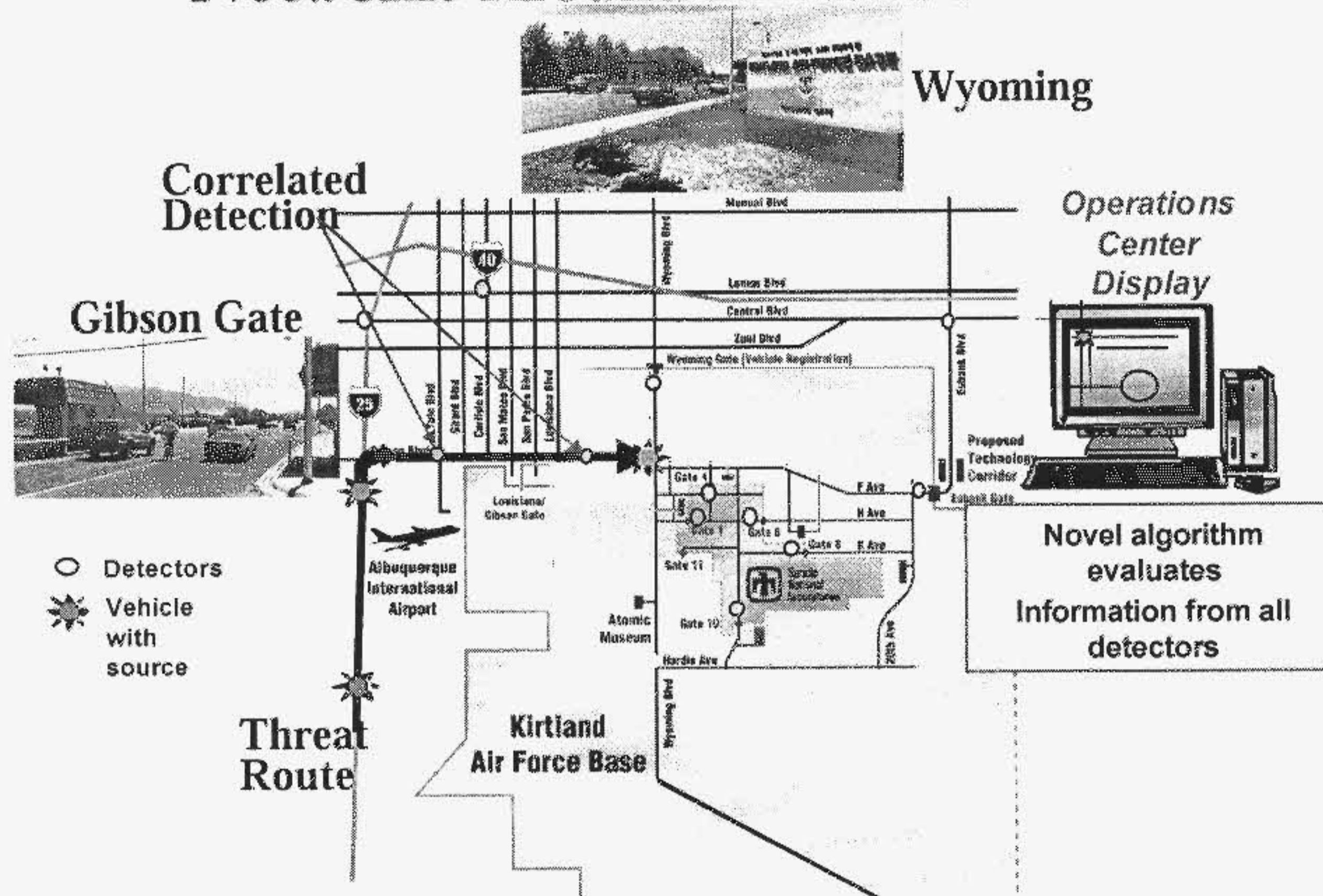


Figure 20.

We show, conceptually, the kind of systems demonstration we have in mind. The task force has identified a military base that would provide a very low-cost demonstration framework. Kirtland AFB happens to be the home to a variety of organizations, including Sandia National Laboratories, part of the field group of DTRA, the Department of Energy, - and Los Alamos National Laboratory is not far away. The Air Force has an existing security structure at Kirtland. The facility is not a SAC (Strategic Air Command) or TAC (Tactical Air Command) base. Rather, it operates in a "landlord" capability as a collective group of people and entities.

The task force recommends that the proposed systems demonstration of a correlated sensor network be sited at Kirtland Air Force Base. A very early version of a correlated sensor network was field-tested for a very short period of time. However, it is critical to field an improved system for a much longer interval to learn how such a system functions in a real-world environment.

The network would incorporate different types of sensors, *e.g.*, radiation detectors, video cameras, vehicle detectors, and high explosive detectors - all of which are existing technologies. One key feature is to use a new algorithm that combines the information from all of these sensors on a real-time basis. The algorithm would examine the data to look for a pattern of detector "hits" that are diagnostic of the expected threat - *e.g.*, consistency with a vehicle moving along

the street grid. The algorithm would then calculate the likelihood and location of possible nuclear sources. This correlation algorithm would provide substantially improved detection, while simultaneously maintaining a low false alarm rate, crucial for detecting weak sources. Without the correlation algorithm, the threshold for detector hits can be lowered in order to see weaker sources, but the concurrent false alarm rate then becomes so high that interdiction is no longer practical.

Kirtland is well suited for this demonstration because it has nuclear reactors, radiation sources, and other nuclear materials on-site. Nuclear material crosses the base perimeter frequently. Since DTRA, DoD, and Sandia are located on the base, much of the needed equipment required to support this demonstration is close-at-hand. And this program could be executed relatively quickly. After the core of the operating system is demonstrated in day-to-day operation in Kirtland's existing security network, it would then be deployed into the urban area adjacent the base. Exercises would be conducted against cued targets or against targets that were detected by remote sensors.

The demonstration should test the capability for current-generation radiation detectors to provide an energy-resolved analysis of the radiation signals. This feature is important for two reasons:

- First, the world contains many radiation sources (medical isotopes, industrial sources, processed materials) that are not the targets for this network. These create "nuisance" alarms that should not activate the interdiction forces. Energy-resolved detectors enable distinguishing these nuisance alarms from the nuclear materials of concern.
- Second, highly enriched uranium (HEU) is very difficult to detect, especially if shielded - yet it is one of the two most likely nuclear materials in a weapon. Compounding the problem is that natural uranium is dispersed throughout the environment (soil, building materials, etc.). Energy-resolved analysis provides a means of distinguishing HEU from natural uranium.

As mentioned above, this demonstration could serve as a test-bed from which networks are deployed out into the city of Albuquerque. Reasonably good working relationships have been established between the cognizant federal agencies and local law enforcement in test exercises conducted against either cued-threats or on the basis of intelligence warning. The system operations would be observed and challenged when running multi-agency, multi-sensor networks.

The task force also believes that a demonstration system like this is a reasonably cost-effective system that could be used to run some of the NEST exercises already being conducted. And because development of new sensors is not involved, we estimate a cost for the initial demonstration of ~\$15M over two years.

Once a capability is developed at Kirtland, we recommend deploying it to critical CONUS and OCONUS bases. The deployed sensor networks would act as a part of the integrated whole of the bases' security systems that are extended outward upon warning (*e.g.*, entering a heightened DEFCON status). In this way, experience will be gained with integrating the extended sensor net with the civilian part of a city or other area, a complex problem for the military.

In addition, the task force recommends that there be an additional test-bed - perhaps at Kirtland - where the integration of sensors into network and traffic control systems can be tested, along with the sensor software algorithms and the interface with intelligence warning and interdiction.

This demonstration offers an opportunity to get past the "bump in the road" for the first time. It enables getting started in a location where we believe there's likely to be a very strong force protection need to test these capabilities for military bases.

In the process of conducting this system demonstration, we believe that, in two years, relocatable systems can be developed and deployed that could be added to the NEST inventory and be available to the FBI and the military to protect assets, *e.g.*, continuity of government in Washington, D.C. This could mean establishing a set of fixed sensors, *e.g.*, in the national Capitol area, with an extendible set of sensors and networks. Through the system demonstration recommended by the task force, knowledge and experience will have been gained in the operation of the sensor net in a tactical situation that enables dealing with an issue that is, in fact, strategic in nature - an unconventional nuclear attack on a major national asset.

THIS PAGE INTENTIONALLY BLANK

2. Intelligence Recommendation

Finding: IC deficient in nuclear technical expertise, especially for strategic/tactical I&W of nuclear threats. There is a need for greater speed and much better sensitivity to technical indicators to support interdiction.

- Nuclear intelligence capabilities are thin in IC
- DOE labs maintain in-depth nuclear expertise including for the IC

Recommendation: "Operationalize" National Labs' technical expertise role for I&W assessments

- Define roles and responsibilities (DCI, DoD, DOE, FBI)
- Establish information sharing protocols and capabilities
- Exercise full system for specific intelligence targets: asset cueing, screening, analysis, synthesis

Cost: \$5M per year

Figure 21.

The task force's second recommendation deals with intelligence. We found the Intelligence Community (IC) to be deficient in nuclear technical expertise, especially for strategic and tactical indications and warning of nuclear threats.

Scientific and technical expertise in the Intelligence Community matrix has diminished, and the "bench" in the nuclear area, in particular, is "thinner" than in the past. Many in the biological and chemical arenas might observe, "Nuclear is a lot better off in this regard than we are..." However, almost all of the nuclear expertise is actually resident in a government-owned distribution of laboratories - not just the weapons labs, but others as well. But most of the intelligence work with which those organizations are actually tasked has been pre-screened by analysts looking at terrorist groups. Hence, an assessment is requested if the analyst sees "something nuclear." The nuclear intelligence capabilities that are actually resident in the processing part of the Intelligence Community, or even the analysis part, are now very sparse where, at one time, they had been fairly robust. Much of the long-term expertise that still exists is resident in the government labs.

Since the 1950s, the decision was made by the Intelligence Community to vest its technical capability strongly in the Department of Energy laboratories, which includes other DOE laboratories along with the weapon laboratories. In recent years, the Intelligence Community's focus has been more and more on these

"Centers." Hence, there has been less nuclear expertise in the "line organizations" within the IC. It has become more and more clear that the ability to detect subtle nuclear signals in intelligence information that might be an indicator of a country's interests (or even a terrorist group's interests) has been reduced within the IC.

There is good reason to believe that the Intelligence Community and the Law Enforcement Community are very good at picking up indicators of terrorist activities. And we are confident that they are very competent at picking up indicators of hostility among countries.

The task force recommends "operationalizing" the national laboratories' technical expertise role for indications and warning assessments. We recommend that the laboratories, in parallel, screen nearly-raw intelligence data for subtle indicators of nuclear technical expertise. This data would include both the information streams containing terrorist information and those that address the interests of countries, such as Iraq, Iran, and others. Analysts must watch for more subtle indicators than merely the presence of plutonium or bombs. One must look for the second-order or third-order effects that are so familiar to people who work in the nuclear business day-to-day.

There is a strong analog between this recommendation and the kind of recommendations that have been made with respect to the Intelligence Community's assessing of the biological threat. Roles and responsibilities must be defined. And while the question is not where the technical expertise lies, there is a bit of a culture problem here. The choice of how to create a laboratory framework in the Atomic Energy Commission was different than that in the Department of Defense, and these differences produce some problems. But these are problems that have been addressed in some fashion during the last 40 years of interaction between the technical experts at the nuclear laboratories and the Intelligence Community.

Clearly, information-sharing protocols must be established to enable a network capability that allows analysts today who are doing studies to spend a portion of each day screening intelligence. We believe that this system should be exercised against specific intelligence targets to look for cueing. This is a relatively low-cost investment - it is at the margin, because the capability is already in-place.

The government entities with responsibility to decide how to do this, presumably through a Memorandum of Understanding, are the Director of Central Intelligence (DCI), and the senior management of the DoD (including Command, Control, Communications and Intelligence [C³I]), the DOE, and the Department of Justice (the FBI). Operationally, this recommendation envisions an arrangement that is only slightly different from today's capability framework. Hence, the task force believes that this is not a difficult operational concept to implement.

3. Forensics Recommendation

Finding: Current nuclear forensics capability is inadequate to support timely response

- The ability to accurately attribute is essential to pre-event and post-event response. The current system is not matched to the problem.

Recommendation: Modernize and improve the nuclear forensics capability and focus the system to better match requirements

Cost: \$50M over 5 years

Figure 22.

The task force's third recommendation goes to the question of forensics, and it has a strong parallel to a recommendation made in the biological arena.

Currently, the task force believes that the nuclear forensics capability is largely adequate. If nuclear material is obtained, it can, in fact, often be traced back to its source. However, the current nuclear forensics capability is not set up to provide the level of evidentiary quality and timeliness of response that is needed to provide the deterrent that assures that the U.S. can act (i) promptly against perpetrators, and (ii) with a high confidence that those identified are, in fact, the culprits. We believe that the characteristics of *timely response* and *accuracy* are, in fact, essential to the pre-event and post-event response. The current system needs to be modernized and improved to better match current and emerging requirements.

This need is hardly arguable among the various groups involved, *e.g.*, the Air Force Technical Applications Center (AFTAC) in Florida, DTRA, and DOE. We need action on this recommendation.

THIS PAGE INTENTIONALLY BLANK

Specific Elements of a Forensics Initiative

- Establish an MOU between DoD/DOE/DCI/DOJ (FBI)
- Multi-agency funding plan should be part of MOU
- Reconfigure DOE and AFTAC capabilities to allow for more rapid assessment, including capability for field measurements
- DOE should establish rapidly accessible forensics database (physical, isotopic, trace, process knowledge). Historical data is perishable; time is of the essence.
- Establish a high level group of experts (“Bethe Panel”) to review technical assessments for attribution
- DOE should establish appropriate working arrangements for international cooperation for access to experts, “proprietary” databases, and samples
- All participants should regularly exercise; publicize capability

Figure 23.

We propose an initiative to establish the nuclear forensics capability that is needed for this threat. Figure 23 lists some of the elements-of-action for a forensics initiative. A nuclear forensics capability requires a community of experts from DoD (DTRA and AFTAC), DOE, and FBI. An MOU should be established among these organizations. A multi-agency funding plan should be included as part of the MOU. A process needs to be defined for properly executing a nuclear forensics investigation. The process should include assignment of well-defined roles for each participating organization. The resulting community of experts will “certify” the science of the nuclear forensics capability.

We recommend a double-level of quality assurance. First, the capability must be validated to provide confidence in the assessment. Protocols and rigorous quality assurance and quality control (QA/QC) should be established for the forensics measurements. Second, we recommend creating a “Bethe Panel” similar to that previously used for foreign diagnostics. This panel of experts would have high visibility. It would provide the final adjudication of an assessment in dispute and ensure a high-quality standard on the output.

The requirement for arriving at an attribution assessment as quickly as possible leads to the need to reconfigure current lab capabilities. It is crucial that the experimental plan for each sample take into account all possible measurements that might be made in order to avoid destroying potential evidence. Laboratory

capabilities must be able to analyze for environmental types of measurements as well as radiochemistry on bulk samples of nuclear materials. To provide an even faster initial assessment, approaches for deploying instrumentation to the field and conducting analyses in the field should be developed.

We need to create a rapidly accessible forensics database. At a minimum, the database should include information on physical characteristics, isotopic compositions, trace elements, and knowledge about nuclear manufacturing processes. Information for interpreting data is currently incomplete and not readily accessible. The database element also includes establishing communications with international experts who may be willing to help without sharing their specific data. This type of international cooperation provides access to experts, "proprietary" databases, and samples. The entire database will be crucial for helping to identify the extent to which attribution can be done using the initial capability. It can then be used to identify gaps and limitations, which will drive new R&D and other initiatives.

It is crucial that the entire forensics capability be tested frequently. The exercises provide validation and an assessment of operational readiness. The exercises can also be used to identify gaps in the capability, especially to the extent that exercises are designed to be increasingly more challenging. The existence of this capability, and its exercises, should be widely publicized. The goal is to create the public perception that we have a strong nuclear forensics capability that can provide credible attribution. The perception of near-certain attribution is a strong deterrent.

4. R&D Recommendation

Finding: The technology and capabilities necessary to address the nuclear problem are not adequate. Current R&D investments responsive to the nuclear threat have sunk to historically low levels.

- Nuclear threat response R&D funds have been diverted to meet pressing operational needs or perceived higher priority R&D investments

Recommendation: DTRA and NNSA should systematically develop and execute a nuclear threat response R&D program that at least in part restores the historic balance between operational needs and sustaining R&D investments. This shared responsibility should be codified in a MOU between DTRA and NNSA.

- Additional R&D resources should be focused on increased effectiveness and affordability.
- The required investment is modest (~\$10 M/yr) and could be partially offset by reprioritizing existing funds.

Figure 24.

The task force's fourth recommendation addresses the NEST program.

NEST has worked well for decades and has produced many tools and capabilities. However, over the last five to ten years, the ratio of investment in R&D versus operations has sunk to historically low levels, and we believe it is now below that which is needed to sustain or build the capabilities that we need. There was clearly a shift over the last five to ten years that put more and more of the available assets into operations.

The task force believes that this imbalance must be corrected. But this is not an enormously expensive investment - it's actually a rebalancing of investments. The task force believes that the key players are NNSA and DTRA and that they should work together to establish an R&D program that, in part, restores that historical balance. This is a shared responsibility, and the task force believes that an MOU would be very appropriate here. At no time in the past have the interests of these two organizations coincide more closely. This is a very opportune time to work the partnership into a formal understanding.

Again, the shifted resources (or the additional required resources) are modest in character - perhaps in the neighborhood of \$10M.

THIS PAGE INTENTIONALLY BLANK

R&D Examples

- Active neutron and gamma interrogation systems
- Gamma imaging
- Unattended remote monitoring systems
- Better and more affordable radiation detectors
- Portable forensics (“lab on chip or in a box”)
- Perimeter networks of sensors with remote processing capability
- Render safe

Figure 25.

Figure 25 shows some examples of the capabilities that we recommend pursuing. They include, for example, active interrogation systems that could actually be fielded, portable forensics, and development of new and advanced perimeter monitoring.

Active neutron and gamma interrogation systems are needed that could be deployed to detect the presence of HEU, and also plutonium, in circumstances where it is shielded. The ability to use shielding to defeat passive detectors is a vulnerability that needs to be addressed. We have known for 40 years how to build active neutron interrogation systems that “probe” an object containing small amounts of enriched uranium with incredibly high sensitivity. We have used this technique to assay barrels of waste material – yet we have never built or made available even a prototypical deployable system.

Gamma imaging systems can serve two purposes. They are useful in providing diagnostic information on devices that might be detected. They also provide a means to reduce the background noise and thereby improve the sensitivity of detection.

Unattended remote monitoring systems are needed for a wide range of applications. Otherwise, the deployment of detectors and sensors will be operationally constrained by the availability of personnel. There will also be a number of locations where remote sensors could be placed where it will not be possible or desirable to station personnel.

Better and more affordable radiation detectors are needed in order to allow wide-spread use by operators who do not have a high degree of technical training.

Portable forensics systems ("lab in a chip or box") are also needed in order to have the capability to rapidly analyze samples for initial characterization purposes. Although more detailed forensics may be necessary for accurate attribution purposes, this initial characterization could be very important in determining the level of complexity of a nuclear explosive device (following its detonation), and in providing a quick determination of the required level of sophistication of the adversary involved.

Perimeter networks of sensors with remote processing are needed to support the correlated network systems demonstrated in the ACTD described in Recommendation #1. The remote processing ability will allow the sensors to use on-site processing to analyze signals being received in order to reduce the total numbers of signals sent to the central processing systems. This reduces the background noise, and thereby false alarms, and also increases the sensitivity of the overall network.

Finally, render-safe R&D is needed in order to expand the capability and numbers of personnel that are qualified to render safe a wide variety of devices that might be detected. Improved technical capabilities could facilitate the expansion of the number of personnel trained for such operations. It could also expand the knowledge base regarding the types of devices and render-safe techniques needed.

5. "Better Control of Materials" Recommendation

Finding: Cooperative programs to secure nuclear materials in Russia are vital to managing the nuclear threat

- Russian materials, 200 tons Pu and 1000 tons HEU, represent a potent source to fuel the nuclear threat
- Most of this material is under substandard safeguards and security
- Dollars spent in Russia to control these materials are heavily leveraged in our favor

Recommendation: DTRA and NNSA, as joint executors of these programs, should jointly develop a systems approach that produces the maximum security of Russian materials in the shortest possible time and at minimum cost to the US

- This strategy should *inter alia* balance investments in securing materials at facilities and sites with investments in search and recovery and securing borders
- The agencies must stay the course as this cannot be done overnight
- It is important to focus on strategies that produce maximum near-term gain in overall security of Russian nuclear materials

Cost: Within current program

Figure 26.

The task force's fifth recommendation, regarding nuclear materials, takes aim at the *sources* of material that could be used to mount an unconventional nuclear attack, rather than trying to detect the nuclear material being delivered to a large target set over myriad pathways.

We want to complement the programs that DOE and the DoD, under Nunn-Lugar, have been executing in protecting Russian nuclear materials and also raising the standard of that protection. The long-term DOE and DoD cooperative threat reduction programs to help Russia secure, reduce, and dispose of their weapons, material, and infrastructure should be continued to at least 2010 at their present funding level (\$650 M per annum). These programs have now been extended beyond their original FY02 termination date, and a second generation of programs has been initiated (partly due to encouragement from the 1997 DSB Report).

There are a number of potentially promising next steps for the second generation of cooperative threat reduction programs:

- Projects that irreversibly reduce and dispose of weapons and materials, *e.g.*, warhead dismantlement and Pu disposition

- The accelerated conversion of some of the weapons production capacity in the ten nuclear cities in Russia
- More urgent consolidation of nuclear materials at fewer sites
- Collaboration to help assure that alternative nuclear fuel cycles and reactor exports are resistant to proliferation by third parties (*e.g.*, Iran)
- Programs (discussed on the next chart) that provide additional layers of materials security in Russia, but which are outside the facilities themselves

While the task force generally endorses these proposals, we note that neither DoD nor DOE has developed a strategic plan for the next ten years in which the options are prioritized and well understood by Russia, the Congress, and those executing the programs in the Administration. We suggest a systems approach to help set these priorities and explain the program.

Our recommendation is that DTRA and NNSA, as joint executors of these programs, need to develop a systems approach that produces the maximum security of Russian materials at their borders. While directly protecting the sources of nuclear material in Russia is important, we do not have the resources to immediately attack every source target in Russia. It will take many years to get appropriate levels of material protection, control and accountability (MPC&A) at all the important sites or to consolidate sites. A systems analysis should identify other areas that can provide a quicker increase in the overall security of these materials from the various threats in the intermediate time frame while we attempt to complete the direct protection of these materials. In particular, we have identified that increased protection at the Russian borders may be one such area, as discussed below.

Russian Ports of Entry



- 307 Ports of Entry: 55 seaports, 187 border crossings, 47 airports
- Greatest Region of Concern: Southern Border

Primary focus should start with the Southern border

Figure 27.

The map in Figure 27 shows the large number of ports-of-entry into Russia. However, only a limited set of these are very high priority targets for large containers moving across the Russian border to, *e.g.*, nation-states that might be associated with Osama bin Laden or nation-states that have, in our judgement, evidenced an interest in nuclear systems.

There are a few programs that are not underway, or are funded at low levels, that provide a layer of defense outside the Russian facilities themselves. Leveraging these programs is substantially more effective than trying to prevent the ingress of materials into every U.S. port of entry. These programs are:

- The DoD-Customs and DoD-FBI programs to assist law enforcement and border control in nation-states on Russia's southern tier with line-item assistance
- DOE's second line of defense to assist Russian Customs agencies
- Extension of ongoing collaboration on MPC&A and nuclear accident response to equipping and training on site and nearby security forces in Russia for the search and recovery of special nuclear materials (SNM) and weapons

THIS PAGE INTENTIONALLY BLANK

6. Systems Analysis Recommendation

Finding: Current understanding of unconventional nuclear threat is insufficient to support a national strategy

Recommendation: Use systems analysis approach to characterize threat classes, targets, and potential responses (OSD(P) Net Assessment, J34)

- Assess strategic impact of unconventional nuclear attacks on U.S. military's roles/missions
 - ❖ Nation-state-level threat
 - ❖ State-supported, sub-national threats
 - ❖ Terrorist groups
- Assess vulnerability of military and other high-value targets
 - ❖ Direct attacks (military bases)
 - ❖ Indirect attacks (strategic ports)
 - ❖ Major cities

Cost: \$2M - \$5M

Figure 28.

The task force believes that our current understanding of the unconventional nuclear threat – whether directed against Diego Garcia or an aircraft carrier – is not very deep. Rather, it is, typically, anecdotal. Currently, threat assessments seem to boil down to, for example, statements such as, “Osama bin Laden wants to use nuclear weapons against the United States” – with no details on how these threats might be carried out. Hence, it is impossible to decide how to respond. In reality, while there are an infinite number of possible specific ways in which unconventional nuclear threats could be carried out, there are a limited number of real physical activities that actually need to be performed.

We believe that more work needs to be done here, and this is a reasonably inexpensive investment. The task force feels, for example, that the Office of the Secretary of Defense's (OSD's) Office of Net Assessment and the J34 might be the sponsors of a set of assessment activities that delve deeper into the scenarios.

We recommend performing systems analysis at several levels in order to attain a better understanding of all aspects of the problem and to “get everyone on the same page,” so to speak. One of the problems in discussing the unconventional nuclear threat is that everyone has his own favorite scenario. The result is that discussion participants often end up talking at cross-purposes.

The task force proposes that the following types of analyses be done:

- First, because we believe that the unconventional state-sponsored threat is increasing in importance, and because this task force is looking at DoD roles and responsibilities, a systems analysis should first be performed on important U.S. military bases, both CONUS and OCONUS, to assess the threat of unconventional nuclear attacks by nation-states seeking military objectives based on asymmetrical warfare requirements. These threats should not be limited to the use of conventional nuclear weapons delivered by unconventional means, but also include the possible use of the United States' own onsite material against us.
- Second, since the threat does not begin with the attack on the bases (which is merely the end-point in a sequence of actions), the analyses need to be extended back to the point-of-origin. An end-to-end systems analysis of possible unconventional nuclear threats by state actors against U.S. military bases needs to be performed. This analysis should specifically define a set of high-level scenarios that represent the classes of possible scenarios developed in the first set of analyses. Models should be developed of the complete process, including: the decision to attempt a nuclear threat; obtaining nuclear material and other resources; designing and constructing (or purchasing) the device; transporting the device to the target; gaining access to the target; using the device; coping with the consequences; performing forensics; and implementing a response.
- Supporting the above studies, subsequent studies should be performed that examine the following:
 - What constitutes deterrence for different possible adversaries? This study would examine a wide range of possible nation-state adversaries with different motives in order to determine what strategies might be effective in preventing them from either conceiving of such a threat or carrying it out.
 - How might the adversary obtain nuclear material or weapons (if required by the scenario)?
 - How might the adversary go about designing and building devices (and possible signatures)?
 - How might the adversary arrange to deliver the device (if required by the scenario)?
 - What would be the possible signatures of such activities, and could improved intelligence detect these signatures and provide increased identification and warning?
- After these directly state-sponsored scenarios have been analyzed, then the studies could be extended to sub-national groups and terrorist groups

and/or to other important military assets such as communication networks, etc.

- Because the main inhibitor to these groups' use of these types of nuclear weapons appears to be obtaining the nuclear materials, we recommend detailed studies on how one would obtain various classes of such materials: nuclear weapons; weapons-capable material; strong radiation sources for use in RDD type devices, etc. These studies would select specific locations at which nuclear material is stored and then model a range of possible scenarios for obtaining the material, ranging from bribery and extortion to direct physical assault.
- Similarly, studies should be done on various categories of targets. What specific threats could be made? How do we currently defend against such threats? What are the weaknesses? What operational or technological resources would be needed to enhance our ability to defend against these threats? How well developed are these resources (existing, near-term, long-term, or impossible)? What can be done to improve our defenses?
- Studies should be done to examine the synergy between weapons of mass destruction threats and general efforts to control terrorism, organized crime, and drug and illegal alien smuggling. Many of the material, organizational, and operational resources and opportunities for terrorists arise from this arena. Many of the methods used in these areas by the government for detection and interception, also apply to reducing the unconventional nuclear threat.

THIS PAGE INTENTIONALLY BLANK

There is a Diversity of Scenarios That Need Deeper Understanding

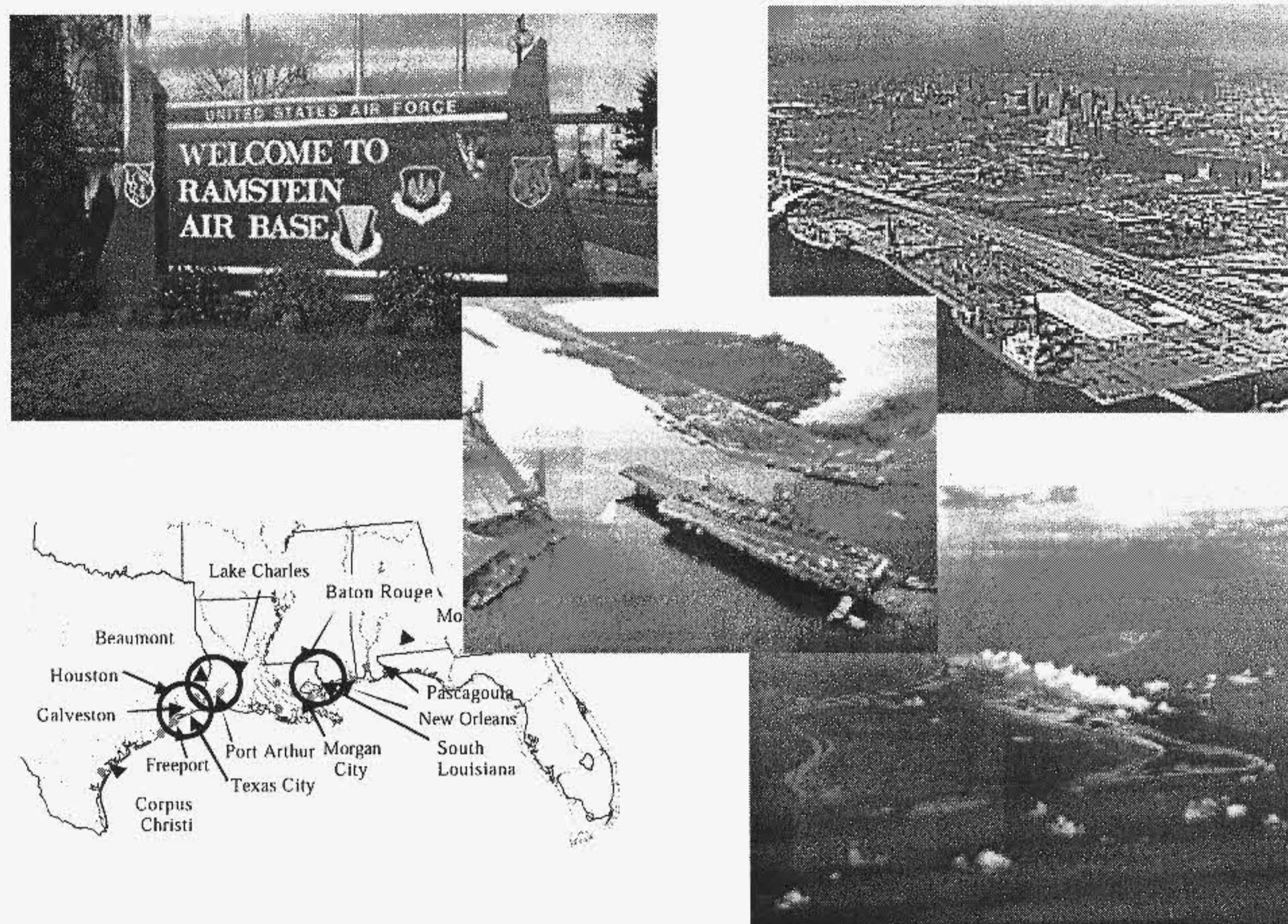


Figure 29.

Example systems analysis scenarios under our sixth recommendation would evaluate, for example, the level of protection that might be appropriate for military bases at home and abroad and for ports of entry into the United States that are of an economic nature (e.g., the St. Lawrence Seaway or ports by which petroleum enters the United States from the Gulf of Mexico).

Analyzing these diverse scenarios will support effective implementation of the other recommendations. For example, process activities and signatures will be identified in an integrated way that will allow more comprehensive and systematic intelligence analyses to be performed to identify threats in time to do something about them. Systems analysis should identify: (i) the areas of greatest potential benefit for quickly increasing the overall security of nuclear materials in Russia, and (ii) weaknesses and improvements needed in how we can defend against these threats. Moreover, the analyses will identify important weakness and needed research and development for improved technology.

Recommendations

1. Deploy technology and system to protect critical key targets
2. Change the processing of intelligence collections to increase the sensitivity of detection of nuclear indicators
3. Improve nuclear forensics capabilities to achieve accurate and fast identification and attribution
4. Rebalance (perhaps enhance) resources to reestablish a strong research and development base
5. Continue investment in Russian nuclear security but create a strategy and systems approach to investment and deployment better matched to threat
6. Develop a body of studies and analysis to better characterize the variety of unconventional nuclear threats

These recommendations are within current program structures, are within the authority of current agencies, and are reasonable in cost

Figure 30.

The task force has made six recommendations. We believe that they would create a more effective national strategy and capability for dealing with the unconventional nuclear threat. These recommendations are within current programs, within the current authority of cognizant agencies and are modest in cost.

Our Strategic Approach

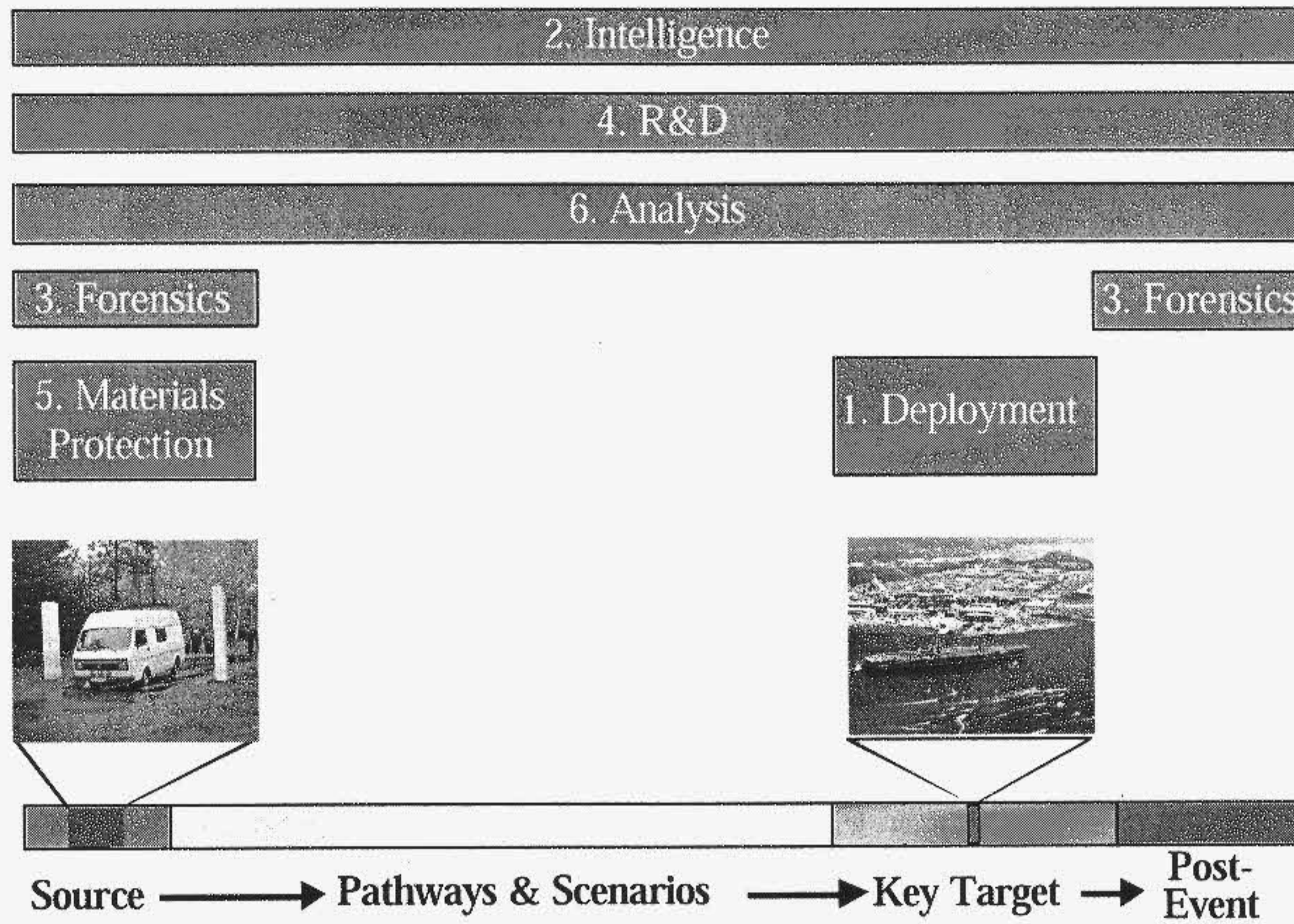


Figure 31.

We summarize our task force’s strategic approach to the unconventional nuclear threat by illustrating the impact of our recommendations when considering the threat evolution – from its source, through myriad pathways and possible scenarios, to the key target, and then to the post-event attribution.

Our first recommendation is to demonstrate the deployment of technology and systems to protect a single example target facility among many possible targets (as indicated by the narrow “slice” out of the broad range of “key targets”). This protective capability can then be extended to other critical key targets. Its implementation provides a basis for extending coverage to additional military targets and then (probably in mobile form) to civilian targets. The demonstration also provides the basis for a long-term test-bed for new technology that would be developed as part of recommendation #4.

Our second recommendation to change the processing of intelligence collections to increase the sensitivity of detection of nuclear indicators spans the entire range of consideration of the unconventional nuclear threat – from source to the post-event phase.

Our third recommendation to improve nuclear forensics capabilities focuses on the source and the post-event phases of the threat sequence.

Like our recommendation on intelligence, our fourth recommendation to rebalance, or enhance, resources to reestablish a strong R&D base also applies to

enhancing our capabilities in all phases of addressing the unconventional nuclear threat.

Our fifth recommendation reflects concern over protecting nuclear materials at their sources, particularly in Russia, and is focused at a number of key, fixed sites, as illustrated by the vehicle passing through the radiation monitoring gatepost.

Finally, our sixth recommendation to perform systems analyses to better characterize the range of unconventional nuclear threats encompasses all aspects of the threat.

The chart in Figure 31 combines our 6 recommendations into a timeline for a potential unconventional nuclear threat to the United States. We have organized our approach around the protection of key military bases or targets of similar importance in a major regional conflict. All of our recommendations are affordable and can be practically implemented over the next few years.

The points of greatest leverage along the timeline of an adversary's development and delivery of an unconventional nuclear device are at the beginning and the end: it is hard to screen for nuclear material at every U.S. border point. Recommendation #5 is to better secure nuclear materials at their sources, and recommendation #3 provides for forensics near the source but, more importantly, prompt attribution so that the threat of U.S. retaliation may act as a deterrent to both acquisition and use of the unconventional nuclear threat.

Timelier processing of nuclear-related intelligence (#2) is essential. Not only does it address the difficult "middle part" of the timeline, but it is also needed to cue the deployment of a mobile point defense or to alert a fixed screen.

R&D recommendation #4 (like #2) applies across the entire timeline - nuclear materials control, search and screening, device diagnostics and render-safe, as well as forensics and attribution. This recommendation rights the imbalance between operations and research.

Summary

Our recommendations will provide protection and deterrence for unconventional nuclear attacks against key military and national targets

When executed, our recommendations provide the basis for extending protection to a broader range of homeland targets

Figure 32.

The task force believes that the unconventional nuclear threat is real and that significant improvements in our deterrent capability can be obtained with only a modest increase in our existing efforts to combat these threats. The task force has provided recommendations for action that will provide significant levels of protection and deterrence for attacks against key military and national targets. These recommendations provide the stepping stones to full execution of the recommendations made in the 1997 DSB Summer Study and will allow us to eventually extend protection to a broader range of homeland targets.

Annex A. Terms of Reference



ACQUISITION AND
TECHNOLOGY

THE UNDER SECRETARY OF DEFENSE

3010 DEFENSE PENTAGON
WASHINGTON, DC 20301-3010

MAR 2 1999

MEMORANDUM FOR CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT: Terms of Reference--Defense Science Board Task Force on
Unconventional Nuclear Warfare Defense

You are requested to form a Defense Science Board (DSB) Task Force to review and evaluate DoD's current state of detection, identification, response, and prevention to terrorist, subnational, or other unconventional nuclear attacks to the U.S.

Tasks to be accomplished:

- Develop general characteristics of the classes of threat that fall into the unconventional area along with an estimate of feasibility and cost of producing such threats.
- Review current areas of detection and response with a focus on areas of potential improvements.
- Pay particular focus on defining the technical and operational elements associated with possible prevention to include integration and application.

The Unconventional Nuclear Warfare Defense Task Force will determine:

- Adequacy DoD's ability to detect, identify, respond, and prevent unconventional nuclear attacks by terrorist or subnational entities.
- The appropriate role(s) and capability of DoD to provide protection against unconventional nuclear attacks in support of Homeland Defense.

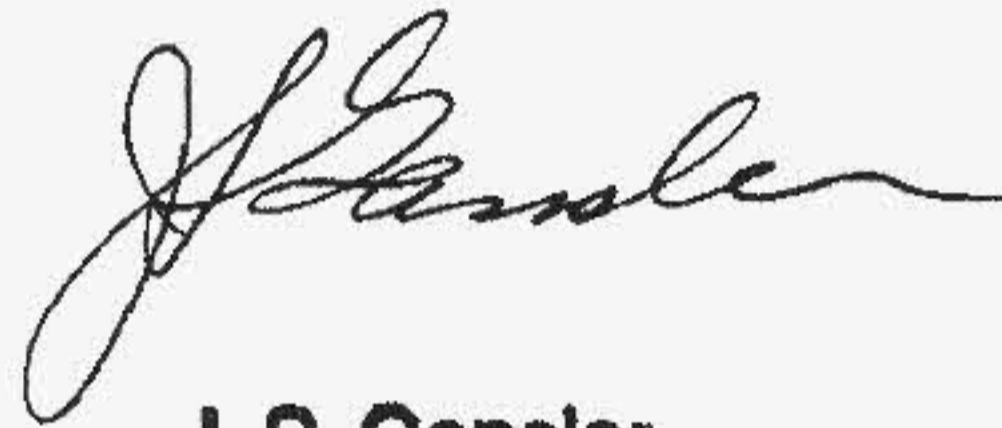
The Task Force should provide the Department with its evaluation and recommendations in a final report by August 31, 2000.

The Task Force will be co-sponsored by the Under Secretary of Defense for Acquisition, Technology and Logistics and the Director, Defense Threat Reduction Agency. Mr. Roger Hagengruber will serve as the Task Force Chairman. Ms. Catherine Montie of the Defense Threat Reduction Agency will be the Executive Secretary; and LTC Scott McPheeters, USA, will serve as the DSB Secretariat Representative.



The Task Force shall have access to classified information needed to develop its assessment and recommendations.

The Task Force will be operated in accordance with the provisions of P.L. 92-463, the "Federal Advisory Committee Act," and DoD Directive 5105.4, "The DoD Federal Advisory Committee Management Program." It is not anticipated that this Task Force will need to go into any "particular matters" within the meaning of Section 208 of Title 18, U.S. Code, nor will it cause any member to be placed in the position of acting as a procurement official.

A handwritten signature in cursive script, appearing to read "J. S. Gansler".

J. S. Gansler

Annex B: Acronyms

| | |
|-----------|--|
| ACTD | Advanced Concept Technology Demonstration |
| AEC | Atomic Energy Commission |
| AFTAC | Air Force Technical Applications Center |
| ASD/SOLIC | Assistant Secretary of Defense for Special Operations and Low Intensity Conflict |
| ATSD/CS | Assistant to the Secretary of Defense for Civil Support |
| CONUS | Continental United States |
| DCI | Director of Central Intelligence |
| DTRA- | Defense Threat Reduction Agency |
| EOD | Explosive Ordnance Disposal |
| HEU | Highly Enriched Uranium |
| IC | Intelligence Community |
| ICBM | Intercontinental Ballistic Missiles |
| JIT | Just in Time |
| MPC&A | Material Protection, Control and Accountability |
| MOU | Memorandum of Understanding |
| NEST | Nuclear Emergency Search Team |
| NNSA | National Nuclear Security Administration |
| OCONUS | Outside the Continental United States |
| RDDs | Radiological Dispersal Devices |
| SLBM | Submarine Launched Ballistic Missiles |
| SNM | Special Nuclear Materials |
| UNT | Unconventional Nuclear Threat |