Report of the
Defense Science Board Task Force
on

Preventing and Defending Against Clandestine Nuclear Attack

June 2004

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

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUN 2004	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Report of the Defense Science Board Task Force on Preventing and Defending Against Clandestine Nuclear Attack	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Office of the Under Secretary of Defense For Acquisition, Technology, and Logistics Washington, DC 20301-3140**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**UU**	**58**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

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.

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

DEFENSE SCIENCE
BOARD

MEMORANDUM FOR THE ACTING UNDER SECRETARY OF DEFENSE
(ACQUISITION, TECHNOLOGY, AND LOGISTICS)

SUBJECT: Defense Science Board Task Force Report on Preventing and Defending Against Clandestine Nuclear Attack

The subject Task Force was established in March 2002 as part of the ongoing DSB examination of DoD capabilities to deal with strategic terrorism, WMD proliferation, and asymmetric threats. The report of the Task Force is attached.

The Task Force addresses the threat of nuclear or radiological attack, by anyone for any purpose in any scenario, against the United States or U.S. military operations, delivered by any means other than missiles or aircraft. In effect, this means hidden/smuggled nuclear weapons, devices, or materials.

The Task Force finds that this threat is serious enough, and that there are sufficient indications that effective means of preventing successful attack might be developed over the long term, to warrant starting a DoD effort to develop comprehensive capabilities in DoD's areas of responsibility. This spiral development/deployment effort would, in parallel, build better understanding of what is technically and operationally feasible, and field operational capabilities as they become available.

DoD efforts to deal with this threat would be part of a nascent national effort, as the Task Force observes. The Task Force identifies certain key DoD roles and responsibilities against this threat that are related to DoD's broader missions, in particular (1) protection of DoD power projection capabilities, CONUS and OCONUS, from this threat; and (2) OCONUS operations to find and safely dispose of nuclear weapons, devices, or materials that could be used for clandestine (or other) attack (consider a failed nuclear state). DoD aspects of maritime interdiction would be involved in both. Coordination with the Department of Homeland Security and others, in both development and operations, will be necessary.

Capabilities to deal with this threat in these and other ways would draw on, and extend, quite a number of ongoing DoD activities, including intelligence, force protection, counter-proliferation, SOF operations, and DoD's Cooperative Threat Reduction activities. As the Task Force points out, defense against this threat can build on DoD capabilities in these areas that are focused on other threats, but the very multiplicity of these DoD activities could result in a fragmented effort to build capability against this particular threat.

My own views align generally with those of the Task Force. The Department should pay considerably increased attention to this threat. This is a new problem with certain unique

features, and there does not seem to be a ready template within DoD for how to approach it. I believe that it is important to start to address it now. The nature of the problem of detecting clandestine weapons of mass destruction – nuclear, chemical, biological, or radiological has many disparate characteristics, but they also share some common characteristics that suggest that the USG's ability to field an effective capability to detect WMD may benefit from an integrated institutional approach to WMD detection. I agree with the Task Force that the key is establishing a DoD program of scope and intent sufficient to raise technical and operational invention to a qualitatively different level.

William Schneider, Jr.
Chairman

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

DEFENSE SCIENCE
BOARD

MEMORANDUM FOR THE CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT: Defense Science Board Task Force Report on Preventing and Defending Against Clandestine Nuclear Attack

I am privileged to submit to you the Report of the DSB Task Force on Preventing and Defending Against Clandestine Nuclear Attack (The title of the Task Force, in its Terms of Reference, was Defense Against Unconventional Use of Nuclear Weapons Against the United States).

The basic views and conclusions of the Task Force were formulated almost a year ago. Since then, I have briefed the work of the Task Force over 35 times, mostly in DoD. The original intent of this briefing regimen was to find out the lay of the land, so to speak, so that our report could identify a substantial number of particular, detailed recommendations that would be immediately actionable. The actual result, however, was the realization that the many actions needed would only be worked out pursuant to a commitment, by the Department as a whole, to pay serious attention to this threat. Accordingly, our recommendations are quite general, as laid out in the report.

The members of the Task Force deserve a great deal of thanks from the DSB for their work. I also want to single out, in particular, people who have supported the Task Force and its extensive briefing schedule: LTC Scott Dolgoff and, before him, LTC Carla Kendrick, both of the DSB office; Mr. Grover Ford and Ms. Melinda Baran of SAIC; and Dr. Don Wolkerstorfer and, later, Dr. Rollin Whitman, both of whom served as Executive Secretary of the Task Force assigned to OATSD(NCB) from Los Alamos. These people all contributed to the substance of the work of the Task Force as well as providing highly efficient administrative support.

I also thank and commend Mr. Mike Evenson and Ms. Cathy Montie of DTRA. They also supported the Task Force in many ways and, much more important, their leadership of DTRA's Unconventional Warfare Defense (UNWD) Program has given DoD a point from which to move forward.

Finally, DTRA's UNWD program would probably not exist if not for the efforts of Dr. Roger Hagengruber, who chaired a DSB Task Force on this subject in 1999/2000.

Dr. Richard Wagner
Task Force Chairman

This page intentionally blank.

TABLE OF CONTENTS

1.0 EXECUTIVE SUMMARY 1

2.0 DISCUSSION 5
- 2.1 *Introduction* 5
- 2.2 *The threat* 7
- 2.3 *National defense architecture* 8
- 2.4 *DoD's main operational roles/missions* 11
- 2.5 *Achieving the needed capabilities* 14

3.0 RECOMMENDATIONS 17
- 3.1 *Make immediate operational changes* 17
- 3.2 *Improve nuclear intelligence capabilities* 18
- 3.3 *Start a spiral development program* 18
- 3.4 *Establish joint warfighting requirements and capabilities* 24

4.0 ASSESSING DEFENSE PERFORMANCE AND THE UTILITY OF POTENTIAL SYSTEMS' IMPROVEMENTS 27
- 4.1 *Radiation detection performance* 28
- 4.2 *Thinking through clandestine attack scenarios vs. protection architectures* 30
- 4.3 *Thinking about the utility of imperfect defenses* 32

5.0 DoD IMPLEMENTATION 35

6.0 CONCLUSION 37

APPENDICES

A. TERMS OF REFERENCE 39

B. MEMBERS AND ADVISORS 41

C. BRIEFERS 43

D. RECIPIENTS OF TASK FORCE BRIEFING 45

E. ACRONYMS 47

F. EXCERPT FROM *UNCONVENTIONAL NUCLEAR WARFARE DEFENSE* (DSB SUMMER STUDY 2000, VOLUME III) 49

This page intentionally blank.

1.0 EXECUTIVE SUMMARY

In this report, *clandestine nuclear attack* means a nuclear or radiological attack

- By anyone for any purpose,
- Against the United States and/or U.S. military operations,
- Delivered by means other than (military) missiles or aircraft.

A large subset of this threat is the smuggling of nuclear weapons, devices, or materials for use against the United States.

Since the 1950s, there has been sporadic concern about the threat of clandestine nuclear attack (previously referred to by other terms), but little has been done. Since the early 1970s, some capability has existed in the Atomic Energy Commission (AEC) and later in the Department of Energy (DOE), and in the Department of Defense (DoD) to deal effectively with certain very limited scenarios, but until very recently the de facto national position has been that the threat was too unlikely to warrant concern and/or that nothing could be done about it if it was considered likely.

The Defense Science Board (DSB) Task Force on Preventing and Defending Against Clandestine Nuclear Attack was chartered in March 2002 to review DoD's responsibilities and current capabilities, and to make recommendations for changes and improvements in DoD capabilities with regard to this threat.[1]

Today, it would be easy for adversaries to introduce and detonate a nuclear explosive clandestinely in the United States. In or near a city, such an explosion would kill a great many people. Any nuclear explosion by an adversary against the United States would have repercussions that could profoundly impact the nation politically, economically, and even culturally in a variety of ways. Events would be set in train that could affect world history, perhaps in catastrophic ways.

Competition between offense and defense is a central theme in the history of warfare. During the Cold War, active and civil defense were factors that significantly influenced strategic postures (though actual deployments were limited on the U.S. side after about 1965). In the post-Cold War, post-9/11 world, with the emergence of a wide range of new and diverse threats, defenses have assumed even greater importance. DoD, for example, expends major efforts to develop and deploy missile defense.

It is a central thesis of this report that clandestine nuclear attack and defense against it should be treated as an emerging aspect of strategic warfare and that it should warrant national and DoD attention that is as serious as that devoted to missile defense. Indeed, in a way somewhat similar to one of the aspirations for missile defense, defense against clandestine nuclear attack could help to prevent its emergence as a form of warfare. DoD has important roles to play in dealing with the threat of clandestine nuclear attack, although unlike missile defense, DoD is not the sole player.

With a serious national commitment to a multi-department program that would be small compared to many other defense/security efforts, it appears possible to create a multi-element, layered, global, civil/military complex of systems and capabilities that can greatly reduce the

[1] See appendix A for the Task Force's terms of reference and appendix B for a list of the Task Force's members.

likelihood of a successful clandestine attack, achieving levels of protection effective enough to warrant the effort.

DoD has roles to play in every element or layer of such a global defense, but we identify two particularly important roles for which DoD has exclusive responsibilities, and a third where DoD's responsibility is not exclusive but is critical. The exclusive DoD responsibilities are (1) to conduct counter-nuclear military operations to find and deal with hidden nuclear weapons and materials outside of the continental United States (OCONUS) and (2) to protect DoD installations and operations everywhere against clandestine nuclear attack. The third important DoD role is to provide support to other departments and civil authorities for elements for which they are responsible. If DoD can build effective capabilities for its exclusive responsibilities, it will have gone a long way toward having the capabilities for effective support to civil authorities.

DoD has not yet adequately assumed its roles in a comprehensive manner vis-à-vis the threat of clandestine nuclear attack, although there are small, isolated capabilities and programs scattered throughout DoD, some of which are excellent. The DoD programs that would, or should, result from serious attention to this problem—as articulated in this report—would be much smaller than missile defense programs, but many times larger and more comprehensive than today's small and fragmented efforts, and would be tightly interwoven with a wide range of DoD operations.

Building DoD capabilities to defend against this threat in its areas of responsibility should be an integral part of the defense transformation efforts already underway in DoD. The overarching recommendation of this Task Force is this: *for* ***DoD to carry out both its exclusive and its support responsibilities vis-à-vis the clandestine nuclear threat, it must develop substantially expanded and improved military force capabilities specific to this threat***. These capabilities would also have elements in common with protection and other operations against other threats.

To enable and stimulate that development, DoD should establish a program element in this area and start a spiral development/deployment effort that includes (1) a several-fold expansion of the DoD RDT&E program and (2) limited but immediate expansion of certain operational capabilities based on procurement of equipment utilizing currently available technology. More detailed recommendations for both come later in this report. DoD capabilities and programs should, of course, be congruent with those of other departments, especially the significant emerging effort in the Department of Homeland Security (DHS). But DoD should not wait for a well-coordinated national program to emerge before undertaking its own developments.

Improved intelligence capabilities to identify clandestine nuclear attack operations are crucial. However, for two reasons this report does not address this need (more than to say that it is important). First, improving intelligence in general is getting a great deal of attention, and virtually all such improvements will pertain also to this threat. The Task Force can add little to this effort. Second, although improvements relevant to *nuclear* intelligence are also needed, the 2000 DSB Task Force on Unconventional Nuclear Warfare Defense made sound and detailed recommendations for such improvement. We emphatically reiterate them. (Relevant excerpts from the 2000 DSB Task Force on Unconventional Nuclear Warfare Defense can be found in appendix F.)

To achieve the necessary military capability, DoD should establish joint warfighting capability requirements in this area and move to organize, train, and equip accordingly. Consideration should be given to establishing a military discipline (similar, perhaps, to the Army's Chemical Corps) that encompasses the necessary skills for this area (perhaps in conjunction with capabilities for dealing with other weapon of mass destruction (WMD) threats).

The cost of this effort will be several-fold larger than what is currently being spent in DoD in this area but small compared to many other defense programs. For the first few years, the principle costs will be for the recommended spiral development program, including limited initial deployments/operations. DHS has recently begun a substantial R&D program. The total cost of the requisite national R&D program will be somewhat less than a billion dollars, spread over five to eight years. (Details are in the body of the report.) We estimate that DoD R&D cost for developing DoD-specific capabilities will be perhaps a third of the total national R&D cost.

A few years after the start of the development, procurement of improved DoD equipment will become significant. Procurement costs are more difficult to estimate, since we believe that R&D and quantity procurement can result in significantly reduced equipment costs, but it is difficult to estimate the extent of the reduction at this time. Overall, we expect DoD procurement costs over perhaps a decade to total a few billion dollars, mainly for procurement of some tens of thousands of detectors/sensors. We venture no estimate of DoD operations and maintenance (O&M) costs, except to say that we expect it to be less than O&M for other efforts in combating other WMD, in part because there will likely be some elements in common with them.

The strategy of this Task Force has been to brief its findings and recommendations widely before writing this report so that (to the extent possible consistent with the Task Force's basic views) (1) the report could be adapted (as it has been) to the responses, and (2) we could thereby make our recommendations as actionable as possible.[2] Given the previous national as well as DoD history of lack of attention to this threat, the general agreement found almost everywhere in DoD about its seriousness and about DoD's responsibilities is heartening. However, to date, no comprehensive DoD program yet exists, and few capability-improvements have been made.

As is to be expected, people inside and outside DoD held mixed views about the potential for making headway against the threat, and uncertainty existed about what the metrics for success might be. These are important issues, better understanding of which will develop along with the programs we recommend. A summary of current understanding, including a discussion of the utility of less-than-perfect defenses, is found in section 4 of this report (pages 27-34).

Some skepticism also existed about the scope and potential for payoff of the research, development, test, and evaluation (RDT&E) program we recommend. At the request of the Assistant Secretary of Defense for Homeland Defense (ASD(HD)), Task Force members and their support prepared two detailed documents on aspects of the utility of current technology and the prospects for improvement. One summary conclusion is that detection systems with

[2] Appendix D contains a list of recipients of the Task Force's briefing.

order-of-magnitude better performance can be developed in two to perhaps five years, and that this can enable new operational capabilities for the defense, such as rapid, wide-area search and detection that can substantially close off a significant fraction of the attacker's options. Excerpts from one of these documents are included in this report on pages 29-30. It is now being published by the Institute of Electrical and Electronics Engineers (IEEE).[3]

In addition, at the request of the Director of the Office of Program Analysis and Evaluation (PA&E—at the time, Dr. Steve Cambone)—and later, at the request of Dr. Dale Klein, Assistant to the Secretary of Defense for Nuclear and Chemical and Biological Defense Programs (ATSD(NCB), Task Force Members have participated in developing a program plan for the DoD spiral development/deployment we recommend. Section 3.3 of this report, "Start a spiral development program" (pages 18-23), provides an overview of the recommended national and DoD program. A more detailed DoD plan is being prepared by the Defense Threat Reduction Agency (DTRA) at the time of this writing.

[3] R. Byrd, *et al*., "Nuclear Detection to Prevent or Defeat Clandestine Nuclear Attack," Los Alamos Manuscript LA-UR -04-0629, submitted to *IEEE Sensors Journal*, *Special Issue on Sensors for the Prevention of Terrorist Acts* (2004).

2. DISCUSSION

2.1 Introduction

The DSB addressed this threat in previous studies conducted in 1997 (also chaired by Richard Wagner) and 1999/2000 (chaired by Roger Hagengruber). Much has changed since then. The 11 Sept. 2001 attacks demonstrated the intent of terrorists to inflict massive damage. Nuclear proliferation has proceeded apace, with North Korea and Iran achieving nuclear weapon capability or coming closer to it, and it could spread further. The United States is engaged in a war against terrorism, and DoD is beginning to devote significant effort to combating WMD. The Department of Homeland Security (DHS) has been established. Thinking about the threat of clandestine nuclear attack has changed, and some efforts to explore defenses have begun. However, one thing has not changed: little has actually been done against the threat of clandestine nuclear attack.

The DSB Summer Study on Transnational Threats (1997) first developed the ambitious idea of a very large, multi-element, global, layered civil/military system of systems of scope sufficient to have some prospect of effectively thwarting this threat. There was little resonance with this vision (outside of the Task Forces in 1997 and 2000), but since then, and especially since the attacks of 11 Sept. 2001, it has begun to be discussed more widely. This report will revisit such a national/global system, largely as context for the main focus of the Task Force: DoD's roles and capabilities.

Following briefings from many government agencies and subject matter experts,[4] the Task Force arrived at its basic findings and recommendations in early 2003. Since then, those results have been discussed in over 40 meetings within DoD and elsewhere, leading to certain refinements.[5] This report reflects the outcomes of that process and weaves together viewgraphs used in the discussions with elaborating text.

[4] See appendix C for a full list of briefers.
[5] See appendix D for a list of recipients of the Task Force briefing.

The Task Force's mandate

- "Nuclear terrorism"? Not only terrorists, also enemy state's SOF, or…. And possibly during "conventional" war, as well as terrorism, and…
- "Unconventional nuclear attack"? What's a conventional one? (There have only been two.)
- Our de facto Terms of Reference: "Nuclear or radiological attack, by anyone, against the United States and/or U.S. military operations, delivered by means other than military missiles or aircraft." Yes, should think through all possibilities, but mostly….
- Clandestine nuclear attack on the U.S. homeland, or U.S. bases or military operations anywhere, by anyone.

So many things have changed about this subject since the Task Force was chartered in March 2002 that the name of the Task Force has changed twice. In addition, the Task Force concentrated its efforts on certain key parts of the original charter and ignored other parts. The chart above sketches some of this evolution.[6]

Even the final term arrived at, *clandestine nuclear attack*, may not fully capture the Task Force's scope and focus. For example, a nuclear attack on the United States using a cruise missile or an unmanned aerial vehicle (UAV) launched from a merchant ship in offshore waters (a subject examined, among others, by the 2003 DSB Summer Study) would be considered a clandestine attack. The Task Force did not focus on the end game of such an attack, but instead focused on the adversaries' preparation for the attack and possible interdiction points. For example, the attacker would have to get or develop the weapon somewhere, transport it, and bring it onto the ship in some way. Those portions of the attack route are very much within the Task Force purview.

The Task Force concentrated almost entirely on enemies' clandestine attacks with nuclear explosives—nuclear weapons that might have been stolen or sold; a state's nuclear weapons clandestinely delivered by its military forces; or nuclear explosive devices improvised by non-state entities using stolen, bought, or lost fissile material. Early in the course of the study, the Task Force heard several briefs on radioactive dispersal devices (RDDs) but decided to concentrate almost exclusively on the nuclear explosive threat, treating RDDs as a lesser-included case. If the necessary measures are taken to deal with the nuclear threat writ large, then the RDD threat will be addressed. While an RDD attack may be more likely, the impact of it would be vastly less than for nuclear explosives, for many reasons that extend beyond the differences in the damage produced.

[6] The Task Force's Terms of Reference are included in the report as appendix A.

2.2 The threat

Why this threat should be taken very seriously

- We may be at a turning point in the history of global security
  - Will the conjunction of the *methods* of "terrorism" and the *technologies* of mass destruction become dominant?
- Nuclear knowledge, materials, weapons are oozing out of control
- Enemies – current and potential -- have, are developing, or are seeking nuclear weapons
- Clandestine delivery is especially dangerous. Difficulty of attribution limits deterrence, enables third-party provocation in crises
- If a successful nuclear attack occurs
  - immense fatalities
  - a disastrous turn in history?
    - common use of WMD?
    - upset nuclear stability among major powers.
- This threat is likely to persist and grow (unless….)

Methods and propensities for covert/clandestine operations aimed at creating immense destruction, by whatever means may be available, are spreading. Clandestine nuclear attack is one such possible conjunction.

Nuclear weapons are oozing out of control. Nuclear weapons technology and knowledge continue to spread. Nuclear explosives themselves, and nuclear materials, are spreading into hands hostile or potentially hostile to the United States. They are spreading to places and regions where the prospects for effective control to prevent their loss and stem their continued spread are highly uncertain.

A successful clandestine nuclear attack would have import extending far beyond the immense immediate casualties. A successful attack on the United States would change how Americans live and perhaps even alter the fundamental nature of democratic institutions in America and throughout the world. It would set in train events that could destabilize the global nuclear weapons regime and lead to fundamental and deleterious changes in the global security environment. For example, due to the immense casualties and the difficulty of determining responsibility, clandestine nuclear attack could leverage third-party provocation in a crisis to an unprecedented extent.[7]

[7] Dr. Fred C. Iklé, former Under Secretary of Defense for Policy and a member of the Task Force, has written presciently on the import of strategic terrorism, the spread of nuclear weapons, and their connections. See, for example, Fred C. Iklé, "The Second Coming of the Nuclear Age." *Foreign Affairs* (January/February 1996) or Fred C. Iklé, "The Next Lenin: On the Cusp of Truly Revolutionary Warfare," *The National Interest*, Spring 1997.

Events that have never happened before but which would be catastrophic if they did occur, and for which motive and capability exist, belong in a special category of risk management. It may be necessary and sometimes useful to speculate on the "probability" of rare or unprecedented *natural* occurrences, where physical laws provide some basis for estimation, but where human adversaries are involved, no adequate calculus is available. The "likelihood" is simply indeterminate, and the risk must be managed on the basis of the consequences.

Diplomatic, political, and other military efforts to limit this and related threats are obviously essential and are being variously pursued, but they are beyond the scope of this Task Force. It would be imprudent, however, for the nation to assume that these efforts will be fully successful. This report addresses how to deal with the threat that will remain. We first sketch out how the nation as a whole might deal with this threat, and then devote the body of the report to what DoD's roles and capabilities are and should become.

We are in the midst of dramatic change in the nature of warfare, and the prospect of clandestine nuclear attack and prevention/defense against it should be seen as an integral part of that change. DoD is in the midst of a transformation, and developing capabilities to deal with clandestine nuclear attack should be an integral part of it.

2.3 National defense architecture

A future, many-dimensioned, global, civil/military prevention/protection system of systems

- Effective protection and control of nuclear weapons and materials everywhere.
- Effective nuclear intelligence capabilities to warn and for interdiction.
- A **deployable force capability** for comprehensive, large scale, forward counter-nuclear and nuclear-protection operations. (Ground, maritime, air.)
- Very large, layered deployments of improved detection systems/networks, in the U.S. and abroad
  - Civil and DoD; at sources, along transport paths, around targets
- Ability to quickly respond to detection and either 1) destroy the weapon/material or 2) secure and safely disable or dispose of it.

……

- Consequence mitigation
- Effective forensics for attribution

All layers benefit from other measures taken in the Global War on Terrorism

DoD has some role in every category

The concept for a national protection/defense capability outlined here and elsewhere in this report is much larger and more ambitious than was in anyone else's thinking until the 1997 DSB Summer Study. Before that, no one (as far as we know) had thought in terms of a system large enough in scope to have some possibility of dealing effectively with this difficult threat. Before the last few years, this threat was considered as (1) unlikely enough that there was no

need to invest in research to defend against it, and/or (2) too difficult to mount an effective defense against it.

The Task Force believes that it may be possible to develop a multi-element, layered, global, civil/military system of systems and capabilities that would greatly reduce the likelihood of a successful clandestine nuclear attack. This system would have nuclear-specific elements that would be complemented by the myriad other prevention/protection measures being taken in the global efforts against terrorism and WMD writ large. It would weave together improved monitoring and control of nuclear weapons and materials at their sources, with layered global detection and interdiction of clandestine nuclear attack operations, to both dissuade many who might consider mounting such attacks and defeat many of the (fewer) attacks that would be attempted. Because attempts of this sort are not likely to be frequent, significant attenuation of the threat in this way is an appropriate objective. Prospects for success are discussed later in the report.

One example of the scope of the system we posit is the deployment, in the United States and overseas, of perhaps a few hundred thousand sensors—many of them improved radiation detection systems—in a multi-layered architecture. This detection architecture would be one element of the larger overall architecture. (Most of these sensors would be deployed and operated by civil authorities, but DoD would be responsible for certain elements described later.) A second example, for which DoD has exclusive responsibilities, is OCONUS: special operations forces-like, counter-nuclear military operations of a scope much larger and more capable than is currently the case, involving in some scenarios perhaps a few thousand trained military personnel.

One important element of the overall architecture is a global, geographically layered system of sensors and response capabilities that can detect and then interdict threat items as they move along the many possible and complex routes between their source(s) and their prospective target(s). The layers are shown in the chart below.

Layers of a global civil/military prevention system

- Secure/protect material/weapons at sources, including production, civil fuel cycle. Detect/prevent removal.
- Detect/prevent matls/wpns leaving source nation (e.g. Russia)
- Detect/prevent exit from OCONUS ports, airports
- Maritime interdiction
- Detect/prevent entry into US at ports, airports, borders
- Detect/prevent movement within the US
- Detect/prevent at perimeters of targets – cities, bases, other
- Detect/prevent within area targets

A very rough estimate for civil detector deployments for all layers in the United States and overseas—along roads, at ports and airports, around and within cities, etc.—is 100,000 to 400,000 detectors. Procurement of such a civil system might cost a few billion to a few tens of billions of dollars. (The ranges account for uncertainties in the architecture and in the extent to which R&D and competitive quantity production can reduce costs.) For the DoD responsibilities mentioned earlier, less than 30,000 detectors would be needed, costing a few billion dollars to procure. We have not tried to estimate DoD's operating and management (O&M) costs. These costs could vary widely, depending on the technologies used and how these roles are incorporated into the Services' and commands' force structures. Both the civil and the DoD systems would be acquired in three or four phases of spiral development and deployment, from 2004 to around 2015.

So far, the architecture discussed has been for the purpose of preventing a successful attack, and we believe this must get the lion's share of the emphasis. But there may be a successful attack, either before we can construct an effective defense, or because no defense can be perfect. So the program must also look at what might happen after an explosion. Improvements can be made in both mitigating the consequences of a successful attack, and in attributing the attack to its perpetrators. Ability to identify the perpetrators, if known by potential attackers, can help to deter. R&D opportunities exist in both consequence mitigation and in attribution, including forensics. The Defense Threat Reduction Agency (DTRA) and DOE's National Nuclear Security Administration (NNSA) have laid out responsible programs in these areas, and they should be pursued.

Perhaps the most important thing to say about what happens after a successful attack is that the government must be able to move quickly, and be seen to be doing so, to prevent a second one. A second successful attack is likely to have even greater political consequences than the first. After a first successful attack, many fiscal, legal, and political constraints that

might have limited protection capabilities are likely to be removed or lessened. It will be possible to surge the defense, and it will be imperative that all long-lead preparations be made beforehand in order to allow surge to be as effective as possible. (Protection could also be surged on the basis of certain kinds of warning. Surge is discussed somewhat more on pages 31-32.)

2.4 DoD's main operational roles/missions

Prevention and protection against this threat is an integral part of DoD's historical mission: protecting U.S. territory from enemy attack. For air and missile defense, the responsibility is (essentially) exclusively DoD's. Today, of course, the Department of Homeland Security, the FBI, and others have responsibilities for many aspects of civil protection, including aspects of defending against clandestine nuclear attack. However, DoD has roles to play in every one of the elements and layers of the global architecture sketched in the preceding section. The matrix below lays out several of them.

DoD's main operational roles and missions

Type of Operation	Area of Operation: OCONUS	Area of Operation: CONUS
OCONUS military operations **– Conventional** **– SOF and "SOF-like"** **– Maritime**	Exclusive to DoD	
Base/force protection	• Exclusive responsibility • Host nation assistance?	• Exclusive responsibility • Civil authorities must help
Support to civil authorities (e.g., consequence management)	May have to play major role	Many aspects, including cases beyond capacity of civil authorities? (Surge?)

Mission will require thousands of trained, equipped troops

Among these, the key ones are:

- OCONUS military operations
- Base/force protection, CONUS and OCONUS
- Support to civil authorities.

The first two are uniquely and exclusively DoD responsibilities. With regard to the third role—support to civil authorities—DoD's roles are not unique and exclusive, but are very important nevertheless. (We do not discuss support to civil authorities further. As will be discussed throughout the remainder of this report, if DoD can develop capabilities to do the jobs that are exclusively its own, it will be well on the way to capabilities for much of civil

support.) To do these missions well will require a many-fold expansion of the number of personnel with the requisite skills. This, and its possible implications in organizing, training, and equipping, are discussed later in the report.

The Task Force was charged with assessing DoD's current capabilities. Since both the nature of the threat and what needs to be done to meet it have changed so much over the past few years, it would not be particularly useful to assess each current DoD activity in detail. What is important about the current activities is that *DoD would not be starting from scratch to build a more comprehensive capability*. The dedicated and competent people who have been involved—in some cases for decades—are a rich, though limited, resource for moving ahead.

The next two viewgraphs/pages discuss objectives for the two areas that are exclusively DoD's responsibility: (1) OCONUS counter-nuclear operations and (2) protection of DoD forces, installations, and operations.

Future full-spectrum, in-theater counter-nuclear operations and capabilities

Should include:

- Force/base protection against nuclear attack
- Nuclear quarantine of adversary's "perimeter"
  - Including maritime interdiction
- "Nuclear situational awareness"
- Locate/identify and deal with adversary nuclear weapons/devices, materials, facilities, by
  - Standoff strike/attack (many other efforts, incl. DSB TFs)
  - Extensive SOF-like operations to secure and safe them
- Nuclear consequence management
- Attribution

A much larger, more complex force capability than envisioned in the past

- How organize, train, equip?
- Create a new "military discipline"? (For WMD as a whole?)

In the future, the United States may conduct military operations of varying intensity, including war, in places where nuclear weapons are present that could be used against the United States or its operations. These weapons may or may not be the main reason for DoD operations in the region. The enemy may control the weapons, or government authorities—friendly or hostile—may have lost control of the weapons. (Consider, for example, failure of a state that has substantial nuclear weapons.) Alternatively, if nuclear weapons are not originally present, U.S. forces and military operations overseas may be the target of attack by weapons introduced clandestinely from outside the area of our operations. In any of these or similar cases, one of DoD's prime jobs in hostilities would be to prevent indigenous or outside nuclear weapons (or devices) from being used in clandestine or overt attacks against the United States and/or against U.S./allied forces.

Forward-area operations to this end should include: (1) nuclear quarantine (in both directions) of the country or of regions within it; (2) many and widespread nuclear search operations, perhaps opposed; and (3) an ability to dispose safely of weapons or materials that are found—in effect, a smaller, forward-area, DoD-only version of the layered, civil/military global detection and response architecture described earlier, and of which this DoD capability would be a part.

In some cases, the weapons' locations may be known with enough certainty to allow their destruction by air or missile strikes. The Task Force did not address such strikes per se; much attention is already being devoted to improving stand-off strike capabilities. However, in most or many cases, it would be necessary to conduct in-the-area search and render-safe operations, either instead of, or to complement, remote strikes. DoD currently has some capability to do this, but it is extremely limited. Plausible scenarios could require a thirty- or hundred-fold expansion in capability. Nuclear quarantine of a nation or a region within which weapons might be present would have much in common with force/base protection in CONUS vis à vis the deployment and use of large sensor networks and capabilities to respond to detection. We discuss this next.

Protection of DoD installations, forces, and operations, CONUS and abroad

- Concept:
  - Detection systems/networks in areas surrounding bases
  - Detection systems/networks at gates/perimeter
  - Response forces for interdiction and to secure threat devices
  - C4I systems: data fusion, network algorithms, conops
- DTRA 2002/2003 few-day demonstrations at 4 DoD bases ($50M)
  - Near-COTS technologies. Develop conops. Leave-behind.
  - Limited capabilities
  - Basis for limited, near-term deployments with current technology
    - A learning base
- Major improvements available mid-term and future from RDT&E

Goal: Effective detection/response at and around all key DoD installations

DoD must assure protection against clandestine nuclear attack of its bases and installations, forces, and operations at home and overseas. The concept is a layered detection and response capability. This would include capabilities deployed off-base—in cooperation with local authorities, at the base perimeter and entrances, and within the base. These capabilities would all be linked by appropriate command and control (C^2) and data management in carefully thought out concepts of operation (CONOPS). During 2002/2003, the Defense Threat Reduction Agency (DTRA), in its Unconventional Nuclear Warfare Defense project, carried out partial demonstrations of such systems and capabilities at four CONUS bases, using

commercial off-the-shelf (COTS) technology. These experiments would form the basis for the initial limited deployments recommended earlier and discussed below.

2.5 Achieving the needed capabilities

Limiting factors and technical capabilities

Current limited technical capabilities, for example:

- Current limited technical capabilities
  - Radiation detection
  - Render safe
  - Forensics
- Residual paradigm-lag: limited conception of the needs and the opportunities for prevention/protection

Technical capabilities can be made much better:

- True ten years ago, even more today
  - Despite widespread misperceptions to the contrary
- RDT&E programs to improve them have been constrained by
  - Perceptions that threat not real
  - Narrow scenarios (extortion, rather than war)
- **Working toward better equipment will expand conceptions of prevention and protection goals and architectures**

For decades, in the small efforts that have been underway in this area, the perceived threat was someone using a clandestinely developed and emplaced nuclear explosive device for extortion—a narrow variant of what is today called the terrorist nuclear threat, which is itself a subset of the clandestine attack threat addressed here. This narrow conception of the threat led to a correspondingly narrow conception of response: cued search of a very limited area. This narrow paradigm, coupled with general skepticism about the seriousness of such threats, in turn limited technology development to a smattering of small projects. In a descending spiral, the resulting limited technologies eventually resulted in inhibited thinking about larger threats and appropriate responses. Today, the paradigm is war. The stakes are much higher, and the need for specialized technologies and processes to mitigate this threat has increased commensurately.

As posited earlier in this report, effective defense against this threat would have many dimensions. Although improvements in technology are not all that is required, they are crucial across the board. Many technologies are needed for a variety of purposes:

- Protection of materials and weapons at their sources,
- Detection of the presence or transit of weapons/materials,
- Response,
- Render safe,
- Attribution, and

- Consequence management.

Recent technology-development in these areas has been very limited, as shown below.

Current programs to develop improved technical capabilities

	Funding		
	Past	FY02	FY03
• DoD			
– DTRA	~$3M	$75M	~$25M
• Four base-protection demos, R&D.			
– Other	small	small	small
• NNSA			
– NEST, nuclear smuggling, CTR, etc.	~$20M	~$55M	~$25M
• Other USG: ~ no R&D, very small procurements		small$	
– (DHS planning includes ambitious R&D)			

No current program or collection of programs, in DoD or anywhere, is sufficiently comprehensive or ambitious in relation to either the threat or the opportunities for improvement

The above chart illustrates the level of effort that has been devoted to RDT&E in this area in the past. These estimates, collected by the Task Force, are uncertain to perhaps a factor of two, in part because the boundaries and definitions of the technology base that should be included are poorly defined. For example, solid state devices are used in radiation detection, and there is tremendous R&D activity in this area in a wide range of other applications. The Task Force made rough estimates of what could be considered relevant. “Past” is a rough average over the five years before FY02. The increased FY02 numbers are due to two one-time increments, such as for the DTRA UNWD program that was formed in response to the 1999/2000 DSB Task Force on this same topic. FY03 was a moving target, but the estimates shown above give a fair indication of the expected funding levels. FY04 has also been a moving target, though there have been some increases above the general levels of the past. For the future, DHS is planning substantial increases, to over $100 million for R&D in FY05, with further increases beyond. DoD planning is still fragmented and uncertain.

This page intentionally blank.

3.0 RECOMMENDATIONS

The Task Force makes recommendations in four categories:

- Review current DoD vulnerabilities and make immediate operational changes where necessary;
- Improve nuclear intelligence capabilities;
- Establish a DoD program element for spiral development/deployment of prevention/protection, in DoD's mission-areas, against clandestine nuclear attack; and
- Establish joint warfighting capabilities needs, and organize, train, and equip accordingly.

In short, DoD should establish a comprehensive posture in this area. In the following section, we amplify these areas of recommendations.

3.1 Recommendation: Review current DoD vulnerabilities and make immediate operational changes where necessary

Recommendation:
immediate and near-term operational improvements

SecDef should direct:

- The Services, the JS, and the Combatant Commanders to
  - immediately determine and prioritize DoD vulnerabilities to clandestine nuclear attack
  - make immediate changes to operations to reduce the worst vulnerabilities
- Each Service to:
  - immediately procure and use, for highest priority needs, some equipment based on best technology from the 2002/3 DTRA UNWD demonstration program
  - designate one installation as a standing test bed for developing improvements for installation protection
    - with DTRA

The Task Force examined possible DoD vulnerabilities to clandestine nuclear attack, but did not feel competent to survey and order the vulnerabilities. The competent authorities should do that, and, where possible, the most serious should be rectified immediately. Some vulnerabilities might be rectified by changing operations; in some cases, deployment of attack-detection and response capabilities is the right approach; and in many cases, combinations of the two will work best. For urgent cases, detection and response capabilities should be based on the best technology from the DTRA Unconventional Nuclear Warfare

Defense demonstrations/experiments. Woven in to such near-term deployments should be standing test-beds for evaluating technical and operational improvements.

3.2 Recommendation: Improve nuclear intelligence capabilities

Improved intelligence capabilities to identify clandestine nuclear attack operations are crucial. However, for two reasons this report does not address this need (more than to say that it is important). First, improving intelligence in general is getting a great deal of attention, and virtually all such improvements will pertain also to this threat. The Task Force can add little to this effort. Second, although improvements relevant to nuclear intelligence are also needed, the 2000 DSB Task Force on Unconventional Nuclear Warfare Defense made sound and detailed recommendations for such improvement. We emphatically reiterate them. (Relevant excerpts from the 2000 DSB Task Force on Unconventional Nuclear Warfare Defense can be found in appendix F.)

3.3 Recommendation: Establish a DoD program element for spiral development/deployment of prevention/protection, in DoD's areas of responsibility, against clandestine nuclear attack

This should weave together the following:

- Expansion of DTRA's Unconventional Nuclear Warfare Defense program;
- A several-fold, multi-agency expansion of the RDT&E program; and
- Immediate limited deployments, using current technology, for
  - Base protection and
  - Forward operations.

Elements of a spiral development program

Sequential, iterative development and deployment of:

- Many improved prototype active and passive detection systems and networks
- Several improved technologies for securing, diagnosing, and safely disposing of nuclear materials/devices/weapons.
- Improved forensics methods for attribution

And:

- Develop operational test beds
- Strengthen the relevant science and technology base, including R&D facilities, basic research, simulations
- Strengthen the base in industry for procurements of large numbers of detection systems.

Guided by:

- Scenarios, simulations, red-teaming, architectures, operational concepts (including network concepts), and time-phased deployment strategies.

The spiral development/deployment we recommend is standard in DoD, with deployments and technology improvements going on in parallel, time-phased according to an overall strategy. Implicit are deployments and operational capabilities that are sequentially or continuously improved by the results of RDT&E that is continuously modified by lessons learned in operations.

The national science and technology base for this work is in severe decline due to the moratorium on nuclear testing and the declining needs of the nuclear power industry. Graduate schools, for example, now train few people in radiation sciences or high-energy-density physics. However, there are enough people available to start the recommended program, provided that it is a national priority. As the program develops, it will revitalize the technology base.

RDT&E Recommendation

USD/AT&L should immediately develop and begin execution of a comprehensive, multi-year DoD program for the RDT&E element of a spiral development program for nuclear prevention/protection.

- Near-term DoD funding:
  - $50M in FY06 (first year of full funding)
  - $20M bridge in FY05
- FY05-FY09 estimates:
  - DoD: <$400M, front-loaded
    - (National: ~ $1B)
  - Coordinate with NNSA and DHS, but don't wait for them. Enough planning has been done to start now
- RDT&E goal should be ambitious: to develop technologies and systems with the objective of beating this threat, (and thus to determine whether that's feasible)

The Task Force believes that it is urgent to start a comprehensive DoD RDT&E program that expands the current effort several-fold. DHS is planning a fairly comprehensive RDT&E program to address this threat, and NNSA is working on certain aspects of such a program as well. However, the Task Force is convinced that it will be some time before other departments will be able to carry out the necessary comprehensive, system-of-systems spiral development, of which DoD is already capable.

From the very beginning, the objectives of the R&D programs should be ambitious—ultimately, to develop the technologies needed to beat the threat—rather than merely incremental. Only by trying to do so, will we find out whether such a goal is achievable. Limited goals will not suit the purpose. This is not to say that the program will not have limited, near-term milestones as explicit components of the spiral development program. However, a program of the necessary scope cannot be planned in detail on paper before it begins. It must be started based on setting broad long-term goals, with detailed planning and

downstream milestones emerging later, as many more people become involved and think their way into the problem.

The levels of effort recommended are for what the Task Force believes to be a technology-limited, or a "good-idea-limited," program. That is, more funding than this would be beyond the point of diminishing returns; much less would mean that good ideas would go unexplored.

Recommended:
$150M-plus FY05 National RDT&E Program (13 May '03 version)

• Prevention of weapon/material loss/theft	$11M
– Tagging, security and monitoring, etc., etc.	
• Radiation detection systems, passive and active, imaging, high resolution, networked….	$77M plus
• Passive	($31M)
• Active	($18M)
• Sources for active interrogation	($4M plus…)
• Basic research	($24M)
• Production engineering development	($TBD)
• Non-radiation sensors	(Few $10s M)
• Protection systems: network algorithms, test beds	$24M
• Demonstrations (some included elsewhere)	Few 10s M$
• Crisis response, incl. render safe technologies	$11M plus…
• Forensics	~$10M plus facilities
• Consequence mitigation technologies	$11M

This chart was prepared well before DHS scoped its R&D program. It is included here to illustrate the categories of R&D needed, and our sense of the proportioning of resources among them. DoD's portion of the national program will be smaller, of course, but the profile among categories may be somewhat similar. As of this writing, at the direction of Dr. Dale Klein, (ATSD(NCB)), DTRA is preparing a detailed program plan for DoD R&D in this area.

Two things warrant comment on this chart:

- Non-radiation sensors can be very important in detection of nuclear weapons. DoD has a large technology base in a wide variety of sensor technologies. The estimate for non-nuclear sensor development in the above chart only addresses adaptation of items in that technology base for this specific application. The existing DoD and national technology base is much larger. Our estimate is very imprecise because it is difficult to define the boundary between basic technology development and developments specific to these applications.
- The estimate for demonstrations is rough because it is difficult to define the boundary between demonstrations and the initial limited deployments recommended elsewhere in this report.

The following viewgraphs provide examples of projects in two of the lines above: passive radiation detection sensors and basic research. Radiation-detection R&D is discussed in more detail in a document developed by members of the Task Force and their support at the request of the Honorable Paul McHale, Assistant Secretary of Defense for Homeland Defense.[8] Its purpose is to describe what improved system capabilities could be afforded by R&D in radiation detection. It is not a program or budget plan, but it does discuss many of the elements of a program.

Some weapon/material radiation detection approaches

- Near- to mid-term prototypes
  - Large Compton gamma imager (adapted from neutrino detection)
  - Imaging using cosmic-ray muons
  - Near-field coded-aperture gamma imager
  - Large low-cost liquid scintillators
  - Better (sensitivity/resolution/cost) plastic scintillators (doped, new plastics)
  - Sensitive, cheap, two-sided-directional sensor
  - Automated analysis tools for all detectors.
  - Detectors using in-hand technology, tailored for specific applications: hand-held, rail-car, cargo-container, maritime, special-ops, rugged road-bed sensors; networked; active vs. passive

- Connected networks of detectors – few in a small area (portal); hundreds in/around a city.
  - Architectures, algorithms.
  - Self-assembling systems.

[8] R. Byrd, *et al.*, *op. cit.*

Some supporting/"basic" research/engineering

- Solid-state physics of semiconductor detectors:
  - e.g. organic or ternary semiconductors; room-temperature systems
- Yield/cost/size of CdZnTe
- Physics of low cost, industrial-scale sensor production
- Algorithms for use of very large detector networks
- Pulse-shape discrimination of neutrons from gammas
- Better organic scintillators – liquid and solid
- Cheaper, more sensitive, rugged photodetectors
- Pulsed-power for compact neutron and gamma sources, and for speed-of-light disablement:
  - e.g. fast switch design, target design

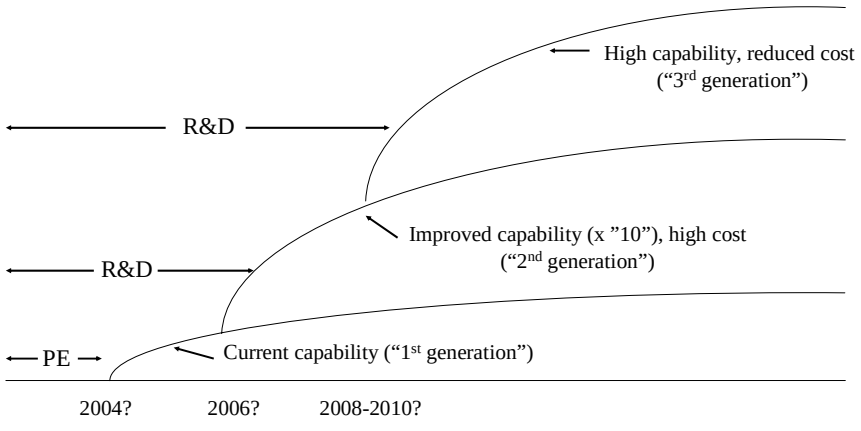
Spiral development/deployment requires making judgments about the time-phasing of R&D and procurements, based on estimates of when improved technology will be available, how much it will cost to procure and deploy, and how much it will improve operational capability. Today, such judgments would be difficult to make in this area for two reasons. First, serious R&D has not yet started (though some funding is now being allocated), and the technical community that will become involved has not yet thought through how the developments might proceed. Second, performance assessment is just beginning. (A summary of current thinking on performance assessment is included below, on pp. 27-34.) Pending that work, the next two viewgraphs (1) posit that there will be three phases of improvement in sensor capabilities and (2) illustrate how those phases might be deployed over time.

Development Phases for Better Detection Technology

- Current Generation (Available in 0 – 18 months)
  - COTS or near-COTS
  - Quantity procurement??
- Next Generation (Available in 1 – 3 years)
  - Times "10" in performance
  - Adapted from existing items, know-how
  - Often expensive
- Following Generation (Available in 2 – 10? years)
  - Performance preserved/improved, cost reduced (a lot?)
  - Many advances come from basic research in materials science.

Tough Issue:
(Detector) Technology Deployment Strategy

Three blocks of development, procurement, and deployment



In the second chart, the vertical axis is indeterminate; it could be either numbers of detectors, or costs for detectors. "PE" is production engineering, indicating that even for first-generation COTS capabilities, quantity procurement is unlikely to be possible without some preparation.

Forming judgments about the time-phasing of deployments and the improvements afforded by R&D requires, among other things, assessment systems' performance as they evolve. This is covered in section 4 (see page 27).

3.4 Recommendation: Establish joint warfighting capabilities needs, and organize, train, and equip accordingly.

Clandestine nuclear attack and capabilities to counter it should be thought of as an integral aspect of warfare, and building capabilities to counter it should be thought of as an integral part of the current transformation of DoD. These capabilities will require a many-fold expansion in the number of military personnel trained for these missions. Much of the discussion so far in this report has focused on the required technical capabilities. This recommendation addresses the matter of organizing and training to achieve the necessary operational capabilities.

Recommendation: military capability

SecDef should task the services, the Joint Staff, and Combatant Commanders to develop:

- organizational structures, plans to train and equip
- operational concepts.

for an enduring, comprehensive military capability for full-scope

- offensive counter-nuclear operations
- nuclear force/installation protection
- nuclear situation understanding

both OCONUS and CONUS.

Create a military discipline with career potential.

Should include due consideration of relationship of nuclear to counter-WMD capabilities in general.

Much of the discussion of the Task Force's findings and results within DoD over the past several months were concerned with how the necessary military capability should be structured. For example, there was considerable discussion on several occasions about the degree of jointness that is needed for each of the several functions. Other than the general recommendation in the chart above, we do not have more-detailed recommendations about how DoD should organize, train, and operate the capabilities that are needed. However, one consideration about this issue warrants comment.

Create a military discipline. DoD should view the capabilities needed in this area as "a military discipline." An example of an organizational structure that embodies a military discipline is the Army Chemical Corps. The Chemical Corps has highly specialized training, some of it highly technical in nature. It has a school. Many officers have advanced degrees in

science. It is large enough to have general officers at the top of its structure. It has an organic intelligence function. At one time it had an offensive capability. (Forward counter-nuclear capabilities could be construed as an offensive capability.) It has what might be called consequence management functions. At about 20,000 personnel, the Chemical Corps is larger than what is needed for countering the clandestine nuclear threat, but not so much larger as to invalidate the comparison.

One aspect of a creating a military discipline is to ensure that professional opportunities are available for advancement. In future military operations in which nuclear weapons are involved that might be used for clandestine attack against the U.S. forces or against the U.S. itself, the combatant commander should have at hand a general/flag officer whose career path would have prepared him or her to advise the commander on the nuclear aspects of the situation. In some circumstances, this flag officer might also control the forces that work the nuclear problem.

In Task Force discussions with the Army Staff, a senior officer in the Chemical Corps suggested that, at least for the Army, the Chemical Corps itself could take on the job of defense against clandestine nuclear attack, thereby automatically assuring that a military discipline is developed. The Task Force is agnostic on this possibility, but it raises the important question of the extent to which the force capabilities and the military disciplines needed to counter the clandestine nuclear threat should be subsumed into broader capabilities and disciplines needed to deal with all WMD threats. These capabilities and disciplines are being developed, in various ways and degrees, in many places within DoD.

There would be some obvious advantages in subsuming the nuclear capabilities within a broader counter-WMD capability; however, there would be a serious disadvantage: our experience is that often the nuclear-specific aspects of the threat are lost sight of, under the rubric of general WMD terrorism. The Task Force is agnostic on how serious the nuclear problem is compared to other WMD/terrorism problems, but we are certain that it is not negligible, and unfortunately it is often treated as such when they are all considered together. This tendency would argue for a dedicated capability/discipline for dealing with the nuclear threat.

One obvious possible alternative would be to incorporate the capabilities needed here into the Services' continuing capabilities to maintain and operate U.S. nuclear weapons. During the Cold War, when the Army, Navy, and Air Force all had tactical/theater nuclear weapons and maintained military specialties and disciplines associated with them, this might have made good sense, and we would not rule it out now. Today, the Air Force's and the Navy's nuclear weapons are almost entirely strategic and they are not closely interwoven with conventional operations as the tactical weapons were during the Cold War—a handicap for some aspects of dealing with the clandestine nuclear threat.

Perhaps each service should do it differently. Somewhat surprisingly, despite the fact that the Army no longer has nuclear weapons, the Army's Nuclear and Chemical Agency (USANCA) maintains a small (a few hundred) but high-quality cadre of personnel trained in all aspects of nuclear weapons, including—for defensive purposes—battlefield operations, survivability, and other competencies. Within the Army, USANCA could be a focal point for building the capabilities and disciplines needed to deal with clandestine nuclear attack. Or perhaps USANCA could become executive agent for development of joint capabilities.

This page intentionally blank.

4.0 ASSESSING DEFENSE PERFORMANCE AND THE UTILITY OF POTENTIAL SYSTEMS' IMPROVEMENTS

Throughout the work of this Task Force, the question has arisen: how effective can defenses of this sort really be? It is a crucially important question for national strategy, for planning programs for defenses, and for using them if and when they are in place. The Task Force has formed the judgment that defenses can be effective enough and that the threat is serious enough to warrant a significant program. But no detailed, analytic methodology exists today to support this judgment. Indeed, our sense is that the question of effectiveness cannot be well addressed in advance of a program that will find out how effective a defense can be by trying to build an effective one. And in fact, even though one component of such a program would be development of analytic methods of performance assessment, it is unlikely that an offense/defense interaction as complex and dynamic as this one will be can be confidently assessed analytically. (Red teaming may help, but insights from red teaming will be limited until some defense capability is actually fielded.)

In addition to the general complexity of the problem, the question cannot be well answered by analysis for at least two other reasons. First, too much of the performance of key systems (e.g., sensors) depends upon operating characteristics that can only be determined in the field. Second, the system cannot be fully specified until after an iterative process of identifying and then working around problems, a process that will happen only as a serious development program proceeds and is coupled to initial operations.

Nevertheless, because we recommend a significant effort, it is only fair that—to the extent possible today—we try to address the question of effectiveness here. It is sometimes said that a valid objective for a defense is simply to "raise the bar" for an attacker or to "deny free rides" by precluding the most obvious attack modes. But a more structured, analytic approach than this is necessary if a serious effort is to be made. In this section, we will attempt three things, all interwoven. The first is to sketch out a rudimentary framework for effectiveness analysis. Second, within that framework, we indicate some of the reasons for our judgment that defenses can be effective enough that a serious program is warranted. Third, we lay out some reasons why an imperfect defense, as this one will be and all defenses are, can nevertheless be effective.

Defense performance is determined by many factors. The performance of radiation detection systems is only one of them, but it is an important one, and we will use such systems' performance to illustrate broader issues.

As with other elements of the protection/prevention architecture, the performance of radiation-based detection systems can be thought of on three levels. First, at the detailed technical level, metrics for radiation detection can be expressed in terms of detection range, detection time, false alarm rates, type and quantity of nuclear material that can be detected, amount and type of deliberate and incidental shielding around the weapon/material, and other parameters. Second, on an intermediate level, such technical metrics—for radiation detection or for other systems components—can be used to assess overall abilities of a significant component of the architecture (for example, systems at ports) to contribute to defeat of attacks in individual scenarios. Third, at the broadest level, performance of the entire, global

prevention/protection architecture would be assessed across the full range of scenarios, including the dynamic interplay between the evolving defense and the attacker's evolving strategies, taking account of the fact that no protection system can be perfect. In this section, we address performance at all three levels in a way that is quite preliminary but, we think, indicates the path forward.

At the level of detailed technical metrics—detection range, detection time, false alarm rates, etc.—much of what this report recommends is based on our judgment that significant improvement is possible in detection-systems' performance in threat scenarios. (The referenced IEEE paper addresses these improvements in more detail.) Relative effectiveness is not too difficult to assess, but assessing absolute effectiveness is difficult for several significant reasons. One difficulty is that the utility of detectors in real operations depends strongly on natural radiation backgrounds, which vary greatly from place to place and often in time. Such backgrounds, and the nature of radiation detection in general, introduce a probabilistic element in assessment of performance, and the significance of detection and false-alarm probabilities is very scenario-dependent. All of this fuzzes concreteness, which creates difficulties in assessing system performance and in planning defense (and is one basis for our belief that performance can only be determined by field experience with real systems).

But these uncertainties also cause problems for an attacker that may even be worse, and that illustrate one aspect of how even an imperfect defense can be effective. If the performance of detection systems increases to the level where an attacker must conduct a complex analysis to find the chinks in our defense in order to have a reasonable expectation for success, deterrence will have reached a significant level. For example, for an attacker to have to measure background radiation around a military base exposes him to counter-surveillance that he may fear, and that will increase the likelihood of successful interdiction. The utility of the overall defense will depend, in significant part, on compensating for the inevitable imperfections in the defense by making the defense at least good enough so that an adversary considering or planning an attack will be uncertain of his ability to penetrate it and thus be dissuaded from carrying out an attack. Designing the technical and operational characteristics of the defense to create such uncertainties will be a key design criterion.

4.1 Radiation detection performance

Despite these difficulties, rough estimates of radiation detection performance can be made. The referenced IEEE paper lays out some approaches to improving radiation detection and attempts to assess the degree of improvement in terms of both technical metrics and scenario assessment. Key points are excerpted below.

Today's capabilities. Only passive detection is available today. Correlated operation of multiple detectors can be done today only for a small number of sensors that can be integrated by human intelligence, assisted by limited automatic processing. With these and other capabilities:

- Plutonium devices can be detected in vehicles at portals, in cargo containers, and in vehicles at speed, if the device is unshielded or lightly shielded.
- Detection of devices containing highly enriched uranium (HEU) is very difficult and varies widely and is limited today to short range. In some cases lightly

shielded devices can be detected at portals. In other cases they can be detected only if they are essentially unshielded.

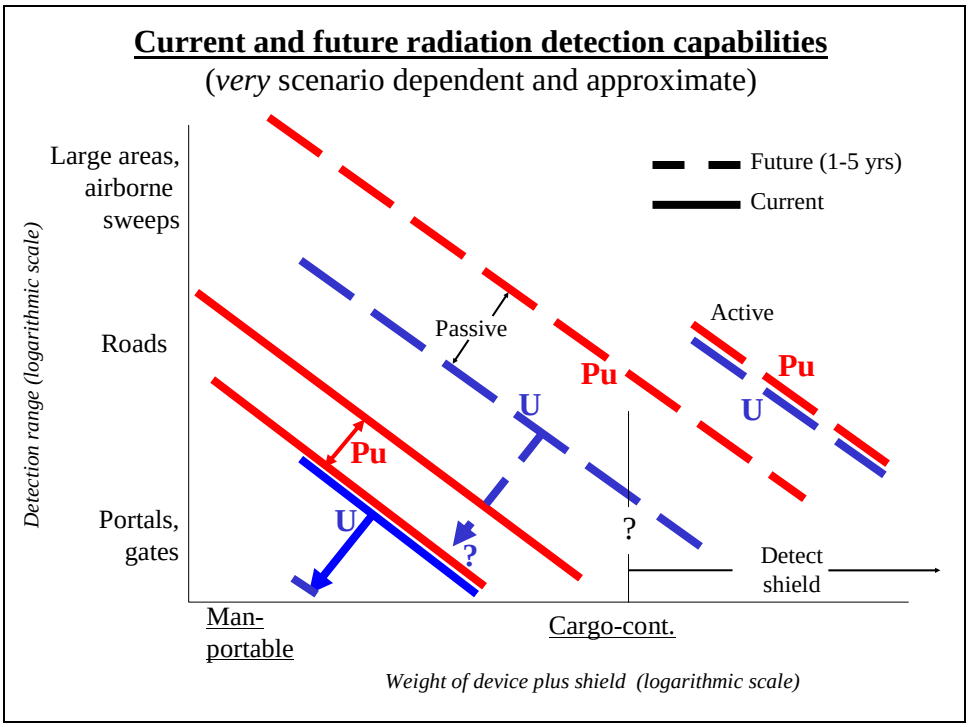
Some high-value targets are defensible, thanks to geographic features that channel traffic through defensible chokepoints, where capable portal monitors can be stationed. Traffic that attempts to bypass these chokepoints (e.g., on foot) is by definition suspect, and can be detected by non-nuclear techniques.

These capabilities may be impaired by high and/or variable natural radiation backgrounds or innocent man-made radiation sources that yield unmanageable false alarm rates.

In the future. This report recommends expanded R&D on radiation detection. The referenced IEEE paper illustrates some improvements in capabilities that would result from R&D. The following points summarize the potential benefits:

- Detection range can be extended by an order of magnitude, opening new defense operational modes such as rapid, wide-area airborne and vehicle sweeps, and monitoring large remote areas and/or extensive road networks. Shielding around the weapon could reduce performance of the detection systems, but the shielding mass can slow down the attacker and expose him to discovery by other means—e.g., detection of the shielding itself.
- Increased range and improved false alarm rejection will enable intelligent networking of detectors. This could enable coverage of road and rail transport over significant distances—e.g., along the U.S. East Coast, where long-distance transport must pass through a relatively small number of choke points.
- Background and innocent alarm rejection will allow detection of HEU in a wider range of circumstances, for example (in certain cases) in cargo that is naturally radioactive (e.g., bananas).
- Increased sensitivity and background rejection could virtually eliminate the effects of *incidental* shielding in vehicles or cargo containers, except for HEU in certain cases.
- More-portable and longer-lived sources for active interrogation will enable widespread screening of containers and vehicles. Advances in detectors and sources will allow operational restrictions on active interrogation due to health and safety concerns to be reduced.
- Radiography using the muons in the natural cosmic radiation could significantly expand detection of shielded devices at portals or in shipping containers. The greater the shielding, the more effective the detection.

The following chart summarizes and generalizes, in graphical form, the above assessments of current and potential future capabilities.

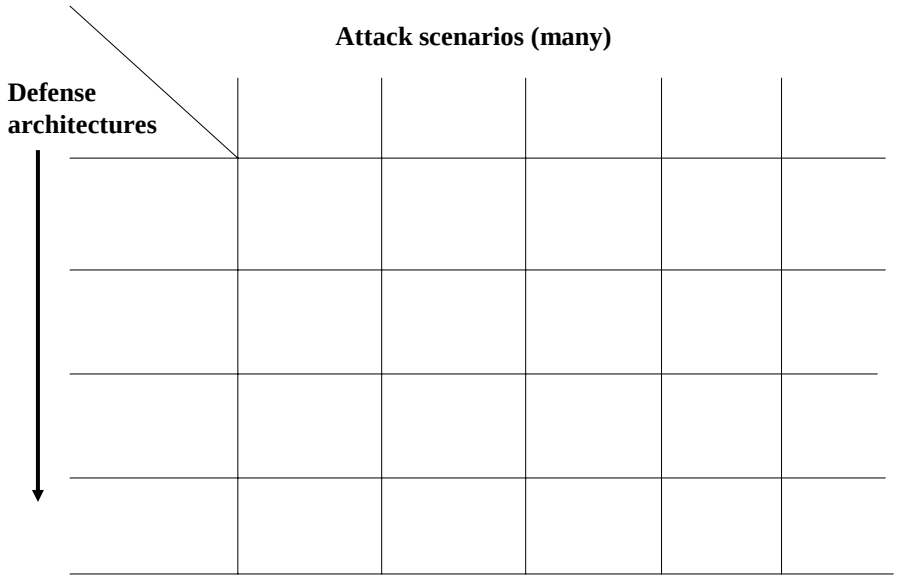


What can be done with radiation detection is complicated to describe. It is a multi-dimensional parameter space, even for a single attack scenario against a single defense layer. There are many possible scenarios, and we have posited a multi-layer defense. The format of the chart above is one greatly simplified way of summarizing some of this complexity. It illustrates a fundamental offense/defense trade between the detection range and time available for detection, and amount of shielding around the device that can reduce the radiation output of the threat object. The detection metric that the vertical axis represents is a function of range and exposure time, and it varies by approximately six orders of magnitude along that axis. The diagonal lines on the chart reflect current and future capabilities, some of which are summarized in the paragraphs immediately preceding the chart. The uncertainties and variations in the vertical location of the diagonal lines are about an order of magnitude, as illustrated by the plutonium current technology line. The relative locations of the lines are less uncertain.

4.2 Thinking through clandestine attack scenarios vs. protection architectures

To move toward the highest level of assessment of overall—evolving defense architectures versus evolving attack mode—it will be necessary to think carefully through the complicated attack/defense interplay shown conceptually in the chart below.

Thinking through this "space"



One aspect of the dynamic interplay between offense and defense, at this level of assessment, is surging the defense, discussed now.

Surge capability. The defense should be designed for surge capability, and evaluating the prospects for success of a defense should take surging the defense into account. Tactical warning could be available, especially if we improve intelligence and other capabilities.

Prepare to surge

- Actionable warning could be available, especially with large detector deployments and improved nuclear intelligence.
  - Confirmed loss of weapon/material
  - Confirmed threat operation
  - Clandestine nuclear attack here or somewhere else
- Alert surge: days, weeks.
- Mobilization surge: months, years
- DoD surge could be
  - For OCONUS ops
  - For support to civil authorities, in numbers/capabilities beyond civil capabilities
- Make long-lead preparations now/soon, including:
  - Procurement capacity, contracts
  - Train the trainers
  - Exercise surging

With tactical warning, many things could be accomplished that might be deemed fiscally and perhaps politically infeasible in the absence of an imminent threat, provided preparations are already in place. Our own clandestine operations could be expanded. Even more widespread deployments of detection systems and response to detectors could be established. Movements of people and goods could be monitored more carefully for nuclear materiel. All measures not prohibited by law or the Constitution could be put in place. These steps would increase the prospects of success.

4.3 Thinking about the utility of imperfect defenses

When and if the community involved in this work becomes able to assess system performance against threats accurately and comprehensively, it will be found that the defense is not leak-proof, as no defense can be. Because of this, some might argue that devoting the level of resources entailed in the Task Force recommendations would be wasted. We believe this is profoundly wrong. No protection system can be perfect, but over the course of history, defenses that are far from perfect have played vital strategic roles. To deal analytically with the issue of imperfect defense, the third level of performance measures—including the overall goals of the defense—must be addressed. The following is a rudimentary first cut at overall performance metrics for a good but imperfect defense.

A layered prevention/protection posture could essentially beat the clandestine nuclear attack threat

- ***Goal***: not perfection. Rather, to greatly attenuate the frequency of successful attacks, (or greatly delay the first one)
- Do this by:
  - Reducing the future frequency of *attempted* attacks by dissuasion/deterrence (by prospect of failure)
  - Thwarting most/many of the (fewer) attacks that are, in fact, attempted.
- Achieve this by (among many other things):
  - Actual protection good enough so that deterrence kicks in.
  - Multiple layers of prevention/detection/interdiction
  - Synergies among layers.
    - Examples –
      1. focus source control efforts on HEU;
      2. protection requires threat to work harder, increasing his operational signatures and chance of discovery.
  - Help from other GWOT security measures

The goal that should be set for a national/global system and its DoD elements is not perfection. Rather, because clandestine nuclear attack attempts will not be frequent, the goal should be to substantially attenuate the frequency of successful attacks (including significantly delaying the first one). Delay and attenuation could provide time to mitigate the threat in other ways, including measures to ameliorate the underlying political and cultural factors that stimulate the terrorist threat, writ large.

Many of us believe that a strong case can be made that prevention/protection can be developed that will substantially attenuate the frequency of successful attacks, by being good enough to (1) dissuade or deter many of those who might consider attempting attacks and (2) thwart or defeat a good fraction of the (fewer) attacks that might be attempted. The deterrent aspect of the protection equation involves the often-great differences between how a defender and an attacker will view the relative capabilities of the defense. The long history of offense/ defense competitions is strongly characterized by both sides taking own-side-conservative views. More particularly, the annals of terrorism and counterterrorism are replete with instances in which a prospective attacker was deterred by aspects of the defense that may have seemed relatively weak and ineffectual to the defender. The terrorist may not be afraid to die, but he (or his master) does not want to fail.

Dissuasion/deterrence by the adversary's fear of failure might work in a variety of ways. One aspect is that an attacker will want to know enough about the defense to design a robust, successful attack. If the capabilities of the defense can be improved enough that the attacker must know the details of defensive measures in place to understand how to best surmount them, then the attacker may expose himself to discovery during the planning phases of the attack or be altogether dissuaded from the attempt.

Creating uncertainty in the attacker's mind will be critical to maximizing the success of defenses which, realistically, cannot aspire to perfection. To exploit the effects of uncertainty, the defense should be deliberately designed and deployed to create as much ambiguity for the attacker as possible as to where the "boundaries" of defense performance lie. Deliberate deception should be used (carefully) as part of an overall perception management effort.

Data that can be used to be more analytic about these and other deterrence effects should be systematically assembled from the annals of counterterrorism.

Many kinds of synergies contribute to defense effectiveness. An obvious one is the effect of a layered defense, as we propose. With multiple layers, each layer need not be highly effective in order for the overall effectiveness to be high. If the layers require different tactics or technologies to penetrate, the attacker's job is considerably more difficult. This indicates a fundamental synergy between a layered defense and the capability to detect the threat by intelligence indicators, including from law-enforcement activities. A more capable and varied defense means that the attacker must mount a larger operation to penetrate it. A larger operation has more (and more observable) signatures. More people with more skills must be recruited and trained; more money must be obtained and laundered; the operation takes longer; and the attacker must surveil the defense more intensively. By increasing the signature of attack planning, the likelihood of discovery increases commensurately. This, in turn, could allow the defenses to be surged, further increasing effectiveness.

Understanding better the performance of protection systems against the full array of clandestine attack threats should be a high priority. In fact, the detailed recommendations of the Task Force for the spiral development program contain elements such as expanded development of modeling and simulation, which will help. (However, the spiral development we recommend should not wait for some comprehensive system study. The whole history of DoD acquisition shows that this kind of understanding does not come from paper studies, but matures out of serious programs.)

These preliminary thoughts about the effectiveness of a defense have led the Task Force and its predecessors to become convinced that reasonable success in mitigating the threat is sufficiently likely that, in light of the seriousness of the threat and of the consequences of successful attack, a serious development program is warranted to learn whether a successful defense is feasible by trying to build it.

5.0 DoD IMPLEMENTATION

The tenor of this report is that the problem of clandestine nuclear attack needs to be seriously addressed, on a sustained basis, by the most senior DoD officials. DoD operates according to a complex set of formal processes for setting requirements, planning, budgeting, executing programs, and operating forces, among other things. Conforming with these processes is always necessary but is often insufficient, especially for emergent topics like this one.

But the bureaucratics matter, too. The last two viewgraphs in the Task Force's briefing touch on a few of the many practical difficulties and details that must be attended to in order for DoD to come to grips with the threat.

Some problems with DoD implementation

- Essentially, no formal "Requirement" (yet?) for prevention of clandestine nuclear attack
- Prevention of clandestine nuclear attack cross-cuts established DoD organizations/programs.
  - Cooperative Threat Reduction (Russia today. Tomorrow?)
  - Counter-proliferation
  - ASD Homeland Defense, ATSD/NCB and others
  - Force protection
  - Special operations
  - Various commands, agencies, others

  Needs (at least) an "architect" who weaves it all together
- Nature of today's DoD R&D budget planning/approval
- Relation to chem/bio
- "Let DHS, NNSA do it"

Some (necessary?) Bureaucratic Steps

- Establish "Requirements"
  - Get this threat "validated" by DIA.
  - Get this mission into the Defense Planning Guidance
  - Get clandestine nuclear attack scenarios into the Contingency Planning Guidance.
  - Probably lots of other things needed
- Organize for it. (It crosscuts many programs/orgs)
  - DoD Directive establishing responsibilities?
  - Name an "architect"? (Within what office?)
  - Set up an IPT? (We hope we can do better.)
  - Something analogous to the Missile Defense Agency?
- A JOC on this topic? Force capabilities needed, how to organize/train/equip?

6.0 CONCLUSION

It is “a new thing under the sun” that adversaries, using very limited resources, can clandestinely and perhaps anonymously do unprecedented things that produce immense immediate damage with potentially profound consequences for the future. To prevent this from coming to dominate the strategic environment will require us to think differently, including about how we allocate resources to mitigate risk. Clandestine nuclear attack and defense against it is one such case. We will not come to understand such problems and their mitigation only by thinking about them. Rather, we must learn by doing. This report has laid out how DoD can begin its part of that necessary process for the case of clandestine nuclear attack.

This page intentionally blank.

A. TERMS OF REFERENCE

THE UNDER SECRETARY OF DEFENSE

3010 DEFENSE PENTAGON
WASHINGTON, DC 20301-3010

ACQUISITION,
TECHNOLOGY
AND LOGISTICS

09 APR 2002

MEMORANDUM FOR CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT: Terms of Reference - Defense Science Board Task Force on Defense Against Unconventional Use of Nuclear Weapons Against the United States

You are requested to form a Defense Science Board (DSB) Task Force to: (1) assess Department of Defense's (DoD) responsibilities, current capabilities, and the scope of activities conducted by DoD to ensure its future preparedness to prevent, deter, detect, identify, warn, defend against, respond to, and attribute attack of the U.S. homeland or U.S. bases or operations overseas by unconventional delivery of conventional and unconventional nuclear weapons, as well as radiological weapons; and (2) recommend improvements.

The Task Force should determine the adequacy of the U.S. ability to detect, identify, respond, and prevent unconventional nuclear attacks by terrorist or sub-national entities. The Task Force should identify capabilities of DoD to provide protection against such nuclear attacks in support of national capabilities in homeland defense. Special emphasis should be given to the following issues:

- What capabilities and procedures are in place or under development in the U.S., and on a worldwide basis (including DoD, Department of Energy, Federal Emergency Management Agency, International Atomic Energy Agency, etc.) to prevent, deter, detect, identify, warn, respond, and protect against unconventional nuclear attacks on the U.S., its forces, its allies, and other U.S. concerns.
- An assessment of current estimates of the unconventional nuclear threat and the implications of new technologies on the threat spectrum, deterrence and consequence management.
- What technologies and procedures will be needed to protect critical key targets such as nuclear power plants, military bases, continuity of government, etc.
- What intelligence needs will have to be addressed to collect sensitive nuclear indicators.
- What improvements need to be made in nuclear forensics.
- Capabilities to achieve reliable attribution of attackers once a nuclear attack has occurred.
- Identification of defense capabilities and postures that have the largest potential for comprehensive protection of military and civilian targets.

The Task Force should begin by identifying actionable recommendations that can be implemented now and provide near-term value (the next six months) as well as recommendations that can be implemented now and provide value in six months to three years. The Task Force should provide its initial thoughts on such near-term recommendations within three months. The final report should include recommendations that require investments from the FY 04-09 Future Years Defense Program.

The study will be co-sponsored by me as Under Secretary of Defense (Acquisition Technology and Logistics) and the Assistant to the Secretary of Defense (Nuclear and Chemical and Biological Defense Programs) (ATSD(NCB)). Dr. Bill Graham and Dr. Rich Wagner will serve as co-chairmen of the Task Force. Dr. Donald Wolkerstorfer, office of the ATSD(NCB), will serve as Executive Secretary and Lieutenant Colonel Carla Kendrick will serve as the Defense Science Board Secretariat representative.

The Task Force will operate 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.

E. C. Aldridge, Jr.

2

B. MEMBERS AND ADVISORS

Members and Advisors

Chairman

Rich Wagner, *LANL*

Executive Secretary

Don Wolkerstorfer, *OATSD (NCB/NM)*

Dr. Rollin Whitman, *OATSD (NCB/NM)*

Members

- Bill Graham, *NSR, Inc.*
- Robert Blitzer, *SAIC*
- LTG Mike Canavan (ret.), *RSL*
- Don Cobb, *LANL*
- John Foster, *Northrop Grumman*
- Stan Fraley, *SNL*
- Tricia Hammar, *NSR, Inc.*
- Fred Iklé, *CSIS*
- John Nuckolls, *LLNL*
- Wayne Shotts, *LLNL*
- Fred Tarantino, *RSL*

Advisors

- Bill Daitch, *DTRA*
- Col Dale DeKinder, *J-5*
- John Harvey, *NNSA*
- Ed Hildebrand, *OSTP*
- Trent Hughes, *USN*
- Col Richard Marsh, *USAF*
- Maureen McCarthy, *NNSA/DHS*
- Dan Smith, *TSA*
- Sara Scott, *LANL*
- Bob Scarlett, *LANL*
- Page Stoutland, *LANL*

Support

- LTC Scott Dolgoff, *DSB*
- LTC Carla Kendrick, *DSB*
- Melinda Baran, *SAIC*
- Allison Burrey, *SAIC*
- Mark Mateski, *SAIC*

When the Task Force was established, Dr. Bill Graham was co-chair. After several months, various unforeseen factors conspired to prevent Dr. Graham from continuing as co-chair. He continued to contribute significantly to the work of the Task Force, however.

Experience among the Task Force members included the following:

- Broad and high levels of responsibility for defense policy, technology development, and threat reduction;
- Responsibility for FBI response to domestic WMD incidents;
- Operations and technologies for searching for nuclear devices and rendering them safe, including command of military units charged with such responsibilities;
- Development and use of sensors of many kinds in wide ranges of applications; and
- Technologies and operations for monitoring arms control treaties.

Virtually all of the capabilities currently extant in DoD for dealing with this threat were represented on the Task Force.

Support was ably provided by those listed. Toward the end of the Task Force's work, the NNSA laboratories devoted significant effort to preparing documents requested of the Task Force by OSD officials.

This page intentionally blank.

C. BRIEFERS

- **March 14-15, 2002**
  Richard Arkin, *NNSA*
  Ron Berger, *DIA*
  Berni Bogden, *FBI*
  Jill Christensen, *DIA*
  Vasanta Collins, *DIA*
  Maj Aaron Danis, *DIA*
  Jeff Green, *Office of the Gen. Counsel*
  John Harvey, *NNSA*
  Robert Hillaire, *SNL*
  Dennis Magnan, *NNSA*
  Cathy Montie, *DTRA*
  Bob Newberry, *SO/LIC*
  Mike O'Connell, *NNSA*
  David Osias, *DIA*
  Carolyn Pura, *SNL*

- **April 16-17, 2002**
  Ron Berger, *DIA*
  Jill Christensen, *DIA*
  Nelson Degangi, *DIA*
  Tom Kuster, *SO/LIC*
  John Poindexter, *DARPA*
  Kari R., *CIA*
  Scott Schafer, *CIA*
  Scott Watson, *DIA*
  Milton Zukor, *DIA*

- **May 23-24, 2002**
  Rob Allen, *LLNL*
  Stephen Dupree, *SNL*
  C. Fields, *SNL*
  Malcolm Fowler, *LANL*
  Ralph "Butch" Hager, *RSL*
  Fred Harper, *SNL*
  Robert Janssen, *LANL*
  Warnick J. Kernan, *RSL*
  Jim Koster, *LANL*
  Mike Larson, *LLNL*
  Scott McAllister, *LLNL*
  Dennis Miyoshi, *SNL*
  Debora Monette, *NNSA/NV*
  Cal Moss, *LANL*
  Mike Pankratz, *LANL*
  Brown Rogers, *LANL*
  B. Rhodes, *SNL*
  Maj. Robert Stevens, *DTRA*
  Richard J. Tighe, *RSL*
  Susan Voss, *LANL*
  Mary-Beth Ward, *LLNL*
  Mike Weaver, *LANL*
  Lowell Wood, *LLNL*
  Rob York, *LANL*

- **June 19-21, 2003**
  CAPT Joseph Bouchard, *NNS*
  Len Connell, *SNL*
  CDR Steve Hanewich, *USCG*
  Mark Laria, *U.S. Customs*
  Bob Nestor, *Virginia International Terminal*

- **July 18-19, 2002**
  G. J. Caporaso, *LLNL*
  MAJ Steve Cima, *AMEDD*
  LTC Tony Feagin, *JPG*
  Robert E. Gold, *APL*
  COL Tom Haddan, *J-5*
  Dick Lanza, *MIT*
  Chuck McBrearty, *AFTAC*
  Ed McCallum, *TSWG*
  Maureen McCarthy, *DOE/NNSA*
  Cathy Montie
  John Penella, *U.S. Customs*
  P. A. Pincosy, *LLNL*
  S. E. Sampayan, *LLNL*
  Michael Weber, *NRC*

- **August 6-8, 2002**
  Mark Abhold, *LNL*
  LtCol David Alcorn, *DTRA*
  Arden Dougan, *LLNL*
  Cathy Montie, *DTRA*
  Sue Ryan, *OSD/CTR*

- **September 24-25, 2002**
  Doug Beason, *LANL*
  Stan Erickson, *LLNL*
  John Gerrard, *DOE*
  Simon Labov, *LLNL*

This page intentionally blank.

D. RECIPIENTS OF TASK FORCE BRIEFING

Briefing Status

- Acting ASD(AT&L)
- Director, PA&E
- DDR&E
- ASD(SO/LIC)
- ATSD(NCB)
- Director, DARPA
- Commander SOCOM and SOCOM staff
- Commander NORTHCOM,
- Army and Air staffs, Joint Staff (3), JWCA/FP
- JASONs, some other DoD offices
- Also NNSA, OSTP, DHS/ HLWG working groups, some other non-DoD
- Office of the Vice President, Science Advisor to the President, Assistant to the President for Homeland Security

This page intentionally blank.

E. ACRONYMS

AEC	Atomic Energy Commission
AFTAC	Air Force Technical Applications Center
AMEDD	Army Medical Department
APL	Applied Physics Laboratory
ATSD	Assistant to the Secretary of Defense
C2	command and control
CIA	Central Intelligence Agency
CONOPS	concepts of operation
CONUS	continental United States
COTS	commercial-off-the-shelf
CTR	Cooperative Threat Reduction
DARPA	Defense Advanced Research Projects Agency
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DoD	Department of Defense
DOE	Department of Energy
DSB	Defense Science Board
DTRA	Defense Threat Reduction Agency
FBI	Federal Bureau of Investigations
FY	fiscal year
HEU	highly enriched uranium
IEEE	Institute of Electrical and Electronics Engineers
JPG	Joint Planning Group
JWCA	Joint Warfighting Capabilities Assessment
LANL	Los Alamos National Laboratory
LLNL	Lawrence Livermore National Laboratory
NCB	nuclear, chemical, biological
NNSA	National Nuclear Security Administration
O&M	Operations and Management
OCONUS	outside the continental United States
OSD	Office of the Secretary of Defense
PA&E	Program Analysis and Evaluation
R&D	research and development
RDD	radiological dispersal device
RDT&E	research, development, testing, and evaluation
RSL	Remote Sensing Laboratory
SNL	Sandia National Laboratory
SOF	special operation forces
SO/LIC	Special Operations/Low Intensity Conflict
TOR	terms of reference
TSWG	Technical Support Working Group
UAV	unmanned aerial vehicle
USANCA	United States Army Nuclear and Chemical Agency
WMD	weapons of mass destruction

This page intentionally blank.

F. EXCERPT FROM *UNCONVENTIONAL NUCLEAR WARFARE DEFENSE*[9]

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

PAGE 44

[9] Defense Science Board, *Protecting the Homeland: Report of the Defense Science Board Task Force on Unconventional Nuclear Warfare Defense*, 2000 Summer Study, Volume III.

"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 [C^3I]), 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.