Protecting the Homeland

Report of the Defense Science Board

2000 Summer Study
Executive Summary
Volume I

February 2001

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

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 no 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

MAR 28 2001

DEFENSE SCIENCE BOARD

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

SUBJECT: Executive Summary of the Defense Science Board (DSB) Summer Study

I am pleased to forward the Executive Summary of the DSB 2000 Summer Study. The overall study was aimed at assisting the Department of Defense and the Intelligence Community in defining their roles in protecting the nation from unconventional attacks on the United States.

This four volume report documents the work of four DSB Task Forces: Defensive Information Operations (Volume I), Unconventional Nuclear Warfare Defense (Volume II), Defense Against Biological Weapons (Volume III), and Intelligence Needs for Civil Support (incorporated in the other volumes). The overarching rationale for the importance of unconventional threats to the U. S. homeland and the key recommendations of the Summer Study are contained within Volume I, Executive Summary.

I endorse the recommendations contained in the Executive Summary and propose you review the attached summary.

William Schneider, Jr.

William Schneider
DSB Chairman

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

MAR 28 2001

DEFENSE SCIENCE BOARD

MEMORANDUM FOR CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT: Defense Science Board Executive Summary of 2000 Summer Study

We are pleased to submit the Executive Summary of the 2000 Summer Study, Protecting the Homeland (Volume I). Volume I is part of a four-volume report documenting the work of four DSB Task Forces: Defensive Information Operations (Volume II), Unconventional Nuclear Warfare Defense (Volume III), Defense Against Biological Weapons (Volume IV), and Intelligence Needs for Civil Support (incorporated in the other volumes). The overarching rationale for the importance of unconventional threats to the US homeland and the key recommendations of the summer study are contained within Volume I, Executive Summary.

As you will find in this report, the task forces see a spectrum of threats to the homeland emerging. The 2000 summer study begins a series of studies by the Defense Science Board aimed at assisting the Department of Defense and the Intelligence Community in defining their roles in protecting the nation from unconventional attacks on the United States. Other studies now planned as a part of this series of studies include Defense Against Chemical Warfare Attack; Countering the Strategic Nuclear Threat in the 21st century; a follow-on study on Intelligence on Threats to the Homeland; and a second study on issues associated with Defense Against Biological Warfare Attack.

The focus of all of these DSB studies is on identifying the technology and operational capability needed to protect the homeland. It is not on the assignment of roles and missions for employing said capabilities.

Significant recommendations are made in these reports including suggestions for implementation and we recommend that you review this Executive Summary and forward to DoD for the Department's consideration with a view towards recommendations contained herein.

Craig Fields
Phil Odeen

George Poste
Defense Against Biological Weapons

Larry Wright
Defensive Information Warfare

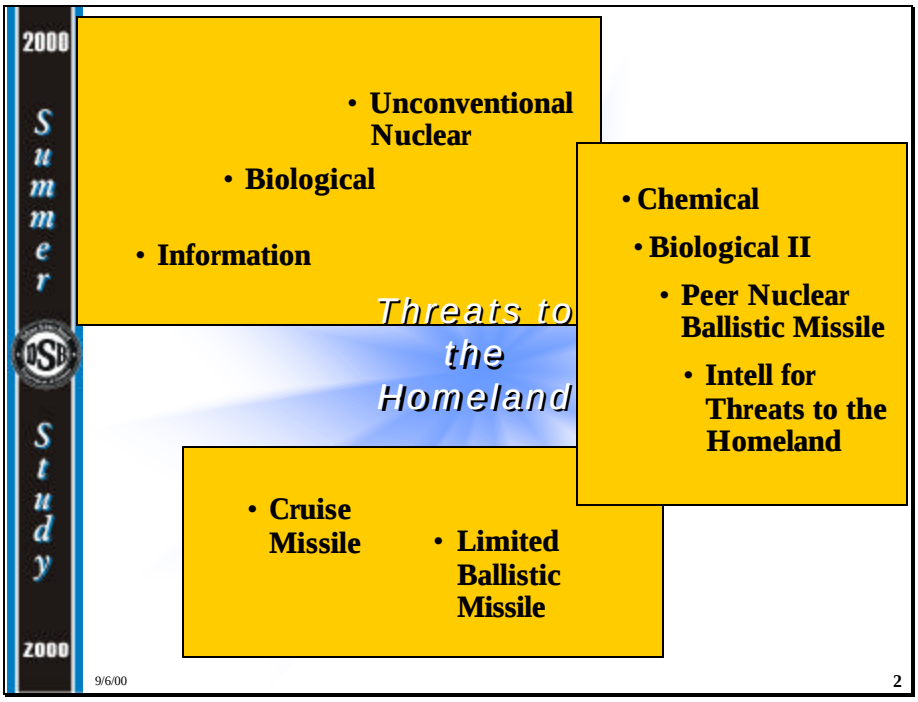
Roger Hagengruber
Unconventional Nuclear Warfare Defense

Ruth David
Intelligence Needs for Civil Support

Peter Marino
Intelligence Needs for Civil Support

Following the end of the Cold War, and the subsequent changes in the geopolitical structure, this nation is faced with a different and unique set of direct threats to the homeland. The motives and methods of these new adversaries, which include countries, organizations and individuals, are quite distinct from those posed during the conflict with the Soviet Union.

There is a new and ominous trend in these threats to the United States homeland. Whereas the nation's historic focus has been on defense of the border, these new threats are not amenable to such perimeter defenses. They require layered approaches that include both perimeter defenses and defense against "insider" threats. The trend toward reliance on the civilian and commercial infrastructure exacerbates the difficulty of such protection. These emerging threats are bringing new demands on the Department of Defense and the Intelligence Community. The Defense Science Board addresses these demands in the 2000 summer study and will continue to do so in a series of other topical studies.



The spectrum of potential threats to the homeland includes:

?? The peer nuclear ballistic missile threat, which remains the most visible threat to the homeland;

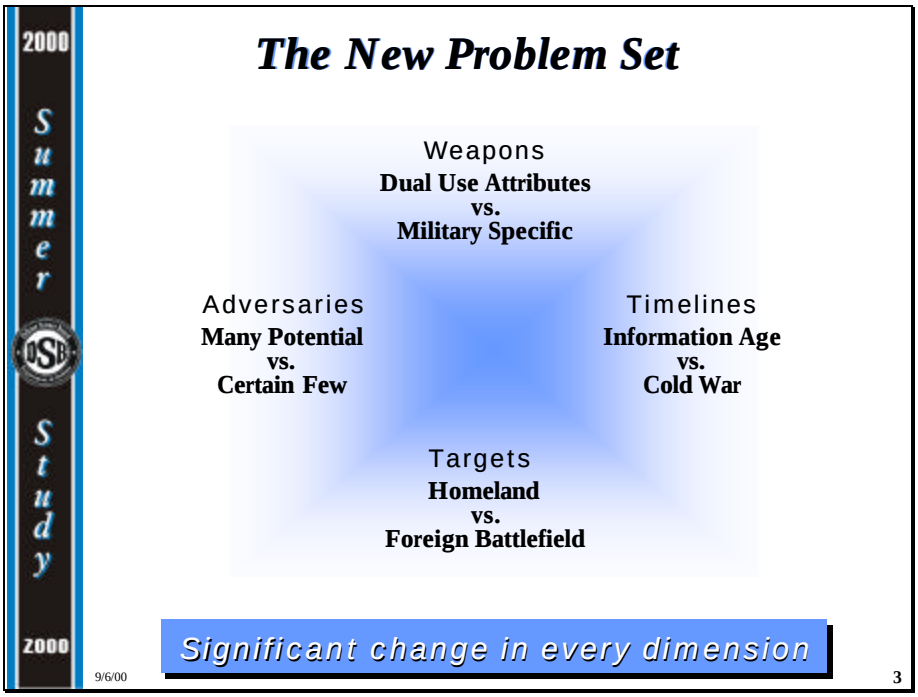
?? A growing limited ballistic threat from several nations with interests inimical to that of the United States;

?? The availability of a large quantity of reasonably inexpensive cruise missiles to many nations on the international arms market; and

?? An increasing proclivity of nations and transnational actors to consider use of weapons with much greater levels of violence – weapons of mass destruction such as biological, chemical, unconventional nuclear and information warfare weaponry.

The Defense Science Board 2000 summer study focused on defense against three weapons of mass destruction (biological threats, unconventional nuclear threats and information warfare threats) and on the related intelligence needs for civil support. Other DSB task forces are or will address chemical warfare threats, peer nuclear ballistic threats, and the unique intelligence needs associated with the full spectrum of threats to the homeland. In the future, the DSB may study the limited ballistic missile and cruise missile threats to the homeland.

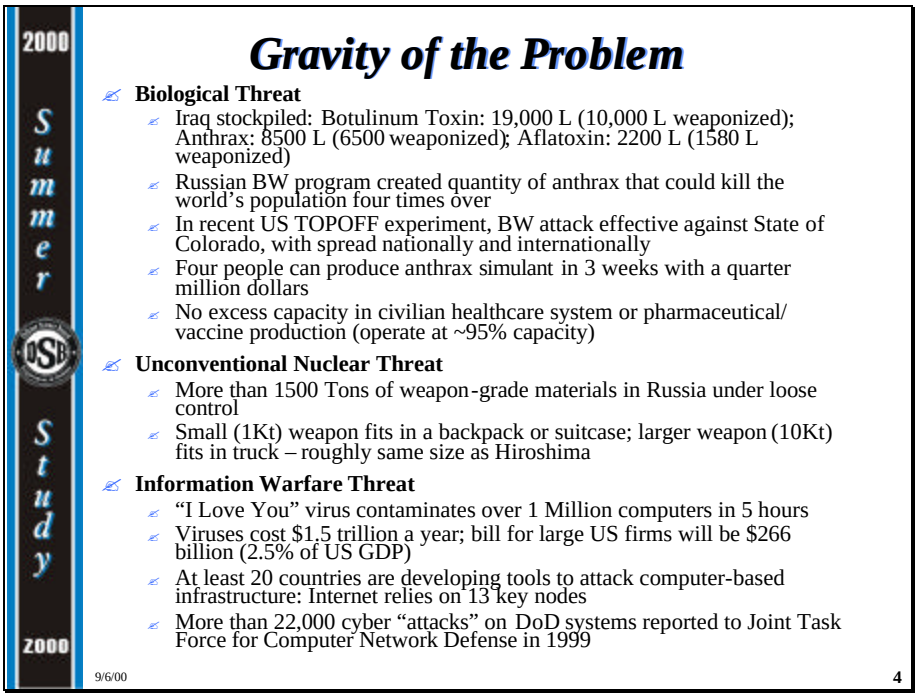
These DSB studies are intended to identify the technology and operational capability needed to protect the homeland. They do not address the assignment of roles and missions for employing said capabilities, whether within the Department of Defense or elsewhere in the US Government. Such assignments are the focus of considerable and continuing interest of a myriad of other groups and, irrespective of the assignment, the needed capabilities do not now exist to provide for adequate security.



The capability base of both the military and the intelligence community must evolve to meet the new demands imposed by this emerging set of threats. These threats necessitate dramatically reduced timelines for response than were acceptable for larger-scale conventional combat during the Cold War. The battlefields of the 21st century now include United States homeland in addition to foreign soils and encompass both military and civilian targets. Additionally, the adversary is no longer monolithic and is less predictable. Weapons are now integrated within the

civilian and commercial infrastructures rather than military specific. This dual-use nature of technology makes capabilities such as early warning, determining what is out there and what can people do, increasingly difficult.

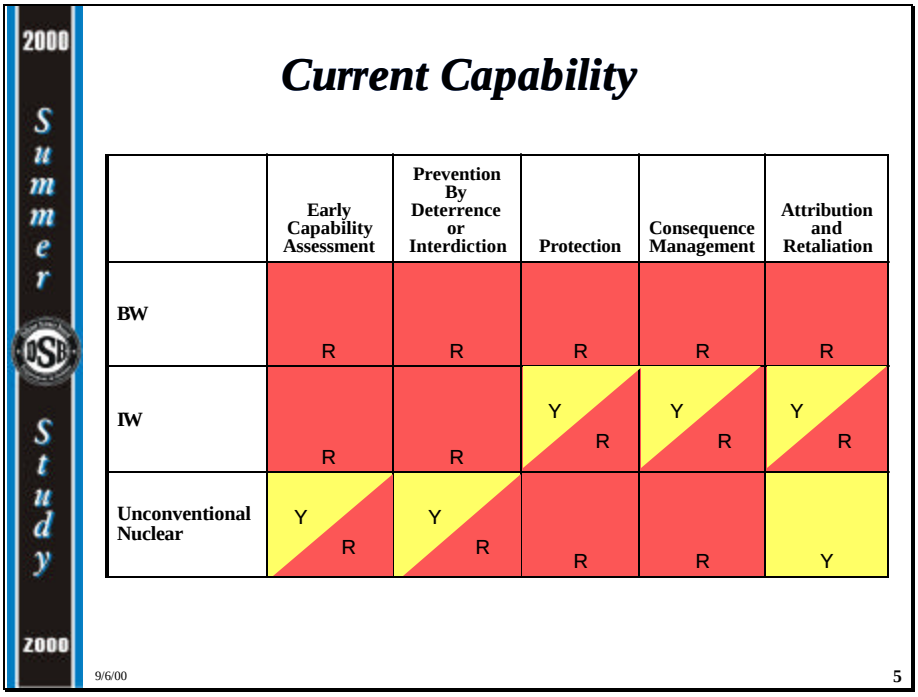
The listing of facts below gives a sense of the gravity of the hazard posed by emerging biological, unconventional nuclear and information warfare threats. Often, such threats are equated in peoples' minds with "terrorism," and "terrorism" is viewed more as an irritating, annoying mosquito bite than as a true threat to the homeland. As these facts indicate, this is not the case.



The capabilities to address this threat spectrum include five interdependent elements:

1. Early capability assessment;
2. Actions taken to prevent attack of the United States, either through deterrence or through direct interdiction;
3. Protection of critical assets and infrastructure;
4. Consequence management, should an attack occur; and
5. Attribution of the perpetrators of such an attack and, in certain cases, retaliation.

It is important to note that, if the United States has a good capability for attribution and if such capability is widely known, it can serve as a deterrent to attack and, in some measure, compensate for limitations in early capability assessment.



The BW task force found that this nation does not have an effective, early capability to assess the BW threat, and, as a consequence, cannot prevent such a crisis (i.e., the nation cannot really trust that 50-100 million Americans will be protected by suits or positive-air-pressure buildings or masks). The infrastructure does not exist to execute the desired consequence management measures. The recent set of exercises in the state of Colorado (TOPOFF) highlighted deficiencies in the national infrastructure. This nation's healthcare system now operates at near 95% capacity and does not have the ability to absorb a mass casualty event. Furthermore, the databases and associated machinery for attribution are not available today, which is why this task force judges this capability as inadequate to the job.

The DIO task force also found many deficiencies in the US capability to defend against information warfare, particularly in early capability assessment and the derived capability of prevention by deterrence or interdiction. The nation's ability to conduct indications and warning, attribution and response is, at best, dilatory, due to complex technical, policy, legal and interagency coordination issues.

The US capability to defend against unconventional nuclear attack is more developed than capabilities against biological and information warfare attacks. There is a significant experience base and some infrastructure to support early capability assessment and hence, crisis prevention. However, the ability to protect against an attack is sorely lacking. This point is increasingly disconcerting given the magnitude and time-scale of devastation associated with a successful attack. Additionally, improvements are needed with regard to attribution.

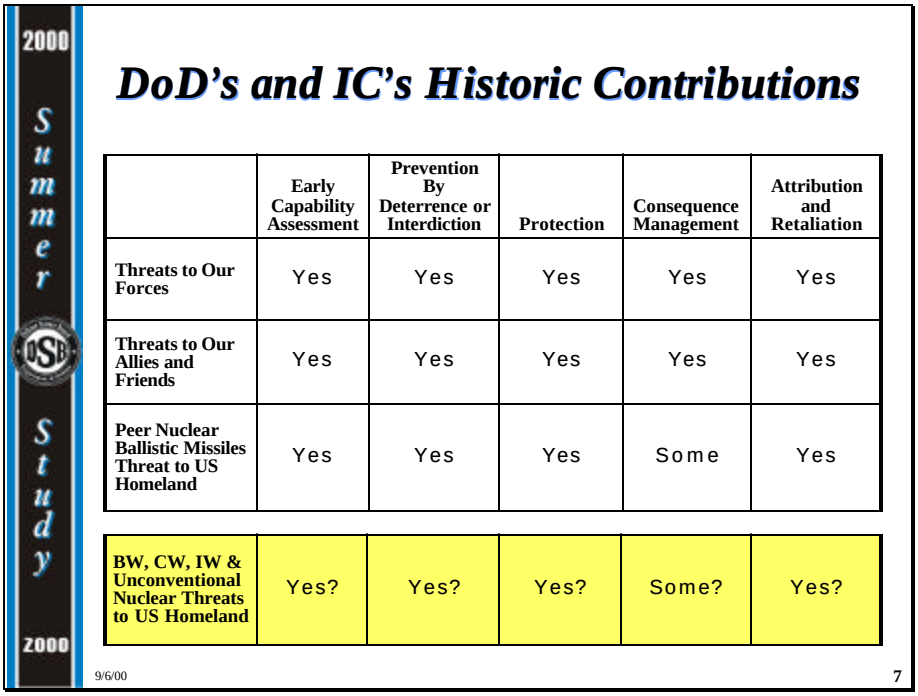
There are many factors, some political and some technical, which contributed to the current state of affairs.

As the remaining superpower, the United States has become a target for both countries and transnational actors. Potential adversaries are more likely to use asymmetric warfare in the future due to a number of factors, the following of which are by no means an exhaustive list. The breakup of the Soviet Union has led to equipment, materiel and human resources being "on the market." Use of these resources for non-traditional attack will prove considerably less costly than mounting a traditional attack. Attribution remains ambiguous in an asymmetric attack, which contributes to the appeal of asymmetric warfare. Additionally, the threat of an asymmetric attack poses danger not only in the physical effects of such an attack but in the psychological fear and damage it could beget as well.

In terms of technology, the biggest driver has been that biological, chemical, and information technologies are very inexpensive and widely available. The trend is toward lower cost, higher performance and even wider availability. Further, skilled human resources are becoming increasingly available and are geographically everywhere. The Internet actually provides a superb command and control system, which was part of its original intent. The United States has become a relatively fragile, complex, interdependent society, which can lead to vulnerabilities that are not fully understood.

While the task force recognizes the broader US federal, state and local government and private sector aspects of meeting evolving threats to the homeland, the scope of the subject was too large to include the full range of national and, even, international issues in this effort. Hence the task

force generally limited its focus to DoD's and the Intelligence Community's capabilities and responsibilities – a large enough set of issues.



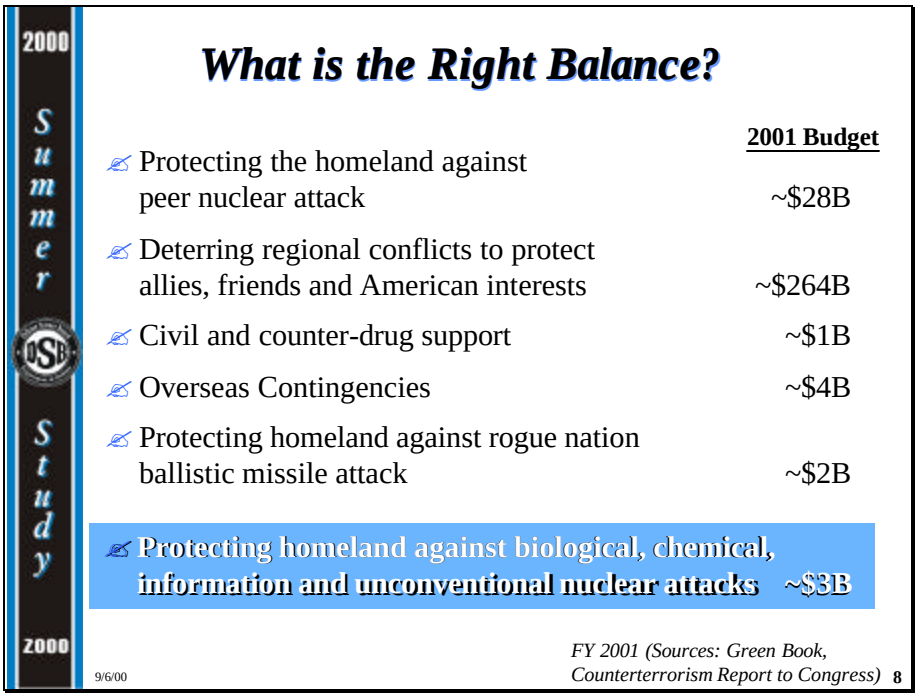
As shown above, the contributions of DoD and the Intelligence Community have historically been substantial in defense of its military forces and against threats to Allies and friends. This is true, as well, in cases where the threat manifests itself in the form of an attack from outside the borders of the United States (e.g., deterring attack by nuclear-armed ballistic missiles).

Although acting in a supporting role to other federal, state and local authorities, the Defense Department and Intelligence Community have significant capabilities to contribute in countering threats to the US homeland posed by BW, CW, IW and unconventional nuclear warfare (e.g., in civil support and consequence management).

These task forces do not make any particular recommendations with regard to the roles and missions of DoD and the Intelligence Community – except to comment that they will likely change given their very strong capabilities. The nation's leaders must become the catalysts for that change. While there is some formality regarding who is in charge (i.e., formally assigned roles), there seems to be a mismatch between those formally in charge and those that actually have capability.

What is the right balance of investment for the Department and the Intelligence Community to be making? The table below provides an indication of today's investment balance (as reflected in the FY2001 President's Budget). The numbers in this table were derived by applying commonplace and, in many instances, mandatory private sector accounting principles to allocate expenses.

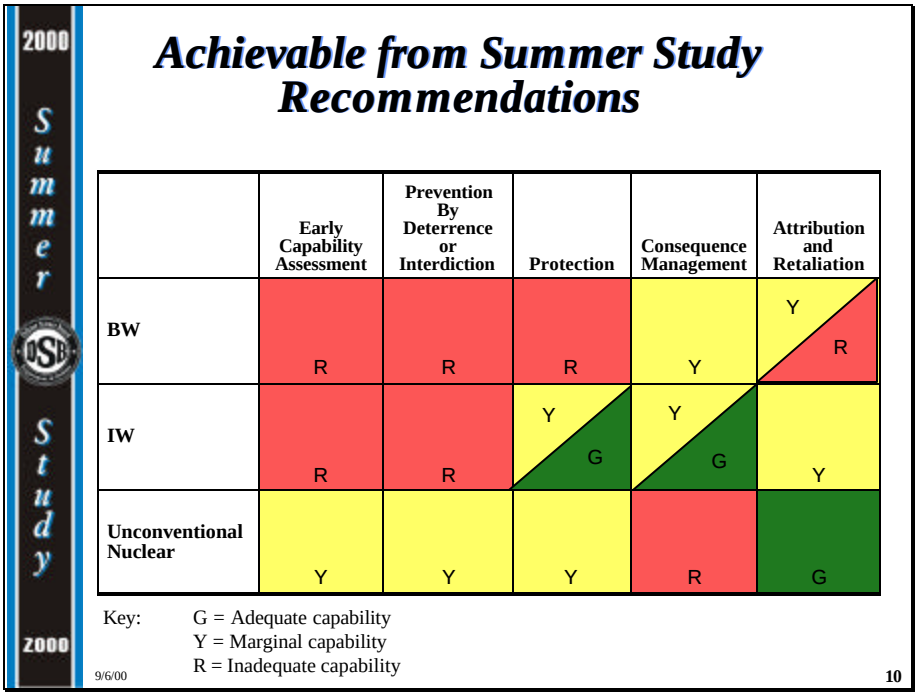
It has been observed, "Here is the Defense Science Board *again* making recommendations to spend money, and there is just no money." The DSB believes that this situation must be regarded as something quite different. This is not a case of "yet another aircraft to go along with the many aircraft we now have." These threats are different, and the DSB sees a more fundamental need for the DoD and the Intelligence Community to restructure their investment balance.



The task force believes that a greater emphasis should be placed on these emerging threats to the homeland than is evident in today's budget allocation. The Department and the Intelligence Community must re-think this investment balance – which is *always* hard in a large bureaucracy.

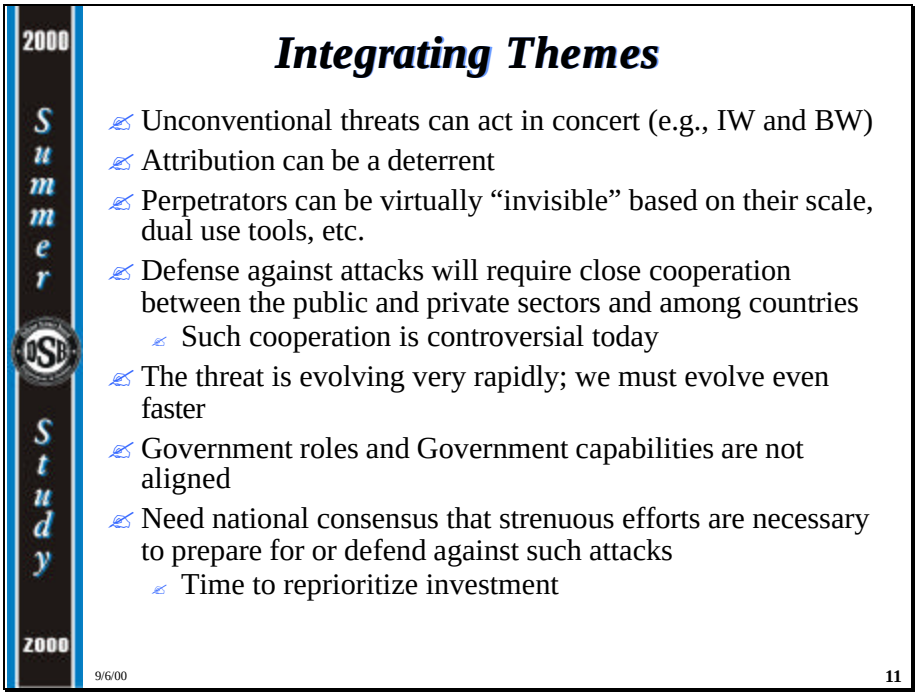
Countering threats to the homeland is the subject of this series of studies. There was no attempt to recommend the investment rebalancing associated with pursuit of such ideas. This activity is left to the Department and its leaders.

Volumes II through IV of this summer study report present a number of recommendations that can provide a basis for progress in addressing three important threats to the homeland. If implemented, these recommendations will have a strong and positive impact on our nation's capabilities, as shown below. But they will not draw the nation into a posture that provides the robust set of capabilities that it demands. Achieving such a posture will require a dedicated and long-term effort. The DSB intends to continue to look for promising capabilities in redressing remaining deficiencies.



As it stands, the recommendations may not make the nation much better off in early capability assessment and, hence, prevention by deterrence and interdiction in all unconventional categories. The exception would be unconventional nuclear weapon defense. There is a broad belief that such a capability would be incredibly powerful.

In its study of defenses against BW, unconventional nuclear and information warfare threats, the summer study found several important integrating themes associated with emerging threats to the homeland (as shown in the table below). Even though these are new and unconventional threats, the nation does not have to discard all of its experience, thinking and posture associated with defense – some of the same thinking applies.



The task forces see unconventional threats acting in concert, not separately. For example, a coordinated IW and BW attack would have a much more devastating impact than either attack conducted alone.

Secondly, the task forces place very high value on attribution as a deterrent. Today, US capabilities for attribution are poor and a perpetrator could operate with anonymity, should he/she choose to do so. With effective (or perceived effective) attribution, such perpetrators would be forced to think twice before attacking the US homeland.

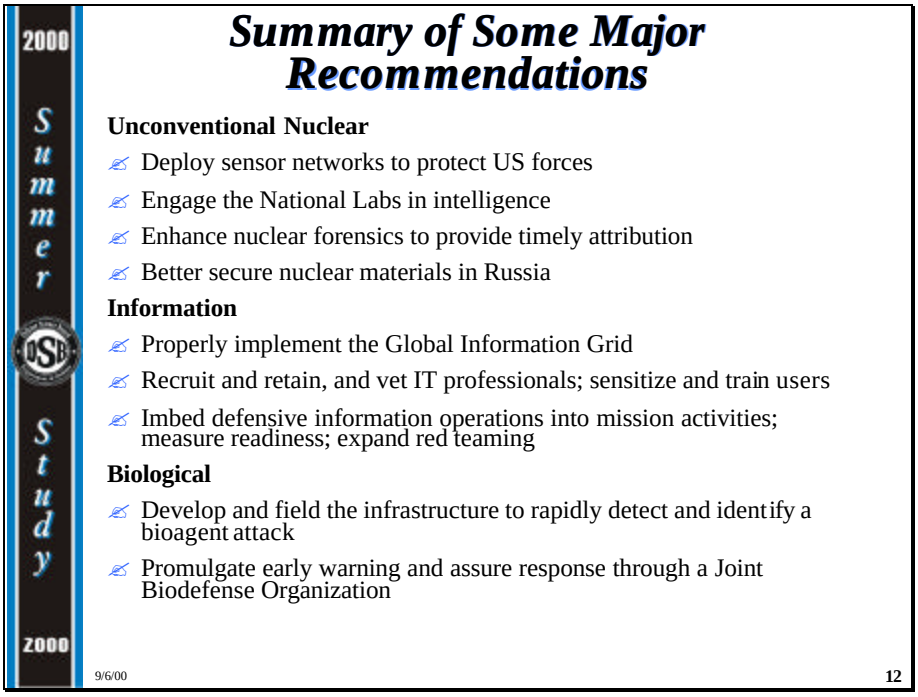
Because of the dual-use nature of the technology and the difficulty of detection, which makes intelligence such a critical issue, the DSB does not see the DoD and the Intelligence Community being effective at early capability assessment of unconventional threats.

Cooperation between the public and private sectors, as well as within and between countries, remains an imperative for successful defense of the US homeland and its allies. The road to partnership is not yet paved, though necessary for the progress that the DSB is advocating. Continued effort and collaboration will be required to achieve this goal.

Worth noting is the fact that the threat is evolving rapidly. The nation's organizational infrastructure is not adequately prepared to keep pace with this evolution and the task forces fear

that America will remain one step behind in its endeavor to keep pace with the techniques employed by her adversaries.

The major recommendations of the DSB 2000 summer study are listed below.



Unconventional Nuclear Threat

The task force on the Unconventional Nuclear Threat focused on two main issues:

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

In response to point (1), the task force found that there is a substantial existing base of capabilities, processes, experienced people, and roles/responsibilities framework within the DoD and DOE for the unconventional nuclear threat (these were primarily within the NEST (Nuclear Emergency Search Team) activities. However, these capabilities and activities, and the underlying strategy, are not as effective as they should be for the emerging nuclear threat.
In response to point (2) we found that the most credible unconventional nuclear threat to the homeland is an attack executed or supported by another country, as opposed to a terrorist threat. Further, that a primary target for such a threat would be our military's war-fighting infrastructure (military bases, main staging areas, strategic sealift and airlift ports, storage areas for overseas pre-positioned equipment and supplies, etc). Additional attractive targets would be civilian

logistics and infrastructures (e.g. energy, transportation) that are essential to effective military operations. Protection of these war-fighting assets and capabilities falls clearly within the responsibility of the DoD. Thus, the task force recommendations regarding DoD's role is to focus on protection and deterrence for unconventional nuclear attacks against these key military and national targets.

The task force makes six specific recommendations, all of which are within current program structures, are within the authority of current agencies, and are reasonable in cost. The principal recommendation is the deployment of protection systems built from existing technology to key military targets. Such systems would also provide a capability to deploy to a wider variety of targets upon warning. Other recommendations are made that would lower the threat by (a) limiting the availability of nuclear materials, (b) strengthening deterrence by improving our ability to attribute an attack by upgrading our nuclear forensics capability, and (c) improve the processing of intelligence collection to increase the sensitivity of detection of unconventional nuclear threat indicators. We also recommend strengthening the existing R&D program to better address the issues of cost, ease of deployment, and effectiveness of detection. Their final recommendation is to perform thorough systems analyses of the unconventional nuclear threat to better characterize the variety of threats and most effective responses.

These recommendations, taken together, form the basis of a more coherent strategy. When executed, they provide the basis for extending protection to a broader range of homeland targets and unconventional threats such as terrorists.

Information Warfare Threat

In its 1996 report, the Defense Science Board recommended that the Pentagon invest an additional $3 billion to strengthen defenses of its information networks. The Department accepted a number of the suggestions made by this task force, but technology has continued to evolve. With the Department's embrace of Web-based technologies, defensive information operations are even more vital now than it was four years ago.

Under Joint Vision 2020, future warfighting plans will be increasingly reliant on high-speed, interconnected information networks to carry out battles, transmit plans, identify targets and even conduct computer teleconferences among far-flung officers. This construct for the military is built on an ability to detect and track the enemy, move that information across continents, fuse it and analyze it, then decide and take action, often under very tight time constraints, sometimes within minutes.

The Defense Department's networks both non-classified and classified ones, as well as its tactical systems are, in part, on commercially available telecommunication assets. Rather than laying cable and launching communications satellites itself, the Defense Department leases the vast majority of those services from private industry, which for economic reasons tend to use the most cost-effective option rather than the most secure. If there is a weakness in any part of the network, the effect could be anything from a minor annoyance to the disruption of a military operation at a critical juncture.

Together with DoD-unique software and systems, the commercial infrastructure forms the underpinning of the "Global Information Grid," or GIG, the interconnected network of sensors and information systems that will allow Joint Vision 2020 to be realized. The GIG is being developed from legacy and new systems, growing in capability with every "node" a system engineer connects to it - and is becoming increasingly vulnerable as well. Each component's vulnerability to information operations exposes everyone else on the grid to the same intruders.

The task force emphasizes that the GIG is a weapon system and must be treated as such. The nation is in an arms race with regard to superiority of such capabilities. Experience suggests that as US defensive capabilities increase, so will the adversary's offense.

The task force concluded the Pentagon cannot tell whether these information systems are hardened and ready for battle; struggles with the relationship between military defensive information warfare operations and law enforcement operations, and has an insufficient capability to restore the system's integrity if it is successfully attacked. Too much money and time is being spent on the lower level threats to the nation's networks (e.g., hackers), and not enough on figuring out how to protect information systems from state and terrorist warriors who understand how to exploit compromised data. Moreover, there is a serious shortage of information-technology professionals on the Pentagon's payroll, and the deficit is expected to grow.

The task force makes a variety of suggestions, the most important being that the DoD implement a consistent security "architecture" for every node on the network that forms the GIG. The Pentagon's entire public Web sites should be moved off the Internet into a more controlled environment, with encryption and digital identity "keys" widely used. The system should be watched over by a host of different intrusion-detection systems. The task force recommends investment in the constant improvement in the security of the GIG, as well as continued research and development on key problem areas such as reconstitution. The task force suggestion creation of a new DepSecDef-led Board to oversee implementation of the GIG and this new security architecture.

To detect potential weaknesses, the task force then recommends that DoD create a permanent opposition force to continuously test its own systems. Further, to help DoD achieve a better capability to recover from a successful information attack, the task force suggest investment in the various computer emergency response teams that have proliferated throughout the Pentagon, standardizing their work, improving their cooperation and creating more of them.

To combat the "insider threat" posed by those with root access to networks, the task force recommends conducting background checks on system administrators. It also recommends beefing up security training for the everyday user of Defense Department networks.

The panelists would also make military commanders responsible for the military readiness of their information systems, and would direct them to pinpoint and redress their vulnerabilities.

The task force also notes difficulties in sharing data between the national security community and the National Infrastructure Protection Center, a division of the FBI created two years ago to

collect information on attacks and viruses, warn the private sector and help the federal government respond. The National Infrastructure Protection Center's practice of restricting information-sharing on incidents and investigations is inimical to DOD's interests and appears to have no basis in law.

If an agreement cannot be reached for better sharing between the Pentagon and the Justice Department, the task force recommends that DoD develop its own investigation-and-warning process and work out ways to share its data with other government agencies and the private sector.

Biological Warfare Threat

The task force on Defense against Biological Warfare concluded that the United States is ill-prepared prepared for a BW attack, asserting that 100 to 1,000 cases of one of these diseases in a single city would tax the nation's health care system. The task force paints a grim picture of the effectiveness of biological warfare. For example, an attack on a city with 100 kilograms of bioagent would kill one to three million people, twice the number of fatalities that would result from a one megaton nuclear weapon. Moreover, because of the commercial nature of the ingredients needed to manufacture viruses and pathogens, biological weapons are harder for governments and monitoring regimes to track and control than nuclear weapons development.

This task force recommends that the Defense Department develop a database of biological weapons, a computer chip to automatically diagnose the diseases in patients, and a computer network that will rapidly warn health care centers about man-made outbreaks.

?? The first step recommended is for the Defense Department to create a "Bio-Print" database that would create "signatures" of the up to 50 bioagents that cause human disease. Acquiring threatening bioagents should be given urgent priority and would not only yield medicines and vaccines against them but also help track leakage of the diseases into "states of concern" like Iraq and terrorist groups. At the same time, it would profile the signatures of organisms used in the private sector for legitimate purposes.

?? The next step would be to create the diagnostic "Zebra Chip" - a reference that compares discerning a zebra from a pack of horses to discerning a bioagent from a multitude of natural human infections. The miniaturized zebra computer chip would provide immediate diagnoses of diseases documented in the Bio-Print database, flagging manmade or unusual diseases to health care workers even before there are symptoms. It would be non-intrusive and disposable, working with a sample collected from a patient during a routine clinical screening. The chips would be introduced in the DOD health care system which serves 4.4 million people, and eventually transferred to the civilian health care system.

?? If the "front line" zebra chip detected bioagents, the Defense Department would then deploy more sophisticated forensic zebra chips designed to probe for the specific agent in question.

?? Once a biological agent has been confirmed, the information would be broadcast on the Biological Warning and Communication System (BWACS), which would warn all DOD health care organizations, military bases, the Reserves and the Center for Disease Control and other civilian health organizations.

At the same time, the task force is recommending that the Pentagon invest heavily in research and development for bioagent drugs and vaccines, and work with the Food and Drug Administration to accelerate the review process. It also recommends the Pentagon fund a $50 million to $100 million manufacturing facility for vaccines or after-exposure drugs in order to speed production.

To provide oversight for all of this development, the task force then recommends the establishment of a new organization that it calls the Joint BioDefense Organization (JBDO). The JBDO would direct the military response to a bioagent outbreak and would coordinate efforts with the civilian sector and media, and would report directly to the president and the defense secretary through the chairman of the Joint Chiefs of Staff. The task force estimates that the above recommendations would require the investment of $3.2B over the FY2002 Future Years Defense Program.