The Defense Science Board
1997 Summer Study Task Force

on

DOD RESPONSES TO TRANSNATIONAL THREATS

Volume III
Supporting Reports

DISTRIBUTION STATEMENT A
Approved for public release;
Distribution Unlimited

February 1998

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

19980427 002

DTIC QUALITY INSPECTED 3

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.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this 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, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	Feb 98	Final, Vol III supporting data, 1997

4. TITLE AND SUBTITLE
Defense Science Board Summer Study Task Force on DoD Responses to Transnational Threats -- Volume III Supporting Reports

5. FUNDING NUMBERS
N/A

6. AUTHOR(S)
Dr. Robert Hermann
Gen Larry Welch, USAF (Ret)

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Defense Science Board (DSB)
Office of the Under Secy of Def (A&T)
3140 Defense Pentagon
Washington DC 20301-3140

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
same as above

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION AVAILABILITY STATEMENT
Distribution Statement A
Approved for Public Release: Distribution is unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

14. SUBJECT TERMS

transnational threat	BW/CW	force protection
terrorism	national security	
WMD	domestic first responders	

15. NUMBER OF PAGES
294

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	N/A	N/A

DTIC QUALITY INSPECTED 3

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

DEFENSE SCIENCE
BOARD

9 Dec 97

Honorable Jacques S. Gansler
Under Secretary of Defense Acquisition and Technology
3010 Defense Pentagon
Washington, DC 20301-3010

Dear Mr. Secretary:

In response to joint tasking from the Under Secretary of Defense for Acquisition and Technology and the Chairman, Joint Chiefs of Staff, the 1997 DSB Summer Study Task Force addressed the Department's Responses to Transnational Threats. In the study, the Task Force concludes that the Department should treat transnational threats as a major Department of Defense mission.

Transnational actors have three advantages: 1) they can have ready access to weapons of mass destruction; 2) we cannot easily deter them because they have no homeland; and 3) they respect no boundaries, whether political, organizational, legal or moral. Further, warning may be short and attribution may be slow or ambiguous. Since the United States is now the dominant military force in the world, potential adversaries will be driven to asymmetric strategies to meet their objectives. As such, transnational threats represent an important national security problem.

Notably, the Department of Defense has the capacity to mitigate these threats with its extensive capabilities, training and experience. In the attached report, the Task Force suggests a multi-faceted strategy for the DoD to address this increasingly important class of threats. This strategy involves the development of an end-to-end systems concept, investment in critical technology areas, and the leveraging of similarities between civil protection and force protection. The Task Force concludes that the Department also needs to increase its emphasis on responding to this threat by more clearly assigning responsibilities and by providing mechanisms for measuring its readiness to respond.

We hope this Summer Study provides insights on how to mitigate transnational threats to the Nation. It stops short, however, of providing a plan. We strongly encourage the Department to take on the task of developing an implementation plan that identifies the appropriate allocation of resources and areas for emphasis.

Craig I Fields
Chairman

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

DEFENSE SCIENCE
BOARD

8 Dec 97

Memorandum for the Chairman, Defense Science Board

Subject: Final Report of the 1997 Defense Science Board Summer Study Task Force on DoD Responses to Transnational Threats

The final report of the 1997 Defense Science Board Summer Study Task Force on DoD Responses to Transnational Threats is attached. This report consists of three volumes: Volume I which presents the major findings and recommendations of the Task Force, Volume II which focuses on force protection and is written expressly for the Chairman, Joint Chiefs of Staff, and Volume III which includes eight supporting reports.

After focusing on this study topic for a period of six months, we concluded that threats posed by transnational forces are an important and under-appreciated element of DoD's core mission. We found a new and ominous trend -- a transnational threat with a proclivity towards much greater levels of violence. Transnational groups now have the means, through access to weapons of mass destruction and other instruments of terror and disruption, and the motives to cause great harm to our society. Since the United States remains the dominant military force in the world now, potential adversaries will be driven to asymmetric strategies in order to meet their objectives.

The Department of Defense has the capacity to mitigate these threats with its extensive capabilities, training and experience. We suggest that the DoD address this increasingly important class of threats through a response strategy that includes six elements:

1. Treat transnational threats as a major DoD mission
2. Use the existing national security structure and processes
3. Define an end-to-end operational concept and system-of-systems structure
4. Provide an interactive global information system on transnational threats
5. Address needs that have long been viewed as "too hard"
6. Leverage worldwide force protection and civil protection

Together these principles will help the Department deal with transnational threats today and in the future. Notably, the task force holds that DoD can respond without a change to national roles and missions, and without change in its own organization. However, the DoD does need to increase its emphasis on this threat, clearly assign responsibilities and measure its readiness to respond. In addition, the

Department should focus more attention on strategies, architectures and plans that address the end-to-end set of capabilities needed.

We thank the Task Force members and the talented group of government advisors for their hard work and valuable insights. Their dedication reflects their belief in the importance of this challenge to the Department.

Robert Hermann, Chairman

Larry Welch, Vice Chairman

Supporting Reports*
Table of Contents

THREATS AND SCENARIOS PANEL

SCIENCE AND TECHNOLOGY PANEL

DOD RESPONSE CAPABILITIES AND OPTIONS PANEL

Operational Intelligence Competency Panel
Nuclear Competency Panel
Chemical Warfare / Biological Warfare Competency Panel
Physical, Launched, and Unconventional Means Competency Panel
Information Warfare / Electronic Warfare Competency Panel
Civil Integration and Response Competency Panel

* Volumes 1 and 2 of this report represent the consensus view of this Task Force along with its analytical results and recommendations. Volume 3 of this report contains materials that were provided as inputs to the Task Force, but whose findings and recommendations may not represent the consensus view of this Task Force.

REPORT OF THE THREATS AND SCENARIOS PANEL

Panel Chairs

Ms. Nina Stewart
Mr. Oliver Revell

Panel Members

RADM Tom Brooks, USN (Ret)
Gen. James Clapper, USAF (Ret)
William Garrison
Mr. Dennis Imbro
Mr. James Moody
Mr. Gordon Negus

Government Advisors

Mr. John Capece
CAPT Jack Cassidy, USN
Dr. Larry Gershwin
Mr. James Hertsch
CAPT Keith Mulder, USN
Ms. Bonnie Phelps
Mr. Peter Probst
Maj Jon Ross, USMC
Mr. Jeff Staats

EXECUTIVE SUMMARY

The Threats and Scenarios Panel of the Defense Science Board's Summer Study of Transnational Threats reviewed the transnational threat in the context of changes in the motivations, goals, capabilities, and trends of states, groups, and individuals. We concluded that the transnational threat is more difficult and dangerous today and in the future than it has been in the past based on a variety of new ingredients. These new ingredients, or "enablers," include the easy availability of information and technology, the proliferation of weapons of mass destruction and delivery systems, the presence of more technically proficient actors, and the increasing linkages of convenience and cooperation between rouge states, organized crime and narcotics groups, extremists, and terrorists.

Some transnational threat actors today are undaunted by the specter of mass casualties. Indeed, a high kill rate is a goal for some extremists who are motivated by hate and revenge. Today, a small number of people can threaten the mass population with consequences only a large nation state in the past could muster. If these same actors profess no tie to national identity, then national boundaries are no deterrence, and attribution, deterrence, and retribution are most difficult to achieve. Several of the most recent terrorist incidents, such as the World Trade Center bombing, the Aum Shinrikyo subway sarin release, and attacks by Libya, were part of a longer term " terror campaign" which went unrecognized at the time.

In examining these groups and individuals, we built upon a forecast of the future global model developed by the intelligence community. In this model, population growth in the third world, transmigration, the diminishing authority of some nations, ethnic rivalries, and globalization of financial structures and economies will help create the motivations and means of some transnational threat actors. For the U.S., as we stay engaged in peace keeping and humanitarian missions, our military dominance will deny most nation states the ability to overtly attack, at the same time that our military operations become most vulnerable to covert strategies. Asymmetric options against us will become more attractive. And terrorism on a large scale has already struck our heartland, ensuring that America will no longer remain a sanctuary from the form of violence prevalent elsewhere.

The Panel also identified several shortfalls in capabilities to identify the threat. Most critical was the requirement for a focused collection strategy as well as the need for a more comprehensive analytical approach, complete with an interactive information system that crosses the government's stovepiped structures.

The panel developed a series of charts and scenarios for use by consumers. One chart demonstrates the damage implications of the B'Nai B'rith incident if 150 grams of anthrax were used. Another model, chart 2, represents a thermometer and measures actual events and casualties against the attack if weapons of mass destruction were used.

Illustrative scenario 1 illustrates a series of subway chemical attacks and information systems disruptions in New York City and Washington D.C. in which a middle eastern group seeks revenge through the use of sarin dispersals and insiders at Bell Atlantic Phone Company.

Illustrative scenario 2 focuses on the release of a highly contagious biological agent, stolen from Russia, and dispersed in Los Angeles. As the contagion spreads, emergency services are rapidly

overtaxed; panic spreads, and the governor declares a state of emergency, appealing to the President for military assistance.

While the scenarios are fictional, none are impossible to achieve. We tried to use scenarios that demonstrate the reality of the transnational threat. Transnational threats interfere with the Department of Defense's ability to perform its mission, to protect its forces, and to carry out its responsibilities to protect the civilian population. However, the Department also has the capacity to help resolve these threats, with its unique capabilities, expertise, and assets.

TRANSNATIONAL THREATS:

The Face of the Future

SCOPE

The Secretary of Defense charged the Defense Science Board with studying transnational threats, defining transnational threats as terrorism (including weapons of mass destruction use), information warfare, organized crime, proliferation and narcotics. The Threats and Scenarios Panel was chaired by Nina Stewart and Oliver Revell, with membership consisting of Thomas Brooks, James Clapper, William Garrison, Dennis Imbro, and Gordon Negus. Its members and advisors represented a wide range of expertise from the intelligence community, the military services, science laboratories, and American industry. The Panel focused on transnational threats in the context of how they impact directly on U.S. national security and defense policies, and Department of Defense personnel and facilities, both at home and abroad, and; how they generate requirements for Department of Defense support. The Panel also studied the threats from the perspective of the opposition's motivations, activities, and capabilities rather than just by the severity of the incident.

STUDY METHODOLOGY

To begin, the Panel took a look at transnational threats from a historical perspective in order to gauge the 21st century outlook. We attempted to identify the constants and changes in practices in terms of motives, targets, and weapons of choice, as well as on self constraints or the lack of them.

To understand current trends, the Panel reviewed the intelligence community's latest estimates, studied open literature, and interviewed knowledgeable persons in and outside government. We also tasked the intelligence community organizations to provide data on group motivations, capabilities, and trends.

This research led to recognition of the new transnational threats — including the "new terrorist" — who may have access to weapons of mass destruction, could be capable of information warfare, or might be linked to crime groups and narcotics trafficking on a massive scale. Transnational threats are not limited to terrorism, but include other destabilizing factors brought about, for example, by organized global criminal groups.

The significance and implications of the emerging 21st century transnational threats is a major policy issue of such consequence that the challenge they represent must be reflected in force structure and military operations. Several illustrative scenarios demonstrate the consequence of these threats to the nation and uniquely to our armed forces, as well as highlight increasing U.S. vulnerabilities.

Finally, the Panel looked ahead in an attempt to understand whether the future consequences of transnational threats become more dramatic or less. It drew heavily from government studies,

such as "Future Vision 2010" and "Global Threat Assessment: Looking to 2016," for much of the environmental factors affecting terrorism and other transnational threats.

THE PERSISTANCE OF TRANSNATIONAL THREATS...

Traditionally, terrorist organizations and individuals have employed violence to achieve a variety of objectives. Some groups, like the Palestine Liberation Organization (PLO) and the Irish Republican Army (IRA), struggle to gain political recognition; others, like Hizbollah or Hamas, terrorize in the belief that their acts add to the glory of their religious convictions. Some, like Timothy McVeigh, murder simply because they are motivated by hate, and seek to punish their victims. Others, like the Somali war lords, use violence as an asymmetric response against an unwanted intervention in their country. Still more may not have particular motivations of their own, but commit violence on behalf of a state sponsor for purposes of political or strategic advantage.

The use of transnational violence persists because it is effective, cheap, and sponsorship often can be disguised or denied. For example, when the U.S. commitment to its forces or policies abroad have been uncertain, as in Somalia or Lebanon, the use of violence to achieve American casualties has been a particularly useful tool in undermining U.S. resolve and forcing a U.S. retreat. Terrorism can often pit public opinion against government policy, and in some instances, has toppled unpopular governments.

...AND THREATENING SEEDS OF CHANGE

While the motivations for transnational threat groups many not change dramatically, operational behavior, and the methods and means these groups use — the "enablers" — do evolve and adapt to contemporary issues, technical capabilities, strategic alliances, and vulnerabilities. The trend of contemporary changes today — the passing of the bipolar world and the wider availability of knowledge and technology — is resulting in the emergence of new dimensions to the transnational threat. For example, the diminishment of communism resulted in the reemergence of a wide variety of formerly repressed ethnic or religious tensions and the loosening of control over nuclear, radiological, biological, chemical, and other related technologies, explosive material, and finished weaponry such as missile delivery systems. Combine these trends with easily available information on weapons of mass destruction and the mix has resulted in a new breed of transnational threats very much different — and more dangerous — from the old. The reality is that transnational threat groups are increasingly tied to one another in new and more cooperative ways that threaten the stability of governments, the financial and information infrastructure, international trade and peace agreements. The fact of increasing cooperation among crime, narcotics, and terrorist groups will provide terrorists with new, more creative ways to raise money, and with a marketplace to shop for weapons and high-tech equipment. The reality is that a small number of people can now threaten others with casualties and consequences heretofore achievable only by nation states.

COPING WITH TRANSNATIONAL THREATS

One component of what makes these transnational threats different and difficult is the fact that they are difficult to deter, detect, and control. National boundaries are not effective barriers, and are often used to an adversary's advantage. With little or no tie to national identity, attribution can be difficult in the event of an attack, and retribution may not be possible.

Another component of our vulnerability is that Americans tend to view transnational threats singularly. That is, we tend to look upon terrorism incidents, even those on a grand scale like the New York City Trade Center bombing, or the Oklahoma federal building explosion, as individual events that do not evidence a sustained campaign against the U.S. This is not the reality. The reality is, a number of terrorist groups have a long-term program of unconventional warfare against the United States.

The Qahdaffi Campaign

When evidence pointed to Libya as the culprit behind the LaBelle Disco bombing in Berlin, which killed two and injured many, the U.S. retaliated with a military strike in April, 1986 against specific Libyan targets in Tripoli. The popular belief for years was that the U.S. attack suppressed Libyan activity in support of terrorism. However, an examination of events in subsequent years paints a far different picture. Instead, Libya continued, through transnational actors, to wage a revenge campaign through the remainder of the decade.

The retaliation began three days after the U.S. strike when Libya purchased from Lebanon and executed hostage Peter Kilbourne. In September, 1987, Abu Nidal (on behalf of the Libyans) hi-jacked Pan Am 73, causing the death of several more Americans. The following April, 1988, the Japanese Red Army Faction, under contract to Nidal, bombed the USO in Naples, killing a U.S. soldier. In a simultaneous effort, one member of the group was arrested in New Jersey with pipe bombs to be detonated at recruiting stations in New York City. The attacks continued. In December, 1988, Libya sponsored the bombing of Pan Am 103 over Scotland, which killed 270 people (including 200 Americans). A year later, in September, 1989, the UTA French airliner was destroyed over Chad by the same group. During this same period, the group was linked to various assassinations of dissident Libyans in the U.S. It also recruited a Chicago street gang to attack U.S. airliners with shoulder fired weapons — a move that was interdicted.

All in all, Qahdaffi sponsored six more attacks, using surrogates for plausible denial, after the LaBelle disco bombing. The facts illustrate the ability and willingness of rouge states or other transnational actors to wage a long and continuous campaign against the U.S. using unconventional warfare and relatively small investments.

Ramzi Yousef Campaign: A Case of Religious Extremism

In May, 1990, a small band of religious extremists headed by Ramzi Yousef assassinated Rabbi Meir Kahane. At the time, the rabbi's death was treated as a homicide, unrelated to national security. It was only later that this assassination was discovered to be part of a larger revenge campaign against U.S. foreign policy that manifested itself in the World Trade Center bombing, in February, 1993. Six people were killed and five thousand were injured, but the terrorists' plans were to kill 50, 000 through the collapse of the towers. They also considered augmenting

the explosion with radiological or chemical agents, which would have pushed the casualty rate far higher.

Ramzi Yousef, the mastermind of the bombing, gave other instructions to his group. He planned a massive infrastructure attack on New York City on the Fourth of July that would have included attacks on the George Washington Bridge, the Lincoln and Holland Oliver Tunnels, the United Nations Headquarters, and the Federal Building. Part of this plan also involved the assassination of President Mubarak of Egypt and U.S. Senator D'Amato, but the acts were interdicted through intelligence and surveillance.

Yousef continued his campaign. In November, 1994, he planned the assassination of the Pope during his visit to the Philippines. His group also planned to blow up thirteen U.S. airliners using explosives smuggled aboard. This particular activity was tested on a Philippine airliner where a bomb was successfully smuggled aboard and detonated, killing one passenger. Had the broader plan been successful, four thousand people would have died.

Aum Shinrikyo: A Chemical / Biological capability

In June, 1994, sarin sprayed from a truck killed seven and injured 200 people in Matsumoto, Japan. The motive and organization of the attackers was not realized until nearly a year later when in March, 1995, the Aum Shinrikyo group released sarin in seven locations in the Tokyo subway system. This attack, directed against national police, killed twelve and injured 5,500. Within the same month, the group attempted the assassination of Japan's National Police Chief. Plans for attacks in Disneyland and against petrochemical facilities in Los Angeles existed as well. It was later learned that the group released anthrax in Tokyo on two separate occasions with no resulting casualties.

The motivation of the group was to create large casualties and chaos designed for political purposes. They claimed they intended to create a conflict between Japan and the U.S., and that they would rise to power as a result of the conflict. The size and organization of the group was enormous: Thirty thousand members, ten thousand of whom were in Russia, with operations in Japan, Russia, Korea, Australia, Sri Lanka, and the United States. They had an asset base of $1.2 billion dollars. The group was testing capabilities to create sarin, VX, anthrax, botulism, and radiological agents. This organization existed without the full appreciation of U.S. or Japanese intelligence. Indeed, the group took advantage of Japan's laws by registering themselves as a religious group, thereby limiting the coverage of the group by law enforcement.

These three more recent cases of transnational threats are different from the way we thought of them in the past. In the past, analysts believed one of the key "tenets of terrorism" was that all terrorists calculated thresholds of pain and tolerance, so that their cause was not irrevocably compromised by their actions. In Brian Jenkins' terms, terrorists used violence "like a volume control knob" in order to gain attention. While U.S. government agency officials worried some about terrorists "graduating" to the use of weapons of mass destruction (and the weapon most officials worried almost exclusively about was nuclear), they believed — based on reports from terrorists themselves — that most terrorist groups thought mass casualties were counterproductive. This was because mass casualties seemed to delegitimize the terrorists' cause, would certainly generate strong governmental responses, and erode terrorist group cohesion. In essence, terrorists were ascribed a certain logic and morality or line beyond which

they dared not tread.[1] Likewise, narcotics trafficking, the proliferation of arms, and scourge of organized crime also have been treated independently of one another, and we have organized our governmental efforts to combat the transnational challenges separately.

The Status of "Classic" Terrorism Today: The Extreme Left

The driving motives for violence by the extreme left were significantly diminished by the recent discrediting and resulting disenchantment with socialism on a global scale. The groups find that their message is out-of-fashion, and they can no longer mobilize the public to their causes. This "demotivation" is a major reason for the recent downward trend in international terrorist incidents, as documented in the State Department's "Patterns in Global Terrorism."[2]

The threat level of all leftist groups globally, once rated high, is now categorized as moderate. Of the twenty-two known groups, three have denounced violence altogether. Indeed, high collateral casualties are inconsistent with the fundamental message of leftist terrorists who profess their goal to be the better welfare of the masses. The Intelligence Community now provides only moderate to low coverage of these groups.

State Sponsorship

State-sponsored terror has seen a notable decline in the last several years for largely three reasons. First, the Middle East peace process has given previous violent groups and states a motive to refrain from terrorism in order to gain leverage and bargaining power at the table. Second, post Cold-War geopolitical realities have brought about many new agreements and growing cooperation among nations in countering terrorism. One of the largest sponsors of terrorism in the past — the old communist East European countries — are now aggressively supporting counter terrorism initiatives.

However, several state sponsors remain who continue to fund, motivate, support, and train terrorists. Iran is by far the most active of these state sponsors, with the greatest long-term commitment and worldwide reach. Iraq remains of concern, but is judged to have a more limited transnational capability. However, attacks within Iraq's own backyard, such as the attempted assassination of President Bush in 1993 during his Kuwaiti trip, and the assassinations of dissidents in Jordan, are more likely to threaten the peace and stability of the region. Syria is judged to be a more pragmatic sponsor, by providing supplies in transit, but has refrained more recently from terrorism in order to enhance its negotiating position in the peace talks. Its loss of USSR patronage has meant a decline in financial and logistical support, but it nevertheless allows some rejectionists to maintain headquarters in Syria. The Intelligence Community has also noted that Hizballah can still receive supplies through the Damascus airport. The newest sponsor, Sudan, was added in 1993 because of its provision of safe haven and training for a variety of terrorist groups. Sudan hosts Usama bin Ladin's facilities. Libya, a notorious state sponsor, has also refrained lately from terrorism in order to obtain some sanctions relief. It continues, however, to target dissidents, fund Palestinians, and provide safe haven for Abu Nidal, all while attempting to avoid accountability for the Pan Am 103 downing.

---

[1] see Brad Roberts' presentation to DSB on June 30, 1997.

[2] "Patterns in Global Terrorism" does not address indigenous terrorism, a rapidly escalating phenomenon.

Radical Islamics

Radical Islamic groups are now the most active in terms of the rate of incidents. Many of these groups are considered separatists, and desire a seat at the recognition and negotiation table. Others, considered extreme Islamic zealots, operate as loosely-affiliated groups (e.g. World Trade Center bombing) and for whom deterrence has less cache. In any event, some of the extremists may operate on the notion that the volume of casualties is an issue of practicality, not morality.

Ethnic Separatists

Ethnic separatist terrorism, as old as mankind, can be temporarily side-tracked by a few contemporary geopolitical developments, but generally, it is impervious to such developments because its root-cause is invariably long-lived. Most of these groups seek world recognition and endorsement; to date, they have not resorted to violence using weapons of mass destruction.

The "New" Terrorist

The argument has been made, and it is one we accept, that while traditional terrorism — in terms of motivations — is still a large segment of the terrorist population, there is a new breed of terrorist for which the old paradigms either do not apply at all or have limited application. These groups — cults, religious extremists, anarchists, or serial killers — must be regarded as serious threats, and the most serious of the terrorist groups today. These "new" terrorists are driven by a different set of motivations: they seek an immediate reward for their act, and their motivations may range from rage, revenge, hatred, mass murder, extortion, or embarrassment, or any combination of these. They may desire mass casualties, or at least not care about how many people are killed in their attacks. As such, they do not make traditional calculations of thresholds of pain or tolerance within a society. These groups tend to be loosely affiliated both internationally and domestically, and may have no ties at all to state sponsorship. They change affiliations and identities as needed, and are extremely difficult to detect. Where traditional groups want publicity to further their cause, many "new" terrorists do not desire attribution; this is particularly true of the religious extremists (e.g. God knows, and will reward). Religious extremism is growing in numbers, and is not limited to the Islamic faith. While the "new" terrorist may have a variety of motivations, some single issue groups (extremists in the animal rights, environmental, and anti-abortion movements, for example) may also pose a significant threat, and should not be overlooked. Additionally, the fact of the millennium is an important apocalyptic milestone for many religious or extremist cults. Many terrorist groups, both traditional and "new," have privatized their practices through a few standard business techniques (such as fund-raising, use of technology, etc.)

One of the more difficult groups to track today are the domestic militia-type extremists. While much is not known about these groups, some commonalties prevail. Many of these groups have substantial expertise. They conduct chats on the Internet talk rooms about various dosage levels of various biologicals needed to cause the greatest lethality. They have also exhibited a fascination with poisons and high explosives, along with more standard military personnel and weaponry. Contrary to some popular opinion, these types of groups are growing even after the devastating attack in Oklahoma City, and they are building skills, developing international connections, and are exhibiting growing political sophistication. Their targets are diverse: they may attack federal buildings, military personnel, specific racial groups, corporate icons, or

multinational companies. They capitalize on (and heighten paranoia) of the growing fear among some Americans of big, intrusive government.

Terrorists have shown a propensity to mimicry, so it is with alarm that analysts today view the chemical attack precedent set by the Aum Shinrikiyo in Japan because it shattered the paradigm that "terrorists don't do weapond of mass destruction (WMD)." In fact, the B'Nai Brith incident in Washington D.C., along with several others, have shown that terrorists are watching, reading, and learning. They are greatly motivated by government actions (or, in some instances, inaction). The Oregon Cult poisoning several years ago (lacing the salads in several fast food restaurants with salmonella and poisoning the town's water supply) in the attempt to sicken voters was a recent example of terrorists using a biological toxin. Additionally, the World Trade Center attempt at mass casualties, and the actual mass killing within the federal building in Oklahoma City are precedents, in that terrorists demonstrated a desire to inflict mass murder on our homeland.

Also new today is the proliferation of knowledge and technology among many criminal, terrorist, and narcotics groups. Many of these groups are building skills in state-of-the-art communications, and weaponry. The Internet, for example, provides world-wide communications capability and new tools for operational C3I, targeting, fundraising, and propaganda dissemination. They are achieving new global links and support from one another in cooperative ways.

The Globalization of Proliferants, Organized Crime Groups, and Drug Lords

Twenty years ago, intelligence specialists viewed proliferents primarily through the lens of nation states seeking the ultimate weapon and from the scope of east-west conflict. Chemical and biological weaponry was only a minuscule afterthought of the whole nuclear problem. Organized crime and narcotics, while scourges twenty years ago, were not among primary intelligence targets; they fell within the domain of law enforcement problems, by and large. Crime groups jealously guarded their turf, and tended to view one another as competitors rather than allies. Today, each of these categories are priority intelligence targets, with a wide array of government participants working the problems.

The traditional characteristics of organized crime groups remain relevant today. Generally, they are affiliated by familial, ideological or ethnic ties that instill loyalty and reduce the likelihood of law enforcement or intelligence infiltration. The purpose of their activities has remained unchanged: they seek money (read large sums of cash) and status or power. They will often seek to provide government-like services so that the local populace will learn to rely upon them. Finally, criminal organizations will almost always seek to establish respectability and legitimacy, often through philanthropic acts, the controlling of local businesses, and provision of local employment opportunities.

One of the outcomes of the globalization of economies and technologies is the relatively new linking and intermingling of disparate crime and narcotics organizations with terrorists. Analysts have been dismayed to find that even the most notorious crime groups with global reach — such as the Italian Mafias, the Russian crime groups, the Nigerian enterprises, the Japanese Yakaso, and the Chinese triads — are developing new working relationships, cooperative arrangements, and networking with one another, with drug cartels, and with insurgent and terrorist organizations to take advantage of one another's strengths and to make inroads into previously denied regions. This has allowed terrorists a new means to raise money as well as provide them

with a marketplace to purchase sophisticated weaponry and other high tech equipment. This cooperation, for example, has long been seen among Colombian drug lords and Italian crime groups in exploiting the West European market, but now is seen in New York City and in Eastern Europe with drug and financial crime networks between Russian and Italian groups.

As organized crime groups become increasingly international in the scope of their activities, they are also less constrained by national boundaries. The new lowering of political and economic barriers allows them to establish new operational bases in commercial and banking centers around the globe. The willingness and capability of these groups to move into new areas and cooperate with local groups is unprecedented, magnifying the threats to stability and even governability, especially in weak or failed states.

Organized crime groups also pose a direct threat to DoD security and integrity. For example, organized crime's cooperative arrangements with other transnational threat groups can compromise DoD's efforts against drug traffickers and terrorists. They can target DoD personnel for access to technology, information, goods and materials for resale on the black market and for acquisition or high-value weapons.

The narcotrafficking industry today remains as resilient. It effectively adapts to interdiction and counternarcotics efforts by re-routing, changing the way it operates, and increasing production. This resiliency is due in large part by an unabated appetite of consumption. Indeed, more recent evidence portrays the rise of "narco-democracies", such as Mexico and Belize, characterized by political assassinations, intimidation of the judicial system, and the corruption of governments.

All of these transnational groups are becoming more professional criminals, both in their business and financial practices and in the application of technology. Many of them use state-of-the-art communications security (COMSEC) that is better than what some nation's security forces can crack. This includes sophisticated but easy to use encryption and steganography tools.

The proliferation of knowledge through the Internet goes well beyond COMSEC; there are a plethora of sites with significant information concerning high explosive, nuclear, radiological, chemical, and biological weaponry. Transnational groups and others can gain insights into technical issues regarding the construction and use of these weapons. Also, there are literally hundreds of computer network attack tools on the net that can be downloaded and used, in many instances, with "point and click" simplicity. There are also numerous sites which address vulnerabilities of government and private sector networks and suggest effect attack strategies and techniques.

A case in point has recently surfaced based on a report on the international threat posed by Russian organized crime issued by Washington's Center for Strategic and International Studies (CSIS) and in testimony by FBI Director Louis J. Freeh before the House Committee on International Relations

Director Freeh said that Russian organized crime networks pose a menace to U.S. national security and asserted that there is now greater danger of a nuclear attack by some outlaw group than there was by the Soviet Union during the Cold War. He said that U.S. law enforcement agencies take "very seriously" the possibility that nuclear weapons could fall into the hands of Russian criminal gangs and added, "We have to take drastic steps to prevent and detect that." Freeh said that about 30 Russian crime syndicates operate in the United States, trafficking in drugs, prostitution, fraud schemes and other illicit activities. While Freeh and others have warned

previously of the power of such crime networks in Russia, this was one of the first public acknowledgments that the groups have taken root in the United States.

Freeh said the Russian syndicates conduct the most sophisticated criminal operations ever seen in the United States, based on their access to expertise in computer technology, encryption techniques and money-laundering facilities that process hundreds of millions of dollars.

The CSIS report states that "Russian organized crime constitutes a direct threat to the national security interests of the United States by fostering instability in a nuclear power," and that, "Russian organized crime groups hold the uniquely dangerous opportunity to procure and traffic in nuclear materials."

The Challenge of Information Security and Infowar (IW)

While a number of excellent studies — both classified and unclassified — have been produced on the information warfare threat, the panel has found much pulp journalism and hyperbole attendant to this subject. That the National Information Infrastructure (NII) and its Defense Information Infrastructure (DII) subset is vulnerable to IW attack is unarguable. Last year's Defense Science Board Summer Study on Defensive Infowar points this out well, as does a newly-produced National Intelligence Estimate. The challenge comes in providing context and a proper appreciation of the nature of the vulnerabilities and the extent of the threat.

Vulnerabilities within Infrastructures

Traditionally, the information warfare threat has been associated with the telecommunications infrastructure and the ability to communicate. This remains a primary area of concern. But the government (especially the Department of Defense) is also growing more and more dependent upon the commercial power, transportation, energy, and finance communities, and these communities are also vulnerable to attack. All of these major national infrastructures share a common dependency on computer driven management and control systems. With the passage of time, technical and economic imperatives have driven these infrastructures to more and more dependence on networked computer driven systems. Indeed, the complexity of the software involved in the "system-of-systems" that drive some of the major infrastructures has become a major concern in itself.

By virtue of this increasing dependence on networked computer driven systems, all of these infrastructures possess some degree of vulnerability to infowar attack. The challenge is to define what are critical vulnerabilities versus day-to-day vulnerabilities with which the infrastructures are accustomed to dealing and which they manage quite well. The job of definition has not been accomplished.

Some of the critical infrastructures (e.g., the Public Switched Telephone Network (PSTN)) have been the subject of hacker attacks for years. A number of the major companies operating networks which comprise the PSTN have very robust programs to defeat toll fraud and ensure network continuity. Others have placed less emphasis on this problem and, while a structure exists to facilitate cooperation among the various companies, the level and quality of the cooperation is mixed. There are other infrastructures where not a great deal of attention appears to have been dedicated to this issue at all.

No meaningful, comprehensive analysis of the vulnerability of the various critical infrastructures has been accomplished and, until such an assessment takes place, it will not be possible to

portray accurately the potential transnational infowar threat. For purposes of this Summer Study, it can only be observed that vulnerabilities exist, they are imperfectly understood and are being addressed in an uneven fashion by industry and the government, and that this presents transnational groups with an opportunity to conduct infowar attacks. These attacks would clearly be disruptive, but it is not yet possible to assess the degree of disruption they are able to cause or its impact upon the Department of Defense. The President's Commission on Critical Infrastructure Protection, which is due to report in October, should provide the first piece of analysis in this regard.

Vulnerability — Foreign Made Components

Economic considerations have driven more manufacturing of information technology (IT) components off-shore. Many computers are manufactured and assembled entirely off-shore. Others may be assembled in the United States, but include components originating off-shore. An increasing amount of software code design and writing is being accomplished abroad and a significant number of pre-programmed chips are designed and programmed in foreign countries with no U.S. personnel having total access to the design architecture or the code.

Modern electronic telephone switches and other telecommunications devices have computers at their heart and thus have the same dependency on foreign manufactured and/or programmed components.

Firewalls are computer-driven devices designed to protect networks from unauthorized intrusion. Not only do these devices share the same vulnerability to foreign manufactured components, but the largest selling firewall in the United States is foreign made and the software which drives it is completely proprietary.

This dependency on components and pre-programmed chips — devices which may originate in foreign nations whose identity is not even known to the purchaser — creates a vulnerability to hidden software "trap doors," software programs that are susceptible to external manipulation, or hidden information "time bombs" in the form of code designed to cause a certain event to happen at a certain pre-programmed time. It would appear that, while this situation is understood in a very general sense, there has been very little real focus on the vulnerability it presents.

FACTORS INFLUENCING THE FUTURE

Global Stresses

A number of global stresses in the 21st Century will impact directly on the range and scope of transnational threats. Population growth — over 1 billion worldwide, 95% in developing countries — increase demands on infrastructures, water, energy and select territories. Global economic growth of 80% will continue to spur disparity between the "haves" and the "have-nots" because the growth is predicted to be uneven on a regional, national, ethnic and social status basis. Occasional "failed states" will fuel domestic disorder, mass cross-border migration, and mass humanitarian needs. Some nations will face diminishing authority and influence as a result of global information trends.

21st Century Threat Environment

Our description of the transnational threat is based on several important assumptions — assumptions that the intelligence community, through its publication, "Future Visions 2010,"

also made. First, we believe the continued globalization of the economy, information, and technology will provide significant new opportunities for those seeking to terrorize or intimidate. This is because the interdependencies created by such networking provide a broader base for greater destruction, especially in the areas of infowar. Concurrently, these very trends may also provide new and better means of tracking, capturing, preventing or deterring these same bad actors. We also assume our own growing dependency on computer-driven systems in government, within industry, and throughout the Nation's infrastructures of oil and gas, finance, communications, power, and transportation.

Second, there will be no consequential direct military threat to the U.S. or her allies, and U.S. nonmilitary objectives increasingly will shape military operations. Many nation states and groups will seek to find an asymmetric response to perceived U.S. military dominance since they will have no match to U.S. conventional forces. The most plausible areas for exploration for them would seem to be subversion, insurgency, terrorism, and the production or acquisition of weapons of mass destruction, coupled tightly with deniable covert action.

21st Century Global Role of the U.S.

We also assume that U.S. presence, policies and leadership will remain a major stabilizing force in the world, which will require a range of credible offensive military capabilities, forward military presence and surge capabilities, and independent and coalition operations. In short, the U.S., as the sole remaining superpower, will continue to maintain its role as world policeman, and be involved in situations that do not directly threaten U.S. interests, such as Bosnia.

Moreover, we can assume that the U.S. support of certain nations such as Israel whose very existence some Palestinian or other Arab groups oppose will continue to fuel export of extremism to other regions of the globe.

Major theater warfare differs both in character and consequences, but do not differ substantially in the seriousness of the problem, as the chart below depicts.

Major Theater War	Major Transnational Terror Action
▪ Imminence of action normally detected and degree of response underway, if not prior, at least by commencement of hostilities ▪ Vital US interest at stake which results in direct US intervention ▪ Nation committed to war with another State ▪ Purpose of commitment clear in public's eyes and usually widely supported ▪ Unlikely that US soil attacked; troop casualties normally explainable and tolerated ▪ Military campaigns usually contained and lead to a decisive conclusion ▪ Coalition partners often join due to coincidence of interests	▪ TNT actions have potentially low signatures; often a total surprise to leadership and casualties ▪ Significant US casualties lost and/or vital US capability destroyed ▪ Nation may not have a target to attack; possibly seen as impotent ▪ Purpose of attack may be unclear and difficult to explain ▪ Risk of TNT attack on US soil both likely and easily carried out ▪ Unanswered TNT actions may lead to additional "copycat" actions by other TNT groups ▪ Reluctance for other nations to become directly involved; seen as internal matter or cost of involvement seen as too risky (becoming TNT target also) ▪ Success of persistent or pervasive TNT actions likely to necessitate restrictions to democratic freedom and individual liberties.

A credible future global model depicts an environment that will require an activist foreign policy in order to sustain world stability, continuing foreign presence, and occasional military interventions in areas of conflict. This same model exacerbates stresses that traditionally motivate transnational threats. Thus, the transnational threat to the United States and her citizenry will become more significant over time, and soon may be considered as important a mobilization issue as conventional warfighting. As some governments struggle with unchecked population, transmigrations across borders, domestic disorder, and failed state services, they may lose their capacity to govern effectively, allowing criminal groups and radical extremists to gain influence and control.

At the same time, U.S. military operations will be subject to a growing list of vulnerabilities. All phases of combat operations, mobilization, logistics, command and control, engagement, and cleanup will be more and more dependent on digital communication and information systems, and thus susceptible to information operations. There will be fewer logistic sea and air points of departures and delivery in support of major military operations, which make the departure points more attractive targets for WMD attacks. Most future operations will be urban operations and require contact with host populations — conditions at odds with preferred force protection practices.

CONCLUSIONS ABOUT TRANSNATIONAL THREAT TRENDS

A review of the survey of motivations and trends of the major international terrorist groups and various other studies lead us to draw a number of conclusions.

The transnational threat problem is a product of our times. It is different and more dangerous than ever before, due to:

- The proliferation of technologies and knowledge — the enablers
- The proliferation of world actors, which include nation states as well as terrorists, anti-government militia, narco-traffickers, and global crime groups
- U.S. military asymmetry denies other nation-states an overt attack against the U.S.
- The strong correlation between U.S. involvement in international conflicts and an increase in terrorist attacks against the U.S.
- The U.S. is no longer a sanctuary from massive violence
- Transnational actors have more dangerous motives — mass casualties and destruction are goals.

Moreover, the United States will remain a significant target for terrorists; almost half of all known international terrorist groups consider the enemy worthy of attack. Department of Defense personnel and property are likely to be a significant part of the total U.S. target, especially in areas of peacekeeping and humanitarian missions. Traditional modes of terrorism will remain, and the use of high explosives is still the overwhelming choice of tools for terrorists, because it does the job effectively, it can be relatively low cost, and can avoid the galvanizing issue of mass destruction for those groups who care about such things. This being said, however, the trend towards less numbers of incidents, but bigger bombs and higher lethality, appears here to stay.

The leading question of concern to many, certainly before the DSB Summer Study on Transnational Threats, is the probability of the adoption of weapons of mass destruction by terrorists. To intuitively forecast the eventual use is reasonable. The essence of terrorism is "unignorable" destruction. And weapons of mass destruction are unignorable when used.

It is significant that the precedent for the use of a WMD already has been established by the Aum sarin gas attack in the Tokyo subway on March 20, 1995. However, the distinction that the Aum group were not traditional terrorists but a spike cult group is not a "splitting hairs" distinction. The scope of the WMD threat, and the structure of effective response strategies, are much different if WMD become the preferred weapons of internationally supported and financed terrorist groups than just for isolated cult groups. The distinction involves motives (and thus, likelihood) and capabilities. It is not clear that the rule-the-world motive of the Aum group, along with their other irrationalities, transfers to the body of terrorist groups now on the scene. However, internationally financed and supported terrorist groups are capable of mounting a WMD attack of almost any kind.

In contrast to the fact of the Aum Shinrikiyo sarin attack, there is no conclusive intelligence[3] that indicates an interest in the procurement, development, and eventual use of a WMD of any known international terrorist group.[4] We note, however, that the same does not hold true for certain domestic militia-type groups, who have indicated such an interest. *A "reasonable person" would conclude, therefore, that the likelihood of "classic" terrorist organizations (extreme leftists, most radical Islamics, and ethnic separatists) resorting to WMD use is unlikely because such an act would delegitimize their continued existence.*

Such deterrence factors do not inhibit the "new" terrorist. Because their motivations differ from that of the traditional, the most likely perpetrators of a WMD attack against the U.S. will be loosely affiliated, transitory groups (the "new" terrorists), many of whom may attempt to punish or to seek revenge for a perceived injustice. Neither strategic nor tactical intelligence warning is likely if the perpetrators of a WMD attack fall into this category. Moreover, the U.S. will face increased difficulty in tracking and analyzing these groups due to the groups decreased desirability for attribution or publicity. Likewise, influencing these groups in any meaningful way will also be difficult.

If terrorists determine to inflict mass casualties, *will organized crime organizations provide terrorists with the weaponry of mass destruction* (if the terrorists do not demonstrate a nascent capability to do it on their own)? Some organized crime groups (the Russian groups come to mind) have already demonstrated a capability in the proliferation of weaponry short of mass destruction (such as ballistic missiles, launchers, etc.). Some groups clearly possess the knowledge, infrastructure, and funding necessary to acquire such weaponry, but whether any such groups would risk exposure and illegitimacy in this manner is not known. For the purposes of detection and prevention, *we must assume that the threshold is not inviolable due to the huge financial benefit that might be derived from such procurement, and the ruthless nature of some crime lords, especially if they believed the procurement could not be traced back to them.*

---

3 As noted elsewhere in this report, we should not be too sanguine about this lack of evidence. The information gaps within the Intelligence Community in this area are wide and deep.

4 A resurgence, for example, in leftist terrorism, with the scenario that a group alters their motives to where massive casualties has a rationale relative to their goals, is possible, but not very likely.

Despite whatever tool terrorists select, the fact of increasing cooperation between crime, narcotics and terrorist groups will provide terrorists with a new, more creative ways to raise money and a marketplace to shop for weaponry and high tech equipment.

Weapons of mass destruction are not the only highly destructive tool terrorists may use. As the government becomes more and more dependent upon commercial-off-the-shelf information technologies, products, and networks/infrastructure, it will become more vulnerable to the infowar threat. This vulnerability includes denial of service or data corruption that could result form malicious code inserted in software written abroad.

We have broken down the threat into that which is presented by professional foreign intelligence and military organizations and that which comes from what is loosely described as the "hacker community." In the first instance, there are several nations which are assessed to have a potential to do significant damage to the NII/DII, but the likelihood of these nations exercising this "war reserve" capability in peacetime is slight. However, in peacetime, these same nations are likely engaged in probing our systems, collecting intelligence, and testing our safeguards. Over time, additional countries, to include countries like Iran which have a tradition of supporting terrorism, will also acquire the capability. Thus, the threat from foreign government-supported organizations will increase from slight to moderate within five years.

In addition to foreign nations placing more emphasis on developing infowar capabilities, there is growing evidence that drug cartels and other transnational groups — to include some terrorist groups — have recognized the potential for infowar and are developing capabilities. In fact, some groups already target information infrastructures today for the purposes of collecting intelligence and have used physical attacks to disrupt service. Within the next five years, if they don't already possess them, it is highly likely that with the increasing availability of attack tools and information on the Internet and in other public media, some transnational groups will establish infowar attack capabilities.

The threat today from the "hacker community" is, in itself, little more than a nuisance threat in terms of doing significant long-term damage to the DII. But in terms of acting as a force multiplier for a terrorist attack (e.g. interruption or denial of early warning communications before an event or emergency response communications after an event), their impact could be significant. We believe that while it is possible that transnational groups will use infowar techniques to penetrate systems and collect data — to include targeting data — the most likely use of actual infowar attacks (e.g., interruption or denial of service) would be in conjunction with some other, more dramatic form of attack.

In any attack, the ability to recruit or pre-position an insider in part of the DII increases dramatically the ability of the attacker to gain access and cause mischief by being able to bypass firewalls, access passwords, and other safeguards. The recruitment of a systems administrator could have a potentially devastating impact. If transnational groups are able to place or recruit insiders, the potential for damaging attack — albeit of possible limited scope and duration — increases substantially.

Finally, we note that while we have no direct evidence of any of these organizations using attack techniques to disrupt or deny, neither can we conclusively state that they have not made such attempts. The number of detected attempts to penetrate networks is significant, and the ability to identify the perpetrator has been historically poor. Beyond this, Defense Department analysis

indicates that the number of penetration attempts which are detected and reported are only a very small percentage of the attempts undertaken.

Which Transnational Threat is More Likely? (Where do we put the money?)

All can agree that the nature of transnational threats travels largely in uncharted waters. However, the agreement ends there. Some believe that the most likely future scenario entails the use of a radiological weapon stolen or purchased from East European stockpiles. Others postulate that the "real" threat (the most likely high damage one) is the improvised use of chemical weaponry. Still others firmly defend the notion that the biological threat is the greatest, due to its high lethality, high casualty rate, relative ease of procurement or manufacture, and difficult detectability. Even within our own group, we would categorize the transnational threat differently. Some of us would argue that the threat of a large scale WMD threat is low, based upon the historical persistence of classic terrorism as effective, the notion that terrorism is not monolithic or static, and that group motives are widely diffused and always changing, and that one must cross the Rubicon in using WMD because it remains the ultimate terrorist weapon. Still others of us argue that the threat is at least moderate for much the same reasons.

It is all speculative. For that reason, while we would like to be helpful in determining where scarce dollars should be invested, the truth is the proclamation or mathematical formulation of one favored method of terrorism over another is probably a disservice. If history teaches nothing, it is that we are forever wrong about our assumptions. For example, the threat prediction of chemical weaponry use before Tokyo was considered low. The threat calculation of the likelihood of a massive high explosive attack in one of our major cities was low. The threat analysis of a domestic terrorist group inflicting mass casualties through the use of high explosives in America's heartland was considered remote. What is true, is that given any given set of circumstances, actors, and political environment, one form of attack is as likely as the next. We have tried to draw trend lines in terms of motivations and capabilities and therefore illuminate the field. But not one of us can tell you the final score.

As a nation, it is prudent to seed adequately all areas of the transnational threat by taking the "reasonable" person approach, and view the threats in totality. Like so many other facets of life, taking a risk management approach to the problem by weighing the specific threat against the likely consequences, and calculating the acceptable level of vulnerability and cost, will better enable us to face the changing landscape.

THE GAPS

Threat information about the transnational problem can best be characterized by "we don't know what we don't know." To begin with, the intelligence community does not have wide or deep coverage of most terrorists. In fact, when asked about the level of coverage, the intelligence community offered only one group — the Hizballah — as receiving a high degree of coverage among the forty four known international terrorist organizations on the State Department's list. A similar lack of coverage is prevalent in the domestic arena as well. In fact, some loosely affiliated groups or cults receive no coverage at all. This lack of coverage is not due to a lack of interest, but rather, it is attributed to a variety of factors that relate to managerial decision making, lack of resources, the "hardness" of the target, and legal constraints imposed upon the domestic law enforcement agencies. Consequently, the Nation's national security apparatus may

not receive strategic warning of an incident, and even if it did, specific tactical warning may not exist.

A second major gap in harnessing the intelligence community's resources devoted to the transnational threat lies in the organization and communications support inherent in its stovepiped structure. For example, the Director of Central Intelligence, Centers for Nonproliferation, Terrorism, Narcotics, and Counterintelligence reside in different administrative organizations, have their own communications channels, career paths, incentives, training, and set of customers. While terrorists, crime groups, proliferators, and drug cartels are learning to cooperate with one another for their own mutual benefit, the functional and regional offices within the U.S. Government devoted to tracking these disparate groups lack the means (and sometimes the will) to share information of mutual interest.

In the area of cyberwar, the axiom of "we don't know what we don't know" is particularly appropriate. Since we have an incomplete understanding of the vulnerability of the critical infrastructures upon which the Department of Defense depends to carry out its missions, we have only anecdotal information; a rigorous program to detect, analyze, and counter IW attacks on the government infrastructure does not yet exist. Closely allied to this problem, our understanding of foreign government intentions, activities, methods, capabilities and programs (which could be made to transnational groups) is still very limited.

There has been increasing attention to this problem in the government in general and in the Defense Department in particular, but nonetheless, DoD remains poorly organized or equipped to confront the problem successfully. Organizational responsibilities for the defensive aspects of IW are poorly defined. In some cases, programs overlap; in other cases, there appear to be few if any programs at all. Policy is ambiguous and strong leadership is lacking. In general, the DoD and other government programs designed to address this problem appear to have low priority and are poorly funded and staffed.

It is the American character to believe we can solve all problems with our ingenuity and hard work. But even if the intelligence community were given the means to correct these gaps, there still would remain a significant portion of terrorist planning, preparation and incidents that would surprise. Just as better defenses have turned some terrorists away from harder targets, the amorphous nature of the "new" terrorism, combined with the uncertainty inherent in predictive analysis of chaotic behaviors, means that some events would remain unforeseen. If one accepts the premise that motivations guide pattern analysis, one must also accept the fact that often, motivations are not determined, if at all, until after the fact.

ANNEX:

Charts and Scenarios

The purpose of these charts and scenarios is to illustrate the importance of the problems, establish needs and requirements, assess current capabilities or enhancements, and train and exercise response units.

CHART 1

Chart 1 represents a hypothetical scenario version of the hoax anthrax attack on the B'nai B'rith Center in Washington. The scenario assumes that the planted device was an aerosol can containing 150g of anthrax.

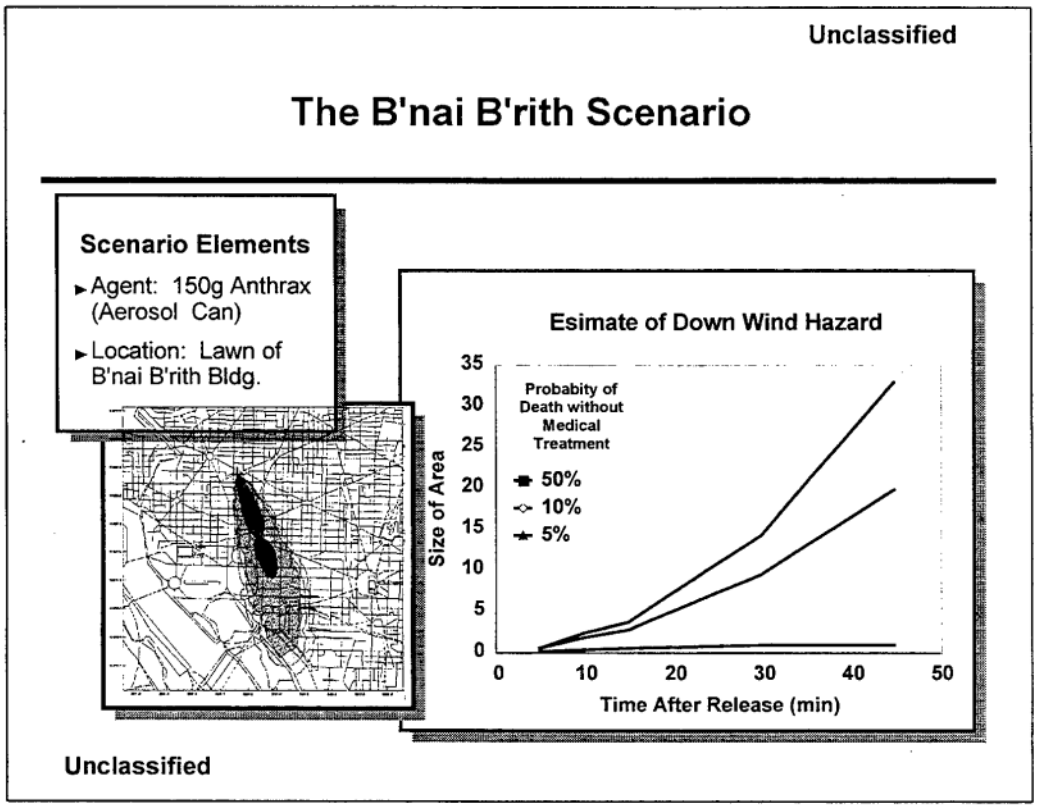


Chart 1

- The dispersion model represents three zones: the inner zone is the area were the consequence would be 50% probability of death without timely medical treatment; the death rate of the next zone would be 10%; and in the outer zone, 5%.
- The three curves represent the are cover as a function of time.
- Accounting for the daytime population of the area covered, after one hour the net consequence of this conceivable WMD attack would be many thousand of fatalities.

CHART 2

Chart 2, represents a thermometer and measures actual events and casualties against the attack if weapons of mass destruction were used.

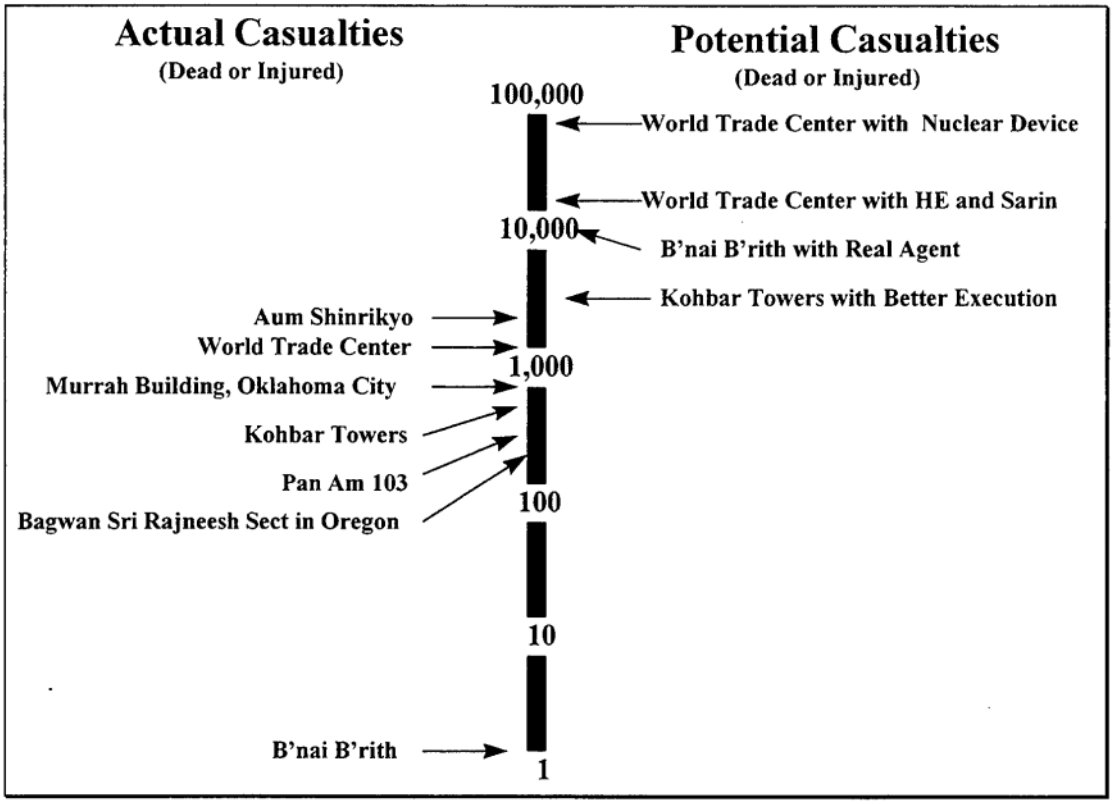


Chart 2

Illustrative Scenario #1:
Subway Attacks in NYC and DC

- Context
  - Middle East group seeks revenge for imprisonment of terrorists in US
  - Sympathizers recruited at NY and DC transit authorities and at Bell Atlantic
- Summary
  - Coordinated explosion and release of sarin in several stations in DC and one station in NY
  - Ventilation system in subways shut down by insiders
  - 911 service interrupted by Bell Atlantic insiders

It is mid-summer 1998 and Washington DC and New York City are enjoying a hot spell. The time of day is afternoon rush hour.

A middle east sponsored terrorist group has long been planning revenge for the arrest and imprisonment of Islamic terrorists in the United States. They have recruited a sympathetic employee in both the New York City subway and the Washington Metro system

and have placed a similar sympathizer in a Washington DC Bell Atlantic Central Office. They communicate among themselves and coordinate their operations over the Internet so as to avoid potential law enforcement wiretaps. Posing as stamp collectors, they pass images of stamp images to one another. Hidden in the images, using the S-Tools steganography tool, are files concerning the detailed planning for the operation. During their initial planning they mutually agreed to use S-Tools and the triple DES encryption algorithm option. The pass phrase they selected to hide and reveal the files, INFIDEL, is the name of their operation.

They have obtained the precursors required to manufacture sarin and have manufactured sarin — filled explosive devices with timers. They provide one of these each to five terrorists, two of whom go to the Metro Center subway station and the third to the Gallery Place station in Washington DC. The fourth goes to the Pentagon station. The fifth is dispatched to New York City. In Washington, the terrorist who goes to the Metro Center boards a blue or orange line train, places his explosive device, and sets the timer as he leaves the train at Mc Pherson Square so that the device will detonate shortly after departing the station, but before it arrives at International Square. The second (Gallery Place) does a similar thing on the Yellow/Green line, getting off at The Archives and setting the device to go off before L'Enfant Plaza. The third (also Gallery Place) boards the Red line, gets off at Metro Center, setting the timer to go off before or at Farragut North. Each carries a cellular phone (stolen) and immediately calls the beepers being worn by the Metro and Bell Atlantic insiders. As soon as he gets four beeps, the Metro employee shuts down both the switching system (and its attendant electronic display) and the tunnel ventilation system by introducing destructive code into the master computer system. The telephone employee simultaneously shuts down the trunk serving the 911 inbound service.

At the same time, the New York City terrorist boards the downtown-bound "A" train at 145th St., gets off at 125th St. and sets his device to detonate in the tunnel between 125th St. and 59th St. He then "beeps" his contact who similarly shuts down the train display and ventilation systems.

Simultaneously, a similar bomb has been planted in the Pentagon station. The bombs go off in all four subway trains and at the Pentagon station. The Washington DC trains are either at, or close to, the three stations that are nearest the White House and major concentrations of Federal employees. The New York City train is in one of the longest tunnels in the system. Both the trains and the tunnels quickly fill with gas, as does the Pentagon station (which is deep under ground), and there is no ventilation system to dissipate the gas. Washington DC police near the scene are able to radio back reports the panic that ensues, but survivors/escapees are unable to reach the police or Fire Departments using 911. Washington Metro and New York subway authorities receive widespread reports of gas in the subway system, but are not able to locate where their trains are because their electronic display system is down. People are streaming out of six or eight stations in Washington DC and a number of stations and emergency entrances in New York City. Emergency vehicles are ultimately dispatched, but they must be dispatched to all the reported locations, which both dilutes their effectiveness and totally shuts down vehicle traffic in downtown Washington DC and mid-town New York. At this point, the TV cameras have arrived and are filming very sick and ultimately a number of dead people. Emergency workers are also being overcome after working long periods of time in unventilated areas.

At this juncture, an anonymous phonecall claims credit for the bombing, stating that, in addition to introducing deadly chemicals into the subway tunnels, it was they who shut down the 911 system in Washington DC and the metro/subway switching systems and they could do this at will to other public transport or public utilities. They also claim that they have spiked the sarin bombs with a deadly biological substance such that anyone in the area—specifically to include emergency workers—would be carrying deadly disease. Panic ensues, with authorities conducting testing to determine what agents might be involved but, in the meantime, holding everyone in a confined area. (Note: You could modify the scenario to include a biological agent really being introduced). Mayors Barry and Giulliani call on the Federal Government for immediate assistance. They request troops to maintain order and chemical decontamination equipment to cope with the chemical warfare (CW) agent. They also request immediate ambulance and mobile hospital support and support to determine the biological agent and neutralize it. At the same time, DoD authorities are trying to cope with the bomb at the Pentagon, and all identified emergency support equipment in the Washington DC area is committed. The traffic jams in both cities preclude the rapid arrival of additional support. Because of the CW agent in the air (and the prospect of biological warfare (BW) agents also being carried), the Secret Service immediately decides to evacuate the President and Vice President, and the TV cameras broadcast their departure by helicopter. Darkness is now setting in and both Washington DC are paralyzed. At the Pentagon, some emergency response planning is underway, but gas has seeped into the building and major portions have been evacuated.

Furthermore, a number of key people have already departed for the day and cannot return because of traffic tie-ups. Inbound telephone service is tied up intermittently due to the volume of calls being made by people seeking to learn the status of family members who work in the Pentagon. The Office of Secretary of Defense and the Joint Chiefs of Staff make plans to transfer command and control to Ft. Belvoir, but helicopters cannot land during the critical first hours of the crisis owing to the priority given to medivac missions.

Scenario #2.
Illustrative Scenario #2: Biological Agent Attack on the United States

- Summary
  - Middle East terrorists obtain a virulent biological agent stolen from a Russian laboratory
  - The agent is released in Los Angeles and the infection quickly assumes epidemic proportions, spreading to other California cities
  - Emergency services are rapidly overwhelmed, public order breaks down, and the Governor calls for Federal assistance

An FBI informant among the Russian émigré population in Brooklyn New York has reported that several months ago, his uncle, Igor Rubinovich Sedler, confided in source's father that he (Igor) would soon come into a large sum of money and would thereafter arrive either in the United States or Canada. Source knows his uncle to be a distinguished biologist working for the Russian Ministry of Defense in some sort of highly classified work.

Source queried his father as to how Uncle Igor would get this money and how he would be allowed to leave Russia, since he had always stated that his work was too critical to the Russian defense effort for him to be allowed to leave. The father said he did not know and that Uncle Igor was being very secretive about this, but he would ask him when he next telephoned.

Last week Igor telephoned and said that he would soon arrive in Canada, but that, sadly, he would not be able to get together with the family any time soon since he would have to lie low. Sources father thought at first that Igor was afraid that Russian authorities might search him out, but Igor made it clear that he was less concerned about Russian authorities than he was about US authorities, but that the family ought not be concerned because "the organization" would protect him. He was critical to them. The "organization" was clearly an allusion to Russian organized crime.

At the same time, a cooperating foreign intelligence organization reported to the FBI that it had reliable information that NORDEX, a well-known Russian mafia controlled corporation, had made arrangements to purchase from a scientist working at a top secret Russian BW installation a highly lethal biological warfare agent for which there was no known cure. NORDEX had a middle east buyer who was willing to pay a great deal of money for this agent for use in retaliation for "US State terrorism". The Russian scientist had already stolen the agent and was in the process of being smuggled out of Russia.

January 1998:

On Sunday, two Los Angeles (L.A.) "street people" are taken by ambulance to the emergency room of an L.A. hospital suffering from convulsions and coughing up blood. Both die soon after arrival, without being diagnosed. Their bodies are sent to the city morgue to await identification. The following day, a young professional woman is rushed from her office to the emergency room of another L.A. hospital suffering from the same symptoms. She too dies before any diagnosis can be performed, but her family insists upon an autopsy. Later that same day two additional cases with the same symptoms arrive at the second L.A. hospital and both die soon after arrival. By that evening there are a half-dozen similar cases at different L.A. hospitals, but none survives long enough for any real diagnosis. By the third day of the outbreak (Tuesday),

enough of these cases have been seen that they have aroused interest on the part of the admitting hospitals and autopsy work commences, but no firm diagnosis can be reached. The symptoms resemble several different maladies, but cannot be tied down to any particular one. Details are forwarded to the Center for Communicable Disease, and efforts to identify the disease intensify.

On day four (Wednesday), emergency room personnel from the first treating hospital are stricken with high fever, convulsions, coughing up blood, and general respiratory system failure. Dozens of cases are being reported by all L.A. area hospitals. Local television stations pick up the story and run it on the evening news. The next day (Thursday) local doctors and hospitals are reporting hundreds of patients with similar symptoms. Most die within 24 hours of reporting the symptoms. Efforts to identify the strain of disease intensify, but there is no firm diagnosis. By the end of day five (Friday), a number of police and ambulance personnel have reported sick. This too is reported by the evening news, and the beginnings of panic are evident. Emergency workers are failing to show up for work. Police and ambulance personnel are refusing to pick up people stricken with this disease. On Saturday, two hospitals are forced to close their emergency facilities due to the number of medical personnel reporting ill. The California Highway Patrol reports extraordinarily heavy traffic as people leave L.A. due to fear of this un-named disease.

On Sunday, record numbers of people are taken to L.A. hospitals, and the hospital staffs are totally incapable of coping with them. Appeals are made to for help from outlying hospitals, but help is slow to arrive. At the end of the day, the first cases of this disease are being reported as far away as San Diego. The Governor returns to town late in the day and declares a state of emergency, mobilizing selected units of the California National Guard both for law enforcement / public safety and to provide emergency medical support. He also petitions Washington for federal assistance.

On Monday (day 9) it is apparent that there is a full-scale epidemic in progress. Hospitals are overflowing and can accept no further patients. The disease has not been identified, but has been given a name and enough people have been treated and survived for there to be some limited data as to effective treatment. However, the epidemic has now made national TV, cases are being reported up and down the west coast, National Guard medical personnel are failing to report for duty and those deployed are requesting permission to return to their communities where they believe their primary medical responsibilities to lie. By the end of the day the number of cases reported is in the thousands and the fatality rate is in excess of 80%. The President declares a national state of emergency and, at the request of the Governor, sends US Army medical units and Military Police to California. He appeals to medical personnel throughout the nation to assist in California and establishes a US Air Force airlift to carry medical personnel to California.

On Tuesday (day 10) the disease has spread to so many California cities that a quarantine is imposed on traffic out of Los Angeles. At the same, San Francisco embargoes aircraft, trains, and buses coming from Los Angeles. Medical facilities in Los Angeles are in a complete state of breakdown, food shortages are being reported, and panic ensues, with rioting and looting reported throughout the area. The Governor declares martial law and appeals to the President for large-scale military deployments.

REPORT OF THE SCIENCE AND TECHNOLOGY PANEL

Panel Chairs
Dr. George Heilmeier
Dr. John Foster

Panel Members
Dr. Alan Berman
Dr. Greg Canavan
Dr. Robert S. Cooper
Prof. Delores M. Etter
Dr. Edward Gerry
Dr. Joshua Lederberg
Mr. Peter Marino
Mr. Walter Morrow
Gen Randy Randolph, USAF (Ret)
Dr. James Tegnelia
Mr. Vince Vitto

Government Advisors
Dr. Alfred Brandstein
Mr. Roy Cooper
Dr. Joseph Dollar
Dr. Matthew Ganz
Dr. Helmut Hellwig
Mr. Richard Hess
Dr. Jasper Lupo
Mr. Paul Pillar
Mr. Earl Rubright
Mr. Tom Tesch
Mr. Frank Wattenburger

INTRODUCTION

The Science and Technology (S&T) Panel examined the technology needs in the context of the overall counter-terrorist problem. The important components of this problem include:

- Gathering and analyzing intelligence data on likely terrorist groups prior to their initiating operations
- Detection of specific operations including weapons development, testing, and transportation
- Detection of transit of terrorists and their weapons through transportation portals and modes
- Tracking of terrorist movements within CONUS or near overseas U.S. garrisons
- Detection of deployment of weapons near targets such as high explosives, Biological Warfare/Chemical Warfare (BW/CW) agents, or nuclear devices
- Protective measures for garrison forces or civil targets
- Remedial measures after a successful terrorist operation

In the context of these needs, the S & T Panel focused on new technical means that could improve the effectiveness of the counter-terrorist program. While focused on this object, the S & T Panel discussed a number of on-going S & T programs that have the potential to contribute. Some of the more important contributions are identified in the next section.

IMPORTANT ONGOING S&T PROGRAMS

There are a number of ongoing S&T programs that are very important to the problem of countering transnational terrorists. Some of the more important of these programs are listed below. These programs will not be explicitly discussed in this report. Our only concern is that these programs must be output oriented rather than slip into an institutionalized program mode.

Tactical Communications Intelligence (COMINT). Terrorist communications can be intercepted by a variety of technologies. Intercepts can be made of wireless phone transmissions, trunk radio and communication satellite circuits and even fiber optic circuits. It is very important to develop this capability as part of an organic system for regional commands.

High Explosive Detection. Federal Aviation Administration (FAA) S&T programs are developing a number of technologies for portal detection of high explosives in amount as small as one pound. X-ray tomography, neutron activation and electro magnet technologies are being explored along with others. The focus of these efforts is on baggage and passenger screening. Currently, there is little or no focus on large area search for high explosives or even on search for high explosives in larger quantities in vans, trucks and containers. The FAA sponsored high explosive detection technology should be applicable to detection of larger quantities although it is likely that the detection ranges will be limited.

Trace Biological / Chemical Detection. Defense Advanced Research Projects Agency (DARPA) programs are underway to emulate the performance of dog's noses that have proven to be more sensitive that any other detection of trace signatures. Unfortunately, dogs remain effective for only short periods on the order of 30 minutes. It is hoped that with an array of biological based detectors responding to different trace signatures combined with sophisticated electronic recognition systems, it may be possible to develop very sensitive trace detection systems for portal applications which could identify individuals that have been exposed to high explosives, chemical and biological agents and nuclear materials.

Vaccines and Biocides. DARPA has undertaken an important program to develop improved vaccines to counter exposure to biological agents. In addition, this program is exploring improved treatments for unvaccinated individuals that may have been exposed to BW agents. This effort is clearly important for both military and civil applications.

Content Based Search Systems. Research efforts are underway to develop semantic understanding systems which can search large data bases for pertinent information without large numbers of false responses such as is the case with current keyword search systems. This new search technology needs to be applied to the extensive intelligence databases in order to increase the efficiency of searches for information on terrorists.

Baysian Recognition Systems. A wide variety of Baysian recognition systems including adaptive neural networks have been the focus of research on automatic target recognition and speech recognition communities. These technologies should be applied to the processing of intelligence and sensor data in order to improve the probability of terrorist detection and also to minimize the generation of false alarms.

High Altitude Unmanned Aerial Vehicles (UAVs). Electro-optical and synthetic aperture radar sensors carried by the high altitude UAVs are the current focus of a DARPA/Defense Airborne

Reconnaissance Office (DARO) program. These systems offer the possibility of surveillance of both suspected terrorist training camps as well as terrorist approaches to garrisoned U.S. forces.

Acoustic and High Power Microwave Disruption of Terrorists. A variety of non-lethal technologies are being explored by the Services that should be useful in attacking terrorist groups or for rescuing hostages. There are several high power microwave technologies that are directly applicable, e.g. the disruption of all electronic communications equipment. Aside from high power acoustic and microwave energy, various forms of sticky foam, high-density fogs, and incapacitating sprays (such as pepper) should be applicable to counter terrorist operations.

Defense Against Information Warfare. A variety of techniques are under development at DARPA and elsewhere aimed at countering terrorist attacks on information systems both civil and military. These techniques generally employ various types of barriers and firewalls to detect unauthorized entry. In the event of successful penetrations, various types of detection systems are under development to permit isolation of the attack. The potential vulnerability of individual system administrators to coercion or corruption cannot be eliminated completely. Nevertheless, damage can be mitigated if no individual system administrator has complete knowledge of the logic of the defensive measures that are in place, and if these measures are changed often on a routine basis so that the value of an administrator's information will attenuate rapidly with time. Such administrative actions would at least constitute an effective form of damage limitation.

Aircraft Self Protection. A variety of microwave and laser-based technologies to counter surface-to-air threats are being developed for large aircraft. These advanced technologies are needed to protect the larger troop and cargo carrying aircraft landing in areas vulnerable to terrorists with readily available shoulder-launched surface-to-air missiles.

FOCUS ON "SILVER BULLETS"

Within the overarching themes of Intelligence Information Collection/Management and Garrison Force Protection, the goal of the S & T Panel was to find a few "silver bullets" that enable important new capabilities. These "silver bullets" were analyzed using the following set of questions:

- What are we trying to do?
- How is it done now?
- What are the limitations?
- What is the new approach?
- Why will it be successful?
- If successful, what is the payoff?

The following sections address seven possible silver bullets using this framework.

4A. INTELLIGENCE ON TERRORIST IDENTITIES, CAPABILITIES, AND INTENT (INFORMATION PROCESSING)

Background

The objective of US intelligence operations that are directed against transnational threats is to discover the identities, capabilities, intentions and plans, of foreign and domestic threat groups. Good intelligence is the first line of defense against attacks both overseas and domestic, and it is a prerequisite for effective defensive measures, for proactive responses, and for longer-term programs designed to weaken threat groups and to impede their ability to organize, recruit, plan, and seek external support.

Terrorists are a very difficult intelligence target. Typically, terrorist acts are carried out by small cells that are highly secretive, well disciplined, conscious of operational security, and ruthless toward anyone suspected of betrayal. Consequently terrorist cells are very difficult to penetrate. Terrorists move easily among — and are not readily distinguishable from — much larger populations of non-terrorists with whom they may share ethnic or other characteristics. Furthermore, terrorists — between and within groups — often differ in ideology, ethnicity, and personality.

The panel believes that existing processes for managing intelligence information are out of balance. Currently the priorities for intelligence collection, the capability for multiple organizations to access needed clues and data in other organization's data bases, and the rule sets and techniques used by analysts to identify real or potential terrorists, needs to be refocused so that transnational threats may be addressed more effectively.

Automated capabilities to correlate, to integrate, and to analyze the material in disparate data sets are rarely available to intelligence analysts. If progress is to be made against the threat of transnational terrorism, analysts must be provided with improved tools to enhance teamwork, cooperation, information sharing, and collaboration within, and between, the many agencies that are focusing on the transnational threat problem. Employing these techniques will improve the over-all US ability to counter transnational threats.

A multiplicity of agencies share the mission of collecting and analyzing intelligence information related to transnational terrorism. These include foreign intelligence agencies such as CIA, DIA, and NSA, as well as local, state and federal law enforcement agencies including the FBI, the INS, the Secret Service, and the Customs Service. Relevant information is collected or used by over 10,000 federal, state, and local law enforcement authorities. Overlapping jurisdictions are thus a fact of life. Unfortunately, inter-agency sharing of data stored in the databases of these many agencies is not accomplished on a routine basis.

The objective of any system for handling and processing transnational threat information must be to achieve a high probability of detecting terrorist activity while triggering only a minimal number of false alarms. The aim, in other words, is accurate and efficient separation of valid threat information from information that does not reflect actual threat operations.

What are we trying to do?

The panel suggests, that the application of evolving techniques that already are employed widely in the industrial sector for searching, merging, sorting and correlating data in multiple independent data bases, can be applied to the transnational terrorist problem to provide intelligence analysts with more effective tools than are now available to help them discover the identities, capabilities, intentions and plans, of foreign and domestic threat groups.

Using these new techniques, once a suspected terrorist operation has been detected, an advanced set of relatively covert micro-sensors can be deployed to provide more precise and detailed information concerning current terrorist locations and actions.

How is it done now?

Currently the processing of counter-terrorist information is heavily dependent on name tracing. Basically, this is a process that relies on searching archived reports and databases for prior mention of the names of individuals or groups that have appeared in a new report. Another commonly used technique is called link analysis. Analysts use link analysis to attempt to identify connections (telephone calls, face-to-face contacts, or other ties) that may indicate terrorist planning, preparation, recruitment, or support activities.

These and other techniques are employed to identify patterns in the operations of particular terrorist groups. Analysts seek to determine the methods, area of operations, and preferred targets of a given group. Much of this work necessarily looks backward to past terrorist incidents rather than forward to possible future attacks. With available analysis tools it is more feasible for analysts to sort and sift information relevant to a known, prior attack than to determine the relevance of information to a possible future event.

What are the limitations?

The effectiveness of current approaches is limited by many factors. Current intelligence gathering techniques do not take adequate advantage of extensive open source data bases that can greatly add to the volume of information on transnational threats. There is an enormous quantity of information in databases that are available worldwide. Predominantly, the information contained in these databases is not relevant to the task of the counter-terrorist analyst. However, there are sometimes a few pieces of valuable intelligence or clues in such data bases (e.g. Mr. "W", a graduate of "XYZ" University, where he majored in organic chemistry and biology, is the nephew of Mr. "U" who was picked by US police for illegally raising money for a known terrorist organization. Mr. "W" has requested a visa to travel to the US without his family.)

The challenge facing an intelligence analyst is not just to find a needle-in-a-haystack, but to find the correct needle-in-a-haystack. Search methods currently in use, which primarily are keyword-based, are not always up to this challenge. An exacerbating factor is the propensity of security-conscious threat groups to use code words in their communications to disguise the content.

Information that might be processed for indications and warnings of terrorist activities is divided among a large number of disparate, isolated databases. Most of these databases are agency-specific and/or task-specific, and they serve certain individual agency purposes well. However, there is no requirement for any agency to enter all relevant information, (modus operandi etc.),

that would be of use to other interested organizations. In some cases, isolating databases also serves legitimate security-related needs to sensitive compartmented information. Unfortunately, many databases are isolated, based strictly on ownership. The current arrangement does not permit search across databases, or the easy and routine correlation and integration of related information from different databases. The fragmentation of information within the US is mirrored by a similar separation of US data from foreign data. Except for a few special-purpose projects with allies cooperation does not extend to the management of joint databases.

There are also the issues of collection priorities, the rule sets that guide individual analysts to their conclusion, in addition to the fact that generally an analyst can only review the ensemble of data bases that are available to members of the analyst's own agency. We believe that the analyst paradigm needs to change if we are going to make use of essentially all of the available information. Today the analyst paradigm is one that is focused on the work of the individual analyst with tools focused on individual task automation.

The problem of developing an effective counter-transnational terrorism database is similar to the problem of developing a national anti-crime database. In both cases, data must be collected, patterns of operation must be detected, and associations and motivations need to be identified. Although the US does not have a national crime information database, countries such as Australia, the United Kingdom and New Zealand do have national anti-crime information systems. Their systems are derived from US technology and they are employed very effectively. In many respects, these national anti-crime databases already have in operation some of the tools and attributes that would be desirable for a national counter-transnational database. In effect, these anti-crime databases provide an existence theorem that it should be possible, using an extension of existing tools and techniques to build the necessary database to counter transnational terrorism more effectively.

The panel also believes that the information management capabilities of national intelligence organizations that are responsible for the provision of indications and warnings of terrorist actions are lagging behind the evolving capabilities of commercial organizations that are addressing the issues associated with the:

- Need for an overall information architecture,
- Elimination of "stovepiped" data bases,
- Application of rule-based systems for filtering, analysis and correlation of data
- Development of tools for collaborative activity (such as groupware for analysts),
- Development of processes for migration (cutover) to new systems.

What is the new approach?

The recommended new approach would be to develop processes that foster analyst teamwork, cooperation and collaboration through the automation of the analysis process wherever appropriate and the development of technology for the search of heterogeneous distributed databases.

There needs to be a move to groupware for analysts and away from tools that are only designed to automate the task of the individual. Such a system would make use of modern object-oriented

database technology to handle multiple representations of data. It would also make the maximum possible use of modern data farming and mining and warehousing techniques that will facilitate development of search and recognition techniques, including those that employ context and content base search (latent semantic indexing).

The panel feels that there is a significant and important contribution that can be made by intelligent software agents. One can define a very specific role for intelligent software agents that might be one that focuses on pursuing the search for confluence of events in multiple databases or pursuing goals over time. There is also a role for profile filters to identify recent activities and interests of threat organizations.

Of equal importance to the gathering and identification of essential data is the development of tools to correlate all-source information that will include both government and civil sector databases.

Why will it be successful?

This approach promises success in two ways. First, commonality will facilitate the integration of data from disparate sources — the making of connections between otherwise meaningless bits of information that is at the core of threat analysis. Second, the application of the most advanced search technology will make it more feasible to find the relevant needles of threat-related information amid the haystacks of extraneous reporting. This approach will be successful because techniques do exist in the commercial world for searching disparate databases and object-oriented databases are being developed.

If successful, what is the pay off?

The main payoff will be an increase in the probability of before the fact detection of terrorist operations, along with a reduction in false alarms. An added payoff will be a reduction in the number of personnel needed to process information, or at least avoidance of the need to greatly increase that number to do a truly comprehension job of monitoring terrorist threats. Analysts within the Intelligence Community already exhibit great skill and diligence in assessing, manipulating, linking, and exploiting the threat information that comes to them. Greater use of modern information processing technology is needed to perform these functions on a scale, and with the thoroughness, needed to meet US interests regarding transnational threats.

An additional benefit that will accrue from the use of improved software search and correlation tools, and the concomitant improvements in indication and warnings of impending transnational terrorist actions they will provide, is that better instantaneous localization is also likely to be achieved. This in turn will mean that a new generation of advanced covert high performance intelligence sensors can be precisely and effectively targeted.

4B. INTELLIGENCE ON TERRORIST IDENTITIES, CAPABILITIES, AND INTENT (INTELLIGENCE SENSORS)

What Are We Trying to do?

The panel suggests that the application of evolving technologies will permit the development and deployment of a broad new family of relatively covert sensors. If on the basis of the improved information processing tools discussed in the proceeding paragraphs suspected terrorist locations can be identified these sensors can be used to refine our understanding of the terrorists plans and intentions.

The objective of improved intelligence sensors we are proposing is to enhance our capability for covertly gathering data on suspected terrorist cells so that the probability of detection can be improved along with a reduction in false alarms.

How is it Done Now?

Currently, the primary source of data on terrorist organizations and their operations involves the use of signal intelligence (SIGINT), open source information such as newspapers, embassy reports and a very limited set of human agent reports (HUMINT).

In addition, overhead imaging data provides some limited amount of information on terrorist training sites. Finally, limited data is also available from short range measurement intelligence (MASINT) sensors that provide limited capabilities to detect various chemical, biological, and nuclear effluents at standoff distances.

What are the Limitations?

As pointed out above, because of the very high security consciousness of terrorist groups, generally, there is very little, if any, information that can be derived from within terrorist groups. Moreover, terrorist groups often come from countries in which the US has no HUMINT capabilities. As a result, little cueing information is available for placement of short range intelligence sensors capable of gathering electro-optic (EO), infrared (IR), acoustic, and mass destruction weapon, diagnostic data.

In particular, current MASINT sensors have next to no capability to detect and identify biological warfare agent production, testing, and transport

What are the New Approaches?

A review of evolving sensor and robotic technology has lead the panel to believe that significant advancement can be achieved in the areas of:

- Micro-Robots
- Bio-Marker Trace Detection

Micro - Robots for the deployment of Covert Sensors

A number of very small miniature sensors capable of obtaining EO, IR, acoustic, and trace effluent data either have been or are under development. The current means for deploying such sensors is severely limited because of the scarcity of human agents available for their deployment and because of the danger involved. Micro robots, both earth traversing and airborne (in the form of micro UAVs) have been proposed for covert deployment of micro-sensors. These sensors are covert in the sense that they are quite small and have a high probability of escaping notice. They can be camouflaged to appear as an insect, a small pebble, a stick, etc. Techniques are under development to provide relatively covert communications back to a monitoring station. Among the techniques being considered for this purpose is the use of optical fibers less than 10 microns in diameter.

Bio-Marker Trace Detection

When human beings work with certain materials or have been exposed extensively to a unique environment their bodies develop specific antigens to these environmental effects. Consequently, if terrorists have had extensive exposure to specific chemical, biological, high explosive, or nuclear materials and/or they have had extended stays in, and exposure to the unique spores in specific target areas, their bodies will acquire specific antigens which generally are not present in the bodies of the general population. In effect the antigens constitute 'bio-markers' which in coordination with other information can be used to identify terrorists. The best means of identifying these antigens would of course be via blood samples. If, as is likely, it is infeasible to obtain a blood sample from a person not in custody or charged with a crime, then other means will be required to obtain a sample for antigen analysis. As future technology is improved, antigens might then be detected at national entry portals as trace contamination on emigration documents or as passports, urine analysis or by other means. With improved detection sensitivities as exemplified by the DARPA program to develop an artificial "dog's nose," it should be possible to identify some potential terrorists by the antigens they carry.

Supporting Technology

Micro Robots

A wide variety of miniature (10-20 centimeters) robots have been or are under development. These devices are capable of both ground locomotion and air vehicle operation. The current designs tend to use the smallest commercially available components such as motors, relays, sensors, etc. The development of MEMS (micro electronic-mechanical systems) components is now underway as a DARPA program. This effort should provide the next generation of very small components including gas turbine power plants, actuators, etc.

Using these smaller components, it should be possible to produce micro robots approaching 1 centimeter in size and air vehicles of perhaps 5 centimeters wingspan. Micro-robots may be a way of covertly deploying sensors and their communication links. The deployment of a 10 micron diameter fiber by a micro-robot would provide a communication link that is essentially invisible.

The main limitation of current design is energy storage and replenishment. With energy limited designs, once deployed, a micro robot would not move any further. A number of approaches are under consideration for allowing micro-robots to scavenge energy from the environment and to store this energy for future mission use. As an example, a micro robot might contain a Carnot engine that worked on the temperature difference between the hot tail pipe and the chassis of a truck.

Biological Marker Trace Detection

The current programs to develop a "dog's nose" as well as the efforts to develop chemical/biological analysis on a chip-sized system for attack warning should provide a great deal of the necessary technology for chemical/biological trace detection system.

If Successful, What is the Payoff?

With the new tag and trace sensor systems described above, it should be much easier to detect and track potential terrorists as they try to enter the US or approach overseas garrisons of US troops. In addition, the micro robot placement of covert sensors should allow the gathering of much better intelligence on the plans and techniques of targeted terrorist groups before they undertake a mission.

5. LOCATE, DISRUPT AND DESTROY TERRORIST NETWORKS

What are we trying to do?

In order to effectively implement countermeasures for transnational threats, we must be able to locate the terrorist physically and electronically. With improved collection capability and information management, we will be able to effectively deny, disrupt, degrade, destroy, and exploit (D4E) terrorist activities, communications, and databases. Our goal is to bring more proactive options to the table that the policymaker and/or warfighter can bring to bear on transnational threats. The objective is to deny the terrorist physical access to specific locations, buildings, or areas and to their communications and computer links/nodes, and logistics acquisition systems. To disrupt terrorist activities we need to interrupt their communications and computer links/nodes, inject false communications to disrupt unit cohesiveness, prevent delivery or acquisition of critical logistics, and even disrupt personnel selectively by incapacitating them. Degrading objectives are similar, but more comprehensive in scope, as the goal is bring down critical communications and computer links/nodes, impair unit cohesiveness and morale, and effectively stop logistics support. Destruction varies from the physical destruction of the terrorist cell to the destruction of their communications and computer links/nodes with non-evasive techniques that can produce a cascade effect that would deny/disrupt/destroy economic and logistics links. Non-evasive techniques provide us with a capability to selectively destroy terrorist leadership and/or networks. Exploitation, based upon current intelligence, has been largely ad hoc based upon random opportunity and has not yet proven viable. The ultimate objective of D4E is to provide field commanders better tactical capability as well as provide the National Command Authority better detailed information providing a variety of responses through the political, information, economic, and/or military instruments of power holding the terrorist and their infrastructures at high risk.

How is it done now?

Current intelligence collection methods, locate terrorist activity, basing, and sanctuaries is carried out through HUMINT, COMINT, SIGINT, and Imagery Intelligence (IMINT). These provide a limited capability to pinpoint terrorists, determine their intentions, and take full measures for D4E. Currently, response actions have been largely limited to physical attack as in the case of the Israelis or the "reserved right to respond" by the U.S. government. Denial, disruption, degradation, and destruction is currently accomplished ad hoc which in most cases has been the result of plain luck (i.e., recent New York City Subway bombers apprehension). The proliferation of global real time news reporting, such as the CNN network, make it difficult to use conventional Psychological Operations (PYSOP) tools such as leaflets or wide area broadcasts. Our current capabilities are contrasted with our projected "what we are trying to do" capabilities in Table 1. This table also summarizes the goals in each of the D4E areas we want to achieve in order to hold the terrorist threat at risk.

D4E Elements	Current Capability	Projected Capability	Goals
Deny	Some limited physical access, comm links	Physical access, physical and electronic comm links, computer access, logistics support, incapacitate personnel selectively	Denial of physical support, logistics support, comm links, computer access
Disrupt	Some comm links, some logistics support, some computer access, arrests of individuals	Physical and electronic comm links, computer access, plan execution, unit cohesiveness, incapacitate/disable groups	Disrupt comms, logistics support, computer access, discredit leadership, stop plan execution or force changes
Degrade	Some comm links, some logistics support, multiple arrests	Physical and electronic comm links, computer access, unit cohesiveness, logistics support	Degrade capabilities in comms, computer access, logistics, cohesiveness, leadership, capabilities, isolation
Destroy	Physical structures, some logistics support, arrests of the entire local cell	Physical structures, physical and electronic comm links, computer access, unit cohesiveness, selectively disable/kill groups or personnel	Destroy options besides physical include destruction and/or countermeasures against comm links, computer access for comm or financial systems, internal trust mechanisms, political mechanisms
Exploit	Some collections info, mainly ad hoc through fragile means	Enhanced collections, comms, computer traffic, manipulation techniques	Exploit collections to determine intent, manipulate comms and/or computer traffic, develop prediction models, provide better protection options at various levels

Table 1. D4E Elements, Capabilities, and Goals

What are the limitations?

Given the conventional methods widely used today to locate, disrupt, and destroy terrorist networks, we must note inherit limitations. Current technical and analytical approaches to locate, disrupt, and destroy terrorist activities are extremely time and manpower intensive and often yield results based on luck with uncertain accuracy and are often too late to influence the result of terrorist activities. These limitations can, in general, be organized into three primary areas.

First, rapid advancements in encryption methods available to terrorist groups significantly challenge our ability to decode and understand terrorist conversations and messages in a timely manner, such as the case of cellular telephony.

Second, terrorist groups tend to operate in decentralized distributed networks. In such an environment it is exceedingly difficult to gain access to their information and communications especially those generated by non-electronic means.

Third, we recognize significant limitations in our ability to disrupt and destroy terrorist activities by influencing the terrorist's perception of his organization and the outside world. These limitations result from: (a) the international media's ability to potentially discover information that is in apparent conflict with our government's "right to know" policy; (b) current information technology available to terrorists, such as the Internet and CNN, provide terrorist with powerful tools from which to validate the information inputs that shape their perceptions of themselves and the world: and (c) our inability to selectively deny terrorist access to communication services.

What are the new approaches?

Existing and new methods can be applied to monitoring and locating terrorist locations. Geo-locating COMINT techniques and communication recognition methods can be used to exploit the electronic communications of terrorist groups providing new and highly efficient means to identify their physical location.

The applications of small, unmanned sensors/vehicles that can be remotely activated provide the means for offensive information operations against terrorist sites. Such systems could employ electromagnetic, acoustic or fiber optic technology. In addition to surveillance efforts such equipment could be used to disrupt and destroy the information operations of terrorist groups. These actions include expanded methods for interfering and denying wireless and computer based communications. In addition, current technology provides opportunities to isolate the terrorists from their supporting community through embarrassing public exposure. Through the use of video and voice morphing and hyper-text substitution we can create misleading internal communications and public images creating misinformation and causing the terrorist to question the loyalty of their leaders and subordinates.

Computer network intrusion methods can also be used to our advantage. Through these methods we can enter the terrorist's information network to disrupt and destroy these critical assets.

Why will it work?

Many of the enabling technologies are being developed by a wide range of organizations such as the movie industry, universities, and DARPA. These individual technologies have been demonstrated in the laboratory but not necessarily in a transnational threat context. Several very small (approx. 10 cm) robots have been demonstrated for various applications such as mine location and clearing. Other robots have been demonstrated carrying video cameras. Cellular phone companies have technologies for locating, following, and billing individual phones. There are many various morphing capabilities that are being developed within the entertainment industry. Many of them have been used in movies for very similar applications - however, they are not real-time. Similarly, many computer hacking programs have been developed and are available on the Internet.

These individual technologies must be pulled together and integrated into system concepts. Any holes must be identified and filled with new technology developments. The system concepts approach will also require development of transnational concept of operations which in-turn may require policy approval/modification.

If successful, what will be the payoff?

If we can pinpoint the location of terrorist cell, then additional technologies can be applied to disrupt or destroy the cell. The better the accuracy of the location, the more options we can have in defeating the terrorist's plans. For example, if we have identified the location of the cell, we can use the small sensors/robots to gain additional information which will allow us to develop detailed plans to best counter the specific terrorists as well as provide vehicles for offensive operations such as disrupting or destroying communications equipment. Offensive information operations could allow us to generate computer generated audio/video transmissions designed to cause discord within the terrorist's cell. For example, images of leaders sympathetic to the terrorist's goals supporting positions counter to the terrorist's could be provided to the terrorists. We can manipulate direct communications to the terrorists from such leaders to possibly direct them to change plans. Such operations could severely undermine the confidence of the terrorists and/or cause them to stop operations for a time.

6. FORCE PROTECTION

What are we trying to do?

The DoD needs the capability to do rapid, continuous inspection of vehicles entering military facilities or compounds for concealed high explosives and the capability to perform rapid inspection of interior facilities if perimeter security is breached.

How is it done now?

The military now relies primarily on physical inspection by soldiers and canine olfaction at portals and perimeters. It has no significant search rate for large areas. Dogs are the classic trace detection system. They can detect the characteristic scent of explosive and/or the other ingredients in the explosive formulation. They are used successfully to do land mine clearance and explosive detection, but have operational problems for routine screening, where they lose interest in the task, which may not be readily detectable.

There are significant differences between civil and military capabilities. The FAA has responded to concern over airline passenger safety over the last few decades by developing a number of technologies for explosive detection that are widely deployed and continually upgraded. These technologies are used below to discuss potential improvements to current DoD capabilities (L. Malotky, "Advances in Security Technology," FAA report, June 1995).

X-ray detection systems are derivatives of medical imaging systems. They have been used for several decades. The first x-ray security systems employed simple x-ray attenuation to produce a shadowgraph of the object being screened. That works well for high-contrast targets such as handguns but is not as effective for unstructured targets like sheets of explosives. Transmission x-ray screening is currently being used for customs contraband screening of trucks and cargo containers, but it is still limited by the difficulty of interpreting the signatures from bulk explosives.

In the early 1990s, two-energy x-ray devices were used to differentiate high atomic number materials, like the iron of weapons, from the absorption of low atomic number explosives. Dual energy systems are in use today in baggage screening systems in which an operator observes the image. As computing power increased and became more affordable, it became possible to develop automated dual energy image explosive detection systems. A significant number of these automatic systems, currently costing about $350,000, are being used to screen checked baggage in the United States and Europe.

X-ray tomography evolved from medical applications requiring precise, non-destructive, two- and three-dimensional imaging of tissue. A computer tomography system, the InVision CTX-5000, was submitted to the FAA for certification as an automated Explosives Detection System, underwent formal certification testing, and was certified in 1994. It takes selected tomographic slices through the object being screened and uses density and size information generated to make a decision on the presence of an explosive threat. It has demonstrated the ability to detect threat quantities of a broad range of commercial and military explosives. It is now deployed in airports in the US and abroad, and the FAA is purchasing over 50 units at about $900,000 each and providing them to air carriers to screen checked baggage.

Thermal neutrons. In the 1980s thermal neutron analysis was explored for the detection of explosives concealed in checked baggage and cargo. Radioactive decay and electronic neutron generators were used. The thermalized neutrons react with nitrogen atoms in all commercial and military explosives to give a 10.8 MeV gamma ray, which stands out from the background, allowing an estimation of the amount of nitrogen present. However, innocent objects in baggage with high nitrogen densities cause false alarms. Following the bombing of Pan American flight 103, thermal neutron systems were deployed in six airports to collect operational information. Their performance and operational availability were good, but they were not accepted by air carriers because of system size, cost and limited ability to address explosives smaller than about 1 kg.

Fast neutrons are scattered by atoms they encounter. The energy of the resulting gamma rays are characteristic of the element, which allows the operator to do an *in situ* elemental analysis. Explosives can be recognized by their characteristic elemental ratios of oxygen, carbon and nitrogen. Elements present in improvised explosives, e.g. chlorine and very high levels of oxygen, may assist in the detection of improvised explosives.

Fast neutrons have been explored in three different geometries. A sealed tube neutron generator with an imaging alpha detector was developed in the early 1980s, in which the collision of a tritium atom on deuterium produces a 14 MeV neutron and a collinear alpha particle. The alpha particle can be imaged and the position of each neutron of interest as a function of time predicted. The timed arrival of a gamma ray from the interaction of the fast neutron with an atom allows one to determine its location in space.

In pulsed fast neutron analysis, neutrons are created in narrow bursts about 1 nanosecond wide, and the gamma ray detectors are collimated to look at one line. The time of arrival of a gamma ray tells the operator where the element is along the line of propagation. The energies of the gamma ray indicate which elements are in the beam. Transmission shadowgraphs can also be done using broad energy range fast neutrons. Specific elements in the beam scatter selected neutron energies. The determinations of which energies are absent allow the determination of which elements are in the beam line and potentially whether explosives are present.

These three approaches are all in the experimental stage. The pulsed fast neutron approach is the most mature. An operational prototype is under construction. It has been used in the laboratory to screen luggage and cargo in 20 foot containers for explosives.

Quadrupole Resonance is the emerging electromagnetic approach. Rather than ionizing radiation it uses an alternating high-frequency magnetic field. An applied 3.5 MHz RF magnetic field interacts with the nitrogen molecules in explosives. Because of their crystalline structure, the field interacts with the atoms only at certain, unique frequencies. Due to their specificity, detection is good and false alarm rates are small. However, because of the specificity of the interaction frequencies, the detection system must interrogate the sample with the correct frequency and pulse train shape for each explosive of interest.

Laboratory testing was accomplished with a large scale coil (300 liters) quadrupole resonance system using 300 lost bags, 100 of which were loaded with threat and sub-threat quantities of explosives. The technology is available commercially in the form of small systems to interrogate parcels for RDX and PETN; other explosives are being added. Quadrupole resonance is the result of research in several countries and partnerships between government and industry. It requires neither massive radiation shielding nor sophisticated image analysis software. It would

fit well into an integrated security screening system in which several technologies worked together.

Trace detection systems have been employed operationally protecting a variety of facilities for at least 15 years. The systems of today are capable of detecting traces of explosives present on a variety of concealments. Dogs are the classic trace detection system; they can detect the scent of explosive and/or other ingredients in the explosive formulation. They are used successfully for explosive detection but have operational problems for routine screening. Scientists have been working to develop an electronic equivalent to the dog's nose since the early 1970's. Current technology is capable of simultaneously detecting and identifying less than one nanogram of cyclotrimethylene trinitramine (RDX) or Pentaerythritoltetranitrate (PETN), volatile explosives, ICAO marking agents, and other explosives of interest.

The challenge in trace detection is not detection; it is the collection of the sample. The molecules of explosives clinging to the clothing of the bomb carrier need to be activated, swept away, and collected. For successful trace detection, the explosive sample must be collected from a surface or air stream, separated from all the background, detected, and identified. Current trace detection technology requires intimate contact with surfaces for residues of low vapor pressure military explosives. Some systems employ fast (typically 5-10 s) gas chromatography to separate the explosive molecules collected from all the other chemicals that may interfere with the detection. Trace explosive detection systems have been operationally evaluated in airports. Trace detectors are routinely used to examine electronic items for concealed explosives, which is a difficult task for x-ray systems with human operators. The false alarm rate is less than 0.2%, with a majority of the false alarms attributable to the legitimate presence of explosive residues. The FAA is in the process of purchasing over 400 trace detectors, costing between $45,000 and $160,000 each, in FY-97 for deployment in United States airports. Trace detection technology continues to advance for the screening of people as well, although how to do it quickly without upsetting the billion plus people that fly every year is a challenge for the FAA.

Trace detection systems have been used in airports in Canada, Germany, and other locations and to protect selected federal installations. The same detection technology is being incorporated into walk-through portals that can be used to screen people for concealed explosives and into a portable car mount to operate at a vehicle checkpoint of opportunity. Some systems have portable sample collecting systems to clear suspect packages. The ability of trace detectors to detect volatile explosives, low volatility explosives, and ICAO markers make them a powerful detection tool with two complementary mechanisms for the detection of high threat plastic explosives: the volatile marker or the nonvolatile explosive. All of these attributes can carry over directly to military applications.

Electron capture. Early commercial explosive vapor detection systems employed electron capture detectors (ECD) to detect volatile explosives, specifically, nitroglycerin and ethylene glycol dinitrate, which are present at high vapor concentrations around many 1970's dynamites. These systems employed preconcentration, semipermeable membranes and/or gas chromatography to separate the explosive molecules from the electronegative components of air. Explosives are very electronegative; that is, they easily capture electrons, which ECD exploits as a sensitive detection mechanism. However, compounds other than explosives are electronegative. Current commercial trace detectors have moved away from ECD for explosive detection because of its lack of specificity and the resulting false alarm problem.

Chemiluminesence is a nitrogen specific detector. Explosive molecules containing nitrogen are separated using gas chromatography from the rest of the materials collected from the air. Once separated, they are pyrolysed to give Nitrogen Oxide (NO) that is reacted with ozone to give excited Nitrogen Dioxide (NO2) that emits infrared radiation. The approach is very sensitive. Specificity is gained by chromatography.

Ion Mobility Spectroscopy (IMS) separates explosive molecules from the air background by gas chromatography and time of flight. The electronegative explosive molecule is introduced into the system and ionized by attaching an electron or a small charged molecule. Most molecules in air are not as electronegative as explosives; therefore, they are not ionized. The charged explosive molecule is carried into an electrostatic field and accelerated. Its time of flight to move through a counter-current drift gas and reach the collecting electrode is measured and is characteristic of its mobility. Detection is made by averaging over hundreds of these fast events. There are several commercial vendors of trace explosive detectors employing IMS.

Mass Spectroscopy is theoretically the ideal instrument to use as an explosive detector, as it should provide instantaneous identification of molecules based on their fragmentation pattern and mass. Although this approach has worked in the laboratory, the cost, complexity and demands of a vacuum system have kept this technology out of the commercial market.

Antibodies are the protective cells formed in the body in response to the introduction of foreign materials. They are also formed in response to the introduction of explosives and the chemicals used in their production. Such antibodies can be detected with the research tools of modern biochemistry. However, those tools are not yet fully developed and would probably require measurement in the bloodstream to provide the biological or genetic materials required for testing. Such tests would be more invasive than others suggested above, and their evaluation could be much more time consuming.

Layered, synergistic approaches are appropriate, as none of the technologies discussed above are ideal by themselves. As noted above, a chemical detection system that detected both explosive and carrier could be much more effective than one that detected only one or the other. And a system that used a combination of x-ray tomography for search and trace detection for confirmation could largely eliminate the weaknesses of both.

What are the limitations?

Explosives can be detected by exploiting the bulk properties or the detailed chemistry of suspect objects. The former is generally faster but less discriminating; the latter is generally more specific but more time consuming and expensive. The optimum combination of techniques has not been found in the FAA program, compared to which the current DoD program is rudimentary. The paragraphs below discuss the limitations of current technologies, and the additional limitations introduced by DoD applications.

The military search and detection capability is based on inspection and canine olfaction. Inspection is susceptible to concealment and deception, which produces low detection rates and low throughput. Dogs are the classic trace detection system. They can detect the characteristic scent of explosives and other ingredients of explosives. They are used successfully for land mine clearance and explosive detection, but tire and lose interest in routine operations. However, they are an ideal tool for perimeter and area searches, if breaches are detected.

X-ray detection is a well developed capability, which is adequate for simple shadowgraphs of readily recognizable objects. It works well for high contrast targets such as handguns but not low-contrast targets like explosives. Dual energy systems provide more contrast, but not enough for automatic recognition. An impediment to the wider use of automatic x-ray systems is their cost, which currently about $350,000.

X-ray tomography has been certified as an automated Explosives Detection System. It has demonstrated the ability to detect threat quantities of a broad range of commercial and military explosives and is deployed at airports in the US and abroad. Over 50 units are being purchased at about $900,000 each to screen checked airline baggage. It is unlikely that such units could achieve the cost, size, and mobility goals of military portal systems, let alone search systems.

Thermal neutrons react with nitrogen atoms in commercial and military explosives to give a hard gamma ray, which stands out from the background, allowing an estimate of nitrogen content. However, innocent objects with high nitrogen densities cause false alarms. In operational tests, thermal neutron systems' performance and operational availability were good, but they were not accepted because of size, cost and limited ability to address explosives smaller than about 1 kg.

For military systems explosive charges are likely to be much larger and truck transport is a favored option; thus, the limitation to > 1 kg is not as severe. Thermal neutrons could be effective in military applications, if the neutron sources and gamma ray detectors are small and cheap, which has not been established by civil programs.

Fast neutrons allow *in situ* elemental analysis, in which explosives can be recognized by their characteristic elemental ratios of oxygen, carbon and nitrogen. Sealed tube generators simplify the construction of the source and the timing of the pulse at the expense of flux. Pulsed fast neutrons complicates the source. Transmission shadowgraphs require measurement of the transmitted spectrum. All three approaches are in the experimental stage. The pulsed fast neutron approach is the most mature. It has been used in the laboratory, and an operational prototype is under construction. The main issues with fast neutrons are their immaturity and sensitivity. As with thermal neutron systems, a limitation to > 1 kg of explosive is not debilitating.

Quadrupole Resonance has good detection rates and low false alarm rates because of its elemental specificity. It requires neither massive radiation shielding nor sophisticated image analysis software. However, it must interrogate the sample with the correct frequency and pulse train shape for each explosive of interest. Thus far, it is available commercially in small systems for RDX and PETN. The cost and mobility of more flexible systems have not been established.

Trace detection. Current technology is capable of simultaneously detecting and identifying less than one nanogram of RDX or PETN and other explosives. The challenge is sample collection. Current technology requires intimate contact with surfaces for residues of low vapor pressure military explosives. Trace detection has been operationally evaluated with false alarm rates < 0.2%. The FAA is purchasing over 400 trace detectors for $ 45,000-160,000 each for deployment in airports. The same detection technology is being incorporated into walk-through portals to screen people for concealed explosives. Their ability to detect both volatile marker and nonvolatile explosives increases detection and selectivity. While costs are slightly higher than desired for military applications, the more serious barriers would appear to be the low throughput (~ 30 s/person and 60 s/vehicle), size, complexity, and lack of mobility.

Electron capture is effective in detecting volatile explosives such as nitroglycerin. However, compounds other than explosives are electronegative, which increases the false alarm rate, and modern explosives have much less volatility, so current commercial trace detectors have moved away from ECD because of its lack of specificity and false alarm rate. Thus, it would be of only limited use for military applications.

Chemiluminesence is nitrogen specific and very sensitive in combination with chromatography. However, the resulting analytical laboratory is complex and expensive.

Ion Mobility Spectroscopy has greater specificity than electron capture alone, but still requires direct sampling and involves a more complex instrument.

Mass Spectroscopy works in the laboratory, but the cost, complexity and demands of a vacuum system have kept this technology out of the commercial market. These factors would be even more of a barrier to military applications.

Antibodies form in response to the introduction of explosives and the chemicals used in their production. They can be detected with the research tools of modern biochemistry. However, those tools are not completely developed, and require measurement in the bloodstream to provide the biological or genetic materials required for testing. Such tests would be more invasive than others suggested above, and their evaluation could be much more time consuming.

Layered, synergistic approaches are desirable. None of the concepts discussed above are ideal by themselves. As noted above, a chemical detection system that detected both explosive and carrier could be much more effective than one that detected only one or the other. And a system that used a combination of x-ray tomography for search and trace detection for confirmation could largely eliminate the weaknesses of both. However, it is difficult to build a synergistic combination of the simplest systems. For example, one energy, two energy, and automated x-ray systems with a detection probability of $p \sim 0.7$ and false alarm probability $f \sim 0.5$ might cost \$50, \$150, and \$350K, respectively. Thus, it would be attractive to use a one energy sensor as a screening device for an automated x-ray systems, but the resulting combination would cost ~ \$400K, have a probability of detection ~ 1 - (1 - .7)^2 ~ 0.9, but a false alarm rate of ~ 1 - (1 - .5)^2 ~ 0.75, which is so high that it would essentially be necessary to re-inspect every parcel, person, or vehicle. For the better sensors, such as x-ray tomography, neutrons, quadrupole resonance, and trace detection, it might be possible to create useful layered systems, but they appear to be large, complex, expensive, slow, and immobile. Thus, the more capable systems might be deployed better by themselves, as a simple screening sensor would not appear to add value commensurate with its cost in military applications.

What is the new approach?

The new approach involves steps ranging from the simple and familiar to the more complex and developmental. A number involve the technologies above, but used in a manner that avoids their limitations in civil applications.

Measuring mass. The first is to weigh vehicles as they come through a portal. Any significant amount of explosive, however hidden to the eye and other sensors, should manifest itself as an anomalous vehicle weight, which could serve as a high-confidence indicator for further screening. Weighing could either be done with a typical weight and balance scale, as used for commercial trucks on U.S. highways, or with a series of speed bumps—comparing the trucks

actual response to its expected response would give an indirect but confident estimate of its mass while permitting greater throughput.

X-rays and neutrons for large vehicles. A second measure is imaging large vehicles with x rays and thermal or fast neutrons. These sensors are less favored by civil investigators because they are limited in sensitivity to ~ 1 kg of explosive. While that might be a lethal amount for an aircraft, much larger explosives are needed to destroy military facilities, so an amount this small could be a very useful threshold for a military sensor. With such a range between the likely ~ 1,000 kg payload and this ~ 1 kg threshold, the resulting ~ 1,000/1 signal to noise ratio should support confident detection with one or more of the simpler sensors.

Screening. Another measure is to pre-screen and/or profile persons approaching portals. This step could involve a number of steps from manual or automated template matching to the establishment of computer files on individuals who frequently enter or attempt to enter facilities.

Trace detection should be practical on military facilities. Those who present themselves at portals are requesting entry. To support that application, they are expected to surrender certain articles such as identity cards, briefcases, and the like and subject themselves to simple searches. They afford the opportunity for direct contact, which is the most difficult step in trace detection, as discussed above. Given that the surrendered items can be swabbed in a few tens of seconds to extract samples, if the simple chemical processing required for trace detection can be effected in the few minutes of current automated systems, it should be possible to fully screen the individual for contact with all explosive materials of interest within the ~ few minute cycle for clearance onto military facilities in foreign countries.

Smart nose. Trace detection could be simplified, and its throughput greatly increased, by the development of "smart nose" technologies, i.e., enzyme mimics and the class of semiconductor array sensors that can do molecular recognition with accuracies approaching those of the dog's nose—without tiring and without loss of attention or sensitivity. While this technology could take 5-10 years to develop, it would represent a fundamental step towards the advanced trace detection sensors for confident detection in affordable packages for proliferated or mobile deployment.

Chemistry on a chip and associated MEMS technologies offer the promise of compact, rugged, and affordable analytical laboratories that could be used in mobile micro-platforms for remote detection of chemical compounds or in distributed arrays for the gathering of intelligence. Although this is probably also on the 5-10 year time scale, it would provide flexible, throw away sensors capable of detecting new threats as well as established one. Semiconductor implementation should make mass production of such sensors feasible.

Canine olfaction. The implementation of the above measures would put the burden of routine search and detection on automated sensors, which would release dogs for the tasks they are best at: area search, quick scans of new areas, detection of distributed supplies of C4, Semtex, and other low volatility explosives, and novel missions for which dogs do not get bored.

Force Protection Associate. The measurement, imaging, pre-screening and trace detection technologies discussed above should be coupled with a Force Protection Associate program. The Force Protection Associate is an integrated set of tools to allow site commanders to perform facility vulnerability analysis, such as determining blast effects on a specific building, and risk management modeling such as portal and road vulnerability analysis and evaluation of the

vulnerability of individual structures. It will also include a wide range of other tools such as intelligence data harmonization/fusion, information on terrorist organizations, local activity monitoring, potential terrorist activities and plans, and information sharing.

Why will it be successful?

Measuring mass. Mass is the fundamental quantity that is most difficult to conceal. As always, it is the best discriminant. A scale is the simplest and fastest way to determine it. Thus, it can serve as a high-confidence indicator for further screening. Knowing the mass in conjunction with a x-ray or neutron image leaves little freedom for an intruder to hide explosives.

X-rays and neutrons for large vehicles. Large explosives are needed to destroy military facilities, so a threshold of ~ 1 kg is very useful threshold for military applications. Its signal to noise ratio should support confident detection with one or more of the simpler sensors.

Screening persons approaching portals has been shown to be effective. It could involve steps from manual or automated template matching to the establishment of computer files on individuals who frequently enter or attempt to enter facilities. The computational burden for comparison and data exchange should not be burdensome.

Trace detection should be practical on military facilities as those who request entry must surrender articles that afford the opportunity for direct collection, which is the most difficult step in trace detection. It appears technically feasible to process them in a few minutes, making it possible to screen individuals for contact with explosives within the clearance cycle for admission.

Smart nose. Enzyme mimics and semiconductor array sensors for molecular recognition are within 5-10 years of development. They represent a fundamental step towards trace detection sensors in affordable packages for proliferated or mobile deployment.

Chemistry on a chip offers compact, rugged, affordable analytical laboratories on mobile micro-platforms for remote detection or distributed arrays for within 5-10 years of development.

Canine olfaction for facility sweeps. The implementation of the above measures would put the burden of routine search and detection on automated sensors, which would release canine olfaction for the tasks it is best at: novel missions for which dogs have long proven their value.

Force Protection Associate. Many of the pieces of the Force Protection Associate have been developed or are currently being studied for their applicability in a military environment. Efforts must now be made to integrate them into a useful product.

If successful, what is the payoff?

Successful pursuit of the technologies and concepts discussed above would make it possible to secure the boundaries of military facilities against attempts to infiltrate high explosives and permit the rapid sweep of its perimeter and interior should such infiltration occur.

Measuring mass would provide a high quality discriminant and indicator for further screening, which would leave an intruder little freedom to hide explosives.

X-rays and neutrons would provide high signal to noise portal search and detection for large vehicles as well as a low false alarm screen for further inspection.

Screening persons approaching portals with template matching to computer files is a proven technique, which is now computationally feasible for real time denial or reaction.

Trace detection on military facilities is simplified by the requirement to surrender articles that permit direct collection, which is the most difficult step. Processing should be possible within the normal clearance cycle for admission at reasonable throughput.

Smart nose technologies represent a fundamental step towards trace detection in affordable packages for proliferated or mobile deployment.

Chemistry on a chip offers compact, rugged, and affordable analytical laboratories on mobile micro-platforms for remote detection or distributed intelligence arrays.

Canine olfaction for facility sweeps. The implementation of the above measures would permit the proper reallocation of dogs for the novel missions at which they have long proven their value.

A ***Force Protection Associate*** program that can portray information on vulnerabilities and correlate information on potential terrorist plans will allow the site commander more time to prepare and counter potential terrorist activities. By understanding the vulnerability of his facility and command the site commander can then apply the optimum degree of protection.

7. DETECT AND NEUTRALIZE BW/CW AGENTS ON AN AREA BASIS

What are we trying to do?

Chemical and biological weapons are threats to the full range of US activities from combat operations to protection of CONUS against endogenous terrorists. The US has substantial familiarity with chemical weapons; however, biological weapons pose a less familiar set of problems. New technology and systems are needed urgently to defeat these types of threats.

This section addresses technologies that will contribute to defense, defined broadly, against chemical and biological threats. It emphasizes concepts that are underfunded or unrecognized opportunities.

How is it done now?

Protection of combat military personnel is accomplished primarily by a system of point sensors and protective gear. Current systems are focused almost exclusively on combat personnel assumed to be operating in a combined chemical/biological and perhaps radiological environment. The development of protocols tailored to the defense of widely different types of populations against the different classes of threats has not begun.

What are the limitations?

The current systems have many deficiencies. We classify these deficiencies in terms of the timeline, and in terms of whether they are a classical chemical agent or a biological agent. Detection of chemical agents is difficult, but substantially less challenging than detection of biological weapons. If chemical detection fails, the action of the most probable of these agents—the nerve agents—is sufficiently rapid that the first individuals exposed show immediate signs that a chemical attack is taking place; there is no possibility for exposure of large numbers of people before the first symptoms appear, as is the case in a biological attack.

Nerve agents. Nerve agents are difficult to detect and characterize at standoff distances. The counteragents used--atropine, pyridostygmine hydrobromide — are themselves toxic, and require care in use. Protective gear is expensive, since nerve agents are toxic by skin contact: there is no effective protection for rear echelon personnel, or for large numbers of civilians. Decontamination following an attack is difficult, slow and involves caustic and reactive solutions (e.g., bleach), and there are no established criteria for declaring an area safe once it is decontaminated.

Other chemical agents. Many of the same criteria apply to blister agents (such as mustard), blood agents, and to others of the many agents that have been considered and developed.

Biological toxins. Biological toxins — especially botulism toxin, staph enterotoxin, ricin and abrin--are more toxic than nerve agents, and have the additional feature that symptoms may not develop for more than 12 hours after exposure. It is therefor difficult to detect an attack by the response of the population that has been exposed. Treatment of these agents is possible if they are detected early, but the detection methods are slow and expensive. For some, once symptoms

have developed, treatment is limited to support. There are no methods of detecting these agents at standoff; detection at short range generally requires immunochemical methods, is relatively slow (15 min after sample collection), and expensive. There are no accepted methods for sampling air and soil to detect these agents. Biological toxins, in general, require that they be breathed or ingested to be toxic, and relatively simple masks afford useful protection; however, these masks are not available in the quantities needed to protect rear echelon military personnel, ports, airbases, and civilian populations. Decontamination is again slow and labor intensive, and there are no simple methods for declaring an area safe.

Pathogens. Pathogens (anthrax, tularemia, plague, glanders, cholera, Q fever, etc.) pose the most difficult problems in detection and characterization. There is no standoff detection, and only limited point detection. The tests that are available now require access to what is effectively a biology laboratory. Since symptoms do not develop for several days after exposure, it is possible, in principle, to have an attack expose large numbers of people (particularly in a terrorist attack on a civilian population) with no indication that an attack had taken place. Since some of these diseases are highly contagious, there is a serious problem of managing a biological attack in such a way that it does not lead to epidemic. In a biological attack, there is a crucial problem of separating those who have been exposed and require treatment from those who have not been exposed; there is no technology for triage now. Protection of the caregivers in the system—from first responders to hospital personnel—relies on conventional methods (protective clothing, isolation), and would be overwhelmed in any serious attack. Decontamination will vary with the agent, and there is no accepted set of protocols for decontamination and certifying safe for them (especially for anthrax, which is persistent in spore form).

There are a series of issues that cut across the spectrum of technologies used in BW/CW defense:

- The cost, sensitivity, and coverage of existing detector systems is inadequate.
- The specificity of detectors against biological agents is not satisfactory, and although there are a number of new technologies being developed that will contribute to this area, the development of effective, fieldable systems is still in its infancy.
- Characterization of biological agents is slow, incomplete and inaccurate.
- Sampling of air, water and soil for biological agents is very difficult, and new ideas are critically needed in this area.
- Decontamination remains a problem that is poorly understood, especially in non-combat environments.
- Technology for deterrence (that is, technical aids to intelligence collection) and for attribution (that is, tools to identify the person or group responsible for a biological attack after it has occurred) are very primitive.

Most of the work in BW/CW defense has been focused on protection of combat operations. It is not clear that combat is where the real threat to national security lies: attacks on ports, logistics chains, support personnel, and on CONUS itself is a more serious problem, and more attention should be focused in these areas.

What are the new approaches?

Where new science has led to new weapons, it will also lead to new defenses. There are a number of new technologies that are applicable to various parts of the BW/CW defense problem. This area is one in which there is no silver bullet that will nullify the entire range of threats. Rather, these technologies offer the potential to build the components of systems that *will* add very substantially to national capabilities in defense.

Characterization: Molecular biology is offering a broad range of tools for genetic classification of organisms that will provide one of the keys to identification of the entities used in an attack. These tools (based on methods for genetic sequencing and for identification of proteins) enormously expand capabilities in this area. They are, however, still slow and expensive, they require skilled personnel to use them, and they must be made more rugged. There is substantial excellent work going on in this area, and it should be aggressively pursued. Programs include work in biochemistry on a chip, genetic sequencing of threat organisms, microfluidic systems, rapid genetic identification, application of mass spectroscopy to biological assays, and a range of others. A key issue now is, while continuing work on these sensors and systems for characterization, to develop systems that are effective in field use.

Collection: UAVs and Unmanned Ground Vehicles (UGVs). Unmanned vehicles offer new opportunities for collection and standoff detection. One of the characteristics of BW and CW is that they are usually airborne, and large-area dissemination would require spreading them in the open air. This type of attack could be blunted by early warning using UAVs equipped either as detector/collectors (with characterization being doing elsewhere) or with on-board microanalytical systems. Sensors developed for such uses would also be applicable as point sensors.

Stand-off Detection: New spectroscopic methods. A range of techniques—differential infrared absorbency or reflectance, ultraviolet light (UV) fluorescence, hyperspectral analysis—all offer opportunities for some stand-off detection. Airborne mass spectroscopy or other microanalytical methodology may offer additional capability.

***Area Defense through Area Sterilization by UV*:** It is possible that some area protection can be achieved by using local UV pathogen neutralization. In essence, one would use "UV searchlights" to irradiate the pathogen cloud, and deactivate at least part of it. This type of technology would not provide complete protection, but it would decrease the area that was contaminated.

Improved Protocols for Vaccination: Vaccination offers a very good method of decreasing the threat of disease. (It is important to point out that the most dramatic decreases in morbidity and mortality from infectious disease in civilian populations has come from successful vaccination, not from the much more expensive and problematic treatment of disease, once established. It is also important to emphasis that for many of the threats that are possible components of a biological attack, there is no treatment once symptoms appear: pulmonary anthrax, botulism and ricin toxicity, and essentially all viral disease fall in this category.) Prevention is much more effective than response in BW and CW. Applied immunology has been an area of enormous advance in science; very little of the advance in this area has been applied to the problem of BWD.

Early Detection of Exposure/Disease: There are a range of techniques that one can consider for examining populations for early disease, well before the development of overt symptoms: early rises in levels of key chemical signals for inflammation and activation of the immune system are among them. The development of fieldable tests that could be used to distinguish from a population those individuals who had been exposed from those who had not would be an enormous contribution to the management of biological incidents (it is less of a problem with chemical incidents, since the development of symptomology is more immediate and more obvious).

Aids for Intelligence: Biomarkers. A system for examining the exposure of animals and people to past environmental influences is now possible in principle, and would provide new tools for analysts (although it would also require new methods of operations).

Why will it be successful?

These proposals for technologies have precedent in existing civilian and military use. Genetic methods are becoming routine in diagnostics and epidemiology for their convenience, specificity and sensitivity; they need to be adapted to DoD use, but the potential to do so is clear. The high level of activity in systems for biochemistry-on-a-chip suggests broad confidence in this area for both civilian and certain military uses. UAVs are already being developed to carry sensors; the BW/CW application simply requires appropriate sensors. Stand-off spectroscopy for detection is not a technology with current precedent, but advances in lasers have only recently made it possible. Vaccination is an area where the civilian sector has not made great investment, for a number of reasons, but the science certainly exists to develop more effective vaccines, adjuvants and vaccination protocols. The biomarkers program is speculative, but again soundly based in immunology.

If successful, what is the payoff?

The payoff would be profound, in our ability to defend against and defeat biological and chemical attack:

- Better warning and characterization of attacks
- Better ability to detect/infer activities occurring before an attack (with the possibility of prevention or deterrence) and to attribute after an attack (and thus to punish the attacker, and to deter the next potential user of CW/BW.
- Technology and systems to defend civilian populations and non-combat military operations.

8. FIND & NEUTRALIZE CLANDESTINE NUCLEAR WEAPONS

What are we trying to do?

The objective of finding nuclear material at entry portals is to provide a secure perimeter as large as a weapon damage radius so that operations could be conducted within it relatively unencumbered. The objective of wide area search for nuclear material to provide a safe zone of similar dimensions in an area in which it is not possible to maintain a secure perimeter, to provide assurance for civilians living at an area at risk, or to provide rapid, wide area search of regions that could conceal nuclear threats to forces in the field.

This rapid, wide-area, and confident detection of nuclear materials is the essential first step in developing the ability to negate terrorist nuclear assemblies or weapons. The ability to detect and negate nuclear materials are necessary to prevent the forced, massive evacuation of urban populations or the disruption of military operations in response to terrorist threats.

How is it done now?

Search. Current portals utilize large volume (~ 4x104 cm3) plastic scintillator which give the highest sensitivity per unit cost. These detectors have very low energy resolution but are effective for the application.

Current wide area search employs man-portable and vehicle-portable radiation detectors to search for radiation sources. These radiation detectors include both gamma and neutron detectors, packaged to be inconspicuous and support a "low profile" search. The man-portable units have a detection range from a few meters to a few tens of meters. The vehicle systems have longer detection ranges, but they also move more rapidly and do not provide a detection range improvement greater than a factor of ten.

Search instruments are based on relative large (few 100 to few 1000 cm3) NaI(Tl) scintillation detectors and on large area (few square meter) moderated 3He proportional counters. These systems are primarily signal to background ratio limited by constraints of size, weight, and collection time. Natural barriers (building walls) of deliberate shielding of the target material further reduce the utility of these systems. Only minor improvements to this basic approach have been seen in twenty five years of development nor are major improvements expected in the future. Solid state detectors such as mercuric iodide or cadmium zinc telluride, while offering improved spectral resolution which reduces the effective background, are currently available only in small (few cm3) sizes which greatly limit the signal. High purity germanium detectors offer high resolution and increased volume (few hundred cm3) but results to date have not justified the large cost of these sensors.

The limited range of these detectors makes search a labor-intensive undertaking. Basically, searchers carry the man-portable detectors through the environment, "sweeping" the area for a detection range (predicted for the target device) on either side of their path. For office buildings, hotels, and government buildings, the range is usually sufficient to allow the searchers to search effectively from areas of public access such halls or corridors. Using established procedures, the search team covers the building exterior and parking areas first. To speed coverage of parking, the man-portable detectors can be "daisy-chained" to make a detector array and the electronics in

a single detector does the signal processing with acquisition times optimized for the speeds and distances involved. Upon starting coverage of the interiors, the search team leader assigns teams to each clearly defined area, usually a floor. The team leader then waits in the security office for reports of radiation detection, special access needs, or other situations requiring his personal attention. He monitors progress and assures safety by constant contact with the teams. Building maintenance or security personnel will assist search teams if the teams require access to areas requiring coverage but not reached from the public access areas. Local law enforcement personnel provide protection. A single search team can cover a single high-rise building (106 ft2) in a single eight-hour shift, including initial briefing, transit to the target building, search, recall, and debrief.

Searchers can be deployed from a small professional search cadre or trained from local fire, police, or public safety personnel.

Vehicle searches use modular detector packages that fit into vehicles borrowed or rented at the site of the search. These can include mini-vans for automobile mobility, harbor patrol boats for exterior search of ships and dock areas, and even fork-lift trucks for warehouse searches. Specialized helicopter-carried search equipment is also available, operated by DOE contractors, but this requires low-level flight and is most applicable to search of large open areas. Vehicle search electronics also includes Global Positioning System (GPS) and real-time telemetry of location and radiation alarms.

Areas searched by either vehicles or portable instruments must be maintained in a "clean" state afterward. For this role local law enforcement or building security personnel may be given simple radiation detectors to monitor packages entering a building or vehicles passing through a roadblock. In case of a radiation alarm they can act immediately to secure the source and call for assistance.

Both portable and vehicle searches are monitored from a central office. Where the search deployment is extensive, a Geographical Information System records the coverage, maintaining real-time records of the status of the teams and the areas covered.

Neutralization. The nature of nuclear weapons imposes special considerations on render-safe of these devices not present in conventional bomb-squad practice as well as many features having common principles and practices. These considerations are design-dependent, therefore the optimum render-safe must be determined on a case-by-case basis based on the design, protection, and firing set engineering of the actual device encountered.

The relevant details of the device are determined by "diagnostics", passive or active measurement methods. The render-safe team uses the knowledge gained from these activities to characterize the device and plan to exploit its vulnerabilities. The diagnostic activities can provide all the information required for selection and application of the existing render-safe options, independent of intelligence input.

The available intervention options include a wide range of potential attack methods. There is no one-size-fits-all disablement option; in fact methods which prevent or reduce yield in one case may, in a closely-related device, increase yield or even cause yield where none would have been possible before. Selection of the render-safe option is based on operational priorities:

- No nuclear yield
- No nuclear material dispersion
- No loss of life
- No damage to property

Clearly, some situations may not allow the render-safe team to choose an option that fulfills all of these.

Upon selection and approval of a render-safe plan based on the diagnostics obtained by specially-trained technicians, explosive ordnance disposal technicians set up, aim, and remotely operate the render-safe option. Containment structures may be added to prevent dispersal of nuclear material in conventional explosions.

What are the limitations?

Current sensors are based on technology with limited sensitivity, range, and growth potential. They can support portal detection but not useful area search rates. Neutron detectors under development will improve ruggedness but not extend range to levels required for search. Charged particle detectors will never be useful for more than inspection at ~ 1 m. Photon detectors based on Ge and high Z semiconductors are likely to remain small, fragile, and expensive and to require cryogenic cooling for the foreseeable future. Those under development will not provide the ranges required for useful area search.

Current operations assume that the weapon is found for them, accessible, known and relatively user friendly. There is no reason to assume that any of these conditions will be met for terrorist operations. In particular, improved capabilities are needed for area search and to address weapons to which one cannot gain access, which are booby trapped, or which are unfamiliar.

What is the new approach?

A novel approach to nuclear weapon detection is the combination of directional information (imaging) and gamma ray energy ("color") to produce a "gamma ray color camera" (GRCC), which might be able to achieve the few hundred meter ranges needed for effective search.

There are efforts underway to use multiple scatter to infer the directions of neutrons and others to use advanced electronics and detectors to infer the direction of gamma rays, so the concept is not totally novel. The new element is the recognition that a sensor consisting of ~ 10,000 ten micron plastic sheets, each ~ 1 m across, separated by ~ 0.1 cm gas gaps containing arrays of ~ 10 micron pitch metalized detectors could provide a very compact, efficient, and inexpensive spark chamber ("Nuclear Counter Proliferation with Gamma-Ray Color Camera Technology," 1994). It has been suggested that still simpler designs based on semiconductor technology could suffice for simpler applications (Wood, 1997).

The array would measure the gamma trajectory by detecting the charge from the secondary electrons produced by Compton electron in the gamma scattering. If it is possible to measure the direction of the Compton electron to ~ 1 milliradian, it should be possible to infer the initial energy of the gamma ray to within about 1 keV. That would take full advantage of the energy resolution of the detector and produce a comb energy filter with lines about as narrow as those of

the gamma rays from the weapon. It would support a energy-optimized range of about 300 m, which would support useful search rates from sensors mounted on trucks or air vehicles (Dickerman and Brackenbush, 1994).

While this approach is promising, acceptable performance from this simple detector array depends on its ability to determine the direction of the Compton electron from the gamma scattering to within ~ 1 milliradian, which is comparable to the expected scattering of the Compton electron from a few sheets of detectors. It is argued that centroiding the distribution of secondaries from the Compton electron can reduce this angular error, but that has not been established. It is also argued that using trajectories with many scatterings would "over determine" the gamma trajectory and improve accuracy, although it is not clear how that would come about. For the baseline design above to achieve its desired 300 meter range, it is be necessary to gain about a factor of 5 from both centroiding charge and trajectory over determination. Should either not prove possible, the filter would not achieve the angular and energy resolution required, and the range would degrade an order of magnitude to levels that would not support useful area search (Canavan, 1997).

Given detection, several improved techniques could be used to negate weapons that were not accessible, safe to defuse, or of known design. One is the used of very high velocity explosively driven projectiles. Such projectiles are well developed; their extension to higher velocities is not stressing. If successful, it should produce little or no nuclear yield; however, it is sensitive to uncertainties about the design of the device.

An alternative disablement mechanism, which has been studied less intentionally, is a thermal blanket or microwave source. While the usual disarm procedure is to escalate means as gradually as possible, for many weapons it is possible to surround them in a high temperature bath and boil or bake off the high explosive. This has the nature of a last-chance measure, but a simple one.

These measures assume that the device is detected and addressed on a time scale very long compared to that of firing and fusing, implosion, and yield. In some cases that might not be the case. One might still be searching for the device when its detonation sequence is initiated. Even then there is at least one concept that might prevent detonation. It is possible to detect the electromagnetic signature of the weapon's detonators, which is almost unique, at ranges of several km. The weapon could then be localized with differential GPS to ~ 1 m at 1 km ~ 1 mr, which is adequate for pointing a particle beam at the weapon to disable it. A ~ 0.1 A, GeV proton beam could preinitiate the weapon by flooding its pit with neutrons so that it would produce little yield. The approach is robust. It should work for Plutonium (Pu), Uranium 235 (U235), and weapons of unknown design, so long as they use simple firing systems to achieve High Explosive (HE) initiation and design approaches to criticality.

Why will it be successful?

The gamma ray color camera should be successful because it combines the three most useful features of a weapon: optimal spatial filtering to optimize the point source weapon signal versus the uniform distributed background; optimal energy filtering to optimize the weapon material specific line sources against the diffuse cosmic background; and the use of an uncharged gamma for long propagation converted to a charged Compton for ease of measurement in the detector array. There is some room for degradation in each of these areas.

If all were to work as claimed, the gamma ray color camera would use optimal spatial-color filtering to produce a sensor with high sensitivity, good mobility, and wide area search. It should produce such sensors with simple, inexpensive, fieldable components. The main remaining uncertainties could be removed by modest laboratory demonstrations.

Kinetic energy penetrator disablement should work for many designs because it is largely a matter of achieving a higher velocity than the implosion. There can be little argument over the a thermal blanket technique's technical effectiveness, as the DoD has accidentally "disarmed" weapons this way through accidental fires over the last few decades without nuclear yield. The issue is whether such a capability is needed for inaccessible, unfamiliar weapons.

The detonator detection-beam disablement is less developed. There is little question that the detonator signatures are detectable over several kilometers or that differential GPS could refine that to location measurements of ~ 1 m. The main issue is the practicality of the beam. The parameters cited above are those of current storage rings, which can be dumped on the time scales cited, with rather better accuracies than those required. Thus, the main issue is not whether such a device could be built or made sufficiently portable for search, it is whether the lack of such a last-ditch search and disablement capability is a serious impediment to civil-military search and neutralization actions.

If successful, what is the payoff?

The new detector technologies discussed above would permit rapid search at portals, securing of perimeters, and search of large areas for threats to military forces and urban populations. That would eliminate the threat of nuclear materials or weapons in those areas that could otherwise cause widespread confusion, create the possibility of massive damage, and open the way to blackmail of civilian and military operations.

The ability to disarm weapons of new or unfamiliar designs would reduce the potential for damage and increase the credibility of assurances to those in those areas. The ability to detect and disarm weapons hidden in the field would reduce or eliminate restrictions on operations and make the occupation of areas accessible to terrorist weapons psychologically feasible in the long term.

References

G. Canavan, "Gamma Ray Color Camera Performance Issues," Los Alamos National Laboratory report LA-UR-97-3458.

C. Dickerman (ANL) and L. Brackenbush (PNL), "Evaluation of LLNL Gamma Ray Color Camera: RDP Panel Task #4," Argonne and Pacific Northwest Laboratories report 1994.

"Nuclear Counter Proliferation with Gamma-Ray Color Camera Technology," Lawrence Livermore National Laboratory LLNL Doc.No.PhysBrief 94-004, 7 March 1994.

J. Vitko, R. James, D. Rakestraw, J. Schoeniger, S. Gordon, "Nuclear, Biological, and Chemical Detection Technologies," Sandia National Laboratories White paper, May 1996.

L. Wood, "Silicon-Based Gamma-Ray Color Cameras: High-Performance, Compact, Mass-Producible, and Cheap," Hoover Institution, Stanford University, 26 May 1997.

9. INITIATIVES THAT WILL ALLOW FOR MORE EFFECTIVE DETECTION AND MITIGATION OF ATTACKS ON THE DEFENSE INFORMATION INFRASTRUCTURE (DII)

What are we trying to do?

The objective of the initiatives that are outlined here is to provide more robust protection of the Defense Information Infrastructure (DII) against attacks by terrorists that will result in the Destruction, Disruption, Degradation, Denial and Exploitation (D4E) of data bases and communication links of the Department of Defense. These initiatives should provide more effective means of detecting and mitigating the effect of attacks on the DII .

How is it done now?

In recent years, the problems associated with protecting the DII against attack have received much attention. The concern of designers of DoD information systems has been to defeat intrusive attacks which may result in the destruction and exploitation of vital data files and to defeat attacks that may result in the denial of information services. Denial of service attacks include any attacks that will limit the DoD's ability to transfer information electronically. Such attacks may include the jamming of communication links (both military and civil) and attacks which saturate the ability of terminals to receive and process incoming data. Other forms of attack may include message alteration or the insertion of false messages by someone who is successfully masquerading as (or actually is) a valid user of a DoD network. Such attacks may result in the degradation of the integrity of some DoD data bases and files, with the associated possibility of inappropriate actions being taken.

For systems that support extremely critical DoD missions the first line of defense is total electronic isolation. This approach which, in effect, establishes an "airgap" between computers is equivalent to keeping all files in a safe which in turn is kept in a guarded vault that can only be entered by trusted personnel with special security clearances. In circumstances where extremely high security, and system reliability and availability is required, the approach is to establish a network of computers and communication links that is isolated from electronic contact and connection with all other systems. This implies that sufficient physical security will maintained to ensure that access to restricted terminals or work stations by unauthorized users will be prevented. It also implies that dedicated encrypted communications links are used whenever data is transferred from one system node to another system node.

Where physical access to terminals and workstations is not, or cannot be monitored, access control is maintained through the use of passwords that allow a user with appropriate authority to gain various system privileges and accesses.

Within the DII, systems that are called firewalls and routers are widely used. These systems provide protection to a local area network (LAN) of computers through the use of logic tables that, in effect, decide whether or not access to given files within a protected domain should be granted to a remote user. Firewalls and routers can provide effective protection if the logic is sufficiently restrictive and is changed frequently enough so that a would be intruder cannot

deduce the decision logic being used, or defeat the system by eaves-dropping and learning currently acceptable passwords.

The designs of firewalls and routers are evolving. The trend in both DoD and commercial systems is to construct logic tables that require dynamically changing passwords, and to employ threat responsive barriers. In systems that incorporate threat responsive barriers, whenever an attempt at unauthorized entry is detected, the requirements for entry into the system are made more restrictive automatically.

Encryption is used to protect the confidentiality of transmission of classified information within a DoD network. In effect, the DoD operates a classified version of the Internet for the exchange of classified data. Although encryption is certainly an effective means for accomplishing the protection of confidentiality, it is not employed in networks where the data being transmitted is unclassified. For all practical purposes, unclassified DoD data is transmitted over the Internet.

Anti-virus software programs are in wide use in the DII, in private and in commercial networks. They provide a capability to recognize and reject the most common forms of viruses or malicious code. As such, they are reasonably effective filters against such attacks. However, there are well recognized limitations in the capabilities of such software. Viruses and malicious codes that contain the attributes that are detected by such anti-viral software can be defeated. Those that are not detected pass through the barrier.

Data base and message integrity is established by a variety of techniques. Data bases are copied to isolated back up files and these files are used to determine if files in current use have been altered. Error correction codes and check sums are used to protect incoming data streams and messages against corruption by system noise or unauthorized modification. Also, techniques are available, on a limited basis, that establish non reputable electronic signatures

In the final analysis, the defense of most DII networks and communications links is strongly dependent on the skills and training of their network administrators. These administrators are trained to follow a set of rules that establish access standards. They do have some software tools that allow them to detect some intrusions by unauthorized users, and they sometimes have the authority and software to modify access privileges for individual users, or to modify the logic tables of firewalls and routers.

Before a system is certified for inclusion in the DII, it must be certified as being in compliance with existing standards for system protection. Although systems must be recertified periodically, configuration control is not maintained on a continuous basis.

What are the limitations of current DII protection techniques?

When we assess the limitations of the techniques currently employed to defend the DII, we must recognize that if available technology is effective against the known set of current threats, it may not be robust against future threats. Simply put, continuously evolving technology precludes a permanent fix. New techniques that may evolve in the future may render currently available defensive techniques inadequate. When we speak of limitations, we are discussing the limitations of the protection afforded by current defensive systems against current threats.

DoD networks that are deemed to be essential to the support of certain critical DoD missions are, in fact, extremely robust against attack and exploitation. This robust defensive posture is achieved at a considerable cost. The cost is severe enough to preclude the wide spread replication

of these techniques through out the DII. The costs that are incurred in the operation of systems that physically limit access to terminals and work stations are substantial, as are the costs of the operation of the security systems that decides which individuals are trustworthy enough to allow access. The final penalty that must be paid in the use of such isolated systems is the costs that are incurred in the operation of stand alone systems

As pointed out above, passwords are used extensively for the protection of the DII. Password protection can vary from trivial to moderately effective. Where the password system permits trivial passwords (e.g. 'DICK" or 'JANE') minimal protection is provided. Where more complex passwords (e.g. "#9JW %A{*BL&Q17 T") are required, slightly better protection is afforded.

A favorite trick of a would be intruder is to eavesdrop on a communications link and to copy the pass words used by remote users. Few if any tools are available that tell a network administrator if anyone outside of the system's firewalls is engaged in the passive monitoring of incoming or outgoing traffic. Consequently, any password protection system will become vulnerable to eavesdroppers if it used often enough. Thus, DoD systems which do not issue new passwords after selected periods of time (minutes, hours, or days) or after a password has been used a specified numbers of times, tend to be vulnerable to snoopers or unauthorized intruders.

In practice, unauthorized users easily and frequently penetrate DoD systems that have poor password protection discipline. Although these penetrations tend to occur predominantly in networks that contain unclassified data bases, penetrations have occurred in classified networks. Frequently, when unauthorized intrusions take place, they are either not detected or reported. From the stand point of a terrorist, the disruption or exploitation of an unclassified data stream may be as effective a means of accomplishing his or her objectives as the disruption of a classified data link.

Intrusions into the DII sometimes occur as the result of the establishment of unauthorized links by authorized users. Although DoD users may establish these ad hoc paths for non malignant purposes, or even inadvertently,, they serve to bypass existing protective filters and barriers and can result in unintended penetrations of classified networks by unauthorized users. In some DoD systems, network administrators do not have tools that allow them to scan, on a continuous basis, for the existence of unauthorized connections within a local network. A more general deficiency relates to the fact that when an authorized user is allowed access within a network, the network administrator has a limited set of tools to allow the determination of whether or not the person who has logged in from a remote computer has any unauthorized connections.

An alternate but parallel limitation of current protection systems is that they transmit much of their data over civil telecommunications links which are susceptible to intrusion, snooping and denial of service attacks

Once an unauthorized user has penetrated the protective barriers in the DII, it is extremely difficult either to detect entry into files or to limit access to particularly sensitive files. Currently, DII system administrators have only a limited set of intrusion detection tools available to them. Few, if any, of the available tools will provide automatic alertment of attacks by sophisticated intruders. As a consequence, network administrators frequently must infer that an attack on the network is taking place on the basis of such indirect evidence as may be available to them. Since some network administrators are better trained and more experienced than others, the ability to detect intrusive attacks is quite variable across the DII.

If an intrusion into a file has occurred, it is often difficult to re-establish the integrity of the data in the file. If the attacker has replaced every 3 in a file with a 5 and every 5 with a 3, the damage will be hard to detect with out making a detailed comparisons with the data in a trusted archival file. Generally, such an attack will defeat the error correcting codes and check sum protection systems that that are in place.

To the extent that the DII is robust against attack, we must recognize that much of the existing strength of the DII defense resides in the skills and dedication of network administrators. They enforce the rules, set up procedures to control accesses, change logic tables in firewalls and routers, and maintain the software of the operating system. Unfortunately, such administrators are personally vulnerable to attacks that may lead to their compromising the system. They (or their family members) may be captured and forced to reveal the logic and access rules of the protective barriers. Also, their trustworthiness might be compromised by bribery or blackmail.

The DII is susceptible to denial of service attacks in the sense that the links that provide connectivity between critical nodes are often single communication paths (copper wire or optical) that can be severed or saturated with little effort by a knowledgeable terrorist group.

As pointed out above, a large component of the protection of the DII resides in the use of logic tables for firewalls and routers. In principle, if an attack is detected, the logic tables can be reprogrammed. Unfortunately, with most of the firewalls and routers currently used by the DII, such reprogramming does not take place automatically on detection of an intrusion or even on warning of an attack.

As with any complex system that has evolved over time, the DII contains many components that are the results of previous procurements that still function well enough to warrant their continued retention . Unfortunately, these so-called 'legacy' systems often contain major susceptibilities to intrusive attack. Until they can be eliminated or retro-fitted with protective software, they will continue to present an inherent system weakness.

What is the new approach?

Information technology is being developed at an extremely rapid pace in response to the ever expanding commercial demands. As a result, the technology necessary to defend the system must also be developed on a continuous basis.

There is no single new approach. A number of broadly based programs are currently being pursued by both DoD and by industry. These approaches, which should provide a significant increase in the robustness of the DII, include:

- Improved barriers that respond automatically to the threat of attack
  - Policy driven access control
  - Software modules or 'wrappers' for the protection of legacy and commercial off-the-shelf (COTS) components
  - More robust protection of the communication infrastructure
- Enhanced intrusion detection and response systems
  - Improved coordination of detection and response functions

- Software to provide better cooperation between intrusion detectors and boundary controllers

- New adaptivity and resource management techniques
- Employment of artificial diversity

The first of these approaches involves the employment of access control barriers that are not static. The concept here is to have controls that change automatically in response to intrusion or to the detection of an attempted attacks.

This approach may be considered to represent a form of policy based generation of access controls. The use of distributed protected enclaves is envisaged, where collaborative decisions between enclaves determines. Protection boundaries will include a dynamic collection of users, hosts, and domains within hosts. In this approach, distributed sets of users operate as if they were behind a common security perimeter. Within an enclave individual files will have labels that indicate sensitivity, integrity, etc. The use of these labels (Object types) allow valid users controlled but shared access. There will be mandatory controls that will specify the access rights of individual users. Policy will be specified via a series of rules called the Domain and Type Enforcement Language(DTEL).

The DII, as it currently exists, is heavily dependent on fragile COTS components and on legacy systems that will not be, or cannot be, replaced in the near future. Unfortunately, there is no current means to evaluate the degree of resistance or vulnerability to attack of such components or systems. New approaches are being developed for the insertion of barriers to attack into COTS and legacy systems. The new approaches that are being implemented involve the development of plug-in software "wrapper" functions. These involve:

- Intelligent filtering, electronic signatures, encryption and dynamic access control
- Modern message authentication techniques to assure message integrity
- Group communication rules and standards and packet switching
- Software systems that will monitor the use of system resources and improved management protocols
- Inter computer node service and resource negotiation tools

Systems are under development that will improve the protection of the communications infrastructure. In these classes of approach a master computer node called the Domain Name Server (DNS) will retain records for encryption keys. The DNS will authenticate resource records using digital signatures based on these keys. A higher level server will perform the key authentication function. Routers will be developed which authenticate routes based on digital signatures. All communication will be encrypted and both snooping and spoofing should be either eliminated or greatly reduced.

As discussed above, system administrators need better tools to help them detect intrusions and attempts at intrusion and to provide them with an automatic capability to take actions to neutralize the intrusion or attempt at intrusion. The current concept is that detection/neutralization tools will and must be an integral part of the design of all new systems.

As an example, a set of sensors is being developed that will detect browsing attacks or attempts at penetration by users without a properly encrypted identification code. When these sensors detect such an attack, the levels of protection and robustness of the network and its essential systems will be increased automatically. A "fish bowl" that simulates the existing file set within the network will be created automatically and the attacker will be diverted into it. The purpose of this diversion is to make the would-be intruder believe that the system's firewall has been successfully penetrated, and to allow his or her subsequent tactics to be observed. In this approach, the most important development will be the software that recognizes browsing and intrusion attempts and the software that will collect and display the history of all past attempts at access to the system by unauthorized users.

Other approaches to solving the problem of intrusion detection involve new methods to:

- Detect highly unusual events or combinations of events using statistical methods, neural networks and machine learning
- Detect activity outside of prescribed bounds
- Use new knowledge based analysis techniques

Denial of service attacks continue to be a vexing problem. There is no complete solution to the problem. Administrative solutions, such as the elimination of dependence on single wire or single channel communications systems, along with the extensive use of both packet and circuit switching, will certainly help to reduce the problem. Denial of service attacks are also being addressed by the development of tools which can trace a path back to the attacker. If an attacker's point of insertion into a network can be located, the attacker can be bypassed, isolated, and if legally feasible, be responded to.

New adaptivity and resource management techniques are being developed. The approach is to develop a capability, such that when unanticipated compromise of resources, system failures and new task arrivals occur the system will automatically direct network communication and computational resources to the most important activities. The premise of this approach is that adaptive architectures for survivability requires decentralized control which in turn implies that:

- Modules will control and will be responsible for the protection of the resources they control
- Modules will be designed to make local decisions that promote the quality of system wide results
- Decision quality does not require massive communication with
- other modules

In the area of artificial diversity DARPA is supporting efforts that will help to provide a robust defense for the DII. Diversity reduces overall losses in that it provides variability hedges against unknown means of attack. One approach is to assign time varying tasks to different nodes of the network. A system with a time varying architecture is much harder to attack than a system with a static architecture. Diversity can also be accomplished by use of :

- Self specializing software with a capability for data driven optimization, re-configuration and algorithm selection
- Linkers and installers that produce randomized load images
- Compilers that vary block placement and code sequences
- Functional and analytic redundancy with the same capability provided by many different individual components .

The potential vulnerability of individual system administrators or venal /disgruntled users to coercion or corruption cannot be eliminated completely. Never-the-less, damage can be mitigated if systems are designed so that no individual user or system administrator, has complete knowledge of the logic of the defensive measures that are in place, and if these measures are changed frequently and routinely, so that the value of an administrator's or user's information will attenuate rapidly with time. Such administrative actions would at least constitute an effective form of damage limitation.

The Panel is enthusiastic about the broadly based approaches being used by components of the DoD and industry, and hopes these efforts will continued. The Panel believes that certain segments of the work outlined above should be developed at an accelerated pace. As an example, the diversity tool kit that is being developed under DARPA sponsorship is scheduled to be fielded as a prototype in 2003. The Panel recommends that funding for this project be increased to allow the deployment of that prototype in 2001. The payoff is too large to allow anything other than a "high-speed" effort.

Why will it be successful?

The Panel is confident that these new approaches will succeed because of the structured technology development efforts being accomplished by both DARPA and industry. The approaches address the infrastructure not just a system or network. We recognize that infrastructure protection must be based on effective considerations in addition to the normal design goals of efficiency. However, a decentralized architecture is proposed. Modules would make local decisions that promote the quality of the entire system; but that does not require massive communication among the modules. The system has both functional and analytic redundancy. The entire approach recognizes that it is impossible to pay the cost of avoiding risk to the DII. Therefore, risk must be recognized and managed. The panel supports these efforts but recommends some additional steps. The DoD should help conduct vigorous interagency coordination to allow the development of proactive measures to protect. Also the traditional weak link - the person - must be addressed specifically in developing solutions. Technology efforts can succeed only if they are integrated with policy, operational and people aspects.

A fundamental and essential underpinning of any proposed technology base for designing and implementing large-scale, robust, survivable distributed systems is a suite of design tools. Ideally such a set of tools would afford designers and implementers a means for describing, constructing and verifying the anticipated behavior of a complex system at all levels of abstraction. The design technologies must be capable of capturing behavioral descriptions, system properties and design descriptions in ways which enable the timely creation and performance validation of a given system implementation. Such a capability is needed because it is impossible to either

anticipate or exercise all possible interactions among the large number of constituent elements in any system of real-world complexity.

If successful, what is the pay off?

By focusing the technology and architectural effort described above the DoD can improve its ability to manage the information warfare challenge to the Defense mission. The Department can also enhance its ability to play a major role in countering information warfare attacks on national centers of gravity. However, the major benefit of mounting a strong technology-driven effort as described above is deterrence. When it is recognized that the essential procedures, processes and mechanisms are in place to effectively and efficiently defend against information attacks, there will be little incentive for adversaries or transnational terrorists to pursue them.

10. INITIATIVES ASSESSMENT

Figure 1 contains an assessment of the impact and the degree of technical difficulties of the silver bullets discussed in this section.

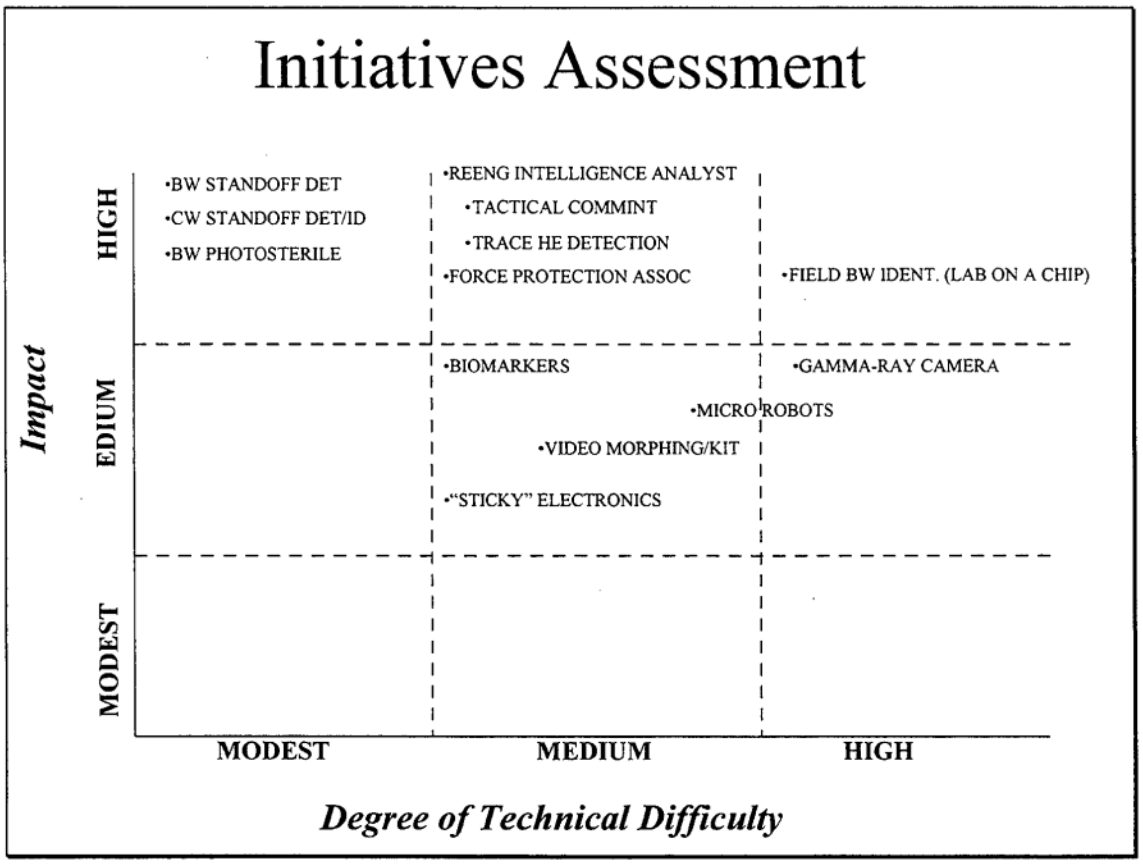


Figure 1

REPORT OF THE COMPETENCY PANEL ON OPERATIONAL INTELLIGENCE

Panel Chairs

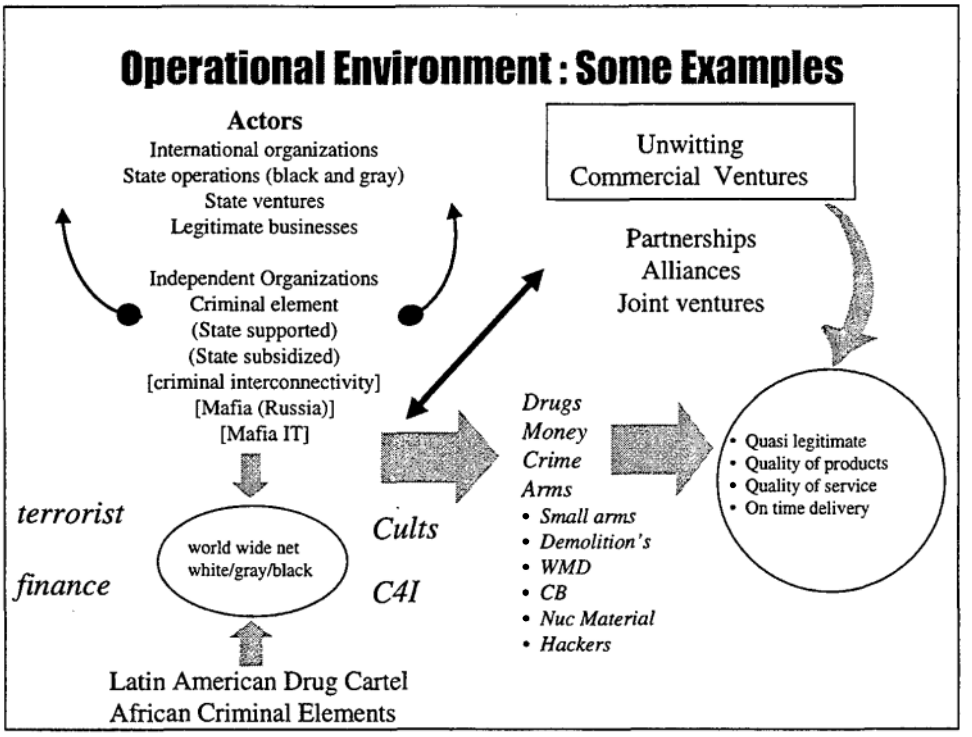
Dr. Joseph Braddock
BG Richard Potter, USA (Ret)

Panel Members

Ms. Rebecca Beaty
LtGen Jim Clapper, USAF (Ret)
Dr. David Dye
Mr. David Geary
COL Kenneth Getty, Jr. USA (Ret)
Mr. Charles Hawkins
COL Thomas O'Connell, USA (Ret)
Dr. Dennis Polla

Government Advisors

Maj Owen Devereux, USMC
Ms. Deborah Dewey
COL Don Faint, USA
CDR Bernie Hamm, USN
Mr. Wade Ishimoto
Mr. Paul Kozemchak
Ms. Beth Larson
CAPT Nelson Litsinger, USN
Mr. Theodore Royster
Mr. David Sanford
Col Stan Shinkle, USAF
Dr. Michael Shore
Col John Tempone, USMC
COL Butch Teston, USA
Mr. Thomas Warren



Operational Environment

Unlike the situation which generally applies in cases of armed conflict, transnational threats flourish in an extremely complex and murky environment. DoD defines terrorism as the calculated use of violence or threat of violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious or ideological. The terrorists could be part of an international organization, a state operation, or state ventures, or even part of a legitimate business. For the purpose of this study, "terrorists" refers to all actors involved in the spectrum of transnational threats.

They could be based in criminal elements which might or might not be state supported or subsidized. They might be part of a gangster government as in the case of the Mafia in Russia.

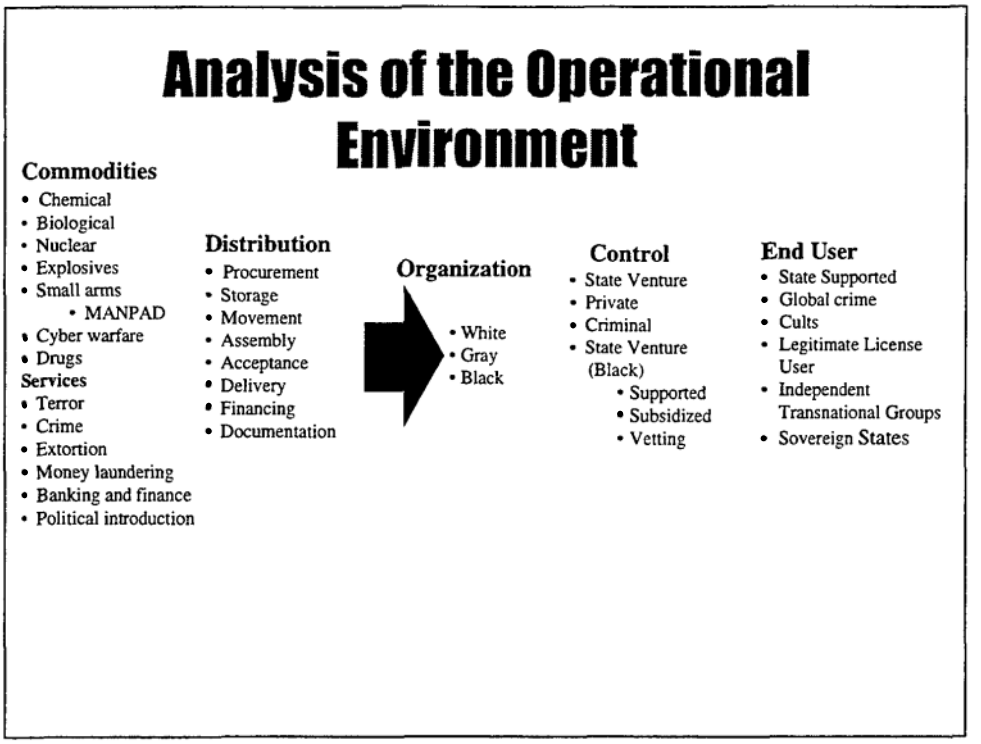
In some cases, terrorists are part of quasi religious groups or clandestine independent organizations even more insidious would be those sponsored by drug cartels or by African criminal elements which have taken over governments.

Commercial activities are often part of the terrorist environment because there are many legal activities which can unwittingly support terrorism. Because of this, partnerships, alliances and joint ventures may occur involving terrorists and purely legal operations.

The means chosen by terrorists are now substantially more diversified than they have been in the past. Thus far, with the exception of the incident in Tokyo, small arms and demolitions have been the principal means. In the future, the means could be chemical, biological, and nuclear weapons or the dispersion of radioactive materials.

Finally, terrorism can be supported and enhanced by information warfare. Today's hackers and insiders are an example of this although they are not identified here as part of terrorist activities. For purposes of the Operations/Intelligence Panel's work, we have set aside information warfare as an activity which we will not explore. However, we would certainly support the idea that terrorists could employ information warfare for a variety of purposes. These could include using it to a) obtain funds, b) disrupt response during an incident, or reduce response consequence activities, or c) wreak havoc or governmental collapse as a means of and by itself.

States, organizations and individuals hostile to the United States may enhance their ability to operate transnationally through formal and informal coordination means. Formal coordination means include state operated chains of command and control as well as multidimensional and electronic communication modes. Informal means may rely on sophisticated measures to achieve objectives but are not formally established or long standing in duration.



Analysis of the Operational Environment

The panel sought to categorize and characterize the elements of transnational threats for purposes of study and analysis.

The categories chosen were

a) commodities,

b) services,

c) distribution,

d) organization,

e) control and

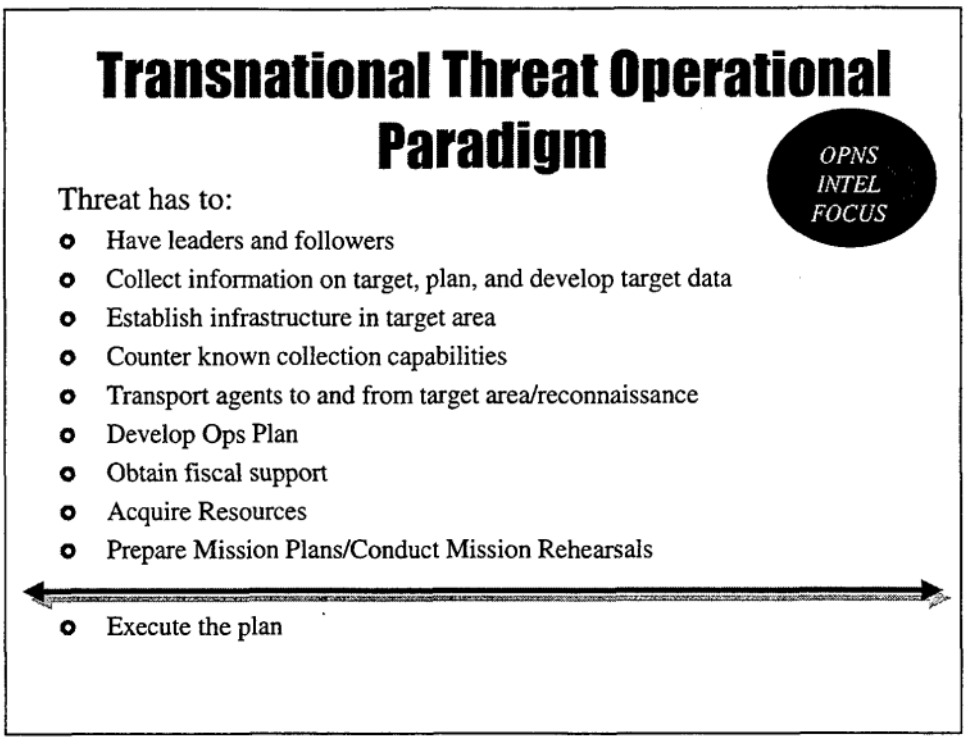
f) end-user.

Commodities include various means such as chemical, biological, nuclear, conventional explosives, and man-portable air defense systems. Services are either direct or supporting. These would include the conduct of the actual incident and supporting activities such as crime and extortion, money laundering, and political activities.

Distribution includes all of those things which involve procurement of the means (weapons), storage, movement, and ultimate delivery.

The organization may be an open organization such as the Palestine Liberation Organization. It could also be gray or completely black and hidden. Its control may be exercised through a state, a private activity, criminal activities, or a form of state venture. An example of this might be a Mafia activity supported from Russia without necessarily having the support of the Russian government. Vetting is extremely important. Our analysis suggest that these groups will use extreme measures for vetting which will make penetration of the group difficult. These extreme measures could include forcing new members of the group to conduct crimes including murder.

The end-user is extremely important because his intent is served by the action. In many cases the intent is political. Sometimes it is revenge. In this regard, the United States is particularly vulnerable since it has its forces and civilians based overseas in many potentially hostile areas. In a sense, they operate in a sea of hostility in an undeclared war.



Transnational Threat Operational Paradigm

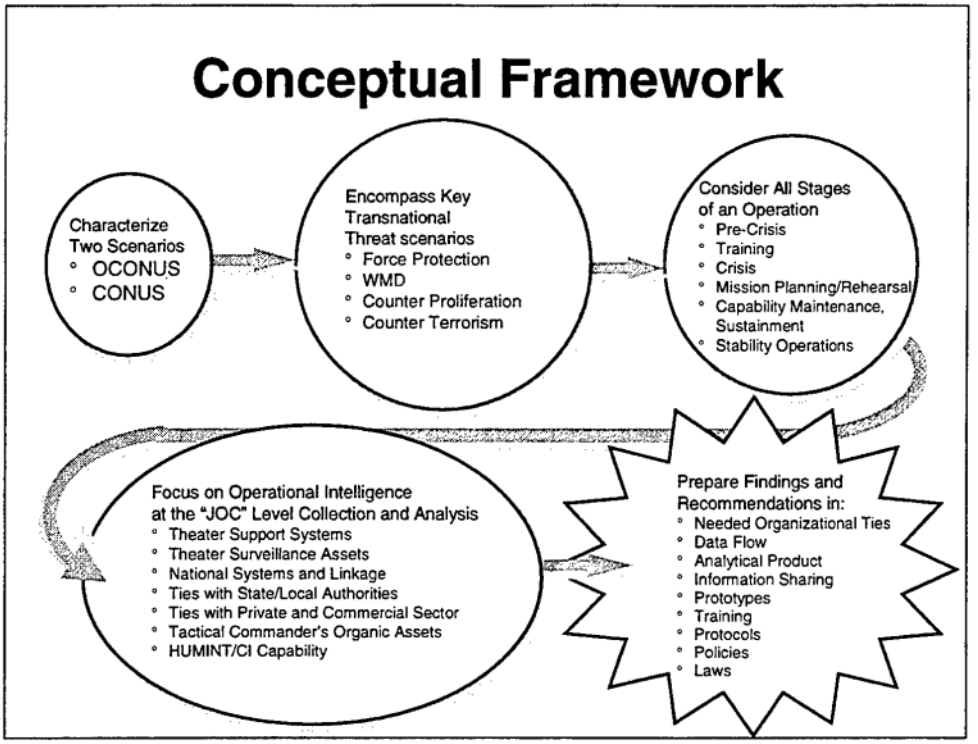
In order to combat the transnational threat or to mitigate its effects should it succeed, its operational paradigm is defined below.

There must be leaders and supporters. They must organize information and develop essential target information. They must establish an infrastructure in the target area and counter known collection capabilities. Their agents must travel to and from the target and conduct reconnaissance.

An operational plan has to be formed. Money is needed to support the plan and purchase weapons, transportation and operational support sites. The mission must be prepared and rehearsed. Ultimately, the mission has to be executed.

Regardless of the type of operation the threat intends to accomplish, the actions above the line is when the threat is most vulnerable to all source collection efforts. It is where the US must concentrate its efforts if it is to preempt or prevent incidents. This is where operational intelligence has its greatest value.

Once the above line actions are completed, the US is generally limited to some form of reactive crisis or consequence management.

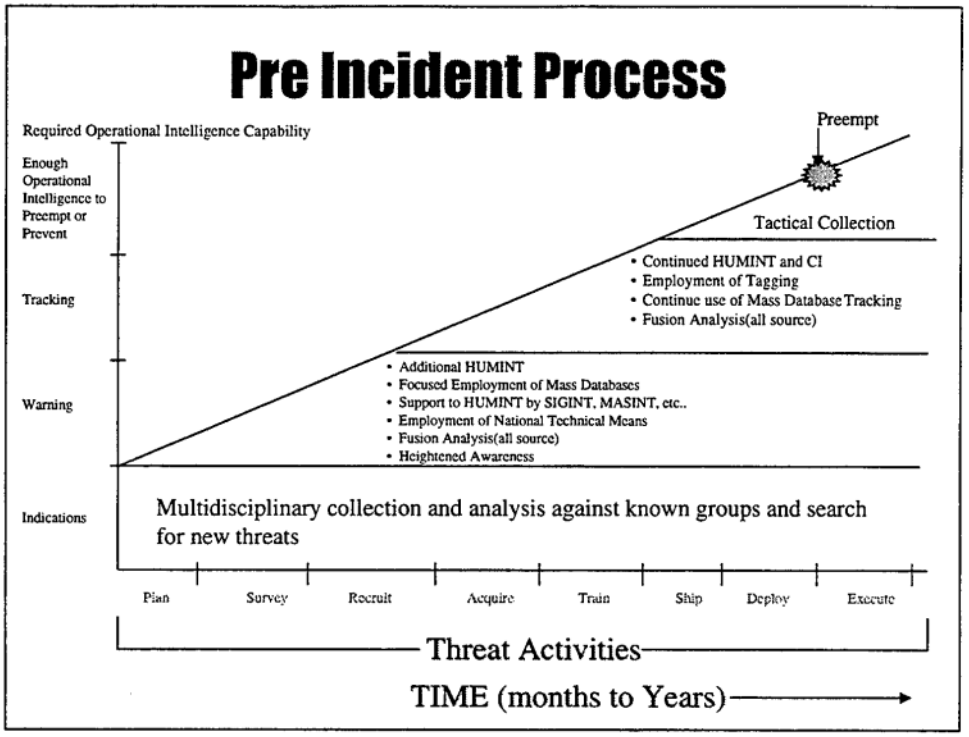


Conceptual Framework

The analysis is based upon consideration of two transnational threats scenarios. One is in the continental United States (CONUS) and the other is overseas (OCONUS) . In addition, the panel reviewed a variety of scenarios that involved a) force protection, b) countering of weapons of mass destruction, c) countering proliferation, and d) countering terrorism. Also reviewed were successful examples of prevention such as measures to limit and deter aircraft hijacking. These were all done in a lessons learned sense.

All stages of the transnational threat operation were considered in order to determine where there were shortfalls and where improvements would be needed. The effort focused on operational intelligence at the joint level employing national systems but placing heavy emphasis on theater support and surveillance systems. Additionally, ties that would be made with national agencies and with state and local authorities were considered. It was assumed that the tactical commander would have organic intelligence assets. An extensive effort was put into examining multidisciplinary intelligence collection capability and its potential in these circumstances. The panel considers a robust overt and clandestine Human Intelligence (HUMINT) capability as an absolute necessity for combating transnational threats. This is the case because of the small signature and narrow window of collection opportunity associated with many segments of the operation and the attendant "noise" masking operational actions.

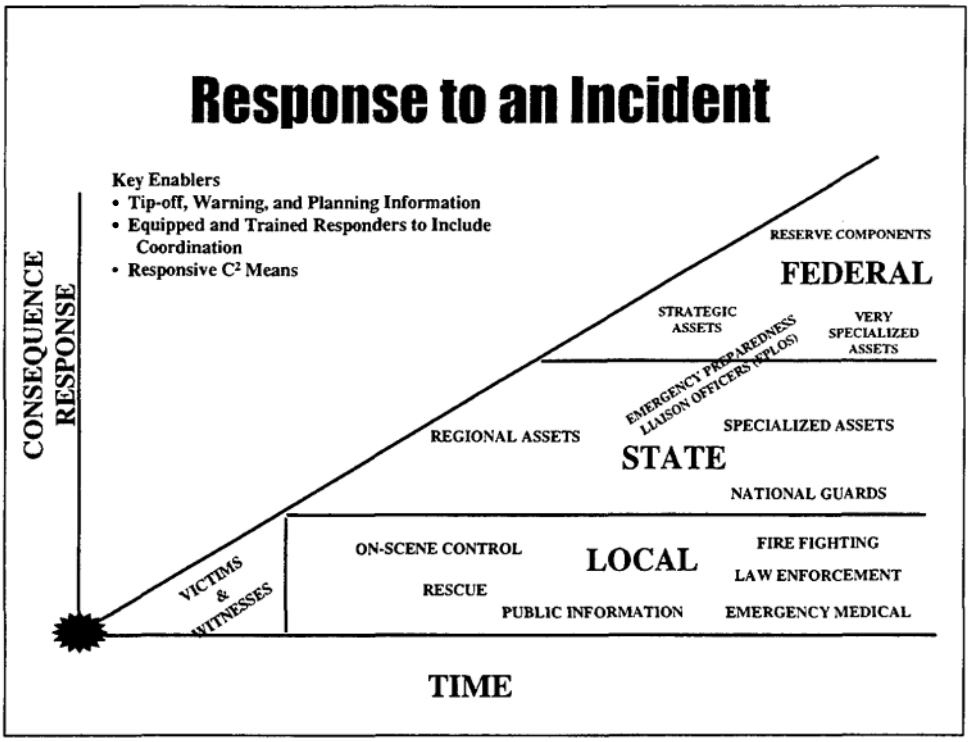
The intent of this conceptual frame is to reach a set of conclusions, findings and recommendations which should be given priority.



Pre-incident Response

Operational intelligence is most valuable prior to an incident because it is the key enabler to preemption or prevention. In the months and years that lead up to an incident, intelligence offers the opportunity to find out the who, the where and the when. Unless we are dealing with circumstances involving a lone terrorist; who has no group connection; and who has sufficient resources to carry out the desired activity, it will generally take a substantial period of time to organize the planned terrorist incident.

To start, intelligence collection should be mounted against known groups. The Defense Science Board Task Force received briefings on the size and extent of these groups. Multidisciplinary analysis with primary emphasis on HUMINT is most valuable. Enhanced liaison and intelligence sharing with other agencies is crucial throughout the process. HUMINT/Counter Intelligence (CI), to be effective, requires close and continuous support from other collection disciplines.



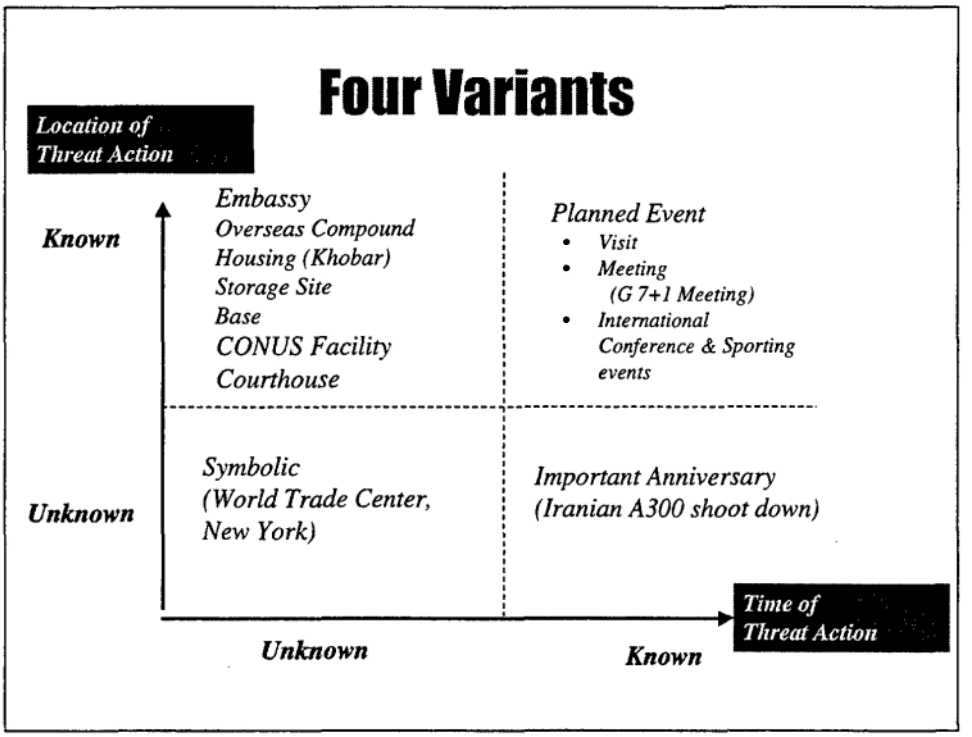
Responses to an Incident

If there is some intelligence indicating an incident may occur, there may be time for response preparation, planning and rehearsal.

The chart describes the generic buildup of activities following an incident. The assumption is that preemption and prevention has not occurred, and the situation requires a consequence management response.

The first responders will be local; rescue teams, fire fighters, police, and emergency medical services. Agencies use existing procedures initially, but may be unaware of the true character of the incident. As more support is deemed necessary, state, regional and federal elements will respond. The combined assets are employed to mitigate the incident and restore normal order to the extent possible.

The role of operational intelligence is to support preemption, prevention and response preparation to incidents. Importantly, each of the depicted agencies are sources of information.



Variants

This chart describes four variants to deal with the location and time of the threat action.

The chart is divided into four quadrants; along the vertical axis, the location of an incident yet to happen is either known or unknown. Along the horizontal axis, time is either known or unknown. Starting with the uppermost right hand quadrant, a planned event is an example of a known-known case. A planned event could be a state visit or a meeting such as the group of 7+1 in Denver. Moving to the left, an incident at a known location but an an unknown time may occur. Examples would be an Embassy, or a housing compound such as the Khobar Towers.

In the lower right hand quadrant time is known but location is unknown. An example of this is an important anniversary such as the shoot-down of the Iranian airliner over the Persian Gulf.

Finally, in the unknown-unknown case is the World Trade Center incident. Another example is the chemical incident in the Tokyo subway system. It is obvious that the worst case is the unknown-unknown case.

Observations

- Known time and location cases are clear
- Known location cases are less straightforward
  - Know where to search
  - Operational and tactical indicators and tracking are advantaged by terrain, event, and long term preparations
- Known time cases are more complex
  - Operational and tactical indicators and tracking depend on local capabilities
- Unknown location and time are most complex
  - Requires broad search using indicators and conversion to tracking where threat is hiding in the noise
  - Addressing and improving Op Intel for this case will improve all other cases

Observations

In those cases where both location and time are known, operational intelligence can be focused, and all agencies can perform necessary coordination. The nation's capability has evolved for many years and, while improvements in operational intelligence can be made, there are now substantial capabilities to support preemption or reaction.

Where only the location is known, the situation is not as simple as the case when both location and time are known. There must be continuing collection and analysis without certain knowledge that an incident will occur. Location provides a narrower zone of search and relies heavily on close-in operational intelligence.

The known time cases are more complex. Any tip-off or tracking information can be of great value. It also focuses and makes more efficient the use of available assets.

The most complex situation is where both the time and location are unknown. Improvements in HUMINT/CI and innovative Signals Intelligence (SIGINT) collection are absolutely vital. Multidisciplinary collection and analytical centers of excellence must support a significantly enhanced intelligence capability.

Challenges and Constraints

- Challenges
  - Different cultures : operational intelligence requirements vs. law enforcement requirements
  - National cultural bias against HUMINT
  - Legal, social and societal implications of engaging in certain intelligence activities (human/civil rights violations)
  - DoD being seen as "Big Brother"
- Constraints
  - Statutory guidelines for activities
  - Security and information flow
  - Integration of information sources and interoperability of information flow

Challenges and Constraints

There are substantial differences in the functions and objectives of the organizations which must respond to transnational threats.

Because of fundamental differences in purpose, law enforcement and defense department agencies approach the collection of information differently. Law enforcement focuses on evidence collection and ultimately apprehension and conviction of the perpetrators. In intelligence operations, evidence and crime scene protection are not paramount considerations. The difference in military and law enforcement philosophies present a set of challenges and constraints to the interagency process.

Among the constraints shown in the chart, statutory requirements and interpretations affect collection, analysis and dissemination. Integration of information sources, security, and interoperability of communication systems continue to hinder cross-agency responses to transnational threats.

Current DoD Posture

- Laws
  - Array of protocols, interagency agreements, executive Orders, legal findings, evolutionary legislation circumscribes operational intelligence
- Policy, Regulations and Directives
  - PDD 39 assigns interagency responsibilities
  - National and international constraints on use of intelligence activities
  - Executive orders defining guidelines for collection activities
- Contingency Plans
  - 0300 and 0400 have extensive intell annexes and guidance
    - ⇨ Tactics, Techniques and Procedures
      - Joint doctrinal literature
    - ⇦ Training, Education and Exercises
- Readiness Posture
  - National Technical Means, procedures are in place for counter-terrorism/counterproliferation
  - HUMINT/CI capability must be strengthened

Current DoD Posture

The Department of Defense carries out its intelligence activities on the basis of laws, executive orders, inter-agency agreements and a variety of protocols. These are continually modified and upgraded as a result of legal findings and evolutionary legislation.

Policies, regulations and directives, form the operational envelope for intelligence activities. These include procedures for approval of activities.

The Department of Defense, has extensive operational plans with intelligence annexes. The regional Commander-in-Chief (CINCs) have responsibilities concerned with terrorism, weapons of mass destruction, counter proliferation, and force protection. CINC Special Operations Command (USCINCSOC) as a supporting CINC is assigned counterterrorism and counterproliferation as a core task.

The DoD has extensive assets at its disposal and also tasks and works with other agencies who have collection and analytical capabilities. The substantial operational intelligence capability which results from this is focused, tailored and employed. However, major improvements in HUMINT are required.

Current Approach to Operational Intelligence

- Conventional/nuclear warfare legacy
  - Grew out of bipolar well-defined threat
  - Focus on mid to high end of conflict spectrum
  - Long-term analysis of trends and activities
  - Explicit planning process
  - Emphasis on national/strategic response
- Less emphasis on transnational threats, military operations other than war, and military operations at low end of the conflict spectrum
  - Multiple, diverse and ill-defined threats
  - Lack focus on low to mid intensity conflict spectrum
  - Long-term collection and analysis shortfall

Current Approach to Operational Intelligence

The current intelligence system and its operational intelligence characteristics are the product of a long evolution. During the Cold War, the priorities for intelligence focused on three principal matters: the state of Soviet nuclear capabilities; those activities which might cause operational and technological surprise; and the status of Soviet general purpose forces and their specialized components. Because of the nature of the Soviet Union and its military forces, it was possible to develop a very robust capability in which small intelligence details could be examined in a much larger context. This strong collection capability provided the foundation which gave the United States an ascendancy in intelligence matters.

This approach was appropriate to a well defined threat which focused on the mid- and high-end of the conflict spectrum. Capabilities were continually improved, with emphasis on explicitly planned national, international and strategic responses.

Little emphasis was directed to transnational threats, military operations other than war, and other military activities at the low end of the conflict spectrum. When such incidents escalated the existing intelligence structure was tailored on an ad hoc basis to meet requirements. What is now required is a more balanced, focused approach.

Options

1. Change nothing
2. Change the process within existing organizations
   - Establish transnational threats as a priority
   - Redirect intell process and emphasis
   - Change investment strategy - renewed emphasis on HUMINT/CI
3. Assign authority and responsibility to a single organization
   - Intell Community "Centers" are one model - but do they work??
4. Establish DoD intelligence" Mission Area" for transnational threats
   - Naval Maritime Surveillance Model for transnational threats
5. Assign responsibility for transnational threats to a CINC

Options

Option 1 - Change nothing. Continue to use the existing system and allow for the emphasis given to transnational threats to gradually make improvement.

Option 2 - Change the process within existing organizations. Establish transnational threats as a priority. This issue will require a change in investment strategy and renewed emphasis on special collection and HUMINT.

Option 3 - Assign authority and responsibility to a single organization. There are centers of excellence for other challenges that could be used as a model. Considering the scope of transnational threats, this center would require substantial resources

Option 4 - Establish a Department of Defense mission area for transnational threats. The Navy currently runs a Maritime Surveillance Center which could be a model.

Option 5 - Assign responsibility for transnational threats to a CINC. This is an evolutionary solution and which has enjoyed successes in the past.

The Panel considered options 2 and 5 the most viable.

Desired Capabilities

- An intelligence process that:
  - Addresses non-traditional target sets, exploits few identifiable signatures
  - Must support implementation of countermeasures, preemption, prevention, interdiction, apprehension and, if needed, retaliation
  - Responds quickly
  - Exploits all sources
  - Reaches first responders at the lowest level with immediate warning and intelligence
- Collection assets
  - Greater emphasis on HUMINT/CI and innovative SIGINT and MASINT; overt, passive and clandestine collection
  - Create the Secure Transnational Threat Information Infrastructure (STII).
- Intelligence analysis and processing
  - Much greater emphasis on analysis of mass data sets looking for subtle correlations
  - Centers of excellence
  - Integration by function or topic not necessarily geography
  - Designed to serve operational and tactical commander
  - Fusion/integration at the operational level
  - Must provide adequate resources to conduct long-term in depth analysis
- New dissemination structure
  - Cross-jurisdictions (combined, joint, state, and local)
  - Transcends current communications problems
  - Highly distributed; operational and tactical users pull data they need easily and quickly

Desired Capabilities

The desired capabilities include an improved intelligence process, expanded collection assets, improved intelligence analysis and processing and an improved dissemination process.

The recommended process is one that addresses non-traditional target sets and exploits small identifiable signatures. It must support implementation of countermeasures, preemption, prevention, apprehension, and retaliation. The system must exploit all sources and a usable product must reach first responders to assist in deliberate planning, training and execution.

While expanded collection assets are principally HUMINT, additional and improved supporting SIGINT and Measurement Intelligence (MASINT) are needed.

In the area of analysis and processing, it is necessary to have a greater intellectual base. Succinctly, this means more people who are better trained and able to interpret bits of information collected in unusual settings. There must be greater emphasis placed on the interpretation of mass data sets. Integration must be carried out by function and topic. The system must be designed to serve both the operational and tactical commander. Fusion and integration must occur at the operational level. The system must be built for the long term, possess in-depth analytical capability, and be resourced adequately.

Finally, in dissemination and holding information, it will be necessary to work cross-jurisdictional problems that involve foreign nations, the Services, National agencies, and state and local responders. Technical and non-technical dissemination issues must be addressed. In the end, the system must operate on the basis of push- pull by operational and tactical users.

Findings & Conclusions

1. Resources and capabilities applied to counter transnational threats are much too small and limited to achieve fully effective operational intelligence
2. Broadly based process improvement is needed for fully effective operational intelligence in order to
   - preempt or prevent attacks
   - prepare and perform consequence management
   - plan, train and rehearse for both
3. No "silver bullets" to immediately improve capabilities
4. No prospect of the threat declining over time. Improved intelligence capabilities will afford predictive insights and may enable preemption and/or prevention of an event or series of events.
5. A comprehensive analysis must be undertaken to address needed capabilities and improvements

Findings and Conclusions

1. Resources and capabilities applied to counter the transnational threat are not adequate to achieve fully effective operational intelligence. There are, currently, a substantial number of groups which can be classified as transnational threats. The current HUMINT/CI intelligence coverage is limited for a variety of reasons and the number of analytic personnel working Weapons of Mass Destruction (WMD) aspects of transnational threats is insufficient.

2. The nature of the transnational threat is such that a broadly based operational intelligence process improvement is needed. There are critical shortfalls in collection, analysis and dissemination. It is also clear that HUMINT/CI, centers of excellence, broad based data management, and dissemination to first responders need substantial improvement.

3. There are no silver bullets to immediately improve capabilities. Improvements will take people, time, effort, and resources.

4. There is no prospect of the threat declining over time. Improved intelligence capabilities will afford predictive insights and may enable preemption and/or prevention.

5. A comprehensive analysis should be undertaken to address needed capabilities and improvements. This applies both to building and maintaining the needed operational intelligence capability.

Findings & Conclusions - cont'd

6. Needed enhancements:
   - Improve HUMINT/CI(overt, passive and clandestine), SIGINT and MASINT collection
   - Expand Foreign Area Officer Programs
   - Strengthen analytic capabilities

7. Expand the scope of connection and analysis:
   - Air transport (passengers and cargo)
   - Border crossings
   - Commodities/technological transfer
   - Financial systems
   - Passport monitoring

Findings and Conclusions (Continued)

6. The enhancements needed include improved HUMINT/CI (overt, passive and clandestine), SIGINT and MASINT collection. This includes improved liaison, low level source operations, and individual awareness programs. Further, expansion is needed in the size and diversity of the DoD intellectual capital base represented by the foreign area officer programs, as well as, a strengthening of the transnational threats analytical capabilities of both agency staffs and community centers of excellence.

7. The concepts and capabilities of existing centers of excellence should be further developed and expanded to encompass tracking of air transport movements, border crossings and transfer of critical commodities and technologies. Additionally, this mechanism offers a fertile venue for enhancement of international cooperation and collaboration. The Navy's Maritime Surveillance System offers a potentially useful model for such community tracking centers.

Findings & Conclusions - cont'd

8. Improved clandestine collection by removing obstacles in two domains
   - Laws, policy and regulations
   - Activity approval

9. Intelligence agencies must provide immediate use operational intelligence to public safety officials

Findings and Conclusions - (Continued)

8. Improving clandestine collection requires obstacle elimination in two domains:

   a) laws, policy and regulation and

   b) activity approval. Particularly in matters involving HUMINT, an effort is required to change existing protocols.

9. Intelligence agencies must provide immediate use operational intelligence to public safety officials. Aggressive sanitization of intelligence material for release to the first responder is critical. Using the local community public safety officials and law enforcement as a "HUMINT" source base for threat warning should be implemented.

A Necessary Precondition

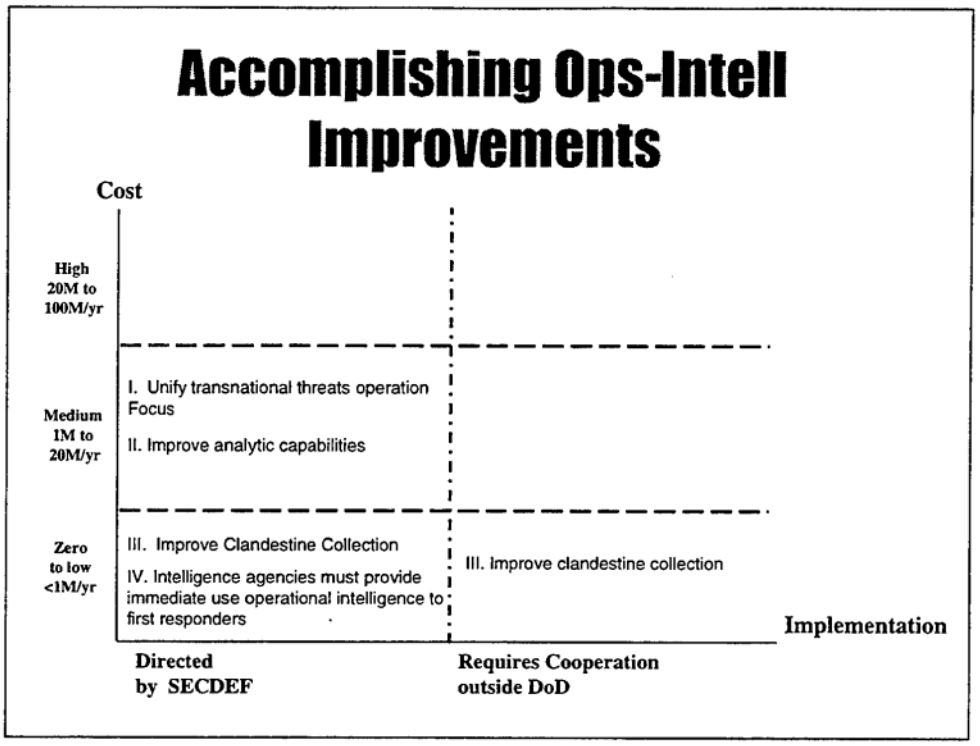
- Within DoD the mission of deterring and preventing transnational threats and mitigating its consequences must be accorded sufficient importance to claim resources, and be sustained for the long-term

A Necessary Pre-Condition

The Department of Defense supports a large number of vital missions and a larger number of critical missions. The impact of initiatives for operational intelligence improvements falls principally on existing agencies and the regional CINCs. There will be competition for resources, particularly when the mission is to be sustained over a long period of time. Executive level sustained emphasis must be placed on resource allocations.

History suggests that only a few missions have the importance and staying power that combating transnational threats requires. The nation sustained substantial efforts in defense and intelligence when national survival was at stake. The state of Soviet nuclear forces and general purpose forces demanded such commitment. The same was true in sub-specialty areas such as air defense and ballistic missile defense.

Combating transnational threats must be accorded higher priority in DoD. Once combating transnational threats is given increased emphasis and resources which follow the required improvements will occur.



Accomplishing Operational Intelligence Improvements

The chart describes in a very simple form, the costs and the implementation difficulties associated with improving operational intelligence. They are divided into a 6-zone chart.

Costs are described in terms of those which are low (cost up to as much as a million dollars a year.) In the next higher category, they are described as medium (1 to 20 million dollar range) and as high (the 20 to 100 million dollar range.)

These costs categories are segmented into actions which could be directed by the Secretary of Defense in one category or require cooperation outside DoD in the other category.

It is seen that improving clandestine collection and improving dissemination to first responders by intelligence agencies can be accomplished at low cost and can be partially directed by the Secretary of Defense.

Unify transnational threats operational focus and improving analytic capabilities can be accomplished at a modest cost. The actions recommended can be directed by the Secretary of Defense.

This display is intended to help with decision making and starting the process of improving operational intelligence.

REPORT OF THE COMPETENCY PANEL ON THE NUCLEAR THREAT

Panel Chair
Dr. Rich Wagner

Members
Dr. Roger Hagengruber
Mr. Roland Herbst
Dr. Fred Ikle
Dr. George Miller
Mr. William Nelson
Mr. John Nuckolls
Ms. Amy Sands
Mr. Fred Wikner
Dr. Lawrence Woodruff
Dr. Mary Anne Yates

Government Advisors
LTC John Betts, USA
Mr. Ronald Cosimi
Mr. Mark Monahan
Dr. John Immele
Col Dale Landis
Mr. Clifton McFarland
LtCol James Mueller, USAF
LtCol Michael Williams, USAF

DEALING EFFECTIVELY WITH THE NUCLEAR TRANSNATIONAL THREAT

With the collapse of the geopolitical structure of the Cold War, the salience has risen of threats to the United States and its interests by organizations and individuals with motives and methods quite different from those posed to the nation during its confrontation with the Soviet Union. Among such threats are *transnational threats:* any transnational activity that threatens the national security of the United States - including international terrorism, narcotics trafficking, the proliferation of weapons of mass destruction and the delivery systems for such weapons, and global organized crime.

Examples of the recent and current transnational threat are familiar to us all. Events such as the 1983 attack on the US Marine Corps barracks in Beirut, Lebanon, the attack on US forces in Somalia in 1993, the bombing of the World Trade Center in 1994, and the 1996 bombing of Khobar Towers in Saudi Arabia are perhaps some of the more notable cases. Such events are the current visible manifestations of two fundamental trends:

Because of the development and spread of technology, it no longer requires the resources of a state to do immense harm to U.S. forces, U.S. interests, and to America itself by creating mass casualties and massive destruction by employing weapons of mass destruction (WMD).

- Changes in the geopolitical structure are such that non-state adversaries increasingly perceive incentives to do so.

These two trends are what characterize the transnational threat in its most general terms.

Because of these trends, the transnational threat could well escalate both in scope and importance in the future. The challenge may be dealing with large, orchestrated campaigns extending over years, rather than isolated events. Furthermore, the use of WMD is already a part of the current threat, and it is likely that it, too, will grow.

The Department of Defense – with the Department of Energy, especially for the nuclear WMD case – has the capacity to contribute extensively to the mitigation of these threats, whether the response involves circumstances where DoD is in charge, or whether the Department is in a supporting role. The 1997 Defense Science Board Summer Study on DoD Responses to Transnational threats addresses DoD capabilities, options and responses to transnational threats, and especially, for DOE as well, the nuclear case.

In summary, the Report of the Summer Study as a whole describes a need for strengthening DoD's response capabilities and has identified six elements of a DoD response strategy for all aspects of the transnational threat:

1. Treat transnational threats as a major DoD (and DOE) mission
2. Use the existing national security structure and processes
3. Define an end-to-end operational concept and system-of-systems structure to deal with such threats
4. Develop an interactive global information system on transnational threats
5. Address problems that have long been viewed as "too hard" – in particular the WMD threats, including the nuclear threat.
6. Leverage worldwide force protection and civil protection synergies.

Together these principles form the structure for effectively positioning DoD and the national security community against the transnational threats of the future.

Volume 1 of the report of the 1997 DSB Summer Study contains some of the discussion and most of the recommendations in this report, as well as lengthy discussion and many other recommendations pertaining to the transnational threat as a whole and to its several particular aspects, of which nuclear is one. Many of those discussions and recommendations contribute to dealing with the nuclear threat. (The report of the 1997 DSB Summer Study is available from DTIC, (703) 767-8274.) In this Nuclear Panel report, we discuss only capabilities and recommendations specific to the nuclear topic. Our recommendations are in bold type , interspersed throughout the discussion that supports them.

While this DSB Summer Study and its Nuclear Panel were tasked to look mainly at DoD capabilities, in the case of the nuclear problem, the Secretaries of Energy and Defense are equally customers for our product. Many of our recommendations are directed at building both DoD and DOE capability and preparing to surge that capability in the event of increased awareness of the threat or resources to address the threat. For nuclear matters, there is a unique partnership between the DoD and DOE. The predominant part of the technology base resides at DOE Laboratories with DOE as the immediate sponsor of their activities, but the DOE national security budget is part of the overall Defense Authorization (-050) account. Operational responsibilities are divided (e.g., DoD assistance for securing Russian weapons, DOE for materials; DOE nuclear search and render safe hardware, DoD explosive ordnance disposal / disable), but must be managed in an integrated, comprehensive way. ***In this context, we reiterate a recommendation of the overall DSB Summer Study: that the Secretaries of Defense and Energy should jointly reaffirm their departments' commitment to work together in this area, as a major mission of both departments, and task their respective departments to define and develop an expanded, cooperative long-term program to develop capabilities to deal effectively with the nuclear transnational threat.***

In focusing on the future, as we have done here, some of the context of current programs is lost. So we want to be clear at the outset that our suggestions imply no criticism - in fact, most of the ideas came from people who are already in the front lines of countering proliferation and

terrorism. With the end of the Cold War the available materials and incentives for WMD terrorism have grown. DoD and DOE have responded with initiatives in such areas as nuclear smuggling prevention and chemical / biological defense for first responders. Our recommendations are intended to build on their good work.

THE NUCLEAR PROBLEM AND THE PROSPECTS FOR DEALING WITH IT

If the required fissile material is available, it is not especially difficult to design and build a primitive nuclear explosive device. It is unlikely (though perhaps not impossible) that it could be done by just a few people, but—because of the diffusion of knowledge and technology over the past decades—it certainly does not require the resources of a nation. It is more difficult to make plutonium or enrich uranium for such a device (although even that is less difficult than it once was), but with the reduced levels of security of nuclear weapons in Russia and of nuclear materials in all the states of the FSU, materials (or weapons themselves) could be obtained from these sources. This development of transnational threat organizations over the last few years adds to the urgency of dealing with the nuclear threat.

The nuclear device which could be built (or stolen or bought) could be small enough to be covertly transported to its intended detonation point by small truck, ship or an aircraft of moderate capacity, perhaps in combination. Such a small device, with potential yield about the same as the weapons used in 1945, could be detonated in a city, or at a U.S. (or other) military base in the U.S. or overseas, or (in some scenarios) against U.S. or other forces in the field.

Such a nuclear explosion could happen at any time. It could have happened, somewhere, while you were reading this sentence. (For example, a weapon or fissile material could have been removed from Russia months or years ago.) Or it might never happen. There is no way to assign a "likelihood" or "probability" to such an event. (It's somewhat like trying to assign a "likelihood" to the existence of extraterrestrial intelligence.) **The reality is that, with the limited protection capabilities we have today, whether such an explosion happens depends almost entirely on whether someone decides to do it, and can get fissile material or a weapon.**

Such an explosion could change the world, even more than any other type of WMD that might be used to kill as many people. The tradition of non-use of nuclear weapons developed since 1946 would have been broken. Attitudes toward nuclear weapons, and the roles they play in regional and global security relationships, could change dramatically, with unpredictable and possibly serious effects on those relationships. If used against U.S. forces overseas, such an explosion could demonstrate a potent and asymmetric counter to U.S. military capability, limiting the ability of the United States to use its military effectively in the many roles they play around the world. If detonated in a city, the unprecedented vulnerability people would feel in their daily lives could lead to changes in political institutions and types of governments—in the social contract itself—of historic import. (These effects could be amplified if the explosion could not be attributed to its perpetrators.) Fred C. IklÈ has developed these possibilities brilliantly in two recent papers. [1] [2]

One possibility discussed by IklÈ, and elaborated by the DSB Summer Study, is a strategic campaign of escalating terrorism of all kinds, orchestrated with long-term intent to achieve the outcomes mentioned above. Depending on the nature and pace of the escalation, democratic societies may be able to adapt to avoid the full social and political impacts. Supporting and

[1] Fred C. Ikle, The Second Coming of the Nuclear Age, in *Foreign Affairs*, Vol. 75, No.1.
[2] Fred C. Ikle, The Next Lenin, On the Cusp of Truly Revolutionary Warfare, in *The National Interest*, Spring 1997.

enabling such adaptation is one strategic objective of developing improved capabilities to counter these threats. A nuclear explosion designed as part of such a campaign could have even more momentous consequences than an isolated one, but the escalation itself would provide a form of warning which could be exploited to surge capabilities to preclude the event.

The possibility that such a nuclear device could be built and detonated has been understood for over thirty years (though the risk from poorly secured materials/weapons in Russia has emerged only recently) and some good capabilities to search for and disable a stolen weapon or a covertly emplaced device have been developed. (See Attachment A for a short history of the development.) But these current capabilities cover only a very limited part of the range of possible threat scenarios. Furthermore, there is not now, nor has there ever been, a comprehensive program to develop, even over the long term, a robust capability to defeat this threat across a wide range of possible scenarios. There are several reasons for this, but one has probably been that it has simply appeared to be too hard, almost no matter how much might be spent.

It is the central assertion of this report that, for costs considerably less than what is being spent on, say, missile defense (and far less than what would be commensurate with the possible consequences of such an explosion), and with a comprehensive long-term program, there is now - for the first time - a good chance that capabilities can be developed to deal quite effectively with this threat—i.e., to cover, with good effectiveness, a much larger part of the range of possible threat scenarios. This is especially true if credit can be taken for the dissuasion/deterrent effect of greatly improved but less-than-perfect protection capabilities. This assertion is based on a combination of existing understanding and capability, some new realizations about parts of the problem/solution space, and prospects for new technical and operational capabilities.

Discussion below provides a substantial basis for this assertion. However, even if one has doubts, we believe that this assertion is the right basis for moving forward. The program to develop the capabilities that we assert are feasible will prove (or perhaps disprove) our assertion.

Accordingly, it is the central recommendation of this report that the Secretaries of Defense and Energy should significantly expand their departments' efforts related to countering the transnational nuclear threat. Added to the current effort, which is largely devoted to current operations and readiness, should be a major program component that looks to the farther future, to develop, over perhaps a decade, a greatly improved capability. This development program should be based on the assumption that, as it becomes successfully complete, procurement and operational resources can then be made available which are much greater than those available today.

Even when this improved capability has been developed, maintaining the substantial assets involved at a high level of readiness may not be perceived to be affordable, either politically or fiscally. What *can* be done is to address the long lead items – such as training, long-lead procurements and preparations to procure – that would be needed to surge rapidly and effectively, if and when circumstances develop that change perceptions of political or fiscal affordability. One such circumstance could be a successful terrorist nuclear explosion; preventing a second one would become the overriding national priority. Another could be an

escalating campaign of terrorism in general, including other WMD. ***Such preparations, starting now even with the limited capabilities that currently exist, should be an integral part of a comprehensive program.***

For the nuclear transnational threat, such a program, though much smaller, would be analogous in ambitious spirit and long view to DoD's many programs to develop the technologies of the Revolution in Military Affairs, and to DOE's program to develop capabilities for stewardship of the nuclear stockpile in the absence of nuclear testing. For both departments, it is an inherent part of nuclear stewardship.

A basic strategy trade is to balance investment between prevention and consequence management. Because of the severity of the consequences in the nuclear case, early detection and prevention must be emphasized.

The following, more detailed discussion and recommendations are the roadmap and outline for executing the central recommendation above.

A Comprehensive Architecture

In the greatly improved posture that the recommended program would develop, the following elements would be woven together into a comprehensive architecture:

- Detecting nuclear threat operations along their entire time line, from planning to weapon emplacement, using a wide range of U.S. and other intelligence and law enforcement assets, to provide warning and for interdiction.
- Securing nuclear weapons and fissile material much more effectively against loss, theft, or diversion, with near-term emphasis on Russia and, over the longer term, fissile isotopes in whatever form, everywhere.
- Detecting the presence or transit of nuclear devices and materials over large areas, using large networks of advanced mobile, transportable and fixed sensors—active and passive—with advanced signal processing, and coupled with advanced search and interdiction methods.
- Gaining access to threat devices which have been located, and rendering them safe or destroying them with as little attendant damage as possible.
- Mitigating the consequences of an explosion: treating casualties, especially with advanced methods for treating radiation-related injuries/illness, and clean-up of fallout or other dispersed radioactive material.
- Developing ways of accurately attributing the operation to its perpetrators. (Forensics is the key capability.)
- Developing a long-term, comprehensive R&D and procurement investment plan between DoD and DOE.

We recommend that, within the context of the overall architecture recommended by the DSB for dealing with all aspects of the transnational threat, DoD and DOE should jointly develop a comprehensive, end-to-end architecture on which to base the long-term program recommended above for dealing with the nuclear threat. This architecture and program should integrate, and create synergies among, all of the elements listed above.

In every one of the categories listed above, there is both some current capability and various prospective improvements, some potentially large, which are in various stages of development and have varying potential feasibility. We now describe those in more detail and state our recommendations about them.

Identifying and Characterizing Threat Operations

While it no longer requires the resources of a nation to build a nuclear explosive and transport it to a target, especially if the fissile material can be bought or stolen, neither is it a trivial undertaking. To build a nuclear device, a team must be assembled, funding obtained, security measures put in place, special facilities and capabilities provided for, and so forth. All along the time-line of such an operation, from initial planning to device emplacement, there are "signatures" that can be exploited by intelligence and/or law enforcement assets. Stealing or arranging to buy material or a weapon has signatures, as does transportation to the target, including surveillance of the target and the access route. Most of these signatures may be small individually, but in aggregate they are likely to be significant.

Experience has shown that even considerably less ambitious and less difficult terrorist operations take time and careful preparation, and therefore also have significant signatures. Although this is not always the case, it is often the case. The more people who are involved in such an operation, and the longer it takes, the greater are the chances it can be detected, (in part because they will make a mistake that creates a signature.) Intelligence and law enforcement have often been able to exploit the signatures of such operations to deflect or defeat terrorist operations. For example, experience in West Germany during the 1970s and 1980s seemed to indicate that if a terrorist operation required more than about fifteen or twenty people, and took more than a couple of months, the chances would be good that West German law enforcement would detect it. And the track record of the U.S. and our allies in recent years is considerably better than is commonly understood, perhaps mostly because it is the failures that make headlines.

Furthermore, improving the protection of nuclear materials and weapons, and improving the capability to detect and respond to the presence or transit of nuclear materials and weapons, will force the adversary to operate in ways that increase exploitable signatures. Optimizing these synergies is a key element in developing the overall architecture recommended previously.

Although all this discussion suggests the potential for significant future capability to detect a nuclear threat operation, the current capability is nowhere near good enough. But there are ways to significantly improve the capability in all its dimensions. The central ones have to do with correlating many disparate, seeming unrelated bits of information of many kinds, from all intelligence sources (and from many sources which may not be "intelligence" at all). Advanced information-management tools, including behavior and inference modeling, can help to pull significant information from large masses of data and guide analysts toward useful correlations. The Nuclear Panel of the DSB Summer Study witnessed a demonstration of a set of information tools which has been used successfully to thwart terrorist operations. Much more could and should be done along those lines, both in general and in the nuclear area. The technology base for such information technologies, as they support counter-terrorism applications, needs to be broadened, and those applications need to be extended beyond the defense-intelligence community into the law enforcement and non-defense intelligence communities. An interactive

Global Information System on Transnational Threats, also recommended in Volume I of the overall report of the 1997 DSB Summer Study, would be a key capability.

Realizing the potential of these tools will depend on improved sharing of information among analysts and agencies in the U.S. and elsewhere; the tools themselves will help. Also, assessing and planning these capabilities requires an improved analytic framework or model of the interaction between threat operations (and their signatures/observables) and intelligence operations intended to detect them. (Think of the intelligence assets overall as a "sensor" in a "weapon" system; the analysis would help to understand and plan how it can be used to acquire and track the "target.")

The DSB Summer Study makes several recommendations for realizing the potential for improving the capability of US and allied intelligence and law enforcement to detect transnational threat operations of all kinds, including nuclear. (These include accelerated and expanded development of knowledge engineering tools and the information system mentioned above, as well as expanded HUMINT and SIGINT operations, and better data sharing and coordination among U.S. agencies and with coalition partners and allies.) However, particular attention should be focused on the nuclear threat because signatures of nuclear threat operations are likely to be larger and/or more exploitable than for other types of threats, and thus the prospects of successful detection greater. We thus make the following additional recommendations.

- ***Secretaries of Defense and Energy should ensure that, as other DSB recommendations for intelligence are implemented, the nuclear dimension is explicitly addressed.***
- ***To support development of the architecture recommended earlier, and to aid operational planning, a tighter linkage of users of counterrorism intelligence, nuclear analysts and intelligence collectors should be established to understand the interactions between nuclear threat operations and their signatures, and intelligence operations intended to detect them. This increased understanding should be reflected explicitly in an analytic framework or model.***
- ***Re-establish a sound and enduring S&T intelligence analysis capability in the nuclear area. Recruit, train and equip a cadre, of analysts with the necessary technical backgrounds. Exploit the resources of the DOE national laboratories more effectively. Plan for a surge capability in the analytical cadre, since incidents of terrorism tend to be episodic, and to respond to possible escalating threat campaigns.***

Securing Nuclear Weapons and Materials

Experience in the U.S. and elsewhere shows that it is possible to achieve and maintain high levels of security for nuclear weapons and materials. The challenge is to approach those high levels everywhere. Since the dissolution of the Soviet Union, such security has diminished in Russia. Through the Cooperative Threat Reduction Programs in DoD and DOE, the DOE Nuclear Smuggling Program, and other efforts, the U.S. is working closely with Russia to improve weapon/material security, including providing hundreds of millions of dollars to supplement Russian funding in areas where U.S. funding and competence provide high leverage on crucial needs.

Progress is being made, but there is a long way to go. Money—dollars and rubles —is necessary but far from sufficient. It is crucially important to create an adequate "security culture" in Russia to replace the one that existed in the Soviet Union (which may have been adequate but would be incompatible with a democratic society). The "insider threat" is particularly important to address. Creating an adequate security culture will be doubly difficult because of the problems—crime, poverty, and morale—that afflict Russia as a whole. To build the needed security culture and to fund what must be funded, the government of Russia must put very high priority on this problem. Almost all U.S. observers and participants feel that Russia could be doing more, but there has been disagreement over what combination of carrots and sticks would be productive, if any.

It is clear to us that a *sine qua non* for further progress is continued U.S. involvement and that, without some level of continued U.S. funding, U.S. influence will diminish significantly. Most of the projects are programmed to wind down in the next few years.

Over the longer term, fissile isotopes in the civil nuclear energy fuel cycle are also a matter of concern, as they can be diverted for use in weapons. IAEA and related safeguards are necessary (and can and should be strengthened) but they will never be fully sufficient for protecting these materials, which are currently stored in thousands of places under a wide range of security measures. A more comprehensive, global regime is needed for protection, control and accountability of these materials, including consolidation into many fewer sites. The proposed Internationally Monitored Retrievable Storage System, which is one approach, is the subject of a current joint DoD/DOE study.

Recommendation: The appropriate offices and Agencies in OSD*, and the DOE should jointly develop a long-range plan to extend the DoD and DOE programs for securing nuclear materials and weapons in Russia, and to augment current international arrangements for securing weapon-usable material of all kinds, everywhere. We single out the more detailed recommendations below not because the topics are new – they are well known to those working in this area – but because they are of particular importance, and to underline the need for program breadth and a long-term view.

- The present *DOE MPC&A* and *DoD CTR* programs to secure the nuclear weapons and material within Russia should be extended beyond 2002.
  - Encourage Russia even more strongly to consolidate its nuclear and weapons materials in fewer sites.
  - Provide ongoing American financial, technical and moral support for projects beyond MPC&A, e.g., warhead dismantlement, Pu disposition, plant closings
- The development of a safeguards culture in MinAtom and MOD should be extended to export and border control agencies. *(DOE, DoD, Customs, FBI)*
  - Collaborate on the development of ongoing, technical cooperative programs between technical experts and customs and border officials in the former Soviet states
- Attention should be focused on helping the Russians deal with the insider threat, including
  - Continue the Lab-to-Lab programs and US support for the projects of the ISTC,

* This report is being written shortly after the publication of the Defense Reform Initiative Report of November 1997. It is not clear yet just how OSD responsibilities in this area will be organized.

- Within carefully set limits, share studies and technology for polygraphy, and methods for effective red-teaming.

- The Russian MPC&A system should be coordinated with local response elements.
  - Extend Lab-to-Lab discussions of nuclear accident response to training responders in Russia in the search and recovery of special nuclear materials (SNM). *(DOE)*
- A comprehensive, international, and long-term program to secure weapon-usable nuclear materials should be developed and extended to other states possessing such materials. *(DOE)*
  - Encourage states to assess their physical protective measures and to upgrade these measures where necessary.
  - Provide assistance to states in their evaluations and upgrades via the IAEA's new International Physical Protection Advisory Service (IPPAS) or by other bilateral means.
- The Nuclear Supplier states of the West should buy all HEU available outside of Russia in the Newly Independent States, thereby eliminating the urgency of developing a safeguards culture and system in at least six countries. *(DOE, State)*
- Convert research reactors from HEU to LEU fuel.
- Security of reactor fuel of certain reactor types (breeder and naval) within the former Soviet Union should be improved. *(DOE)*
- A long-term, comprehensive MPC&A System for the global civil fuel cycle must be developed. *(DOE)*
  - Build on the current IAEA and national efforts.
  - Support the proposed Internationally Monitored Retrievable Storage System (IMRSS) currently under joint study by OSD and DOE.
- *DOE's* nascent R&D program on proliferation-resistant fuel cycle technologies should be expanded, to include collaborative R&D with other nations including Russia and China.
- New technology and systems for automated, continuous monitoring of high-risk materials and nuclear processing (R&D) should be developed and deployed. *(DOE)*
  - Examine the "tagging" of sensitive nuclear materials so their movement can be monitored and, if ever lost, be tracked and identified quickly upon recovery.

Detecting and Responding to the Presence or Transit of Nuclear Materials or Weapons, Using Large Networks of Sensors and Advanced Search Capabilities

Today, DoD and DOE assets to detect and localize terrorist nuclear materials or explosives can be effective only over limited areas or with intelligence warning that closely specifies threat location and time. Clearly, it would be desirable to have closer to *continual* coverage of much *larger areas* (cities or larger), as might be done with wide arrays of very large numbers of detectors (or perhaps with fewer mobile detectors that could sweep large areas rapidly.) With an aggressive, long-term program, it appears, for the first time, that it may now be feasible to develop such capabilities. Here's why.

A central problem with any radiation detector is false alarm rate; if the detection threshold is set low enough to get maximum detection range, natural background radiation (or benign manmade sources) will trigger it. In a large array of detectors, the false alarm rate can be so high that the system fails completely.

Recently, progress has been made in ameliorating this problem using a network logic that correlates "hits" among a large number of detectors using a model of scenario factors such as estimated or measured traffic flow rates between detector locations (in a city, say.) This filters out many false alarms, so that the entire array (or segments of it) can act as if it were a single detector which is very sensitive (because there are many actual detectors) but with a low false alarm rate. ("Nuisance alarms" from the many benign radiation sources used in industry and medicine remain a serious problem that must be dealt with, perhaps by spectral analysis or use of active detectors. See below.) There has been some planning to demonstrate such a network, in a realistic operational environment, incorporating several dozen fixed detectors.

Under the auspices of the DSB Summer Study, with welcome DOE support, LLNL and LANL conducted a "red/blue" interaction to refine how such a network concept could be extended to a large city, using Washington, DC as a model. (Earlier, DoD's Defense Information Systems Agency (DISA) had explored, in very preliminary form, an even more extensive system, including detectors at ports and airports in CONUS and overseas.) The DSB/DOE group iterated toward a linked network of hundreds of mobile and/or quickly relocatable detector systems, and looked at how improved "end-game" response/interdiction forces — extensions of today's capabilities, with improved capabilities — could be used on the basis of warning and threat localization from such a network. There is a complex "offense/defense", move/countermove strategy that remains to be thought through fully to determine how best to design and use such a large area detection and tracking capability.

The DSB Summer Study also looked at advanced technologies for individual detectors, active and passive. There are innovative approaches which hold promise for substantially improving detection in a variety of ways—to detect HEU or shielded plutonium which have low external radiation signatures; to extend detection range and search rate in general; and to discriminate against false alarms. Such advanced detectors could also be useful in ports or airports.

It is now apparent that, for the first time, use of improved detectors and improved ways of using detectors in large arrays, opens the serious possibility of being able to affordably cover much larger areas, and keep them under surveillance over much longer times, than has generally been thought feasible. Such a capability to detect the presence or transit of a nuclear threat device could converge, in a synergistic way, with improved intelligence capabilities to detect threat

operations (described above) to provide, overall, a potent capability to deal effectively with a wide range of threat scenarios.

Realizing this potential will require a long-term DoD and DOE investment program combining technical R&D with advanced operational concepts. Success is not guaranteed, but there is a reasonable prospect. ***Recommendation: DOE and DoD should jointly plan and assure funding for a long-term program to develop and acquire capabilities to detect the presence or transit of nuclear weapons/devices and materials over much larger areas, and with much longer duration of coverage, than is currently possible, coordinated with expanded efforts to respond to such detection more rapidly and effectively. The final phase of such a program should be to prepare to procure equipment in quantity and to train personnel so that, when needed, a capability could be quickly deployed to cover many large cities simultaneously. Consistent with other DSB Summer Study recommendations, the National Guard should become an integral part of plans for such a large-scale surge capability; planning and training for this should start now.*** **The following more detailed recommendations suggest a strategy for acquiring an integrated system of radiation detectors and response forces to screen as well as search larger areas:**

- **As a basic building block we urge the development and deployment of at least a** few dozen next generation Modular Application Search Systems (MASS).[3] The modules should be easily adapted for vehicle or fixed application. They should incorporate next generation data processing and networking capability as well as advanced detectors. *(DOE)*
- DoD and DOE should collaborate to demonstrate, in the near future, the capabilities of a prototype network of detectors (perhaps up to a hundred) in a realistic operational environment in a city and/or around a military base. (This experience can provide insight for the following recommendation.)
- *DoD and DOE* should explore the longer-term development of a system of *several hundred (maybe even a thousand)* networked sensor modules for nuclear search and screening in urban environments, to screen harbors or ports and for military base protection in CONUS or OCONUS. This would be most likely employed as a surge capability of MASS, but would exploit *computing and communications among the detectors* to reduce false positives. In the long term, the network and MASS would be based on advanced detectors and methods developed in the program recommended below.
- A continuing test program under DOE should be established to characterize time-dependent radiation patterns in urban environments and to test and demonstrate networks as well as individual sensors in the proposed architecture.
- *DOE (NN)* should augment current efforts to develop next generation sensors - applicable not only to "terminal defense" of limited areas but broadly applicable to detection and interdiction of stolen nuclear material. This will require additional funds, some of which should be devoted to high-risk ideas. For example,
    - Smart detectors to eliminate false and nuisance positives - emphasis on room-temperature operation, reduced size and unit costs and automated spectral analysis
    - Gamma-ray imaging. In the far term, this may hold the revolutionary promise of distinguishing small radiation signals against background radiation over large areas

[3] Described in Requirements: National Radiation Detection Assets DP-23, 6 Aug 97)

very quickly (perhaps up to square kilometers of area every several seconds). In the near term, less ambitious angular and spectral resolution will permit application to smaller search areas (5,000 to 50,000 sq. meters) and to device diagnostics.

- Detectors (probably active) for highly enriched uranium and shielded material. Detection at extended (from today's capabilities) ranges.

Gaining Access to Threat Devices, Diagnosing them, and Rendering Them Safe with as Little Damage as Possible.

A threat device that has been located could be booby-trapped to detonate when access or render-safe efforts are attempted. Some nuclear devices, perhaps primitive ones especially, are not "one-point safe" – that is, attempts to destroy them, once captured by U.S. forces, could cause them to produce significant nuclear yield. There has been good progress in recent years in designing methods to preclude or limit such yield, but more should and can be done, and devices already known to be effective need to be procured.

The importance of this phase of dealing with the threat varies with the scenario. If the threat scenario is, for example, a suicide attempt with no other goal than to indiscriminately kill Americans, the adversary could use something like a dead-man switch to detonate the device if threatened and make access and render-safe capabilities essentially irrelevant. On the other hand, if it is an extortion attempt, significant time for search, access and render-safe might be available, but the device might be heavily booby trapped, to detonate when access or safeing is attempted. Likewise the level of sophistication of booby trapping is known to vary widely—from easy-to-beat to impossible-to-beat.

On the basis of studies and R&D already done, we believe that with affordable levels of further R&D and procurement, it is feasible to develop access and render-safe capability which will do the job quite well for a wide range (though not all) of scenarios in which such capability is relevant at all. The existence of scenarios in which even a good capability is irrelevant is not sufficient reason not to do what *can* be done. The purpose of this whole business is to narrow the range of winning options for the potential adversary.

DOE and DoD should plan and assure funding for a significantly enlarged and coordinated program to develop and acquire greatly expanded capabilities to gain access to threat devices which have been located and to render them safe or destroy them with as little attendant damage as possible. More ambitious objectives should be to have capabilities that closely approach the physics limits. As discussed previously, we believe that this will require additional funds and that some of these should be devoted to high-risk ideas. Tailored, very rapid response combining DOE and DoD assets and collaboration with trusted allies continue to be encouraged.

To support these general objectives the Panel makes the following particular recommendations:

- Develop diagnostics which describe more accurately and from more remote distances the mechanical assembly and electrical / booby trap construction in an improvised or stolen nuclear device. *(DOE and DoD)*

- Device assessment - provide additional resources and personnel to determine if a device is capable of producing nuclear yield and, if so, how various render-safe options would affect

the yield. *(DOE)* (The Panel is encouraged that this work will help attract and train the next generation of stockpile stewards.*)*

- Develop new methods (DoD and DOE) of rendering safe the remaining classes of nuclear devices not covered by existing render safe methods. Ruggedize these new methods for military use in the field, and test under as near real conditions as is possible. Deploy in sufficient numbers (i.e., more than one) to respond quickly.

In addition to these technical capabilities, operational coordination and planning is crucial. Recently, it has become more widely known that DoD military forces might be used in support of the FBI in a domestic nuclear event, and this has caused some confusion as to who does what, with whom, for what mission. ***Clarification is needed as to roles and responsibilities between DoD units tasked to deal with Transnational Threats in a crisis involving nuclear devices, particularly in the CONUS, and a better mission profile definition needs to be documented for DOE to follow in its support planning.***

Mitigating the Consequences of an Explosion or Radioactive Dispersal that has Occurred

While the consequences of a nuclear explosion would be cataclysmic (and could be very serious for a high explosive induced radioactive dispersal event), they can be partially mitigated. The overall program for ameliorating the consequences of WMD terrorism is discussed at greater length in Volume I of the full DSB report. Its most important feature is the institutionalization of the Nunn-Lugar-Domenici (N-L-D) programs for first responders. **Recommendations: nuclear consequences should be included in the N-L-D program for first responders. For example,**

- Better planning and preparedness not just for a radiological or weapons accident but for the sheer devastation of an actual nuclear detonation. *(DOE, FEMA, DoD)*
- Continue (under N-L-D) to establish the nation-wide training program for first responders <u>including nuclear</u> *(DoD)*
- Train National Guard for nuclear consequence management and exercise a nation-wide linkage of *DoD and National Guard* with first responders. Use National Guard for training & equipping.

In addition, *the Armed Forces Radiology Research Institute (AFRRI)* should complete the development of improved treatment regimes for radiation-caused and radiation-exacerbated injury and promulgate its application among appropriate elements of the first-responder and medical communities.

Attribution

Being able to correctly attribute a nuclear terrorism event to its perpetrators can help to deter the act itself and ensure that U.S. responses are appropriate, and can ameliorate the sense of helplessness that the public would otherwise feel after such an event. The improved capability to detect a threat operation that is underway, discussed earlier, can contribute to attribution after the fact even if it (and the other measures discussed) fail to prevent the event. In addition, there is a wide range of forensics technology that can complement other intelligence/detection capabilities before the event, and contribute to attribution after. One example is analysis of minute samples

of material obtained (perhaps clandestinely) from the vicinity of a threat suspected operation, or from an explosion, which can tell a lot about origins, history and associations of the material. Especially important is identification of worldwide reference data-bases for nuclear isotopic fingerprints and analytical methods which might associate nonnuclear residues with original nuclear sites., and setting up arrangements for rapid access to them when needed.

Science and technology developed over the past several years are rich in potential for forensics, but are not being fully utilized. Very little is being spent in this area. **We recommend a several-fold increase in funding for development of nuclear forensics technology**. This should build on the existing joint *DOE-FBI* MOU and several other programs with *State and the IC.* Such an increase would still represent very small levels of funding, both in absolute terms and compared with what is being spent on other capabilities discussed in this report.

Radioactive Dispersal Devices

A nuclear explosion is not the only way to kill people or create a serious hazard with nuclear material. Radioactive material of many kinds can be dispersed easily over wide areas with standard chemical explosives or in other ways. Radioactive material used in medicine or industry exists in thousands of places and unfortunately can easily be stolen.

While such an event would not be nearly the catastrophe a nuclear explosion would be, it would be much easier to execute and thus harder to prevent. At one extreme, such events may be impossible to prevent. But others may be possible to prevent. The measures and capabilities we discuss and recommend for dealing with the nuclear explosion threat will also expand the range of capability against dispersal events.

Resources Requirements

Developing a capability to deal effectively with the nuclear threat across a broad front will require more resources. More resources are warranted both because of the new prospects for improved capability that we have described, and because the threat itself is now a truly central issue in the national security arena.

The prospects for dealing effectively with the nuclear threat that we have tried to evoke in the preceding discussion demand a long-term view. Over the long term, resource requirements should be viewed in three overlapping phases:

- A five to ten year program to develop the greatly improved capabilities that we assert are feasible. We estimate increased funding requirements for the first five years of this program in more detail below and in Attachment B. (During this period, of course, some level of increasingly improved operational capability will be maintained and exercised.)
- Long lead preparations for later, very large scale procurement and deployment of the improved capabilities being developed.
- Large-scale procurement and deployment. *The full capability we envision could cost a few billion dollars to procure and perhaps several hundred million dollars a year to maintain at a high level of operational readiness.* We believe planning on the basis of this level of future

resource expenditure is commensurate with the possible future threat (or perhaps even the current threat.) Whether or not these resources would actually be requested by a future administration and authorized and appropriated by a future Congress would of course depend on the circumstances at the time. If the future security environment warrants it, these capabilities might be procured and operated as they become available; or they might be kept at a lower level of readiness, able to surge in weeks or months as the situation demands. Be all this as it may, we believe strongly that the development program over the next five to ten years should be planned on the basis that procurement and operational resources at the level we posit here could become available.

The first five years of the program we recommend will require roughly the following additional funding, beyond what is already planned:

Year	DOD	DOE
FY99	$5M	$5M
FY00	$65M	$50M
FY00-FY04	$250M	$600M

We are aware that FY99 budget planning is already quite firm. Accordingly, we show a minimal increase in FY99, which could be reprogrammed within the already existing budget. These amounts could be used for planning the larger increases shown for FY00 and beyond. More accurate costs must wait for detailed program plans. A somewhat more detailed categorization of estimated costs is at Annex B of this report.

Conclusion

We can't be certain that the improved capabilities we have discussed and recommended would suffice, in dealing with the nuclear transnational threat, nor are we entirely certain what "suffice" means over the long term. The history of terrorism and counter-terrorism may contain useful insights. For example, in response to the wave of airplane hijackings in the 1960s and 1970s, anti-hijacking measures were put in place. These measures were, and are, far from perfect, but the frequency of aircraft hijacking dropped dramatically. More recent experience is similar; terrorists are often deterred or deflected when confronted with known counter-terrorism measures that are less than perfect.

If a terrorist nuclear explosion occurs, it will be the first one. If an air hijacking had never occurred before the improved capabilities had been put in place, what would have been the course of events? The analogy is imperfect, but indicates one way to think about the problem, especially since the nuclear event is more difficult for the adversary to achieve.

If the future holds a terrorist nuclear explosion (given our *current* capability and *current* plans to extend that capability), then the *further improved* capabilities we assert are feasible with a comprehensive architecture and a long term program will substantially reduce the future likelihood of such an explosion and/or significantly delay the time when it occurs. Like everything else about the risks of nuclear weapons, over the sweep of history the underlying

objective is to buy time for political and perhaps social developments to take place which would make the risks irrelevant.

Annex A: History of the US and Nuclear Threat Response Capabilities
Annex B: More detailed cost estimates in FY99-FY04

ANNEX A:
A HISTORY OF DEVELOPMENT OF U.S. CAPABILITY TO DEAL WITH THE NUCLEAR TRANSNATIONAL THREAT

The first recorded non-nation-state nuclear threat against the United States occurred in 1970 when a 14 year old high school student deposited an extortion note on the windshield of an Orlando, Florida, law enforcement official. This note contained crude drawings of an "atom bomb" that would have been discarded out-of-hand by knowledgeable nuclear weapon experts; however, there was no system available at the time to evaluate such matters. Considerable consternation ensued.

Later, in 1974, Dr. Theodore Taylor published "The Curve of Binding Energy" in which he expressed his concerns about the probability (and ease) of construction of improvised nuclear devices by terrorist groups. Dr. Taylor, as a former Los Alamos weapon designer, outlined a credible scenario that was reviewed in the New Yorker magazine and received wide attention. Subsequently, a large number of hoax nuclear extortion threats were received by various government agencies. This type of threat has continued over the years, with a current total number over 120, but only one has involved actual nuclear material (low-enriched uranium reactor fuel powder stolen from a Wilmington, NC, processing plant).

Concern had arisen in the nuclear weapon community during the early 1970's that projected growth in world-wide power reactor numbers would generate large quantities of plutonium, which might not be properly safeguarded, and that nuclear device design information would become more available as time passed. Various actions were taken to improve nuclear material safeguards and protect design information, but it became clear that measures were needed to prepare for the possibility of "loose nukes." Accordingly, in late 1974, the AEC Director for Military Applications sent a letter to the Directors of Lawrence Livermore, Los Alamos, and Sandia Laboratories and to the Manager of the AEC Nevada Operations Office tasking them to establish and support what became known as the Nuclear Emergency Search Team (NEST).

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

Another milestone occurred in January 1978, when the team deployed to Canada to aid in locating nuclear reactor debris from the Soviet satellite, COSMOS 954. This successful operation

generated worldwide attention and exposed the team to operations under very difficult environmental conditions. It also provided experience in rapid deployment and had a significant impact on field organization and logistics planning.

NEST deployed to Reno, NV, in 1980 to search Harrah's Club in response to a plutonium radiation dispersal threat. While the threat was never substantiated, the operation demonstrated that they could search a large commercial facility without being detected by the media or public. This was done in a period of 18 hours.

Exercises continued with various military and/or civil organizations over the next few years, but the first NEST field exercise with major FBI participation was held in 1983 in Albuquerque, NM. While this operation provided an opportunity to explore FBI/DOD/DOE field organizational issues, it also tested the concept of conducting searches with local emergency personnel who are trained for the task on the spot. The concept did not work very well, largely because of complexity of the search equipment, and the method used to solve the problem was to train a cadre of approximately 200 "reserve searchers" who could be given annual refresher training and thereby maintained in a qualified status. This concept continues today, although there is a desire to obtain search equipment with built-in intelligence so as to avoid the expense of on-call personnel.

The largest and most comprehensive field exercise that involved the NEST organization, code named "Mighty Derringer," was held in 1986 under the aegis of the National Security Staff. This exercise included high level Washington management participation from DOD, DOE, FBI, CIA, and FEMA, in addition to field elements at locations in Indianapolis, IN, and the Nevada Test Site. Many technical and organizational issues were addressed in this exercise, but the most important dealt with how the Washington management structure would deal with such an emergency. An exercise of this size and scope has not been held since.

Many exercises have been held since 1986, dealing with different military organizations, CONUS and OCONUS scenarios, different technical issues and different physical locations. The most recent that dealt with a US domestic threat was the Mirage Gold exercise in New Orleans, LA, in 1994. Emphases since that time have been on OCONUS scenarios. There is a continuing need to train new personnel to replace those lost through normal attrition, but opportunities for technical teams to practice their skills in the field are limited by available funding.

Throughout its history, NEST personnel have worked to improve their technical capability. However, they still lack tools to deal with various threats that have been defined. There are limitations caused by the laws of physics and by insufficient information about any particular threat with which they must deal, but there are numerous forward looking ideas that have been proposed for search, diagnostics, and disablement use. Unfortunately, this program has had little resource available for advanced R&D, which means that most of these concepts have not been investigated. If the transnational nuclear threat is to be recognized as a high priority national problem, healthy R&D funding of the order of 50M$ per year needs to be applied to exploit these possibilities.

Another problem that has arisen in recent years has to do with DOD teams with which DOE NEST deploys. Original arrangements for joint operations in a domestic nuclear threat problem included US Army FORSCOM EOD personnel for all "hands-on" operations on a nuclear terrorist device. Training for these EOD personnel has included application and use of DOE-developed equipment for diagnostic, disablement and containment use, in conjunction with DOE

scientific personnel. Later training for OCONUS operations has been in support of special operations forces who plan to accomplish their mission without the presence of scientific personnel at the location of a field operation and who have a much more limited technical capability. Thus, DOE teams must train for two different missions with two different military groups. This issue needs resolution by SECDEF and SECENG soonest.

Improved Capability Against the Nuclear Transnational Threat: Additional Costs Beyond Current Budgets / Plans ($Millions)

	DOD			DOE		
	FY99	FY00	Thru FY04	FY99	FY00	Thru FY04
Protect Nuclear Materials						
In Russia:						
♦ Augment CTR & MPC&A		30	50		0	
♦ Extend CTR & MPC&A		5				200
World Wide MPC&A		0	0		5	
Intelligence		10	50		2	10
Terminal Defense						
Networks and Search		5	50		20	200
Access / Diagnostics		5	50		10	50
Render Safe		10	50		10	100
Long Range R&D					5	50
TOTALS	5	65	250	5	52	610

REPORT OF THE CHEMICAL/BIOLOGICAL WARFARE COMPETENCY PANEL

Panel Chairs

Dr. Ted Gold

Dr. Robert Beaudet

Panel Members:

Dr. Robert Boyle

Dr. Jeffrey Grotte

Dr. Mim John

Mr. David Kay

Dr. Donald Prosnitz

Dr. Brad Roberts

MG Jan Van Prooyen, USA (Ret)

Dr. Scott Ward

Dr. George Whitesides

Panel Advisors:

LtCol Richard Benson, USAF

CAPT James Brick, USN

BG Walter Busbee, USA (Ret)

MAJ John Driftmier, USA

Mr. Raymond Geoffroy

LTC Al Hardy, USA

Dr. Anna Johnson-Winegar

Mr. Robert Joseph

CDR Mike McDermott, USN

Maj Ron Marks, USAF

Mr. Robert Mata

Dr. William Shuler

LTC Mike Urban, USA

Dr. James Valdes

TABLE OF CONTENTS

SUMMARY 1

THE TRANSNATIONAL CBW THREAT 7

CURRENT DOD POSTURE FOR COMBATING THE CW AND BW TRANSNATIONAL THREATS 16

ELEMENTS OF A STRATEGY TO DEAL WITH TRANSNATIONAL CW AND BW THREATS 21

- 4.1 Don't Treat BW as Too Hard 21
- 4.2 Defense In-Depth 24
- 4.3 Intelligence 26
- 4.4 Establishing a National Consequence Management Capability Within the National Guard 28
- 4.5 End-to-End System Approach 36
- 4.6 Force Projection and Protection 38
- 4.7 Interagency Issues 41
- 4.8 Enhance it's CBW Defense Capabilities Base 45
- 4.9 Additional Measures to Improve Domestic Response 47
- 4.10 Science and Technology 50
- 4.11 Preventing and Deterring CB National Attacks 56

CONCLUSIONS 59

ANNEX: SCIENCE AND TECHNOLOGY OPPORTUNITIES 62

- Functions and Tasks 62
- Applicability of Existing Capabilities and Those Under Development 76

SUMMARY

"The basic principles of freedom, justice and concern for human life on which our nation was founded have survived major threats during the course of America's history. Today, we face a unique and pervasive challenge to these ideals in the form of terrorism, an increasingly serious threat to the United States and its friends and allies around the world."

While these words, from a report of a high level government Task Force on Combating Terrorism, reflect today's growing concern about this threat, they were written more than a decade ago. The Task Force that issued this report in February 1986, led by then Vice President George Bush, was established in response to the 1980s world wide wave of skyjackings, ship highjackings, car bombings and other acts of terrorism.

Thus, the threat from transnational groups is not new since the end of the Cold War. Indeed, the number of transnational threat incidents per year is considerably lower than a decade ago, a reduction due, at least in part to actions taken by the US Government in concert with other nations since the mid 1980s.

However, there is a new and ominous trend — a proclivity of these groups towards inflicting much greater levels of violence per incident. Some transnational groups apparently now have the motives and are seeking the means, through access to weapons of mass destruction and other instruments of terror and disruption, to cause great harm to our society.

Two incidents in particular are illustrative of the new threat. The perpetrators of the 1993 World Trade Center bombing and the 1995 Tokyo Subway nerve gas attack were aiming for tens of thousands of fatalities. The Aum Shinrikyo Sect that carried out the Tokyo subway attack (killing a dozen people and injuring thousands more), released chemical warfare (CW) nerve agent the previous year in Matsumoto, Japan (an attack which resulted in seven deaths and attracted surprisingly little attention in the US) and prepared to attack US targets. The sect was also developing and testing much more lethal biological warfare (BW) agents. The perpetrators of the World Trade Center bombing reportedly also considered the possibility of combining lethal chemical agents with the high explosive detonation as a means to kill many more.

One must be cautious in deriving "lessons" from this handful of incidents. Certainly we cannot gain much comfort from the failure of these groups to achieve their goals and conclude that such horrendous acts are beyond the capabilities of substate actors. While developing a usable CW or BW capability is not quite as simple as sometimes depicted in the popular press, other groups, even without any state support, will likely be able to put together the requisite mix of technical skills and operational savvy to plan and execute devastating CW or BW attacks.

It is this "new" aspect of the transnational threat — groups with both motives and means to cause great destruction and damage — that is the driving concern of the DSB study. The US may now be facing groups less concerned with gaining political legitimacy and a seat at the table (which therefore had reasons to place some limits on the consequences of their actions) and instead more interested in bringing down the house (motivated by apocalyptic or Armageddonist visions). CW, and particularly BW, offer a means for the few to inflict levels of casualties here-to-fore assumed to require the resources of nations. Furthermore, by their very transnational and subversive nature, such groups do

not provide territories or homelands to hold at risk. This "lack of a home address" may allow transnational groups, not only to mount solitary attacks, but also wage campaigns of terrorism against the US with much greater impunity than nation states could get away with.

This CW/BW Panel (and its parent Task Force) focused on the role of the Department of Defense (DoD) in dealing with this emerging threat. DoD clearly must be prepared to counter attacks by transnational groups that threaten DoD personnel and interfere with DoD's ability to perform its missions. The Task Force also addressed how DoD could contribute to mitigating the more general transnational threat to US society at large. DoD has much to offer — expertise, capabilities, experience — but working effectively to improve domestic preparedness require building on relationships being forged in counter-drug and other activities to achieve unprecedented levels of cooperation with other Federal, State and local agencies.

DoD's role in combating the transnational threat must fit within a larger US effort. While the CW/BW Panel addressed potential DoD roles within this broader context, defining a comprehensive national effort was beyond the scope of this DSB study.

The final report of the 1997 DSB study of the transnational threat urges the DoD to devote more attention and resources to dealing with this emerging danger and recommends a strategy to guide DoD's efforts. This appendix to the report elaborates DoD's role in combating the chemical and biological warfare aspects of this threat.

Our observations and recommendations are summarized in the dozen elements of the following strategy that we propose DoD adopt to deal with the threat of chemical/biological warfare (CBW) from transnational groups.

1. DoD should take the CBW threat posed by transnational groups very seriously and prepare for the long haul. The potential for CBW attacks by transnational groups will not soon go away. DoD expends a substantial part of its energy and resources towards dealing with major theaters of war. It is plausible to assume that a transnational threat attack using CW or BW is just as likely as a major regional contingency and the consequences for the United States potentially at least as severe. As part of its responsibility for domestic preparedness we recommend that DoD make a more enduring commitment to the Nunn-Lugar-Domenici (NLD) program by retaining stewardship in FY99 and beyond, and expending the scope of the program. NLD provides training and other assistance to local emergency responders to help them deal with CBW incidents.

2. Recognize that the differences between chemical and biological warfare agents are at least as significant as their similarities. The means of production are different and BW can be far more toxic: a few kilograms of CW can threaten lives within confined areas or over a few city blocks, while the same amount of BW agent can threaten an entire city. Furthermore, the effects of BW agents occur more slowly than CW, making detection and attribution far more difficult in transnational threat attacks.

3. Don't treat the threat as "too hard". The biological warfare threat in particular can appear so formidable that it can lead to inaction — "its too hard!." It is indeed too hard to devise totally effective defenses or cover all possible scenarios. Our study, while identifying many useful steps and applications for new technologies, found no "silver bullet" that will deal effectively with the entire range of BW threats. A focus on incremental steps that contributes to mitigating the threat and raising

the price to potential attackers is more likely to lead to a sustainable effort in the long run. Thus, there is considerable merit in Richard Danzig's (the former Undersecretary of the Navy) prescription to "think small" with respect to BW defense.

4. Fashion a defense-in-depth strategy and posture but tailor it to the special challenges presented by the CBW threat. Place special emphasis on consequence management and intelligence. All the elements of defense-in-depth — dissuading and denying possession, deterring use, intercepting delivery, mitigating consequences and identifying and punishing the perpetrators — can contribute to combating the CBW threat from transnational groups.

Highest priority should be accorded to managing and mitigating the consequences of a CBW attack. There are two reasons. One, we cannot count on preventing CBW attacks and two, so-called passive defense measures can be very effective in reducing casualties (perhaps by several orders of magnitude through a combination of warning and monitoring, individual and collective protection and timely medical treatment). Clearly, it would be preferable to deny possession and prevent attacks rather than have to try to ameliorate their effects. However, the very small signatures that may be associated with CBW production and possession as well as the multiple, and difficult to intercept, delivery means available to potential attackers implies a leaky front-end of any defense-in-depth. Thus, we must be prepared to deal with the consequences of CBW agent release. Managing the consequences of an attack not only includes minimizing the physical and environmental traumas but also influencing public and media perceptions and dealing with adversaries who might be planning their next move in a campaign of terrorism.

Next in priority is getting smarter about the threat through a more focused and aggressive intelligence effort. The intelligence community (including its DoD components) has only recently paid much attention to the CBW threat, and it has concentrated on the threat from nation states. The intelligence community will need to focus more attention and resources to the substate aspects of the CBW threat. Because of the nature of this threat the effort will be heavily reliant on human intelligence (HUMINT). It will also require new sampling and collection techniques, sensitive analytic capabilities (to pull very small signals from cluttered backgrounds), better communication and sharing of information with law enforcement agencies, more effective use of open sources and involvement in epidemiology studies to assess "outbreaks" of unusual diseases that may provide clues to BW production activities.

While deterrence will play a much lesser role against these substate actors than it did against our Cold War adversary, DoD should not ignore its potential contributions. Among the steps it can take would be to set up (in cooperation with other government agencies) a "Human Factors Assessment Center". Its objectives would be to better understand the motives and values of potential substate users of CBW and to identify means to strengthen deterrent mechanisms against these groups. One fruitful avenue of investigation would be to illuminate both the costs (e.g., exposing vulnerabilities) as well as potential benefits of various ways to "publicize" US capabilities to defeat and mitigate attacks.

5. Build on existing organizations and processes as much as possible. Our main recommendation here is a strong consequence management role for the National Guard and DoD reserve components in responding to CBW terrorism. The Guard offer important advantages: distributed throughout and "owned" by the States, vested interest in local communities, communication and training networks, and they are not constrained by Posse Comitatus.

We propose two main roles for the National Guard (NG): 1) as a major conduit for the CBW defense training (initial and sustainment) that the DoD and other Federal agencies have to offer local responders and 2) as a consequence management "second responder" capability to support local and other state agencies in dealing with CBW incidents.

Both are vital and formidable tasks. Training the first responder community, numbering in the millions and characterized by high turnover, to perform tasks not part of their daily activities, will require innovative approaches and close coordination with centers of expertise in the Services (including Reserve components) and other government agencies. The consequence management "second responder" capability can be achieved by establishing "Chemical/Biological Incident Response Force (CBIRF) -like" units at the State and regional levels. In addition the NG could also contribute to promoting threat awareness at the local level and provide a CBW augmentation force to the CINCs. We offer specifics regarding this recommendation in section 4.4 of this appendix.

6. Get smarter about options to deal with this threat. Mitigating the CBW threats from substate adversaries presents much that is unfamiliar. Our advice is that DoD should do what it has done in the past when presented with new and difficult challenges. Gather a diverse group of smart people and give them the time and resources to get their arms around the problem by taking an end-to-end systems approach. Specifically we recommend setting up two temporary task forces for at least 18 months. One, reporting to the Joint Staff would address the operational aspects of responding to the threat; the other, reporting to the Under Secretary of Defense for Acquisition & Technology (USD(A&T)), the systems and technical aspects. The groups would be integrated together and use analysis, models, simulations, red teaming, experiments and exercises to identify and evaluate materiel, training and operational options. The groups should consider both force protection and domestic preparedness roles for DoD. The objective is to provide a sounder basis for an investment strategy and operational decisions.

7. Recognize and organize around the strong connections among force projection, force protection and domestic preparedness. Our main message is not that DoD should take on a new mission but rather that DoD will be unable to accomplish its core business unless it pays much more attention to the CBW transnational threat. The ability of the US military to project force globally depends on keeping open ports and airfields, both in the United States (points of embarkation, POEs) and overseas (points of debarkation, PODs).

In time of crisis or war, these POEs and PODs may be the preferred targets for paramilitary and transnational threat CBW attacks in order to delay and disrupt time critical US military deployments. DoD cannot project force if it cannot protect its forces (including those in the US) from CBW attacks during deployment. Furthermore, force protection as defined by the DoD extends not only to military personnel but their families as well. Thus, in order to fulfill its force projection and force protection responsibilities the DoD must develop capabilities directly relevant to domestic preparedness. (An attack on a port in the US is an attack on civilians.)

8. Exploit synergy with counterproliferation related CBW defense activities and build on recent initiatives directed toward the transnational threat. The DoD has not been oblivious to the CBW threat, particularly since the Gulf War. While the major concern has been the CBW threat from nation states, some of the current passive defense elements of DoD's counterproliferation activities are relevant to the transnational threat as well (e.g., much of the Defense Advanced Research Projects

Agency's (DARPA) growing Research & Development (R&D) efforts directed at BW defense). (The attack operations and active defense components of counterproliferation are considerably less relevant to addressing the CBW threat from transnational groups). However, we note, that even since the Gulf War highlighted the seriousness of the CBW threat, support in the DoD for robust CBW defense programs has varied. While Secretary Cohen added a billion dollars for CBW defense (over five years) in the recent Quadrennial Defense Review (QDR) exercise, two years ago there was a serious attempt within DoD to cut a billion dollars from CBW defense and counterproliferation. The United Nations Special Commision (UNSCOM) revelation at that time about the formidable Iraqi BW offensive capability during the Gulf War helped block the proposed cut.

Recent DoD initiatives and activities to deal directly with the CBW transnational threat include: creation of the Marine Corps CBIRF, establishment of a Force Protection Cell in the joint Staff, creation of a CBW Quick Response Force under the Army's Chemical/Biological Defense Command (CBDCOM) and a Response Task Force structure under US Atlantic Command (USACOM) for consequence management incidents in the Continental United States (CONUS), leadership of the Technical Support Working Group (TSWG) (a useful interagency effort to focus counterterrorism R&D), the BIO-911 and other Advanced Concept Technology Demonstrations (ACTDs), and the city training and other efforts funded by Nunn-Lugar-Domenici.

Another DoD resource that should be drawn upon to help with the CBW threat is the many years of experience in dealing with local and state agencies in preparing for CW emergencies around US chemical stockpile sites (under the Chemical Stockpile Emergency Preparedness Program).

9. Expand and nurture DoD's unique but fragile CW and BW defense capabilities base. DoD has special capabilities in the CBW defense arena, but these are stretched thin and are vulnerable to "fair share" cuts in this time of downsizing. BW-related capabilities are particularly fragile. Our recommendations to enhance this base include

- Increasing (threefold) the medical staffing at the US Army Medical Research Institute for Infectious Diseases (USAMRIID) and the US Army Medical Research Institute for Chemical Defense (USAMRICD) devoted to supporting Commander-in-Chiefs (CINCs) and domestic preparedness and improving forensic capability.
- Increasing military staffing at the Army's Technical Escort Unit (TEU) to enhance readiness to support domestic preparedness as well as CINC needs.

10. Sustain a broad technology and robust development effort in chemical and biological defense (including detection, individual and collective protection and decontamination). Until recently, CBW defense was not a high R&D priority for DoD. The current effort is largely aimed at protecting US military forces engaged in major combat operations. This effort should be expanded to encompass defenses applicable to the broader definition of force protection (e.g., to include DoD personnel and their families) and to domestic preparedness. Candidates for increased attention include low cost alarms, and masks, stand-off real time CBW detectors, field employable mass spectrometers for BW analysis, rapid large area decontamination methods, decontamination standards, antidote autoinjectors for civilian use, multivalent vaccines and anti-viral agents.

11. Work on critical relationships. We highlight four sets of partnerships/relationships that DoD must establish and sustain in order to maximize its contributions to combating the transnational CBW threat. These are with:

- **Other Federal agencies:** DoD will need to expand on the relationships it has built with other government agencies in responding to natural disasters and supporting the war on drugs. A strong national domestic preparedness posture against the CBW threat will require the heavy involvement of DoD's expertise and resources. A DoD stance of "call us if you need us" will not suffice. On the other hand, our nation's laws and values are not compatible with military control of "domestic operations". DoD must take on deep responsibilities for various aspects of domestic preparedness without having operational command in most circumstances. This posture will present a challenge for a DoD used to being in charge of operations, but the relationships are familiar. DoD must assume the role of the supporting CINC to other agencies (Federal Bureau of Investigation (FBI), Federal Emergency Management Agency (FEMA)), who, depending on the circumstances, will serve as the supported CINC.
- **Local and state first responders:** We have already touched on a critical role for the National Guard in this area. DoD's role is as a provider of expertise, training, advice, tools, equipment, and of follow-on response forces to augment crisis and consequence management efforts.
- **The US biotechnology community:** The US biotechnology community (spread out in universities, research institutes, small biotech firms and large pharmaceutical companies) is the world leader in this field and possesses the knowledge and tools to help DoD understand the threat and devise defenses against it. DoD must forge much closer ties to this community which has little motivation or incentive for such close ties. Brokering this relationship and getting this community involved in defense against the CBW threat will require the involvement of the most senior government officials, as well as support from the Congress, to provide financial incentives, appeals to patriotism (or ego) and perhaps assurances on the strictly defensive nature of the work.
- **The Russian BW program:** Russia still has a robust program involving many tens of thousands of personnel and world-class facilities. It is clearly in the US interest, not only to ensure the termination of Russian offensive BW work, but also to keep this expertise off the street and away from both state and substate entities with an interest in biological weapons. US goals should be to integrate the Russian scientists into the global community. The high quality of their personnel also offers opportunities for joint efforts to improve public health. There are a few pilot initiatives underway which should be evaluated with the objective of identifying potentially larger follow-on projects. These projects would serve as the base for extending the Nunn-Lugar program to cover BW as well as nuclear.

12. Incorporate a capability to surge as explicit elements of DoD's strategy and posture to deal with the transnational CBW threat. A hedge strategy and posture — with a strong surge component makes sense because of the great uncertainties about the CBW threat — it is currently more potential than actual and can evolve in so many different ways. During the cold war, explicit hedge programs, with their inherent uncertainty, found it hard to compete for resources with their less conditionally based counterparts, but the Quadrennial Defense Review identifies a key role for hedge programs in the new security environment. Surge elements of the posture could include investments in facilities, long lead items, cadre training, mobilization plans for Reserve and Guard units, and other actions which would foster a rapid expansion of capabilities.

In summary, the potential of chemical and biological weapons in the hands of transnational groups casts an ominous shadow as we move further away from the cold war. DoD must devote more of its attention and resources to help the nation deal with this grave challenge. Considerable effort is already being invested in improving relevant capabilities and the foundations exist for a much more effective posture.

THE TRANSNATIONAL CBW THREAT

Surveying the Threat

This section will cover

- Definitions and Trends
- Targets
  - Overseas and at home
- Actors
  - Old and new
- Modes of attack
  - Single events, multiple, campaigns
- Chemical and Biological Warfare Agents
  - Differences

As the geopolitical structure of the Cold War collapsed, it enabled increased threats to the United States and its interests by organizations and individuals with motives and methods quite different than those posed to the nation during its confrontation with the Soviet Union.

The nature of these threats are such that they are usually not located in or identified uniquely with any particular nation. In addition, their mode of operation often involves routine movement across national boundaries, including those of the United States.

The Transnational CW/BW Threat is defined to include potential attack on the United States, US military forces, and friends, allies, and interests abroad by non-state or state-sponsored groups with biological or chemical means. The full DSB task force provided an integrated assessment of this threat and a comprehensive DoD strategy for beginning to address it. This report focuses on the chemical and biological dimension of the transnational threat.

The New Threat is Different and Dangerous

Different:

- No geographical base; few or no assets; obscure foreign relationships; unknown values
- Presents difficulties for our traditional methods for intelligence, diplomacy, deterrence, and warfighting.

Dangerous:

- Technology allows transnational threats to threaten and inflict levels of damage heretofore achievable only by nation states
- Transnational threats are hard to detect and deter nature of threat allows the few to conduct campaigns of sequential "shocks" with far greater impunity than nation states could get away with.

Technology diffusion is increasing the threat: The diffusion of technology and materials associated with CBW has increased the potential threat to US forces from both state and non-state actors, as more entities gain the equipment and materials to make and deliver CW and BW agents.

Expertise is widely available: Technical and industrial globalization has accelerated the diffusion of expertise applicable to CW and BW agent production, as has the Internet. Expertise related to weaponization and delivery is reportedly available for hire from Russia and elsewhere, whether individually or through transnational criminal organizations.

The Iraqi example: UNSCOM has revealed just how much can be accomplished by a small group working in isolation from international resources and with modest financial investments.

The Transnational CW and BW Threat is Real and Difficult to Detect

World Trade Center bombing:

- Purpose was to kill 50,000 or more people
- Bombers experimented with chemical agents in truck bomb

Tokyo subway attack:

- Aum Shinrikyo killed 12 people and sent thousands to the hospital
- Had previously used both chemical and biological agents in attacks
- Planned to conduct operations in United States

Oklahoma City bombing also reflected trend toward attacks by transnational threat groups aimed at killing as many people as possible, rather than "just enough" to gain media attention.

For most Americans today, terrorism and the broader set of acts by transnational threat groups are something that happens in other countries. But the United States has not been spared from the new turn in transnational threats, and the CW and BW threats are an important element of this changing threat profile.

The 1993 bombing of the World Trade Center was aimed at killing as many people as possible-at least 50,000 in the tower itself, and more in the immediate vicinity had the building in fact collapsed. Although reports are contradictory, it is widely believed that the truck bomb included a canister of nerve gas intended to cripple emergency first responders. Indisputable is the fact that bombers maintained a laboratory where they developed and produced chemical weapons.

The Oklahoma City bombing similarly reflected a departure from the familiar form of terrorism, "that wants a lot of people watching but not a lot of people dead." The bombers aimed at inflicting maximum casualties on a symbol of the federal government.

In Japan, the Aum Shinrikyo sect developed an extensive CW and BW production base and attack capability over a number of years. It also conducted attacks with chemical (and reportedly also with biological) warfare agents prior to the well known subway attack — some of which were lethal. In subsequent courtroom testimony, it has been learned that the sect contemplated attacks on targets in the United States and developed alternative techniques for smuggling nerve agents into the United States.

Many Americans also believe that the use of CW and BW agents outside of war is unknown in our history. In fact, such substances have been used in more than 250 criminal incidents in the United States over the last two decades, typically by lone perpetrators for purposes of extortion or revenge, but sometimes for political purposes. The FBI also reports a dramatic increase in recent years in the number of cases in which the weapons, technologies or agents of mass destruction have been an element.

Thinking About the CW AND BW Threat - Strategically

Past:

- Classic terrorism was aimed at generating fear in order to extract an immediate political concession from the state.
- Mass casualty attacks were deemed unnecessary and/or counterproductive.
- The non-state CW and BW threat was nearly non-existent.

Present:

- New transnational actors have begun to appear who utilize violence for reasons other than a short-term political goal.
- Motivated by hatred, revenge, a personal holy writ, or a desire to achieve some long-term goal, they may be unrestrained in the number of deaths they inflict.
- CW and BW are an element of their arsenal

Future:

- Classical terrorism and the newer transnational threats coexist.

Both "classical terrorists" (i.e. those seeking political objectives) and today's new class of threats, including those able and willing to employ CW or BW agents (i.e. those seeking transnational aims) seek the operational means to disrupt civil society, induce fear and panic, and demonstrate the inability of government, as presently constituted, to provide security.

While deterrence and prevention of the transnational CW and BW threats must remain primary objectives, thwarting the disruption and consequence associated with such action that do take place may be even more important to the larger objective of limiting the threat. Preventive and deterrent capabilities that are backed by effective means for limiting the consequence acts of transnational groups, thus depriving the CW or BW act of its intended consequence, offers the most effective means of combating this transnational threat.

The effectiveness of the government response to the first cases of CW or BW may have an important impact on the future course of such threats.

Thinking About the Transnational CW and BW Threats – Operationally

- Recognize that the objectives and characteristics used to analyze classical military utility of CW and BW are of limited relevance to possible transnational uses.
- Recognize that threat capabilities range from those with substantial access to state programs to those operating alone and with no access to state programs
- Distinguish CW from BW.
- Distinguish civil from military targets.
- Expect innovation in the tactics of transnational actors, for example:
  - Coordinated campaigns
  - Deception and deliberate hoaxes
  - Mixed agents
  - Unexpected delivery methods
  - Misattribution, etc.

The threat can come from groups ranging from single individuals (the unibomber) to many thousands (Aum Shinrikyo). The threat could be state supported, have access to the financial and technical resources of powerful non-state organizations (crime syndicated) or be totally independent. They could attempt to purchase or steal CW or BW agents or produce their own. They could gain access to "classical" CW and BW agents or they could create their own threats using industrial chemicals (e.g. chlorine), pesticides, anthrax or livestock agents. Further, transnational actors might acquire, with some outside help, novel agents with unexpected properties, lessening the effectiveness of existing detection, protection and therapeutic measures.

Potential US Targets for CW or BW Attack by Transnational Threat Groups are Overseas As Well As in CONUS

Overseas:

- There is a threat to deployed military forces in times of war, near-war, or peace.
- Requirement to addressing CW and BW threats as part of the overall force protection mission.

Domestic:

- There is a threat to the American public and institutions.
- Requires responses by law enforcement and civilian emergency management.
- Military role in bolstering civilian capabilities and developing technology--and in stepping in when crises outstrip local capabilities.

CONUS-based military forces may be targeted by foreign or domestic transnational entities, both abroad and at home. Citizens and military forces of other countries may also be attacked by transnational entities in places where those attacked will expect US military assistance. There is also likely a requirement to have the ability to extend force protection to families and infrastructure, to US diplomatic and business sites and to host nations in a large scale CW or BW event.

The Threat Overseas

OCONUS US forces are in CW and BW harm's way:

- In both Southwest Asia and Northeast Asia, US military forces are deployed to deter aggressors assumed to be armed with CW and BW.
- Temporary deployments for peacekeeping and other operations also put US forces in places where chemical and biological weapons may exist.

Use of CW/BW can be an effective asymmetric strategy:

- Confronted with overwhelming US conventional power, aggressors may see CW/BW threats as attractive for dissuading US intervention or coalition formation and see CW/BW attacks as effective at defeating arriving forces.

Forces in battle are not sole target:

- In crisis and war, CBW can be used to attack US military infrastructure (overseas and at home), dependents, and host nation support assets.

The CW and BW threat to Outside the Continental United States (OCONUS) forces is real and immediate. US forces are deployed in precisely those regions where these weapons are proliferating, where state sponsors are found, and where there are both groups and individuals strongly motivated by hatred of the United States.

If those states find themselves at war with the United States, their leaders are likely to use all means available to retain their grasp on national power. For this purpose, they may see CW and BW as useful, especially in modes of attack other than on the immediate battlefield.

Given the higher cost and higher signature of nuclear weapon possession, use of CW or BW agents may be more likely than nuclear weapons. A capability to kill many Americans may be viewed as necessary to induce the desired media coverage, public hysteria, and shock to US decision makers to deter US engagement or to cause disengagement.

The Threat to the US Homeland

- The bombings of World Trade Center and of the federal building in Oklahoma City signaled the existence within the United States of individuals and groups motivated to kill as many people as possible.

The domestic threat is evolving in much the same ways as the foreign one:

- Technology, materials, and expertise on CW and BW agents and delivery techniques are diffusing.

Illicit domestic interest in poisons is not new:

- Between 1974 and 1994, chemical substances were used in about 170 criminal activities and biological more than 30, for extortion and other purposes. About one quarter of the perpetrators had a political goal.

The bombing of the World Trade Center Tower was a reminder of the presence within US borders of transnational actors with a strong hatred of American power, society, values. Oklahoma City was a wake-up call to the existence within the United States of individuals and groups willing to kill in support of religious, ideological, or political beliefs.

Transnational Threat Groups: Real and Potential

- Remnants of classical terrorists
- Ethnic groups and separatist movements
- Religious extremists
- Anti-government militia
- Narco-traffickers and other transnational criminal organizations
- Others motivated by a desire for revenge, to expunge a hated enemy, or to sow anarchy
- Individuals who utilize violence to try to change the course of history

Ethnic and separatist violence is not unknown to America, nor is violence motivated by matters of class or religion. But our history includes few instances of violence by groups or individuals motivated to cause mass casualties.

Today, it is possible that a mix of social, economic, political, religious, and other factors might coalesce in the militia movement to cause a new, unprecedented form of domestic violence, one in which mass casualties are seen as both necessary and just.

Between 1994 and 1996, over 800 militia or Patriot groups were identified. More than 15% of these had direct ties to the racist right (Aryan Nations or Ku Klux Klan); others motivated by hatred of the federal government ("a terrorist state"), by fear of the New World Order (and its supranational and multinational corporate representatives), or by extreme religious fundamentalism.

Militias have produced ricin and other BW agents, are stockpiling antibiotics, are currently recruiting new members among cropdusters, and have practiced plans for attacks on the Bureau of Alcohol Tabacco and Firearms (ATF), Internal Revenue Service (IRS), Army Corps of Engineer facilities, and other federal facilities.

CBW Attacks Could Be Part of an Orchestrated Campaign by Transnational Groups

TYPE:	Isolated Events	Multiple Events	Orchestrated Campaign
EXPERIENCE:	*Some US*	*Extensive global*	*"Next Lenin"*
IMPACT ON DoD MISSION OVERSEAS	*Casualties limits operations*	*Seriously constrains erodes coalition support*	*Mission failure disengagement*
IMPACT ON NATIONS	*Localized societal trauma*	*Serious economic & national impact*	*Creates national upheaval*

CW and BW attacks may be isolated, single events, with no or few fatalities. They may be aimed at a single individual, facility, or institution. More ominous, they may be pursued in a campaign aimed at

transforming public attitudes toward the state or even collapsing society. BW attacks across very large areas and in multiple cities that cause unprecedented peacetime human suffering are within the reach of groups operating with state sponsorship. Fred Iklé[1] has described the potential change that might be forced on society by a "next Lenin" willing to use Weapons of Mass Destruction (WMD) to achieve his purposes and skillful enough to conduct campaign style attacks on one or more societies.

Isolated events: Likely to produce localized trauma and not to have significant political repercussions, whether at home or abroad, assuming fatalities are few. But even isolated events could be politically significant if they lead to loss of life and property unprecedented in peacetime.

Multiple events: Can be caused by a single group or result from uncoordinated "copy cat" attacks. If domestic, likely to generate public debate about whether the government can protect the public, as well as fear of future social upheaval. If foreign, likely to erode support for US presence and policies and possibly to limit US ability to achieve its local objectives.

An orchestrated campaign: If domestic, could undermine American's fundamental sense of security, lead to a sharp crackdown that unleashes a caustic national debate about the status of our constitutional order, while precipitating further social conflict. If foreign, could lead American public to conclude that a foreign military commitment is not worth the costs.

N/C/B Differences

- The frequent grouping of nuclear, chemical and biological warfare threats within a single weapons of mass destruction category masks fundamental differences.

Nuclear: The requisite preparations to develop, produce or secure a nuclear device and deliver it offer many opportunities for detection and disruption, given their scale and cost. The device itself provides signatures that can be used to detect and disable the device. It is extremely difficult to mitigate the blast or long-term health effects of such attacks.

Chemical agents require smaller investments of time, energy and money. Large-scale attacks require effective delivery systems, large quantities of agent, and sound operational practices. An event involving a chemical agent is likely to have immediate consequences. Decontamination and other treatment can do much to mitigate effects, but only after the fact.

Biological agents require much smaller investments and simpler delivery means. An event may not be detected for hours or days, and in some cases weeks – or never. If conducted with infectious transmissible agents, its effects may be uncontrollable, especially given the ease of long distance travel.

---

[1] The Next Lenin, Fred Iklé, 1995 (more complete reference)

Chemical/Biological: Biological and chemical agents are very different

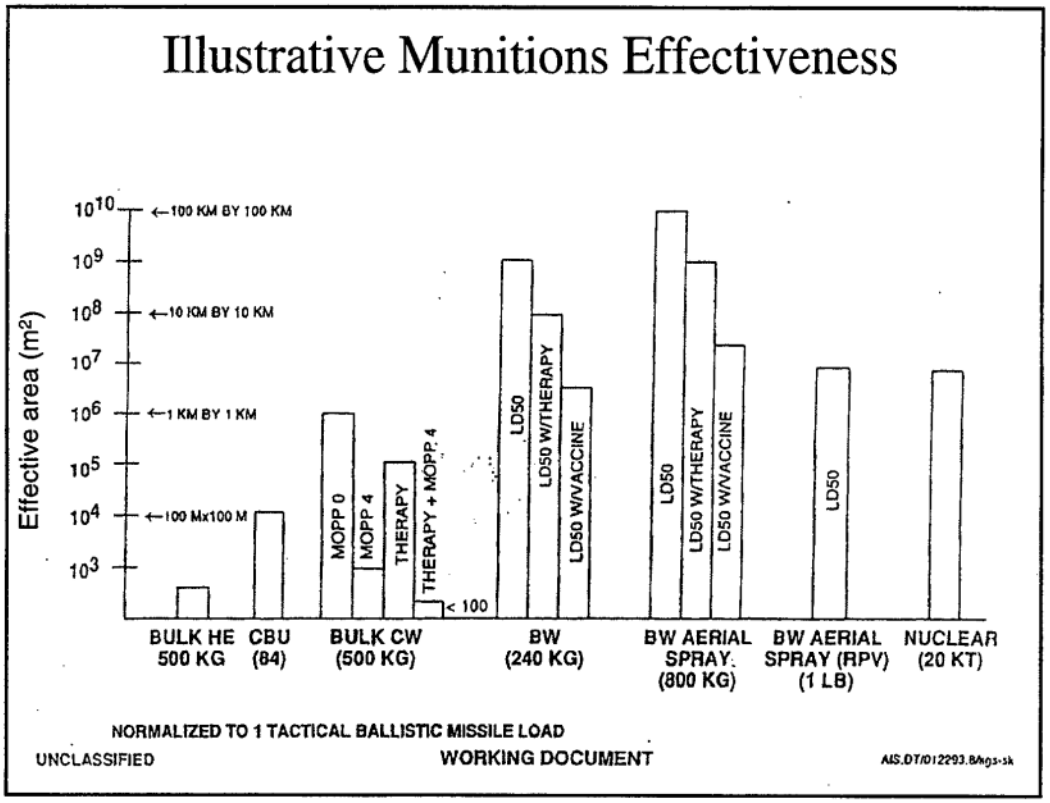
Property	Biological		Chemical	
	Botulism	Anthrax	Nerve (Sarin)	Mustard
Lethality	1-2 organisms (10^{-9} mg)	10,000 organisms (10^{-5} mg)	1 mg	15 mg Respiratory
Time to Symptoms	12-24 hrs	3-4 days	Immediate	2-24 hrs
Lifetime	1-2 days in sun	Must decontaminate	Volatile	Non volatile, must decontaminate
Dispersal methods	Aerosols, food & water	Aerosols	Aerosols Spray tanks evaporation	Aerosols And Liquids
Preventive protection	Protective mask Vaccine	Protective mask Vaccine	Protective mask For VX, full protective clothing	Protective mask Full protective clothing
Preparation methods	Fermentation	Fermentation	Chemical synthesis	Chemical synthesis
Precursors	Small strain sample	Small strain sample	Chemical reagents	Chemical reagents
Detection methods	Immunoassays antibodies	Immunoassays, antibodies	IMS, Mass Spectrometry (MS)	IMS, MS
Time to detection	hours to days	hours to days	Seconds	Seconds
Treatment	Ventilation	Ciproploxin/ doxycycline	2-PAM & Atropine	None

The above table highlights other differences between biological and chemical agents. Two examples are given in each case. Anthrax is a particularly lethal pathogen. The other BW example — botulism — is a toxin, a chemical produced by living organisms. The BW threat agent also includes viruses, Ebola being an especially virulent example. Viruses are biological agents that are quite small in size, require a host to survive, are non-detectable and the only treatment is supportive therapy.

The two types of chemical agents shown are nerve and blister agents. Sarin is given as an example of a highly volatile nerve agent and mustard as an example of a vessicant. Nerve agents also come in more persistent forms (e.g. VX and GD). VX acts percutaneously and requires a full protective ensemble.

Generally, chemical attacks would be discovered immediately. The effects of mustard will not show symptoms (a reddening of the skin and blisters) for at least 2-12 hours. On the other hand, depending on the pathogen, biological attack victims might not show symptoms for up to 21 days. It would be very difficult to distinguish a biological attack from some normal infection if the pathogen is endemic to the area.

Probably the most significant difference between CW and BW attacks is that a biological attack can produce three to five orders of magnitude more casualties with the same total amount of agent (see figure below). Also, biological agents can be grown almost anywhere using materials purchased from a local grocery store, while chemical agents must be prepared stoichiometrically from precursors. However, there are several different routes, some of which require only precursors that are readily available.



CURRENT DOD POSTURE FOR COMBATING THE CW AND BW TRANSNATIONAL THREATS

DoD Capabilities

- DoD has much to offer
  - Strategic inventory
  - Unique CBW capabilities
  - Growing experience
  - New initiatives
- However, critical capabilities are spread thin and eroding

A distinction is made between crisis and consequence management. Crisis management encompasses those tasks necessary to interdict, isolate, move, disarm or destroy a WMD and to collect evidence for legal prosecution. Consequence management, includes those DoD and other assets that can assist with protecting emergency responders, identifying agents, applying medical triage and stabilization, decontaminating casualties and facilities, and managing public perception. These two different problem sets clearly require an integrated solution.

DoD has Much to Offer

Current Competencies: Strategic Inventory

- Ready standing forces, widely distributed globally and in the US
- Experience with organizing, equipping, and training forces to deal with BIG problems
- Experience in conceiving, developing, and fielding high performance systems to operate in stressful environments
- Extensive intelligence assets
- Special forces capabilities
- Existing contingency organization, foreign and domestic
- CBW defense capabilities including research, training, and operations

The Department has much capability to offer in response to the transnational CW and BW threat. A top level survey of DoD's inventory for dealing with the CW and BW threat indicates a breadth of capabilities and relevant expertise that is unmatched anywhere else in the government. Some of DoD's capabilities are highlighted above.

DoD Has Much to Offer

Current Competencies: CBW Defense

- Active and Reserve Component Chemical Unites
- Specialized Units: (CBIRF, TEU, 53U, Explosives Ordnance Disposal (EOD) Group, Air Force Radiation Assessment Team, etc.)
- Research/Training Institutes: (USAMRIID, USAMRICD, Nuclear Medical Research Institute (NMRI), Army Chemical School, Air Force Technical Applications Center, Radiobiology Research Institute, etc.)
- Specialized Response Teams: RTF, JSOTF
- CBDCOM (Chemical Depots, Edgewood Research, Development and Engineering Center (ERDEC), CSEPP)
- Defense Special Weapons Agency (DSWA)

Some of DoD's capabilities for addressing the transnational CW and BW threat are listed above. Army chemical defense units in both the active and reserve components have personnel trained in protection, detection, and decontamination. Although their training and equipment traditionally is focused to the battlefield environment, they do have some experience in applying their skills to transnational threat scenarios. Special units such as the Tech Escort Unit (TEU) and CBIRF have missions that directly support domestic incident response and as such have equipment for such scenarios along with the associated training requirements (particularly with TEU).

DoD response assets also include a variety of research and training institutes with a cadre of subject matter experts that can supply needed expertise and years of first hand experience. DoD response teams are tailored to provide DoD assets in support of the lead federal agency for a crisis management (Joint Special Operations Task Force (JSOTF)) and/or a consequence management (RTF) situation.

There is a relevant base of expertise in the Army's Chemical Stockpile Emergency Preparedness Program (CSEPP) and its experience in working this emergency preparedness program with local, civilian communities, as well as the equipment and technical expertise found at the chemical stockpile locations.

DSWA has been deeply involved counterproliferation matters, including support for BW threat assessments as well as providing force protection assessments to combatant and facility commanders.

DoD has Much to Offer

Current Competencies: Operational Experience

DoD Exercises:

- DoD Exercises
- Mirrored Image
- Calypso Wind
- Excaliber '96
- Terminal Breeze
- ITRAP Series
- Ill Wind
- 1997 Interagency Exercise "Measured Response 97-2" in Denver

Events/Incidents:

- Murrah Federal Building Bombing, Apr 95
- Democratic and Republican National Conventions
- 1996 Summer Olympic Games
- 1997 Inaugural
- 1997 Denver Summit of the Eight

DoD's experience base for dealing with WMD incidents is growing through exercises and actual events. Some of the recent exercises and events are listed above. Display Select and Mirrored Image were both interagency Command Post Exercises (CPXs) hosted by DSWA that involved nuclear or improvised radiological devices. Calypso Wind was a preparatory CPX for the Atlanta Olympic Task Force. Excalibur '96 was a Headquarters, Department of the Army Continuity of Operations exercise with a WMD and natural disaster scenario. Terminal Breeze, a recent tabletop exercise involving representatives from Virginia, Maryland, the District of Columbia and Federal agencies and departments, employed a scenario that included a sarin attack on the Washington area metro subway system.

The Interagency Terrorism Awareness Response Program (ITRAP) is a series of counterterrorism exercises sponsored by the National Security Council (NSC) and run by the ASD (SO/LIC). The FEMA sponsored Ill Wind seminars and exercises focus on chemical and biological scenarios.

In addition to these exercises, DoD has supported both crisis and consequence management efforts during an actual events, including the bombing of the Murrah Federal Building in Oklahoma City and the Summer Olympic Games in Atlanta. DoD also prepositioned response assets and/or conducted first responder training for the Democratic and Republican National Conventions, the 1997 Presidential Inauguration, the Denver Summit of the Eight Conference and other events.

DoD has Much to Offer

There is Lots Underway to Improve Capabilities

- Elements of the counter proliferation effort, aimed at across-the-board improvements in military capability to deal with NBC threats, are relevant to the transnational CBW threat as well
- Creation of Joint Staff element focused on force protection (Combating Terrorism Deputy Directorate, J-34)
  - Ongoing vulnerability assessment with DSWA
- Preparations by CINCs
  - Modification of CONPLAN process to include terrorism
- Nunn-Lugar-Domenici funded effort for first responder training, etc.
- New R&D:
  - ACTDs: 911 Bio, airfields and ports
  - TSWG increased investments in CW and BW defense
  - DARPA BW Defense R&D initiative
  - DoD/DOE cooperation on CB R&D
- SECDEF QDR commitment of $1B plus-up on CBW defense – mostly to procure CBW defense equipment

Nunn-Lugar-Domenici legislation in 1996 directed the Department (delegated to the US Army CBDCOM) to provide emergency response training, advice, and assistance to the incident response community. The recently initiated city training and hot line programs are in response to this legislation. Other tasking under the legislation includes providing assistance for developing a rapid response team (note the recent standup of the RTF) and in acquiring and maintaining an inventory of physical equipment and assets. DoD is also charged with conducting appropriate T&E for preparedness and to assist in the procurement of equipment to interdict WMD movement.

New R&D activities include Advanced Concept Technology Demonstrations (ACTDs) to address both interior and external releases, the accelerated growth of the DARPA BW defense initiative (~$50M annual budget), and coordination with the DOE Chemical/Biological Nonproliferation Program. The Technology Support Working Group (TSWG) is an interagency program for coordination and management of the introduction of new technology into the counterterrorism community.

However Critical Capabilities are Stretched Thin and Eroding

- Tech Escort Unit (TEU) operations substantially increased without additional staffing
  - Deployed 200+ days last year
  - Further personnel reduction planned (27 person reduction by 2000)
  - Increase civilian/military ratio detracts from readiness
- Pressure on CW expertise base
  - CBIRF required 60% of Marine Corps NBC specialists
  - Active Army/R&D/medical reductions (part of general downsizing)
  - Chemical storage/demil sites will be closed over next 10 years
- Of 50+ new DIA slots on CT, only one focuses on CB

Bio capability especially vulnerable

- ***Small base cannot withstand "fair share" cuts***
- ***Only 6 USA MRIID professional support all CINC operational medicine needs***
- ***Recruiting/retention of world class people very difficult in current environment***

The panel found that critical capabilities within DoD are being stretched and severely eroded. For example, the Army's TEU currently has personnel deployed over 200 days per year. Although the unit has recently received authorization for ~30 civilians, it is targeted to lose 27 military positions by 2000. TEU's increasing operational tempo (OPTEMPO), coupled with the shift to greater reliance on civilian personnel, will soon begin to impact its readiness posture.

Other examples include:

- CBIRF uses 60% of the Marines' battlefield specialists;
- Considerable decline in the Army's Chemical Corps and R&D chemical specialists has already occurred;
- Useful expertise resident in the chemical storage and demil operations personnel will all but disappear within 10 years unless an active knowledge transfer program is undertaken;
- Intelligence community CW and BW specialist staff is very thin.

Perhaps most worrisome is the thinness of DoD's BW defense expertise. Under the downsizing pressures facing the DoD, key organizations have few personnel to perform critical operational tasks.

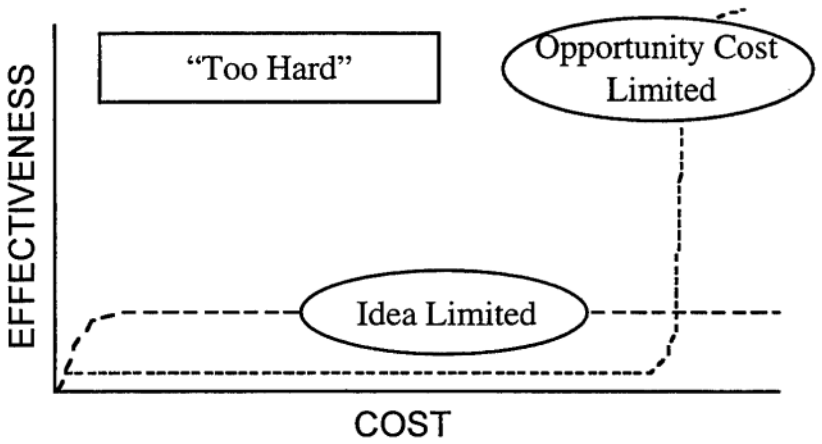
ELEMENTS OF A STRATEGY TO DEAL WITH TRANSNATIONAL CW AND BW THREATS

In this section, we elaborate on the strategy elements we recommend for use by the Department in response to the evolving transnational CW and BW threat.

4.1 DON'T TREAT BW AS TOO-HARD

Thinking About Our Options – "Too Hard?"

- Cost-effectiveness relationships among response options for the CW or BW transnational threat are not yet understood
- Not without analog
  - US grappled with similar ambiguities in Cold War with strategies of flexible response and deterrence
  - Seminal thinking on Cold War strategy was done in late 40s to late 50s
- Preoccupation with the most stressful threat or on achieving a perfect solution leads to assigning problem to "too-hard" category

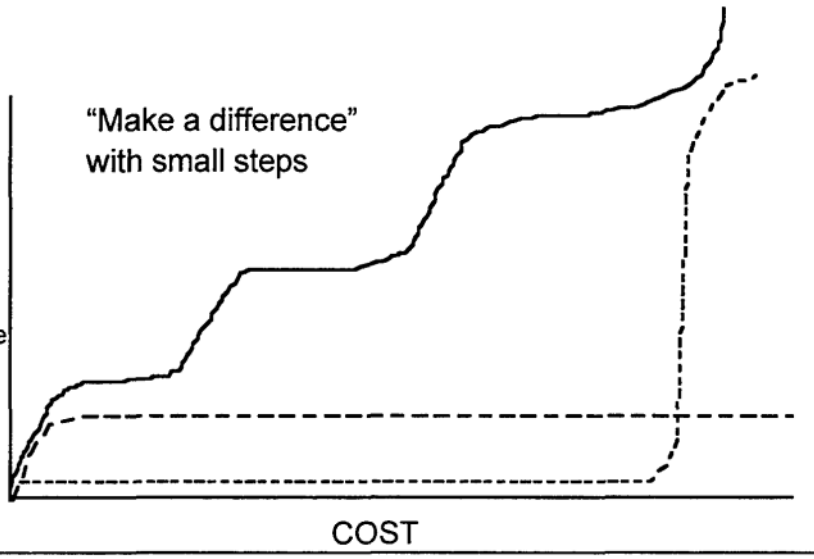


In thinking about our options in response to the transnational CW and BW threat, we must avoid being trapped into a belief that "it's too hard." Such an assessment will likely paralyze further action or investment. Currently the cost effectiveness relationships among the various response options are not well understood for this threat, but such a situation is not without historical precedence. For example, it took the United States a decade of thought and debate from the late 1940's to late 1950's to develop our base strategies for nuclear deterrence, that eventually evolved to flexible response.

Another trap to avoid is that effectiveness must be measured against the most stressful threat or must embrace the perfect solution. In these cases, we will quickly find ourselves limited by either ideas, dollars, or both, while missing opportunities to invest in useful capabilities.

Thinking About Our Options – "Making a Difference"

Many "too hard" or "too costly" problems – from aircraft hijackings to missile defense – are being tackled with an incremental approach



Alternative choices for effectiveness – such as minimizing the number of people exposed or assets contaminated or raising the difficulty for an adversary such that he might show his hand, or providing confidence to the public and our allies that we are serious about addressing the threat - lead to an incremental approach for improving our capabilities to deal with the transnational CW or BW threats.

Selecting the steps and their sequence in a systematic way is strongly recommended; in fact, it is the gist of the architectural effort recommended by this panel. While many things are happening in an ad-hoc manner to improve our capabilities, **the analysis to identify the highest priority actions is missing**.

An Incremental Approach Recognizes That the Threat Scenarios Space is Broad

- Upper Left: Strong exercise opportunities with recent high-profile events (e.g., Olympics, Inauguration, G7 + 1)
- Upper Right: Consequence mitigation at high-value locations (e.g., Capitol, aircraft, subways) through pre-deployment of detectors, containment, medical supplies, etc.)
- Lower Left: Training and equipping 1st/2nd responders to provide effective "rapid projection" capabilities
- Lower Right: Invest in intell to minimize

Time / Location	Known, Temporary	Unknown
Known	Pre-deployed personnel and assets	Pre-deployed material and equipment
Unknown	"Rapid projection" force	Most difficult

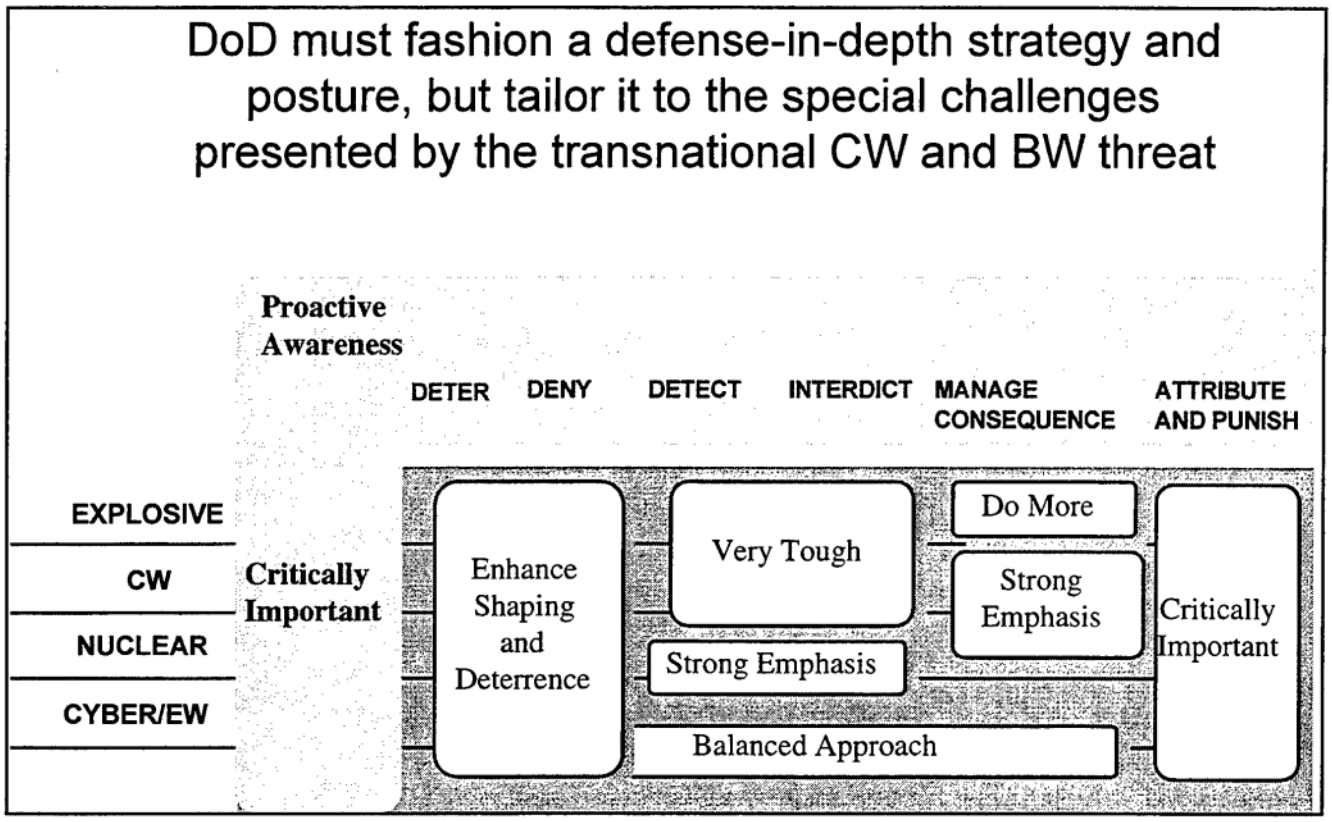
- Recent excercise experience in upper left
- Other corner present different CONOPs, training and material challenges
- But don't get hung up only on most difficult problem
- Effective Intell move problem up/left, makes protection easier

The "known-known" case provides excellent opportunities to exercise the total system, such as was done already in cases of the Atlanta Olympics, the Inauguration, and the Denver G7+1 meeting. Pre-deployment of equipment and materiel is being addressed modestly with the training kits provided to the cities under Nunn-Lugar-Domenici (NLD). We propose an expansion to NLD to distribute more equipment (detectors, medical supplies, etc.) and to evolve better processes (e.g., sprinkler system or fire hose based decontamination, interior ventilation control) for use in the civilian sector.

The rapid projection force notion of the lower left quadrant of the above figure aims at developing a well trained and equipped first (fire, emergency medical) and second (National Guard) responder community throughout the nation. Such a force will be particularly effective with warning, but will also be a strong element of the pre-deployment strategies of the upper quadrants as well.

The "most difficult" quadrant, besides benefiting from advances in the other three quadrants, also presents a strong motivation for improved intelligence so that any situation is driven to one of the other quadrants.

4.2 DEFENSE-IN-DEPTH



We believe that the Department needs to place special emphasis on consequence management and intelligence. All the elements of defense-in-depth — dissuading and denying possession, deterring use, intercepting delivery, mitigating consequences and identifying and punishing the perpetrators — can contribute to combating this threat.

Highest priority should be accorded to managing and mitigating the consequences of a CW or BW attack. There are two reasons for establishing such approaches. First, we cannot count on preventing CW or BW attacks. Second, so-called **passive defense measures can be very effective** in reducing casualties (perhaps by several orders of magnitude through a combination of warning and monitoring, individual and collective protection and timely medical treatment). Clearly, it would be preferable to deny possession and prevent attacks rather than have to try to ameliorate their effects. However, the very small signatures that may be associated with CW or BW production and possession, as well as the multiple and difficult to intercept delivery means available to potential attackers implies a leaky front-end of any defense-in-depth. **Thus, we must be prepared to deal with the consequences of CBW agent release**. Managing the consequences of an attack not only includes minimizing the physical and environmental traumas but also influencing public and media perceptions and dealing with adversaries who might be planning the next move in their campaign. (see chart below)

Consequence Management is not Limited to Treating Casualties

- Sorting and treating casualties (which requires identification of the CW/BW agent or agents employed and may require patient decontamination).
- Cleaning up residue of CW/BW attack (both on-site contamination and secondary contaminated facilities such as hospitals and ambulances).
- Cooperation among federal, state, and local (and perhaps foreign) entities, including law enforcement agencies seeking to preserve evidence.
- Cooperation with the media to avoid public panic.
- Thwarting responsive adversaries – dealing with potential multiple incidents
- Achieving a just result – whether retaliation against a state sponsor or known terrorist group or legal punishment of domestic perpetrators.

Next in priority is getting smarter about the threat through a more focused and aggressive intelligence effort. The intelligence community (including its DoD components) has only recently paid significant attention to the CW and BW threats and has concentrated on the threat from nation states. The Intelligence Community will need to focus more attention and resources to the transnational aspects of the CW or BW threat. Because of the nature of this threat, the effort will need a broad spectrum of intelligence means with particular emphasis on human intelligence (HUMINT). It will require new sampling and collection techniques, sensitive analytic capabilities (to pull very small signals from cluttered backgrounds), better communication and sharing of information with law enforcement agencies, more effective use of open sources, and involvement in epidemiology studies to assess "outbreaks" of unusual diseases that may provide clues to BW production activities. (Discussed in more detail in the next section).

While deterrence will play a much lesser role against these transnational actors than it did against our Cold War adversary, DoD should not ignore its potential contributions. Among the steps it can take would be to set up (in cooperation with other government agencies) a "Human Factors Assessment Center." Its objectives would be to better understand the motives and value systems of potential transnational users of CW or BW and to identify means to strengthen deterrence mechanisms against these groups. One fruitful avenue of investigation would be to illuminate both the costs (e.g., exposing transnational actor vulnerabilities) as well as the effectiveness of US capabilities. It will be important to "publicize" US capabilities as one element of deterrence. (See section 4.11 for additional discussion of the role of deterrence.)

4.3 INTELLIGENCE

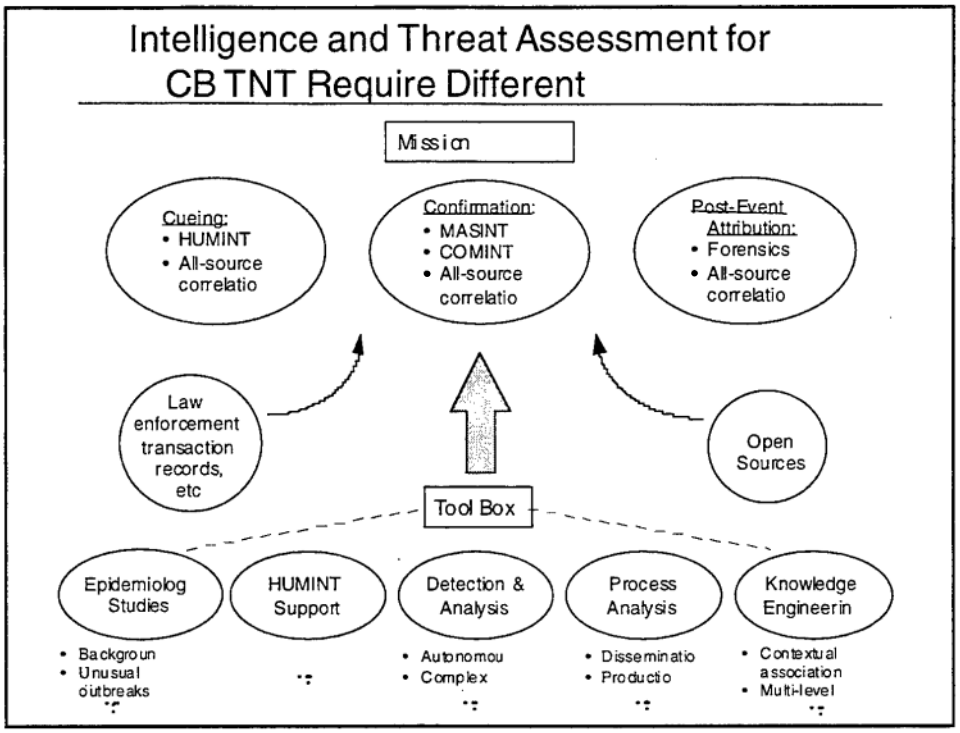
Get Smarter About the Transnational Chemical/Biological Threat: Improving Intelligence

- Chemical ≠ Biological
  - Acquisition paths, weaponization and dispersal, effects, etc. differ significantly
- Intelligence and threat assessment approach
  - Large HUMINT and open source elements with Measurements and Signatures Intelligence (MASINT) support
- Linkage between intelligence and active operational elements
  - Many clues within local law enforcement, both CONUS and OCONUS
  - Global information system on transnational threats would help

Our understanding of transnational threats, in general, and especially the chemical and biological variants, is much less mature than the traditional conventional or nuclear threats. Getting smarter about these threats requires improvements in our information gathering and analysis capabilities. A recognition that transnational chemical and biological weapons differ in the fundamental signatures associated with acquisition, weaponization and dispersal, effects, and vulnerabilities leads to the need for specialized expertise for each.

The approach to improved intelligence and threat assessment for both will need to be rich in HUMINT and open source analyses with an important technology assistance from Measurement and Signatures Intelligence (MASINT) collection. This basic approach differs in emphasis from the more technology-rich approach employed for conventional nation-state threats because of the ambiguous signatures of both transnational actors and chemical or biological agent in a complex background environment.

A third consideration, integral with the second, is the establishment of tighter linkages between intelligence and operational elements (including law enforcement). For example, local law enforcement will often encounter suspicious activities, but pursue them no further without the added associations that link the activities into a more complete picture of dangerous efforts (e.g., as happened from the World Trade Center case). Other linkages to public health organizations, for example, could be useful in tying unusual disease outbreaks, with local and regional clues to pinpoint a CW or BW production facility. On the operations side, those elements responsible for public safety or force protection should be sufficiently in the know to take preparatory steps should an event carry any warning. These linkages, when considered in their entirety, lead naturally to the notion of the Global Information System on Transnational Threats as recommended in the overall study.



The relationships among disparate information sources is elaborated in the above chart. Ideally, one would look to intelligence support first for cueing, followed by confirmation, such that the threat is intercepted before any agent is disseminated. Should an event take place, then intelligence support would be critical for attribution. The approach for transnational CW or BW threats, however, will require a significant departure from our more traditional reliance on National Technical Means (NTM), since the signatures associated with acquiring a chemical or biological capability, especially by a transnational threat group, are very low and ambiguous, and not well understood. Cueing must therefore rely heavily on HUMINT, Signals Intelligence (SIGINT), and MASINT. With HUMINT tip-off, MASINT and possibly COMINT can then be targeted to help confirm acquisition and/or deployment activities. Should an event take place, the laboratory sample analysis capability of the threat assessment community will prove invaluable in identifying the perpetrators.

All of these efforts will be dependent on parallel information and data analysis capabilities that draw upon and properly fuse input from any number of sources: open sources (news sources, technical journal and conference entries,...), transaction data bases (purchases, shipments, permit applications,...), law enforcement records (complaints, arrests,...), public health sources (disease outbreaks, spread,...), etc.

In order to adequately address this threat, additional investment is needed to develop a more complete "tool box" focused on the specific needs for the chemical and biological threats. Some examples of the elements and subelements of the tool box are noted in the above figure. Especially important to addressing the biological threat is epidemiology studies that tie public health information on disease outbreaks with background environmental characterization in order to assess the "unusual" nature of any outbreak. Further association with less open knowledge of suspect production sites and/or correlation of the outbreak propagation with meteorological data could lead to pinpointing a facility for sampling and analysis via MASINT means. Good MASINT will in turn depend on the availability of

robust detection and field laboratory analysis means to pull small signals from an extremely "dirty" background. Both HUMINT and MASINT must be augmented with careful process analysis to develop a pre-operational understanding of what a production process could look like, where it could be leaky (i.e., where the best sampling points might be), etc.

There needs to be more aggressive exploitation and adaptation of state-of-the-art knowledge-engineering tools, which will be the critical enablers for the all-source assessment efforts that underpin every stage of intelligence support for this difficult threat. "Intelligent software agents" and "data farming/mining/warehousing," describe the types of information technology advances that need to be applied in this area. In addition, there is a need to disseminate the information among many users. Further, suppliers to the system will require sophisticated multi-level access/security architectures to allow entry to the system only at the appropriate "need-to-know" level. Both the Defense Advanced Research Projects Agency (DARPA) and the National Security Agency (NSA) are supporting R&D to develop many of the information analysis and "intelligent agent" tools.

4.4 ESTABLISHING A NATIONAL CONSEQUENCE MANAGEMENT CAPABILITY WITHIN THE NATIONAL GUARD

The National Guard

Our Principal Recommendation for Improving Response Capabilities

- That the Secretary of Defense direct the Secretary of the Army to establish a national consequence management capability within the National Guard, augmented as necessary by the Army Reserve Component, to support state and local agency responses to domestic CW and BW incidents.
  - Tasks:
    - Establish a consequence management capability to provide initial and rapid Title 32 and Title 10 support to state and local agencies
    - Conduct sustainment training and exercises for 1st Responders building on initial Nunn Lugar legislation utilizing existing Distance Learning Centers, Joint Training Centers, and the assets of the National Interagency Counterdrug Institute (NICI)
    - Develop the capability to support CINC CM JTFs
- Allocate resources required to sustain the National Guard effort

It is recommended that the Secretary of Defense direct Secretary of the Army to establish a national consequence management (CM) capability within the National Guard to support state and local agency responses to domestic chemical and biological incidents.

The support to be provided by the National Guard should entail both Title 32 and Title 10 responsibilities. This means that the Guard would respond to a State Governor under Title 32 and could be quickly federalized under Title 10 to support a larger federally-coordinated effort. Additionally, the Guard would respond to the Nunn-Lugar-Domenici (NLD) legislation by providing training for first responders and integrating exercises utilizing the Guard's existing Distance Learning Centers (DLC's) and the National Interagency Counterdrug Institute (NICI).

The Guard should also be tasked to support the Combatant CINC's Joint Task Forces for Consequence Management (CINC JTF-CM). The assignment of National Guard CM assets to CINC JTF-CM's would fill a current capability void to which only the CBIRF is now available.

In order for the National Guard to assume this mission, sufficient resources must be committed over time.

National Guard: Why

- National Guard will be involved regardless
  - DoD can enhance their effectiveness to deal with CBW incidents
- Have a vested interest in community, integrated, civilian skills, local knowledge
- Stable assignments, long-term expertise, extensive networking
- Not constrained by Posses Comitatus (in State status)
- Already required to be integrated into Civilian Incident Management System (IMS)
- Many Interstate Agreements already are in place

The National Guard belongs to the Governor of each respective state. In most state and local domestic emergencies (e.g., hurricanes, blizzards, tornadoes, earthquakes, etc.), the Governor quickly resorts to the state National Guard to augment local agencies for providing relief to the community.

The Guard is homegrown, has a vested interest in the community and will be used by the Governor. In many cases Guardsmen may already have the individual skills, as part of their civilian career/volunteer work, to conduct consequence management duties. Guardsmen normally stay with their units for long periods of time. There is little personnel turbulence or large turnover. There will be continuity. Additionally, the Guard works with state and local emergencies agencies on a recurring basis and can easily be integrated into the Civilian Incident Management System (IMS). Through close coordination among regional State Adjutants General, there are interstate agreements already in place that would facilitate National Guard regional responses to assist in consequence management.

National Guard: Roles

- Provide a national consequence management capability to support state and local agency responses to domestic CW and BW incidents
- Support 1st Responder Training/Exercises
- These capabilities will support an additional mission: augmentation of Combatant CINCs JTFs for Consequence Management

The ability to save lives and turn victims into patients following a biological or chemical incident is directly related to the amount of trained and effective resources that can be brought on scene in the least amount of time. First responders understand that they will be on the scene first, and that they may be the only resource available for up to eight hours. Depending on the magnitude of the event, the level of training and their expertise, this timeline may be unacceptable.

The National Guard could embrace two key roles. It is uniquely placed for providing a national consequence management (CM) capability to support state and local agency responses to domestic chemical and biological incidents. Additionally, its vested interest in the community can be capitalized on to conduct and integrate training and exercises for first responders at the regional, state, and local levels. This training would sustain the Nunn-Lugar-Domenici initiatives and provide an integrated, coordinated approach that would enhance local, state, and federal responses to chemical and biological incidents.

The National Guard's consequence management capabilities could also be used to augment the Combatant CINCs with their consequence management mission. The CINCs are currently tasked to provide consequence management capabilities in their specific area of responsibilities in accordance with CONPLAN 0400. The CINCs currently have no consequence management resource other than the Marine Corps' Chemical Biological Incident Response Force (CBIRF). Utilizing the National Guard CM capability would provide a force multiplier to the CINCs.

National Guard: Consequence Management

- Adapt CBIRF Model
  - Rapid reaction capability
    - Establishes link with 1st Responders; makes initial assessment
    - Initial recon/decon/medical and logistics assistance to 1st Responders
  - Sustained decontamination and medical treatment capability
  - Augment 1st Responders – turn victims into patients
- Integrate into Civilian Incident Management System
- Integrate with FEMA Regional Offices and with state and local agencies
- Exercise and train with FEMA regions, state and local agencies

A template already exists for consequence management — it is the Marine Corps CBIRF. The National Guard should consider adapting the CBIRF model in developing its national consequence management capability. A capability based on the CBIRF model would provide the rapid reaction necessary to support CW or BW incidents. The ability to respond, for example, in two hours within a state greatly enhances first responders' ability to mitigate the damage of the event. The Guard should be able to quickly link up with the first responders, make an initial assessment of the event, conduct RECON of the site to provide initial agent identification and recommended protocols, provide individual decontamination for the first responders and provide medical treatment and assessment as required. Following this initial assessment, a larger more substantial force could be deployed to augment the initial National Guard response. This force would deploy with more robust decontamination and medical capabilities, as determined necessary by the initial Guard assessment team.

A critical element to National Guard success will be its ability to integrate into the Civilian Incident Management System. Integration is already in place in a number of states and regions, but must be incorporated in all states and regions. This will facilitate the integration into the FEMA regional offices as well as state and local agencies.

The Guard, as the implementer for sustaining Nunn-Lugar-Domenici, provides the necessary training to its members and to first responders, that can be the basis for integrated training and exercises conducted with FEMA regions, and state and local emergency service agencies.

National Guard: Training

- For curriculum development, utilize National Interagency Counterdrug Institute (NICI) along with US Army CBDCOM, Chemical School, and other national centers of CW and BW defense expertise
  - Apply DoD standards
  - Common standards pertaining to all 1st Responders
- Utilize existing Distant Learning Centers and Joint Training Centers (JTCs) for educating state, NG, Coast Guard, other reserve personnel and state and local 1st Responders
- Utilize consequence management, assets training the trainers
  - Provide quality assurance and adherence to standards
- Integrate training and exercises with federal, state, and local agencies
  - Support regional FEMA offices and local emergency plans
  - Develop CONOPS for command and control integration and information/intelligence sharing

The recommended method of addressing the National Guard training and exercise responsibility is to build on what is already in place. Currently the National Guard operates the National Interagency Counterdrug Institute (NICI). Established in 1991 to provide education and training for DoD, federal, state and local law enforcement agencies (LEAs) involved in counterdrug activities, NICI includes three training centers: San Luis Obispo, CA; Meridian, MS; and St. Petersburg, FL. Its curriculum includes interagency counterdrug training as well as military support for civil authorities (MSCA). NICI has experience in developing curricula based on interagency requirements and input, conducting research and analysis, developing specialized courses as well as conducting host agency training courses. NICI is developing courses for WMD responder training, emergency response exercises, and planning and managing the consequences of the acts of transnational groups. NICI's budget to support counterdrug training is $3.7M per year, and $3.0M to support MCSA training.

Utilizing NICI as the training hub for consequence management and using the established Distant Learning Centers (DLCs) in state National Guard armories, the training and exercise program can quickly reach a wide audience. Specific training modules could be developed that meet individual state and local standards and provide the bridge from the federal level to the local level.

Active involvement of state and local agencies is crucial to the successful development of the curriculum, at the federal, state and local levels. The thrust is to build on what is already known, develop the synergy for interaction among all agencies, and develop the necessary playbooks with the appropriate operational concepts for command and control that can be utilized by local, state, and regional activities when faced with responding to a chemical or biological event.

National Guard: CINC Augmentation

- CBIRF is only existing CINCs chemical/biological CM asset
- Designated Regional Chemical-Biological Incident Response Teams could fill void
- Assigned to CINCs Joint Task Force for Consequence Management (JTF-CM)
- Provide training and planning assistance as part of an Advanced Concept Technology Demonstration

There is a natural relationship between CBIRF and the National Guard. As the National Guard CM capability comes on-line, CBIRF can assist by establishing a "train the trainers" program that will educate Guard personnel on the CBIRF concept of operations, and provide cross-training of personnel in a multitude of tasks. It is envisioned that, once the Guard capability is established, CBIRF will serve as a federal CM asset for pre-planned events, e.g., the Olympics, Inauguration, etc. Also, CBIRF could initially serve to augment the National Guard in support of an event. CBIRF can also serve as a testbed for operational and technology innovation (including participating in Advanced Concept Technology Demonstrations) and development of the tactics, techniques and procedures. As the National Guard gains proficiency in the consequence management mission and assumes the training and exercise integration responsibility, CBIRF would be phased out.

National Guard: Implementation Options

- Mission Profile: Decontamination/medical stabilization/triage and training more appropriate than crisis management task associated with TEU/EOD
- Implementation Options
  - Individual state/regional response capabilities
  - Full-time support/part-time/mix
  - Dedicated mission/additional mission for operational units
  - Equipment/equipment upgrade
- Adapts tactical medical unit/Disaster Medical Assistance Team (DMAT) hybrid model
- Leverage Innovate Readiness Training (IRT) capabilities (OSD Reserve Affairs start-up program)

Several potential missions were examined for appropriateness for the National Guard. One was combining the consequence management (CM) elements of CBIRF with the identification and movement elements of the Army's Technical Escort Unit (TEU). However, the amount of specialized training required to assume the TEU role would detract from the main thrust of consequence management. Therefore, we recommend the National Guard should only take on the consequence management tasks of reconnaissance, decontamination, medical triage and stabilization, and training rather than the crisis management tasks associated with the TEU.

Implementation options include establishing individual state CM capabilities, establishing regional response capabilities, or a mixture of both state and regional capabilities. The question of full-time support, part-time support, or a combination of full-time and part-time support will in large part be

tied to the level of commitment at the state or regional levels, as well as the amount of federal resources available.

The designation by the Guard of a dedicated mission vs. additional mission will reflect the importance that the Guard places on the mission. To be able to integrate completely with local, state, and regional emergency response agencies, be responsible for continued training, and continually refine tactics, techniques, and procedures requires a full time mission and cannot be effectively accomplished as an additional mission.

The Guard could adapt the CBIRF Table of Equipment as the nucleus for its outfitting. CBIRF would serve as the testbed for new equipment and technology enhancements. The Guard would be able to take advantage of the CBIRF advances.

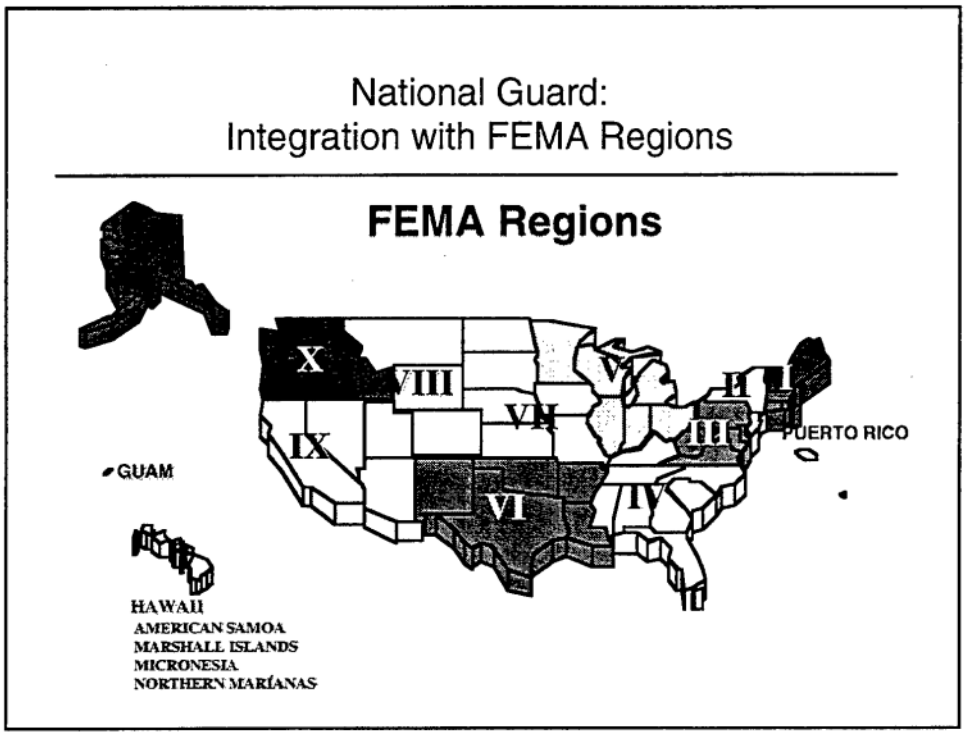
National Guard: One Proposal for an Integrated Capability

- 54 State/Territory Rapid Assessment Teams (48 personnel per Team)
  - Provides initial assistance to 1st Responders; similar to CBIRF 120 man rapid reaction force
- 10 Regional Chemical-Biological Incident Response Units (180 per Unit)
  - Supports states within region
  - Provides enhanced medical/decontamination capability
- 4000 personnel ~ 1% of National Guard structure
- Staffed 25% full-time with rapid recall capability
  - Dedicated team/unit mission
- CBW defense equipment based on CBIRF Table of Equipment
  - For National Guard nuclear emergency response, task DDR&E for evaluation/recommendation of appropriate equipment

The National Guard should establish 54 state/territory Rapid Response Assessment Teams (RRATs) and 10 Regional Chemical Biological Incident Response Units. Each state Adjutant General should establish an RRAT to assist first responders with initial agent identification, initial command and control, decontamination and medical treatment and assessment for follow-on National Guard and/or DoD assets. The team would have the capability to provide initial equipment for protection of first responders, to include individual decontamination. The RRAT could consist of approximately 48 personnel, fully manned, equipped, and capable of being deployed statewide within 2 hours of notification. The RRAT would be loosely based on CBIRF's rapid reaction force, but would not need an integrated logistics and security element, and therefore the RRAT would not be as large as CBIRF's 120.

The National Guard Bureau would also establish 10 Regional Chemical Biological Incident Response Units closely aligned with existing FEMA Regional offices. Memoranda of Understanding among the state Adjutants General within each region would be developed to effect manning, command and control responsibilities, and training and exercise integration. The unit would have the ability to conduct large-scale decontamination, medical triage for affected victims, and medical stabilization to augment the RRAT and first responders. The unit would be modeled after CBIRF with approximately 180

personnel assigned. The lack of an integral logistics support package and security element would permit a somewhat smaller number of personnel than CBIRF. The regional unit would be able to respond to an incident within 4 hours of notification. The RRAT would make the initial assessment and advise the regional unit on the magnitude of the event and recommended assets for deployment. Staffing of both elements would be with 25% full-time personnel. Total personnel dedicated would be about 1% of the National Guard structure. Equipment would be based on the CBIRF Table of Equipment and emerging technologies as tested by CBIRF. The Assistant to the Secretary of Defense for Nuclear, Chemical, and Biological should evaluate and recommend appropriate equipment for a National Guard nuclear emergency response capability.



The 10 National Guard Regional Chemical Biological Incident Response Units could be aligned with the existing FEMA regions shown above.

National Guard: Estimated Investment Need

- No new structure; redirection from existing assets
  - State Rapid Response Assessment Team
    - $4M per unit startup; $1M each year sustainment
    - Total startup: $200M (over 3 years)
    - Total sustainment each year: $50M
  - Regional Chemical/Biological Incident Response Unit
    - $12M per unit startup; $2M per year sustainment
    - Total startup: $120M (over 3 years)
    - Total sustainment each year: $20M
- Total Cost
  - Initial startup: ~$325M over 3 years
  - Sustainment: ~$75M each year

The costs required to outfit the National Guard with a consequence management capability are based on the redirection of personnel assets to fulfill this new mission area. There will be no additional force structure investments. To establish a Rapid Response Assessment Team (RRAT) in each state requires $4M for initial equipment and infrastructure and $1M each year for sustainment. Each Regional Chemical-Biological Response Unit would require $12M in infrastructure and equipment investment, as well as $2M for sustainment each year. For both the RRAT and Chemical-Biological Response Units, the infrastructure and equipment requirements could be phased in over three years. The total cost for the National Guard program would be about $325M over three years and then about $75M each year for sustainment.

National Guard: Potential Obstacles/Challenges

- Redirection of existing assets
- Requires substantial initial investment and sustained support
- Requires Memoranda of Understanding among State Adjutants General within each FEMA Region to form regional response units
- Specialized training required before operationally effective
- CINC resistance to NG support

For the National Guard to assume this mission, several obstacles will have to be overcome. First, this is a new mission for the National Guards, a mission to be assigned within existing assets. We do not recommend additional personnel. A challenge will be to redirect existing assets from other units to form the Rapid Response Assessment Teams and regional Chemical-Biological Incident Response Units.

For this mission to be successful, the Adjutants General from states within each FEMA region must endorse Memoranda of Understanding that formalize the establishment of the regional response units to include personnel, facilities, command and control, funding, and training. Before these teams and units are employed, extensive specialized training will have to be accomplished to ensure that there is a high and uniform standard of excellence throughout.

The substantial initial investment and required support for sustainment are obstacles that must be overcome in order to be successful. A conscious effort to commit to the required funding must be made at the Secretary of Defense level to ensure that the assets are available to support the National Guard effort.

Can the National Guard provide the consequence management support to the CINCs as advertised? The CINCs may resist any support in the belief that the National Guard will not be able to deliver when required and will not be adequately trained. Commitment to participation in CINC exercises and conducting ACTDs in the CINC's area of responsibility (AOR) to demonstrate consequence management capabilities may overcome this potential resistance.

4.5 END-TO-END SYSTEM APPROACH

Get Smarter: Implement an End-to-End System Approach

Why:
- Problem and possible solutions are diverse and crosscut many DoD missions, functions, and organizations

What:
- End-to-end system design and CONOPS encompassing deterrence, detection and interdiction, prevention, consequence management, attribution, and response

Products:
- Definition of interface and hand-off requirements
- Identification of technical needs and requirements
- Priorities for R&D, acquisition, exercises and training
- Identified and costed hedges to deal with uncertainties
- Evolutionary paths, options to keep pace with threat
- Tools - models, simulations, analytical expertise - to continue the process

A critical recommendation for dealing with the transnational CW and BW threat is to develop and evaluate our defensive options through a systematic end-to-end systems approach. An end-to-end systems approach would link end objectives, from near to far term, with organizational and operational frameworks, and demonstrate how investments in individual capability improvements lead to enhanced overall effectiveness.

Translating that broad statement to more concrete terms, the architectural approach provides the products listed above. These products provide the basis for a defensible and sustainable program to continuously improve the country's effectiveness in dealing with this complex threat.

Establish Two Temporary Organizations to Initiate End-to-End Systems Development

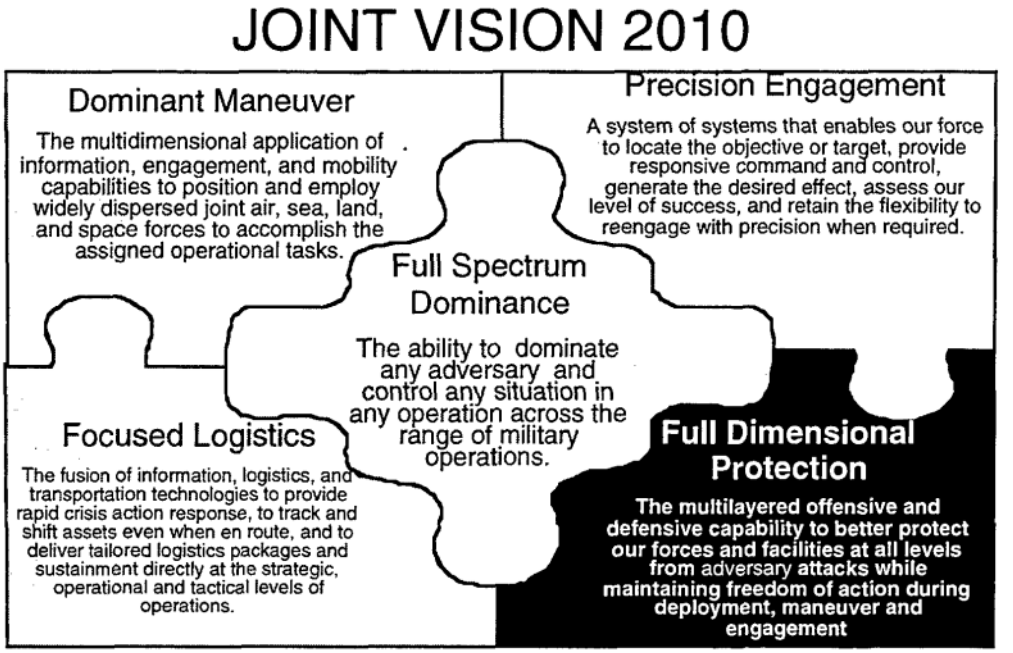
- CJCS: Task Force in Joint Staff to develop operational/systems construct and Master Plan (initial deliverable in 6 months)
- USD(A&T): Systems engineering team to provide systems architecture, exercise support, modeling and analysis capabilities in support of Task Force efforts
- Important ingredients:
  - Recruit "best of best" – analysis and technical and operational experts
  - Use "Red Teams" extensively to emulate responsive threats
  - Introduce modeling and simulation to evaluate alternatives
  - Strongly emphasize exercises and tests, not just paper studies
  - Address both force protection and civil protection/response scenarios
  - Complete baseline in 18 months at cost of ~ $30M

As discussed in Volume I of the task force final report, two temporary organizations should be staffed to undertake this task. These organizations would be expected to make use of both simulated and live exercises to test out concepts and to have a "Red Team" element. While there is synergy in the technical needs for the force protection and civilian protection missions, the operational players are different enough to warrant parallel efforts for each mission, but with built-in, frequent exchanges between the two efforts to identify and build on commonalties. The DoD can take a lead role for force protection, and thus, an initial focus on force protection (e.g., deal with attacks on points of embarkation in the US) may facilitate the required interagency participation.

We must take our best ideas, test them out, learn how to improve, and repeat the process. Testing can span a wide range of mechanisms that include simulated as well as live environments, tabletop to field exercises, and it should address start to finish (crisis through consequence) in increasingly more complex scenarios (single event to campaigns, known time/place to an unknown in either or both dimension).

The transnational CW and BW threat must be considered as a driving scenario within this process. Further discussion of the end-to-end systems approach can be found in Section 2 of Volume I. A key point made within this volume is the importance to the Department of building on synergy between force projection, force protection and curl protection. In addition, Volume II of the Task Force final report is devoted to related force protection issues, findings and recommendations.

4.6 FORCE PROJECTION AND PROTECTION



DOD MUST HAVE A COMPREHENSIVE PROGRAM THAT ADDRESSES ALL ASPECTS OF TRANSNATIONAL THREAT USE OF WMD AGAINST US FORCES

Joint Vision 2010 established Full Spectrum Dominance as the focal point of all future military operations. The four elements of Full Spectrum Dominance are: Dominant Maneuver, Focused Logistics, Precision Engagement, and Full-Dimensional Protection. Of these, Full-Dimensional Protection provides the imperative to build a comprehensive program that addresses the issue of asymmetric threats to US forces.

Past efforts in providing Force Protection have focused on deployed or forward stationed units. The aftermath of Khobar Towers and J34's base vulnerability assessments are expanding that awareness to the full spectrum of facilities at which forces, equipment, supporting civilian, and accompanying families are stationed, both at home and abroad.

The need to provide Full-Dimensional Protection builds on existing programs and applies across the entire range of military operations. It recognizes that transnational threats or attacks against CONUS locations or host nations will affect military operations. Potential effects of these incidents include negative impact on the US public and our coalition partners support for military operations and an inability to meet our military objectives.

Concept for Future Joint Operations

"To achieve full spectrum dominance, the military will have to operate with other government agencies and nongovernment organizations and agencies. The military needs to coordinate and consult rather than command and control integrated operations with information operations, private volunteer organizations, and nongovernmental organizations. Thus, the military needs to understand them and complement their strengths without degrading the joint force mission." (CFJO Chap 8-30)

The Concept for Future Joint Operations (CFJO), May 97, identifies the need for the military to coordinate and consult with other government and civilian organizations.

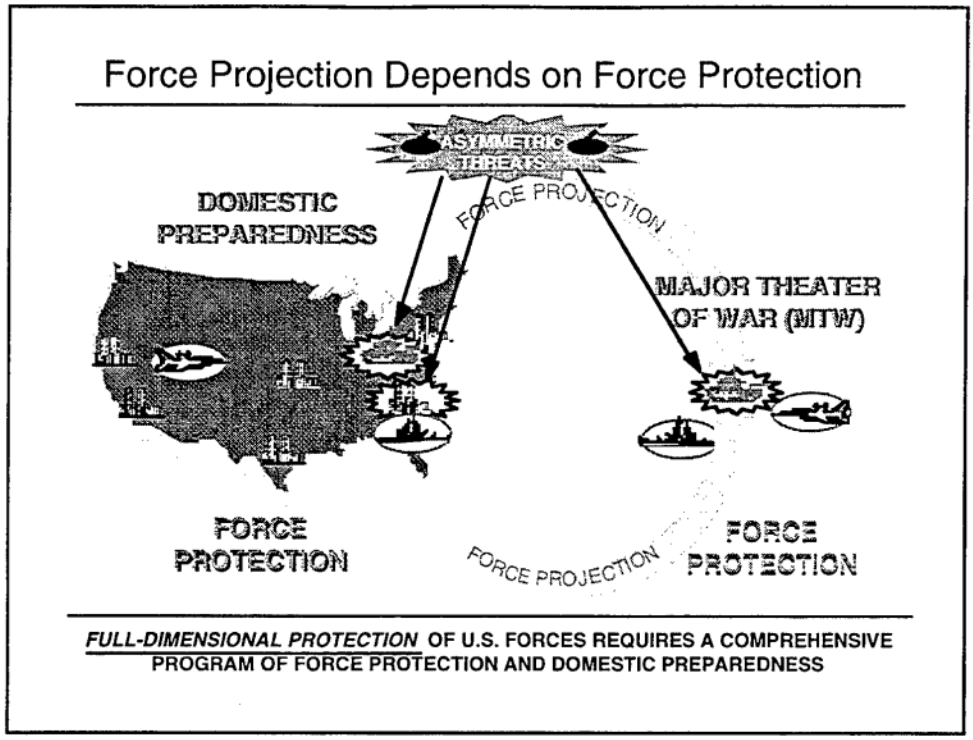
The CFJO further states that the military needs to understand and support the needs of other organizations and complement their strengths without degrading the JTF mission. This is especially true in order to be prepared to respond to domestic terrorist WMD incidents and meet the operational demands of projecting US forces.

The military will have a growing requirement to rely on the civilian infrastructure to support the demands of maintaining a robust Force Projection capability. Transnational threat incidents involving WMD will likely result in large consequence management efforts that requires DoD resources. If the incident occurs as a part of a planned effort to disrupt US deployment of forces, the ability to meet operational timelines can be compromised.

DoD's leadership in helping prepare for the domestic terrorist threats will have an immediate positive impact on its core mission of maintaining a Force Projection military. Further, the synergy between the DoD efforts in force protection and DoD's support to domestic preparedness will put in place a more effective consequence management and mitigation structure[2].

---

[2] Volume II of this DSB Report is devoted to Force Protection issues, findings and recommendations.



As depicted in the above chart, there is a very close relationship between Force Protection, Domestic Preparedness, and the ability to sustain a robust Force Projection posture. Asymmetric threats, such as transnational threat WMD use against military or civilian sites, have the potential to disrupt effective deployment of US forces and challenge a commander's ability to provide Full Dimension Protection.

There are direct parallels between a military commander's requirement to provide Force Protection at installations, ports and airfields and the evolving mission of Domestic Preparedness. The increasing reliance on the civilian sector to provide critical support functions to the military necessitates a comprehensive program addressing deterrence of and coordinated response to WMD incidents. Consequence Management operations will require a surging of local and national assets to respond quickly to and mitigate the effects of WMD incidents.

It is essential that military commanders recognize that Full Dimension Protection encompasses a wide variety of potential asymmetric threats. These threats include direct action against military installations and forces and the collateral effects from incidents that are directed against civilian targets.

DoD's commitment to strengthening the Domestic Preparedness of our civilian responders has the immediate benefit of improving DoD's strategic capability to deploy forces and provide Full Dimension Protection. In addition, US coalition partners will be more likely to support combined operations if the US can demonstrate leadership and a credible consequence management response to WMD incidents.

4.7 INTERAGENCY ISSUES

Other Federal Agency Perspectives Regarding DoD Response Capabilities

- Principles in interagency were interviewed regarding their views of DoD in support of domestic response missions
  - FBI, FEMA, Public Health Service (PHS), State, CIA
- Both DoD specific and broader national issues emerged
  - DoD: good news/bad news
  - Nationally: improving capabilities, but considerable growing pains

A subteam of the Chemical-Biological Warfare Competency Panel interviewed individuals at other federal agencies who work with DoD in both the domestic (FBI, FEMA, PHS, CIA) and force protection (State, CIA) missions.[3] They provided their perspectives about what was and wasn't working and what could be improved for both DoD and the national posture overall. The broadest summary statement of what was learned is that, in addressing the potential employment of CW or BW, the federal, state, and local capabilities and interfaces are relatively immature, but improving. In the process of improving, there are natural growing pains as roles and responsibilities get sorted out and capability gaps identified.

[3] The paper summarizing the findings of these interviews has been published under separate cover by the Sandia National Laboratories team that conducted the interviews.

DoD is Recognized as Doing Some Things Very Well

- Technical expertise
  - FBI relies on DoD for weaponization issues
  - USAMRIID a "critical resource" for IC
    - Historical relationships
    - Unique missions and functionality
  - Detection and decon
  - Transportation
    - Emergency response team insertion
    - Victim dispersal
- "Makes things happen"
  - Used to taking control of a problem
  - "Impressive" operations once set in place
  - Well developed and exercised capabilities for established missions
  - Force of personalities often commanding
- Some relationships
  - With CIA (Defense Intelligence Agency (DIA), USAMRIID)
  - "Generally good" with FBI for domestic operations and training
  - "Major partner" for medical disaster relief
  - "Great" with DOS

On the positive side, DoD is recognized as having the preeminent capability for dealing with the transnational chemical or biological threat. Its unique resources, typified by the TEU and USAMRIID, are critical to other agencies. Its dedicated transportation resources are relied upon for rapid insertion of other agency assets, such as national medical teams. The military training to "make it happen" once committed can lead to rapid action that many other agencies are not routinely trained for. It appears that on selected point-to-point interfaces, as exemplified in the list above, DoD relationships are very solid. This seemed to be the case most often where some longevity could be associated with the relationship.

In Other Areas, DoD Is Not Viewed as Favorably

- Poor internal coordination
  - Overlapping parts of massive bureaucracy not well coordinated
  - Dispersed functionality
  - Nobody's (everybody's?) in charge
  - No accountable chain of command
  - Service/branch independence confuses roles
- Poor interagency skills in supporting roles
  - Used to "taking charge"
  - Lack of coordination with partners
  - Unfamiliarity with local capabilities and needs
  - Confusing interfaces
- Mismatch between civilian needs and DoD capabilities
  - Infrastructure-dependent equipment (e.g., outside Operational Safety and Health Administration (OSHA) regs)
  - Well-practiced battlefield roles not necessarily well suited
  - Tendency to "grab & run" w/o understanding interfaces, protocols
- Reluctance / inability to share some resources
  - Specialized equipment
  - Competing internal priorities for resource & service allocations (e.g., with disaster relief transportation assets)

Those interviewed identified a number of areas where improvement is clearly needed. The sheer size of DoD and the widely distributed responsibilities within the Department were perceived as leading to poor internal coordination and no clear accountability. To an outside agency trying to deal with the Department, the interfaces are confusing. A second perceived shortcoming stems from the contrast of DoD being in charge for their principal military mission, but having to assume a supporting role in domestic missions. Lack of familiarity with regional, state, and local capabilities and responsibilities, and DoD's propensity to superimpose its own approaches has caused communications break-downs with those communities as well as with their federal partners.

The mismatch between military and civilian needs and requirements in dealing with the chemical and biological threat makes much of DoD technical and operational capabilities inappropriate. The situation is further compounded by the lack of accepted standards for equipment to deal with these threats in civilian environments. Even when DoD equipment or resources are well matched to the civilian mission, other agencies cited examples where those capabilities were at best reluctantly shared because the civilian support mission takes a back seat to the warfighting preparedness mission, in spite of standing interagency agreements and emergency authorization for those assets.

Technical and Operational Needs Were Identified

- Environmental backgrounds
- C/B TNT tactics, doctrine(s), & decision indicators
- Interagency data base, info system interface & compatibility
- Rapid incident assessment and response
  - Agent detection & id
  - Notification protocols and priorities
  - Tailored response plans
  - Timely insertions of emergency response resources
  - Protocols and equipment for victim management
  - Decon procedures & equipment
  - Appropriate material handling techniques (hazmat, forensics...)
- Training
  - Accelerated, end-to-end
  - Specialized personnel
- Equipment and decontamination standards

Of interest to the panel was the list of technical needs that were identified among the agencies interviewed. The list is largely consistent with the recommendations for S&T determined by the S&T panel (S&T report is also contained in this volume). Of special note here is the need to characterize environmental backgrounds in order to pull out a chemical or biological agent signature, either early in the intelligence collection phase, at an intermediate stage to locate a source during a crisis, or after the fact in managing the consequences so that appropriate actions can be taken, from dealing with victims to collecting samples for forensic analysis to cleaning up.

Many interviewed voiced the need for protective equipment standards. DoD, with its special knowledge base of both chemical and biological agent effects, should become the technical advisor to OSHA and other regulatory agencies on such standards. In addition, decontamination standards need to be developed.

4.8 ENHANCE ITS CBW DEFENSE CAPABILITIES BASE

Infrastructure: What to Do?

- Technical Escort Unit (TEU)
  - Provide four 12-person ready response teams
    - 1 for JSOTF (to make 3), 2 for CONUS, 1 to support FBI, United States Secret Service (USSS) and local law enforcement, plus expanded intelligence and communications section
    - Requires 65 military personnel
- USAMRIID & USAMRICD chemical and biological medical team
  - Enhance support to domestic preparedness training and CINCs plus improve forensics capability
    - Add 20 (up from 10) medical diagnostic/treatment personnel to USAMRIID
      - 8 Physicians (4 infectious, 4 preventative), 12 techs/contractor
    - Add 15 (up from 6) medical personnel to USAMRIID
      - 5 Physicians, 3 Med Service Corps, 1 Admin, 6 contractors

Critical CW and BW capabilities within DoD are being stretched severely and eroded. The Army's TEU currently has personnel deployed over 200 days per year. Although the unit has recently received ~30 civilian authorizations, it is targeted to lose 27 military positions by 2000. TEU's increasing OPTEMPO coupled with the shift to greater reliance on civilian will soon begin to impact its readiness posture.

TEU's ability to meet its expanding missions could be strengthened with an enlarged intelligence and communications section. We suggest TEUs add four response teams, each made up of chemical and biological technicians as well as Explosive Ordnance Disposal technicians. One team could support the JSOTF (to complement the two existing teams). Two teams could support the overseas deployment requirements to assist the regional CINCs, one based on the east coast and the other based on the west coast. A team could be tasked to support the local and federal law enforcement community (FBI, US Secret Service, ATF, state and local law enforcement). To support this expansion, TEU needs about 60-70 additional military personnel (additional civilian positions will not be particularly helpful to support the increased readiness requirement).

The teams that support the CINCs as well as first responder training at USAMRIID, focused on biological, and USAMRICD, focused on chemical, should be expanded three-fold (15-20 additional government (medical) plus about the same number of contractors). In this case, the government medical personnel should be civilian (to provide continuity).

Leverage Counterproliferation and CBW Defense Programs

- DoD programs to leverage and encourage additional R&D:
  - Treaty monitoring/ verification programs
    - Forensic analysis capability
    - Portable chemical agent detectors
    - Large-volume air sampling systems
    - Individual protection
  - Storage and DEMIL
    - Comprehensive emergency management and first responder programs
    - Integrated monitoring, detection, and warning systems
  - Chemical Stockpile Emergency Preparedness Program
    - Local, state, and federal consequence management interface
    - Prepositioned equipment and emergency operations centers
- All of these programs should be evaluated for applications to force and domestic protection

The DoD should examine its counterproliferation (CP) and CW and BW defense programs more closely to identify additional opportunities to leverage this effort to help respond to transnational threats and their employment of CW or BW weapons. Relevant capabilities exist in detection, forensics, transport modeling and air sampling, which help support the Chemical and Biological Weapons Conventions, and as part of US chemical weapons storage, demilitarization, and emergency response programs.

Of note also is the DOE's new Chemical and Biological Nonproliferation Program (CBNP). DOE technology development efforts in detection, transport modeling, and decontamination are already being evaluated to assess their applicability to supporting response to a chemical or biological incident.

Leverage Chemical Defense Programs

- Present situation:
  - Extensive expertise and technology exists or is under development in DoD and DOE programs
- DoD programs to leverage/encourage additional R&D:
  - Treaty Monitoring/Verification Programs
    - Forensic analysis capability
    - Portable chemical agent detectors
    - Large-volume air sampling systems
    - Individual protection
  - Storage and DEMIL
    - Comprehensive emergency management and first responder programs
    - Integrated monitoring, detection, and warning systems
  - Chemical Stockpile Emergency Preparedness Program
    - Local, state, and federal consequence management interface
    - Prepositioned equipment and emergency operations centers
- All of these should be evaluated for application to force and domestic protection

The Army has had a long-standing and well funded program in chemical warfare defense. Also, during the last decade, the Army has funded additional programs pertaining to Chemical Weapons Convention treaty verification, destruction and safe storage of the CW stockpile, and a Chemical Stockpile Emergency Preparedness Program to protect the communities in the proximity of the chemical depots. These programs have developed new instrumentation to monitor and detect CW agents that may be applicable to transnational threat scenarios. All of these programs should be evaluated for application to force and domestic protection

As an example, some of the techniques developed for treaty verification may be useful in forensic analysis during crisis management or for monitoring decontamination operations. Monitors (such as ACAMS) might find use as an alarm in high-risk facilities.

4.9 ADDITIONAL MEASURES TO IMPROVE DOMESTIC RESPONSE

Other Improvements for Domestic Response

- Enhance 1st Responder capabilities - establish standards
- Increase exercises
- Institutionalize Nunn-Lugar-Domenici
- Stockpile critical materiel

In addition to the National Guard, the panel suggests four additional measures to improve our domestic response posture in protecting against CW and BW attacks.

1. Enhance first responder capabilities by DoD taking the lead in bridging the gap between OSHA and DoD individual protective standards. This effort would lead to the development of standardized equipment and operating procedures that could be utilized by both first responders and DoD personnel supporting the effort.
2. Increase exercises among federal, state, and local agencies to integrate capabilities with command and control procedures, and develop playbooks for seamless transitions between levels of support.
3. Develop a surge capability that provides stockpiles of equipment and vaccines and/or antidotes capable of being rapidly brought to the scene of a chemical or biological incident.
4. Retain stewardship for Nunn-Lugar-Domenici within the DoD. Provide the investment necessary to maintain the effort over time to ensure both first responder and DoD consequence management readiness.

Recommendation : Enhance 1st Responder Capability

- DoD work with OSHA to help develop C/B standards for the civilian & first responders
- As part of CINC Force Protection support: TSWG develop equipment to protect DoD civilians and dependents
  - Designed to OSHA standards and to meet first responder requirements
- Use National Guard Rapid Response Assessment Teams to provide state-tailored WMD response training

Today, military protective masks and suits are designed for the "typical" 18 year old, 70 kg, male soldier. Certain of this equipment do not work well for individuals of different sizes, ages, or physical conditioning. In addition, due to legal (including insurance) reasons, fire fighters and other first responders cannot use equipment which has not been certified to meet OSHA standards.

As part of the force protection mission, a regional CINC must protect military as well as DoD civilians and DoD dependents. However, today the DoD has no personal protective equipment for non-military personnel. The DoD should develop protective equipment that could be used by dependents and DoD civilians. The interagency program of the Technical Support Working Group (TSWG) provides an appropriate forum for meeting both DoD non-military and civilian needs. Working in cooperation with OSHA to determine appropriate standards, the equipment developed by the Department to protect its civilians could be certified to meet these new OSHA standards. This equipment could then be made available for purchase by the first responder community.

The National Guard Rapid Response Assessment Team could provide training for the first responders. This will allow DoD training to be directly transferred to the first responders. It will also help develop the critical personal relationships so necessary during a crisis.

Recommendation: Expand Exercise Program

- Integration of crisis and consequence management is critical-requires practice
  - Frequent (quarterly) expanded Interagency Terrorist Awareness Program (ITRAP) table-top exercise which include CM organizations (e.g. FEMA, PHS, state and local units)
  - Conduct quarterly regional exercises (like NORTHERN EXPOSURE) to develop consequence management relationships, demonstrate comm, check procedures, and build relationships

The command and control relationships among federal organizations is not straightforward as the situation migrates from crisis management to consequence management. In some scenarios, particularly involving a BW release, consequence management could be well under way before the true nature of the crisis was understood. Overlaying such federal relationships on top of the region's first responder community shows the inherent complexity of responding to incidents involving chemical and biological agents. All command and control relationships, as well as each group's tactics, techniques and procedures should be tested and practiced on a regular basis.

This practice can be done in various ways. To test command relationships, table-top or command post exercises should be used. We recommend an expansion of the current Interagency Terrorism Awareness Program (ITRAP) so that all crisis management and consequence management agencies would get

involved. Recent steps to include chemical agent release as the pacing scenario has helped practice against this important threat. Future ITRAP exercises should include simulated BW agent release. We recommend ITRAPs frequency be doubled, to occur every quarter.

To test and rehearse tactics, techniques and procedures, more robust exercises, like the FBI's upcoming NORTHERN EXPOSURE, should be conducted. These exercises would not require the entire responder teams (e.g., not a fully staffed fire company), but instead could include the key leadership and their communications sections. An important benefit of this type of exercise would be the development of interpersonal relationships before a crisis.

Recommendation : Nunn-Lugar-Domenici

- Expand and institutionalize Nunn-Lugar-Domenici
- $200M per year DoD program for indefinite duration
- Secretary of the Army as the responsible official

The Nunn-Lugar-Domenici Amendment on Domestic Preparedness as part of the FY97 National Defense Appropriations Act recognized the current gaps that exist in the national capability to respond to incidents involving WMD. DoD was directed to provide emergency response training, advice and assistance to first responders; assist in developing a rapid response team; conduct testing and evaluation of preparedness; assist in developing and maintaining an inventory of physical equipment and assets; and assist in procuring equipment to interdict WMD. The Act allocated $84.7M in FY97 and FY98 and terminates on 1 October 1999.

To implement the recommendations for increasing our consequence management domestic preparedness, Nunn-Lugar-Domenici should be expanded and institutionalized. Readiness is a continuing effort; resources must be dedicated to sustain the effort. The DoD program should be recognized as one of indefinite duration. Doubling or tripling the current funding (to about $200M per year) could produce substantial improvement in national capabilities. The Secretary of the Army could remain the executive agent for implementation. This would capitalize on the Secretary of the Army's responsibilities for coordinating military support to civil authorities and the National Guard Bureau.

Nunn-Lugar-Domenici: Specialized Equipment

- Specialized detection and monitoring systems
  - For rapid assessment
- Medical supplies including antidotes
  - Prepositioned in FEMA regions and with National Guard response units
- Protective gear
  - In hands of first responders
  - Stockpiled OSHA-certified gear for response augmentation
- Device disablement
  - Ability of specialized units to respond rapidly
- Decontamination equipment
  - Available for large scale events

All adapted non-military use-standards, affordability, ease-of-use

The lack of standardized specialized equipment available to all federal, state and local agencies degrades our consequence management capabilities. Medical supplies, to include vaccines, should be pre-positioned within the ten FEMA regions, available for rapid delivery to an incident site. Protective gear, capable of meeting both OSHA and DoD standards, must be procured in sufficient quantities to provide first responders with confidence in their capabilities. Additionally, due to the scarce assets available to disable devices, trained specialized units within FEMA regions capable of isolating and dismantling devices will expand first responder deterrence capabilities.

4.10 SCIENCE AND TECHNOLOGY

In this section the panel offers its judgment of where the gaps are in the science and technology effort and recommends areas for additional investment. A more detailed discussion is provided in the Annex of this report.

DoD's science and technology (S&T) efforts to enhance CW and BW defenses have not been motivated by the transnational threat. During much of the cold war, CW and BW defense S&T efforts were driven by the Warsaw Pact military threat to the North Atlantic Treaty Organization. Later in the cold war, and continuing today, CW and BW arms control treaty monitoring became important. More recently the primary driver has become dealing with the CW and BW threats to US military operations from regional adversaries in the context of major regional contingencies. Much of the S&T effort undertaken for these other missions is also relevant to defense against the transnational CW and BW threats. However, additional S&T investment will be needed to deal with the new situations and environments presented by the CW and BW transnational threat.

Science and Technology Gaps in Ongoing DoD and DOE Programs

	Detection/ Identification	Protection		Decontamination	Intel Support
		Individual	Collective		
Fielded Capabilities	• Chemical Agent Monitor (CAM) • Biological Integrated Detection System (BIDS) • SMARTkit test ticket • Integrated Biological Agent Detection System (IBADS) • Tier I Biological Particulate detector	• Vaccines: anthrax and botulism • Chem. agent auto injector • Protective clothing and masks • Chemical prophylaxis	• Modeling and simulation (battlefield)	• DS2 decon solution • DS2P decon solution • Hypochlorite	• Monitoring • Data mining
Ongoing Programs	• Aerosol science: autonomous collection and concentration • Biological recognition sites: genetic probes, recombinant antibodies • Mass spectrometry: Matrix Laser Desorption Time of Flight (MALDI-TOF), electrospray • ISIS test tickets • Genetic Technology; • Polymerase Chain Reaction (PCR), • DNA chips • Stand-off Detectors • Microsensors	• Vaccines: Joint Vaccine Acquisition Program (JVAP) • Therapeutics	• Modeling and simulation (urban)	• Enzymatic decon of G & V agents	• Signature I.D. • Epidemiology • Bio background • Automated data mining
Gaps	• Medically-derived detection thresholds • Pathogen genome sequences • Stand-off real-time detection • Multi-agent autonomous detection • Detection interferents • Detection triggers	• Variable autoinjectors • Multivalent vaccines • Disposable protective suit • Anti-viral agents • Radioprotectives • Bio-mask	• Safing • Rapid triage	• Large-area non-corrosive decon (HD, VX, novel OP agents) • Decon standards	• Production facility detection and location

The above chart summarizes the CW/BW Panel's impressions and judgments about CBW defense "capabilities." These capabilities and programs were developed, largely, for the protection of US military forces on the battlefield and not to counter the transnational threat. Capabilities are shown in four categories: detection/identification; individual and collective protection; decontamination; and intelligence support. Assignment of some capabilities (e.g., modeling) to a particular category is arbitrary. Capabilities within each of these categories are designated as either 1) being already in

existence, 2) under development or 3) deserving of more attention. Vaccines show all three status categories, reflecting the existence of vaccines against anthrax and botulism (two of the most usual suspected BW threat agents); an ongoing program to provide an assured source of these vaccines and finally the desirability to have vaccines that work against a much larger variety of BW threat agents.

Suggested S&T Strategy

- Sustain strong S&T program to improve US ability to conduct military operations against CW and BW armed adversaries
  - Dealing with CW and BW threat to points of debarkation and embarkation is particularly important
  - Much of this effort is also relevant to force protection and civil protection missions against CW and BW transnational threat
  - Current S&T programs for arms control and monitoring can also contribute to dealing with transnational threat
- Identify areas where additional S&T investment can make important contributions to redressing CW and BW transnational threats
  - Some of these are identified in the following charts
- Use the Technical Support Working Group (TSWG) to identify and pursue short and mid-term improvements
  - Increase their budget for CW and BW defense items
- Increase effort to engage US biotechnology community in the search for solutions to the BW threat
  - Build on emerging DoD and DOE efforts

Since the capabilities in the preceding chart address conventional military means and not those unique to the transnational threat, the following recommendation charts may identify solutions for gaps that have not been included above.

CW/BW Recommendations: Areas for Additional S&T Investment

- Detection/Identification
  - Remote sensing system for biological threats
  - Evaluation of sensors being developed for other purposes in possible application to providing early warning of CW and BW threats
  - Low-cost autonomous alarms for building Heating, Ventilation Air-Conditioning (HVAC) systems
  - Inexpensive, unattended, automated biological detectors with minimal maintenance, sensitivity, and good differentiation
  - Practical mass spectrometers for biological agent characterization
  - Enhanced epidemiology, thru field studies, education of needed personnel, better data collection and dissemination
- Protection
  - Chemical/biological filter systems for facility air
  - Improved protocols for vaccination against BW agents
  - Biological masks – military and civilian
  - Rapid diagnostics to determine exposure to CW and BW agents (particularly important for biological incidents since development of symptoms are generally more immediate and obvious for chemical agents)
  - Atmospheric agent transport models to support consequence management

S & T can make important contributions to detection and identification, protection of personnel, treatment, monitoring and decontamination.

There is a need for low-cost CW/BW alarms. Very low false alarms rates are desirable, but if not, perhaps alarms that are properly placed and interpreted intelligently, can be extremely useful. (e.g., smoke alarms in the home are often set off by other causes.)

The detection of biological attacks remains a most serious shortfall. There are no reliable autonomous detectors against biological agents dispersed as particulates in the atmosphere. The Biological Integrated Detection System (BIDS) is a mobile laboratory supported by four people, two technicians to run the tests and two other to support the power generators, etc. Present systems depend on collecting particulates and then analyzing them by various biological tests. These systems require human intervention and manipulation, and use "wet" systems that require continual logistic support.

Biological systems directly connected to semiconductor chips and mass spectroscopy (MS) hold promise for major improvements in this area. Proper treatment of the biological samples at the front end can lead to interpretable MS signals or fingerprints. The civilian sector is now developing biological chips based on DNA identification. Similar methods directly tied to chips that then convert the results into electrical signals that are more readily adapted to alarms and detectors should be examined. A key issue for the DoD is transforming these emerging technologies into systems that are effective in the field.

CW/BW Recommendations: Areas for Additional Investment (cont'd)

- Decontamination – interception
  - Non-destructive analysis of captured munitions
  - Decontamination foams for isolating and neutralizing captured munitions
- Decontamination– consequence management
  - Wide area decontamination methods and chemicals
  - Decontamination techniques for sensitive equipment (e.g., electronics)
- Protocols and standards for chemical and biological decontamination: "when is clean clean enough?"
- Support for intelligence
  - Biomakers (to determine previous exposure)
  - Data-mining
  - Tracking personnel, equipment purchases, precursors

Some non-destructive analytical methods have been developed for treaty verification purposes (e.g., nuclear techniques such as neutron activation). Such methods are capable of detecting the presence inside a container of certain elements that are indicative of chemical agents. These techniques are useful for determining if a captured device might be a chemical munition.

Foams containing decontaminating agents have been develop for other applications. They should be considered for containing undetonated chemical munitions prior to movement.

The DoD, and the nation at large, currently lacks capabilities to respond to a large-scale BW attack (as well as a large-scale CW attack if a persistent agent, such as mustard, were used,) in which some means of wide area decontamination would be required. Also, costly and delicate equipment that have been contaminated, such as electronics and computers, would probably have to be discarded unless some non-destructive means is developed to decontaminate them. Presently, there are no such methods.

A recurring problem is being able to decide when something has been decontaminated satisfactorily. Methods used in the chemical demil program are inadequate for potentially large-scale CW events. Present techniques (5X) require heating an object to 100° F for 15 minutes, clearly an impractical approach. Other criteria must be identified and demonstrated, as appropriate for attacks on urban areas.

Leverage Biotechnology Revolution

- Extensive biotechnology expertise in government, industry, and universities
  - Genetic screening, diagnostics, DNA sequencing, immunology, "naked" vaccines, rapid drug developments, point-of-care analytical capabilities
- DoD/DOE reaching out to this community
  - DARPA's long term biological R&D ($50-60M)
  - DOE/National Labs initiative ($25M)
- Additional opportunities to adapt biotechnology efforts to BW defense
  - Human genome projects provide templates for BW defense
  - Commercial sector would need BW defense-specific information
- However, this community is not interested in working on BW defense
  - Additional incentives needed
- DoD must support the application of these technological advancement in the civilian sector to the BW defense challenge

Biotechnology activities in the Department of Defense and the Department of Energy that can lead to improvements in biological weapon defense are dwarfed by those in industry and academe, all of which can be leveraged to accelerate this process. Though the government is funding a number of initiatives through DARPA and the DOE, there are additional opportunities to exploit in the civilian sector. For example, the technologies being developed by the human genome project are directly applicable to sequencing the genetic structures of pathogens that could lead to improved detection methods and treatments. With the appropriate inducements, greater leveraging of these capabilities is possible. DoD may have to fund military specific application of the technologies.

The US biotechnology community (spread out in universities, research institutes, small biotech firms and large pharmaceutical companies) is the world leader in this field and possesses the knowledge and tools to help DoD understand the threat and devise defenses against it. DoD must forge much closer ties to this community, which has little motivation or incentive for such close ties. Brokering this relationship and getting this community involved in defense against the CBW threat will require the involvement of the most senior government officials, as well as support from the Congress, to provide financial incentives, appeals to patriotism (or ego) and perhaps assurances on the strictly defensive nature of the work.

4.11 PREVENTING AND DETERRING CB TRANSNATIONAL ATTACKS

Don't Ignore Roles for Prevention and Deterrence of CB Transnational Attacks

Prevention:

- Constrain the perpetrator's ability to conduct CW attacks
- Domestically, a responsibility of law enforcement agencies, including FBI counter-terrorism unit.
- Foreign, DoD plays a role, but a limited one.

Deterrence:

- Shape the perpetrator's will to conduct CB attacks
- Limited utility; but some value

Part of what distinguishes the transnational from the state threat is the very different dynamic involved in preventing and deterring aggression. Because of these differences, there is a tendency to dismiss efforts to prevent and deter transnational threats. But prevention efforts can help to mitigate the threat, and efforts to deter can contribute to minimizing the threat if properly conceived and focused.

Steps to Preventing Foreign Threats

- **Sustain CINC focus in theaters:** Maintain strong top-down emphasis on identification of transnational threats
  - Cooperate with host nation to track and constrain transnational groups
  - Supplement with effective interdiction capabilities
- **Focus on state sponsorships:** State sponsorship remains the shortest route to the most lethal attacks
  - Reinforce restraints on state sponsorship
  - Punish sponsors
  - Utilize export coordination mechanisms, such as Australia Group, to monitor flows of technologies and materials

Other steps could extend international cooperation. These include utilizing the international legal framework. Prevention is strengthened by international cooperation among like-minded countries. Significant diplomatic efforts over last decade have helped to expand and enforce various counterterrorism protocols.

Continuing G-8 collaboration is important. The nations have cooperated since the spring of 1995 to define an agenda of common action and to work each part of the agenda. The next event is a meeting hosted by the US in December where the G-8 nations will identify opportunities to coordinate R&D on technologies for countering WMD.

A Cooperative Threat Reduction Program for BW

- Yeltsin acknowledges Russian offensive program difficult to close
  - 40,000 people dispersed among world-class facilities
  - Expertise and technology can migrate to transnational threat
- Pilot Cooperative Threat Reduction efforts specifically on BW:
  - US National Academy of Sciences' led joint research on 7 topics
  - DOE proliferation prevention program
  - Separate DOE joint epidemiological study ($0.5 million)
- Goals:
  - Integrate scientists and facilities into global community
  - Improve public health
  - Promote transparency on past program
- **Recommendation:** evaluate pilot efforts in order to scope and identify follow-on projects.

One measure for preventing the use of BW weapons can be taken in the context of the Cooperative Threat Reduction Program between the United States and Russia. To date, this program has focused almost exclusively on nuclear weapons, materials, technologies, and expertise. The risks on the BW side dictate that the Cooperative Threat Reduction (CTR) program be expanded to also address BW containment. Several small pilot projects are in place.

DoD should evaluate these projects in order to identify follow-on work useful for improved public health and BW defense. The potential long term benefits (especially to nonproliferation) are substantial. But so too are the potential risks of facilitating continued offensive work in Russia.

Deterring Transnational CB Attacks

- **Periodically reiterate the national commitment to track down and punish perpetrators of WMD attacks.** Ensure that a consistent message is sent from all levels of USG.
- **Create and use a Human Factors Assessment Center to get inside adversaries' heads, understand, and exploit what deters.** Analogue utilized in Evident Surprise 96 and 97
- **Threats and demonstrations may be ignored or misunderstood.** Deterrence may contribute little to preventing the first major attack, but it could have great impact on a second
- **Give these limits, periodically demonstrate the US ability to detect, interdict, disrupt, and, if necessary, manage the consequences of attacks.** But demonstrate without compromising capabilities

A US response to a first attack that is perceived to be efficient, compassionate, and successful in securing a just outcome may discourage copycat attacks. But the opposite may be true as well: gross inefficiency may signal incompetence. Failure to minimize suffering may transform public attitudes toward government. Failure to punish perpetrators--or heavy-handedness in doing so--could incite further violence.

Other steps could contribute to deterring CB attacks on military forces. These include funding the US Special Operations Command (SOCOM) to continue improvements in Special Operations Forces (SOF)-related interdiction capabilities and charging CINC USACOM with preparing to conduct highly visible deployments of protection and consequence management capabilities in time of near-war. It could also include charging DIA with increasing its attention to CW and BW aspects of the force protection problem. Focus on signs of weakening restraint by state sponsors and cooperation between non-state groups and transnational criminal organizations and strengthening coordination among DIA, CINCs and local (host nation) law enforcement agencies.

To Deter Domestic CB Threats

- **Request FBI forensic plans:** Request that FBI draft a plan for the selective development of DoD assets useful for forensics work associated with CB threats (e.g., Tech Escort, CBDCOM, USAMRIID).
- **Implement militia restrictions on active duty and guard personnel:** Implement the stated intent to prohibit the participation of active duty personnel in militia and militia-like movements.
- **Avoid steps that motivate transnational threat acts:** Observe Posse Comitatus scrupulously. No single act could more readily incite the anti-federal militia movements than a use of active forces domestically that abrogates legal restrictions.

DoD agencies have capabilities useful for domestic law enforcement purposes in the CB area. Tech Escort has operational investigatory skills. USAMRIID has unique forensics capabilities. DoD does not have a good grasp of domestic law enforcement needs for which its skills might be useful. It should invite FBI leadership to offer a strategy and then refine and implement the plan.

Racist and other violence on military bases has periodically alerted DoD to the presence of organized elements in the US military, elements that have sometimes used military service to acquire operational skills for terrorist purposes. These alerts have led to calls to ban membership in such organizations and recruitment on bases, bans that have not yet come into being.

No single act could ignite the militia movements into an aggressive campaign against the federal government than a use of military force domestically that violates the Posse Comitatus restrictions. They are highly alert for such acts. Some recent domestic operations have not been well explained to the public, such as the nighttime special forces exercises. If explained at all, this has fueled the rhetoric of these movements.

CONCLUSIONS

Reviewing Key Findings

- **The threat:**
  - The CW/BW threat is both different and dangerous.
  - The right steps will help to mitigate it.
  - Inaction may fuel its growth.
- **DoD's current posture:**
  - It has made many good starts and has many valuable assets for a national effort.
  - But key parts of the base are thin and getting thinner. It is also not focused on the transnational threat.
  - An incremental approach is appropriate.

Reviewing the Strategy

- Accelerate the climb up the learning curve. Get smarter about the threat and responses.
- Address the specific CW and BW threat elements of the force protection mission.
- Address DoD's responsibilities to support domestic contingencies
  - Retain stewardship of N-L-D
- Prepare for the long haul:
  - Organize for the mission
  - Fix the interagency
  - Reverse erosion of existing capabilities
  - Pursue improved S&T assets
  - Prepare to surge
- Across the board:
  - Adjust responses for difference between C and B
  - Exploit CT, CP, and civil overlaps
  - Enhance critical relationships

Payoffs from the Strategy?

- Preventive measures can help to deter or dissuade attacks and limit the copycat attacks that typically follow terrorist innovations.
- Consequence management capabilities can help to keep casualties and fatalities to peacetime numbers by acts of nature or manmade catastrophe or, in time of war, to numbers suffered historically.
- Effective – and legally correct – coordination between civil and military responders will help to allay concerns about military role in domestic affairs.
- After any serious transnational attack, a burden of proof will fall on government to show that it did as much as possible beforehand to prevent the event, to equip responders to minimize suffering, and to secure a just result.

Highlights of Recommendations (A WAG at the Costs)
(Costs not Additive)

♦ Augment TEU to expand readiness	~65 military
♦ Enhance USAMRIID, USAMRICD medical teams	~35 medical
♦ Institute end-to-end systems approval	$30M over 18 months
♦ Conduct more CBW exercises (table, top, CP, and field)	~$20M-$30M
♦ Develop military decon and civilian equipment (OSHA) standards	~$5M
♦ Grow TSWG to emphasize CB and Force Protection	~$30M-$35M (grow to)
♦ Retain stewardship of an expanded Nunn-Lugar-Domenici	$200M/yr (including some of other costs shown)
♦ Initiate and evaluate additional pilot prevention projects with Russian BW community	$10M/yr
♦ Engage biotech industry via direct Presidential appeal	
♦ Increase intelligence community effort in CBW threat assessment tenfold	~$150M-$200M

- We also endorse SECDEF call for $1B plus-up in CW and BW defense programs per the Quadrennial Defense Review (QDR) recommendation

In addition to more personnel for TEU and the Army chemical/biological medical teams, other steps are recommended. These include:

- Institute end-to-end systems approval
- As emphasized in other sections of the report, exercises, particularly with interagency participation, should be increased and address the full set of crisis to consequence management

functions. DoD's participation will require $20-30 million for an approximate doubling of current efforts.

- Today, the services have no decon standards which would allow, for example, a "dirty" air filter to reenter a clean base. Such cleanup standards must be developed. The DoD should also help develop civilian self-protection standards with OSHA.
- The Technical Support Working Group (TSWG), the interagency development program, should at least double its efforts, on developing chemical and biological equipment to support military and appropriate civilian responders.
- Retain stewardship an expanded Nunn-Lugar-Domenici.
- The Cooperative Threat Reduction program aimed at protecting Russian nuclear assets (personnel and materials) should be expanded to encompass Russian BW weapons and capabilities.
- No less than the President should engage the biotechnology industry to help develop options and solutions for dealing with the biological threat.
- To improve the nation's capability to warn of and, hopefully, deter such an attack, the intelligence community should greatly increase its emphasis on the BW threat. This effort will require nearly $200M/year increase in resource allocation.
- Support of the SECDEF's recent intent to provide $1B over the FYDP to improve Chem/Bio defense.

ANNEX: SCIENCE AND TECHNOLOGY OPPORTUNITIES

This annex elaborates upon the discussion in section 4.10 and provides additional details on the Science and Technology opportunities to contribute to the mitigation of the CBW transnational threat.

This annex is divided into two sections. The first presents sets of charts that identifies the functions and tasks that must be accomplished to achieve the overall objective and highlights some shortcomings and gaps for each of these functions and tasks. There are two sets of charts: one for the biological threat and the other for the chemical threat.

The second section discusses the applicability of current DoD chemical and biological defense capabilities to the transnational threat challenge and the potential of programmed new capabilities and ongoing technology efforts to fill some of the shortcomings and gaps.

I. FUNCTIONS AND TASKS

Functions that Contribute to Mitigating the CBW Transnational Threat

- Prior to an Incident
  - Intelligence and analysis
  - Early warning for
    - High-value, high-risk facilities and events
    - Lower-value, lower-risk targets
  - Protection of personnel
- During and incident
  - Interception
- After an incident
  - Crisis management
  - Consequence management
    - Immediate
    - Later
  - Attribution

For each of these functions listed in the above chart, the following sets of tables identifies some of the critical tasks that must be performed to accomplish the overall mission of thwarting the CBW threat from transnational groups. Gaps and shortcomings are highlighted.

Biological Threats

Operation	Activity	Objective	Responsible Organizations	Examples of Technologies or Devices	Needs/Shortcomings/ Comments
Intelligence & Analysis	Epidemiology	Analysis of publicly available data for warnings of non-natural occurrences (e.g. biological agent testing). Exposures during production.	Domestic: FBI, CDC, PHS. Foreign Intelligence community.	Data mining tools	People, time and money intensive. Transfer of information channels are not delineated. Requires a new/revised intelligence operations plan. Domestically , this is being done by CDC and WHO.
	Tracking of manufacturing equipment	To identify the construction of a potential production facility.	Domestic: FBI, Foreign Intelligence community. Dept. of Commerce	NPC Commerce. PHS, CIA, DIA , NSA have database	Legitimate trade and manufacturing hides illicit activities. This could be onerous unless the parameters such as size and quantities are well defined. However, certain materials that are not widely used in licit trade could be earmarked for tracking. Must identify distinguishing characteristics for dual and multiple use capabilities. Probably useful for large production facilities only.
	Tracking of trained personnel	• Training? • Where are they going? • What programs or deployment do personnel have? • What ports of entry do they pass?	Domestic: FBI Foreign Intelligence community.	Data mining NSA. CIA, DIA Database of US trained scientist.	Could lead to the identification of facilities and the likelihood of a threat. Very time and money intensive unless suspected personnel can be identified from other sources.
	Infiltration of suspect groups	To identify nature of organization and source of production.	Domestic: FBI, Foreign Intelligence community.	Database Intel functions General screening procedures Medical diagnostics Environmental monitoring	Requires prior intell to learn of the existence of groups. Must recruit agents in group or emplace an agent. Legitimate trade and manufacturing hides illicit activities

Biological Threats

Operation	Activity	Objective	Responsible Organizations	Examples of Technologies or Devices	Needs/Shortcomings/ Comments
	Surveillance of suspect production facilities	Sample water sources for typical waste from a fermentation facility including volatile organics (associated with fermentation).	Domestic: FBI Foreign Intelligence community. State Dept.	Point biosensors. Mobile bio-lab such as BIDS & IBADS techniques. Simple detectors and screening devices. Large volume samplers. Telemetry	Requires on-site testing and screening and access to waste streams. Must be able to remove samples to a laboratory. Must have simple testing kits to screen to determine when samples are worth further analysis taken. And maintain chain-of-custody
	Monitoring of large test areas	Collect large volume aerosol samples with a sampling device to monitor open air testing.	Domestic: FBI, Foreign: Intelligence community.	Large samplers such as used in nuclear monitoring programs.	Requires advance knowledge of test times and locations.
Early warning (lower risk sites)	Continuous monitoring of common facilities, e.g., federal buildings, casernes, etc.	To install "smoke detector-like" alarms in buildings to screen air in building.	Domestic: organization owning facility. Foreign: organization owning facility	"Tier I" simple aerosol samplers would act as smoke alarms. Tier II detectors that use UV as well as particulate counts. Biosensors. Atmospheric modeling. UGS.	Device must be reliable and have low enough false alarm rates. Inexpensive. Sensors must be carefully located relative to airflow in buildings to detect most likely/most severe attacks. Background particulate levels must be determined prior to installation. Some confirmation procedures must be determined to check when an alarm occurs. There are 10^{-8} gm of protein per liter of air on an average. This will cause alarms in non-specific detectors.

Biological Threats

Operation	Activity	Objective	Responsible Organizations	Examples of Technologies or Devices	Needs/Shortcomings/ Comments
	Pre-planning and threat assessment	To prepare emergency procedures in the event of an attack.	Domestic: organization owning facility. Foreign: organization owning facility	Modeling and Sensitivity Analysis Sensor placement planning Evacuation routes Protective equipment	Each procedure must be building specific. Requires inspections and planning for each site. Device must be reliable and have low false alarm rates. Probably expensive.
	Alarms at ports of entry	Detect biological agents and precursors crossing international borders. Precursors include media, cell cultures..	Coast Guard Customs Border Patrol	Passive sensors	Must distinguish bio agents from legitimate bio materials. Biological devices have no unusual detectable signature. Not very likely that small amounts would ever be detected. Could not differentiate accidental contamination from planned one. Only good if leaks occur
	Screening of food and water	Protect civilian and military food and water sources.	Domestic: Dept. of Agriculture, FDA	DNA test kits ELISA assays Gene chips ISIS antibody kit	Must determine the sensitivity levels required and distinguish normal contamination from BW. Logistical Problems with large number of samples that would be required. Maintain chain of custody
	Screening of Agriculture	Protection of agricultural and livestock from infestation by organisms.	Domestic: Dept. of Agriculture, FDA Foreign: host country.	Agricultural monitoring. Genetic Diversity. Rapid PCR ISIS Kit	Knowledge of specific threats. What is consequence management of agricultural attack? Difficult to identify motivation: accidental or planned.

Biological Threats

Operation	Activity	Objective	Responsible Organizations	Examples of Technologies or Devices	Needs/Shortcomings/ Comments
Warning for high value targets and special events, e.g., G7, Olympics, etc.	Exterior alarms at conference sites and other targets of opportunity	To install real time alarms for high risk or probability sites	FEMA? FBI? DOJ?	Point or standoff biosensors • BIDS • IBADS • Port/Airfield Sensor • Joint Point • JBREWS • UV LIDAR	Must distinguish bio agents from background, must be inexpensive, very low false alarm rate. Collect samples for further analysis and maintain chain of custody. Agent clouds from covert attacks can be very small, requiring large numbers of detectors to provide indications of attack. False alarm problem.
	Setup of mobile lab	To prepare for the analysis of CB agents in case of a threat.	FEMA? FBI DOJ	Analytical instrumentation • Commercial Analytical Equipment • BIDS • Test kits • PCR/LCR	Rapid response. Expensive

Biological Threats

Operation	Activity	Objective	Responsible Organizations	Examples of Technologies or Devices	Needs/Shortcomings/ Comments
Warning for US forces	Provide warning of covert attacks on US forces in assembly areas	Detect attacks in order to treat exposed forces in a timely manner and, if possible allow forces to don protective gear and re-position other forces.	Intel, CIA DoD	Point or standoff equipment • BIDS • IBADS • Port/Airfield Sensor • Joint Point • JBREWS • UV LIDAR • IR LIDAR • MEMS • PCR/LCR • Gene chips • Sequencing for hybridization	High sensitivity against small attacks. Must collect samples for further analysis.
Warning for support forces, host nation and contractor personnel	Provide warning of attacks on personnel providing logistic support to US forces	Detect attacks in order to treat exposed personnel in a timely manner and, if possible, allow personnel to don protective gear.	Host nation Military Intel Agencies	Point or standoff biosensors BIDS IBADS Port/Airfield Sensor Joint Point JBREWS UV LIDAR IR LIDAR	High sensitivity against small attacks, very low false alarm rate. Must collect samples for further analysis and maintaining chain custody. Need inexpensive "adequate" masks. Large areas to be covered. Procedures must be adopted that do not cause panic, flight of personnel.
	Rapid Agent viability testing	To assess whether or not response is necessary.	PHS, CDC	Marker dyes	Quick (minutes) determination of agent viability is required. Must determine if toxins are "native", i.e., biologically active or just immunologically responding to an antibody or reacting with a DNA primer. Must collect samples and preserve them. Present methods require a development time.

Biological Threats

Operation	Activity	Objective	Responsible Organizations	Examples of Technologies or Devices	Needs/Shortcomings/ Comments
	Protect personnel	Provide passive protective garments and mask against biological agent.	Military organization inside perimeter Host nation outside perimeter	Masks BDU, JSLIST, dust masks Respirators Hospital masks	Inexpensive "adequate" masks Must filter out particles in the 1-10 micron range. Especially for non-military personnel, masks must be readily available and relatively cheap.
Protect personnel	Provide passive and active immunity	Minimize vulnerability of personnel to biological agents.	Military organization inside perimeter. Host nation outside perimeter.	Vaccines, antisera development programs for likely threat agents.	Must provide protection against many times lethal dose. Must ensure that vaccine will protect against aerosol threat (not just normally occurring disease) since we know that some vaccines (plague) work against endemic disease, but not against aerosol. DARPA programs for broad spectrum coverage. Knowledge of agents, determination of who receives immunizations well as who is identified for booster regimens to maintain immunity. Must assess potential side-effects of vaccines or drugs . Current programs are traditional in nature; i.e. they are working on a vaccine for each specific agent (this is the state of the art technology)- the DARPA program has the potential of developing a more generic approach. We do not have the technology now for an omnivalent vaccine.
	Active therapy	Block binding of toxins and viruses to target sites	Domestic: Local governments and health and military organizations. Foreign: Military and host countries, USAMRIID NMRI	Small molecule databases; protein binding site modeling Development programs at DOE and pharmaceutical labs.	Identify small molecules to interfere with toxin and viral binding to specific target sites. Must ensure that interference does not alter normal cell function; must identify side effects but the Concept of Naked DNA as a vaccine is promising.

Biological Threats

Operation	Activity	Objective	Responsible Organizations	Examples of Technologies or Devices	Needs/Shortcomings/ Comments
Interception	Capture, isolate and transport captured devices and to avoid the spread of disease.	To capture any device prior to dissemination. To containerize the device.	Local law enforcement FBI, CID EOD, CDC, PHS	Containers Standard EOD devices such as x-ray, pins, etc.	Prior bio program provided containers for bio weapons which met and exceeded ICC standards.
	Deactivation Demilitarization	To deactivated and destroy organisms in a bio weapon.	Local law enforcement FBI, CID EOD	Water/foam Oxidation/hydrolysis High gamma doses Heat Chlorinating Fire fighting foams	Standard methods for sterilization can be used here. R & D needed to provide new materials equivalent or better than BPL and EY+TO but not carcinogenic
Immediate Consequence management	Identify exposed personnel	To prevent contaminated persons to leave site and cause secondary contamination. Begin treatment before symptoms appear. To separate casualties into groups to treat those that need it most. Isolate unexposed.	Domestic: First responders Local health organizations FEMA PHS Foreign: Military and Host country. Local health organizations	Antibiotics for bacterial diseases. Antisera for some toxins. Limited information and availability of antiviral drugs. Ongoing R&D to assess effectiveness of antibiotics against known threats when delivered via aerosol. Additional development programs for neutralizing monoclonal antibodies	Cheap, simple assay for field use. Cost of antibiotic regimens. Problem assuring compliance with extended use (14 days or more). Logistics of administering IV drugs or antisera. Possible side effects of antibiotics, other drugs, or other treatments (i.e. serum sickness from horse derived antitoxin. Legal ramifications of restraining private individuals from leaving scene.

Biological Threats

Operation	Activity	Objective	Responsible Organizations	Examples of Technologies or Devices	Needs/Shortcomings/ Comments
	Prospective Epidemiology	Monitor effects of treatment .	CDC Armed Forces Institute of Pathology	Standard epidemiology Extensive database	Time to accomplish.
	Analysis of node where attack was carried out	To determine the source and to model the cloud transport limits for immunization of possibly exposed people.	FBI, CDC	Atmospheric models.	
	Coarse Decontamination	• Achieve "adequate" clean-up. • Risk management.	First and second responders	Deacon materials including chlorine water and others.	What is "adequate" decontamination?
Later consequence management	Treat exposed personnel	Minimize casualties	Local Health Organizations, CDC, PHS	Antibiotics, antisera, supportive technologies	Problems with compliance with need for long-term use of antibiotics. Expensive Logistics. Current approaches are resource intensive.
	Cleanup region around US Site • CONUS • OCONUS	Prevent secondary aerosolization and further contamination	Fire and Rescue teams		No clear designation of responsibility.
Crisis management	Forensic analysis of the site of exposure	To determine the perpetrators	Domestic: FBI		
Retribution	Gather evidence	Identify and apprehend perpetrators.	Local Police, FBI, CIA, CID		

Chemical Threats

Operation	Activity	Objective	Responsible Organizations	Examples of Technologies or Devices	Needs/Shortcomings/ Comments
Intelligence & analysis	Monitoring of accidents	Analyze publicly available data for warning of non-natural occurrences (e.g. poisoning).	Domestic: FBI. Foreign: Intelligence community.	Data-mining tools CBIAC Chem/Bio information Services	People- and $-Intensive. Presupposes that some accidents occurred. Rapid dissemination of information to responsible agencies. Local State and Federal
	Trace shipments of precursor chemicals and equipment.	To identify groups or sites that may be producing chemical agents.	Domestic: FBI. Foreign: Intelligence community.	Tracking devices and beacons. Fluorescent tags, RF tags, GPS. Tracking techniques used by FedEx.	Must have some interaction with the commercial sector that sells the chemicals. Difficult to track small quantities; cost of technologies. Only useful for standard or suspected agents. Often many synthetic routes to an agent. Dual use of many precursors.
	Tracking of purchase of equipment used to produce agents.	To discover suspect purchases of equipment used in the preparation of agents and materiel including protective masks and clothing.	Domestic: FBI Dept. of commerce Foreign: Intelligence community		Equipment for producing small amounts of agents is not unique to chemical agents or other toxic materials. Toxic agents can easily be produced in a standard chemical lab equipped with fume hoods. but bathtubs have also been used
	Monitoring of atmosphere.	Collect large volume air samples to monitor open air testing.	Foreign: Intelligence community Domestic: FBI.	Spectroscopic techniques, remote sensing. High volume air samplers	Dollar and people intensive. Require prior intelligence. There may be no testing of the devices.
	Penetration and monitoring of suspect groups.	To assess if groups are involved in illicit activities that could lead to transnational threats.	Domestic: FBI. Foreign: Intelligence community.	Grab samplers and non-specific sample "tickets." Chemical dosimeters (absorbents as part of clothing); swipe samples.	Requires HUMINT, SIGINT. Susceptible to many false alarms. Not always easy. Difficult to penetrate religious cults .

Chemical Threats

Operation	Activity	Objective	Responsible Organizations	Examples of Technologies or Devices	Needs/Shortcomings/ Comments
	Chemical surveillance of suspect sites.	To monitor emanations from suspect production facilities.	Domestic: FBI Foreign: Intelligence community.	GC-MS Spectrometer with air probe; Grab samples. Remote sensing.	Must intercept plume. Require high vapor sensitivity and specificity. Requires prior knowledge of suspect sites. Dedicated analytical satellites.
Low-level early warning for lower risk targets	Threat and Vulnerability Assessment.	Inspection and preparation of site to mitigate damage and casualties in the event of an attack.	Domestic: government agencies. Federal government for Fed buildings.	Need threat assessment and inspection teams.	Expensive, must have library of spectra of possible threats. Absence of designated POC for threat assessment within the military. Requires cadre of trained inspectors. Must develop criteria for "vulnerability".
	Alarms in buildings and other potential vulnerable locations.	To install permanent sensors to: 1. Monitor chemical agents in a/c systems and entry ways. 2. Perimeter monitoring. 3. Inside large civilian bldgs.	Civilian: government agencies. Military: Corps of Engineers. Chemical Corps units, TEU, EOD.	Cheap, multi-agent, very low false alarm rate (obviously scenario dependent) point alarms. M8 alarms, CAMS ACADA Small devices on chips.	Device must be inexpensive, reliable and have relatively low false alarm rates, and respond to multi-agents. Existing military alarms have high false alarm rates, and are designed for detecting high concentration levels of standard threat agents. They are designed for battlefield environments.
	Alarms at ports of entry	Detect chemical agents and precursors crossing international borders.	Customs	1. Activation analysis for sulfur and phosphorus. 2. For volatile compounds, portable air sniffer. 3. Tools for base security.	Not very likely. Difficult unless prior intell. Precursors can be readily obtained in country. Alarms only effective if material is leaking
	Water and food monitoring	Detect the contamination of food and water by chemical agents.	Local government agencies, Dept. of Agriculture	Trace chemical analyzers. Water test kits.	Requires extensive inspection unless prior intelligence is obtained. . People and $ intensive.

Chemical Threats

Operation	Activity	Objective	Responsible Organizations	Examples of Technologies or Devices	Needs/Shortcomings/ Comments
Warning for high value high risk targets. e.g. G7, Olympics, etc.	Alarms in conference sites and other targets of opportunity.	To install real time alarms in high risk sites such as sports arenas, airports, personnel, etc.	Civilian: Local government aided by DoD. Military: DoD	1. Minicams 2. Perimeter alarms 3. Personnel alarms	Must be real time and detect medium concentration levels of agents; cost is less of a concern. The threat agents must be selected beforehand. Existing alarms are designed for known threat agents.
	1. Preparation in case of attack; 2. Escorts	Protection of: 1. Forces 2. Embassies	DoD	GS MS with air samplers	1. Expensive, must have library of spectra of possible threats. 2. Absence of designated POC for threat assessment within the military.
	Predeployment of on-site mobile lab.	To prepare for the analysis of CB agents in case of a threat.		Analytical Equipment CWC Treaty Lab already used in Olympics	Useful in large high risk events such as Olympics, etc. Helpful in crisis and consequence management.
Warning for US forces, host nation and contractor personnel	Provide warning of covert attacks on personnel providing logistic support to US forces.	Detect attacks in order to treat exposed personnel in a timely manner and, if possible, allow personnel to don protective gear.	DoD DoS Country of origin Prime Contractors	Point or standoff biosensor	High sensitivity required against small attacks, very low false alarm rate. Must collect samples. for further analysis - chain of custody Inexpensive "adequate" masks Large areas to be covered. Procedures must be adopted that do not cause panic, flight of personnel. Requires access to off-post sites. This could be difficult in host countries. No CONOPS.
Protect personnel	Provide passive defensive garments	Protect against chemical agent.		Masks and IPE equipment. Civilian masks and IPE equipment	Especially for non-military personnel, masks must be readily available. for rapid donning.

Chemical Threats

Operation	Activity	Objective	Responsible Organizations	Examples of Technologies or Devices	Needs/Shortcomings/ Comments
Interception	To capture a device before its activation	To capture munitions and terrorists prior to release of the agent.	Domestic: Local Law enforcement agencies. FBI Foreign: TEU	1. Foams, decontamination 2. Neutron activation and radiography 3. Standard EOD equipment. 4. Decon enzymes (OPAA/OPH)	Current foams may not contain decontaminants for chemical agents.
	Neutralization of the agent	To neutralize the chemical agent	TEU Local Agencies EOD	Water/foam Base neutralization Oxidation/hydrolysis	Standards required
Immediate consequence management	Identify exposed personnel Contain these casualties from contaminating others. Triage	Begin early treatment before symptoms appear. Prevent further contamination of treatment sites and dispersal of casualties. To separate casualties into those requiring immediate help and those that are noncritical..	Local government agencies. CBIRF PHS TEU Medical personnel Local government agencies	Scanning point detectors such as CAMS FLIR Standard civilian and military procedures and medical equipment	Simple detectors that could be programmed to detect any threat or non conventional agent. Must be readily available. Problem: civilians leaving hot zone.
	Decontamination	Achieve "adequate" clean-up. Risk management.	Local government agencies TEU CBIRF	Decontamination equipment including hot water and steam pressure hoses.	What is "adequate" decontamination? When is a site or surface properly decontaminated?
Later consequence management	1. Decontamination 2. Certification and Assessment tools	Triage of equipment	Equipment Operators		1. Large area and sensitive equipment decontamination. 2. Triage of equipment for decon 3. Standards for decon level for "chronic exposure not established."

Chemical Threats

Operation	Activity	Objective	Responsible Organizations	Examples of Technologies or Devices	Needs/Shortcomings/ Comments
Crisis Management	Organize and supervise all responders	Require good communication for responders in protective gear	Local responders, FBI, Military	Voice activated transmitters and receivers	
Retribution	Protect evidence	To apprehend and convict perpetrators.	Domestic: Local police, FBI Foreign: CID, Host nation.		Political Guidance

2. APPLICABILITY OF EXISTING CAPABILITIES AND THOSE UNDER DEVELOPMENT

This section discusses the applicability of current DoD chemical and biological defense capabilities to the transnational threat challenge and the potential of programmed new capabilities and ongoing technology efforts to fill some of the shortcomings and gaps. Applicability to biological or chemical threats is indicated by C or B in parentheses; applicability to Force Protection or Civil Protection is indicated by FP or Civ in parentheses.

Detection/Identification Existing or Under-Development Capabilities

- Early Warning:
  - Perimeter Defense:
    - Remote sensors, active and passive
    - Systems of point detectors
- Biological Integrated System (IBIDS)

Early Warning:

Remote sensors, active and passive. (CB) (FP)

The DoD as well as the civilian sector have developed a broad spectrum of laser and spectroscopic passive devices to detect emissions and aerosols. These devices could be useful to provide perimeter early warning alarms against chemical and biological attacks. Though some attempts are being made to provide remote sensing of biological attacks, the concentrations of microorganisms required to cause casualties are very low relative to background particles, and the spectroscopic signatures are not sufficiently unique to provide confidence that this technique will be satisfactory.

Systems of point detectors. (CB) (FP)

The DoD as well as the civilian sector have developed a broad spectrum of detectors for both chemical and biological threats. A cross section of these have been included in the tables. Those that are under development are given below.

A grid of point sensors for biological and chemical attacks is being developed under the Port/Airfield and Joint Biological Remote Early Warning System (JBREWS) ACTDs. Such systems could be used to form a perimeter defense to detect a terrorist attack as well as any other biological or chemical attack providing the source is outside the grid.

Networks are more important for biological than for chemical detection in order to make up for shortcomings in BW detector sensitivity and specificity.

Detection/Identification
Existing or Under Development DoD Capabilities
Early warning for Lower Risk, Facilities

- Sensors
  - Ion Mobility sensors
  - Small particulate counters with fluorescence detection

A number of small simple, inexpensive detectors being developed for other applications are applicable to this task. Some examples are given below. They are relatively cheap and could be installed in a number of low risk facilities, but --like smoke alarms--are susceptible to false alarms.

Ion Mobility sensors (CW) (FP & Civ)
DoD has developed and fielded a family of alarms based on ion mobility detection that could detect attacks on facilities. Though the present devices are battlefield hardened, the cost could be reduced by simplifying the devices. Such alarms could be installed in the intakes to ventilation and A/C systems and other points of entry into buildings. Such an approach might be suitable for federal buildings, post offices, etc. Background data is required to determined what the false alarm rates would be. Doctrine would need to be developed to define appropriate responses to alarms.

Particulate Counters With Fluorescence Detection (BW) (FP & Civ)
The Army has developed some small particulate counters (Tier I) and is improving this device by adding a fluorescence detector (Tier II) which can reduce false alarms by seeking fluorescence in the proper frequency region for triptophane in some amino acids. Again such devices could be installed in ventilation system intakes and at port of entries into buildings. However, there is minimal specificity. The Army is also developing the JBREWS detection system, which may provide a low cost sensor with better specificity. Background data in possible target areas should be obtained to determine if such an approach is viable or would lead to excessive false alarms.

Detection/Identification
Existing or under development Capabilities
Early Warning for high value high risk facilities.

- Sensors
  - Small gas chromatographs
  - Small particulate fluorescence detectors
  - Biological Integrated Detection System (BIDS)

For more important and valuable targets that are at risk, more expensive approaches are attractive and feasible. These might only be installed for limited duration, for example, to protect a special event or respond to intelligence information. The types of devices to be considered include:

Small gas chromatographs (CW) (FP & Civ)
Larger investments in detection techniques are feasible for very high risk targets. Thus devices such as small chromatographs, and "gc-ms" might be practical and affordable given a high probability of a threat. The Army for protection and surveillance of its chemical munitions depots and chemical munitions destruction facilities has developed a set of alarms and procedures that can detect the presence of standard chemical agents at very low concentration levels with high confidence levels.

Small particulate fluorescence detectors (BW) (FP & Civ)
Small particulate detectors with some fluorescence detection such as the Tier I and Tier II detectors described above can be wedded to small rapid PCR devices being developed. The Army is developing the Port/Airfield sensor—an automated sensor that can identify agents from a pre-specified set. Current PCR devices require hours to complete analyses. Current devices now under development can test within minutes. However, there are still numerous technical barriers to address, such as level of sensitivity and specificity. The utility of this sensor for high-value facilities should be investigated. However, you have to know in advance what you are looking for, and have all the reagents available.

Biological Integrated Detection System (BW) (FP & Civ)
The BIDS system was developed for battlefield applications. The system is a "lab on wheels." It monitors and collects atmospheric particulates. If the air has a large number of particulates in the 1-10 μ region, it tests the samples for pathogenic microorganism. The units are available and have been used for high risk targets such as the Olympics.

Detectors and Alarms

- Low-cost autonomous alarms for building HVAC systems
- Biological Detectors
  - Bio-chips
  - Mass spectrometers for biological organisms

Low cost autonomous alarms for building HVAC systems (BW) (FP & Civ)
For early warning in federal buildings, foreign housing facilities, and other low value, low risk targets, low cost, permanently installable detectors with reasonably low false alarm rates are needed. No such devices exist at this time. For high value targets, more expensive systems under development should be investigated.

Biological Detectors (BW) (FP & Civ)
Biological agent release, unless advertised by the perpetrators, may not be detected until symptoms appear, which can be several days or more after the attack. It may not even be obvious if the attack was a biological attack or a naturally occurring epidemic. Under these circumstances, it will be difficult to identify the location of the attack or mitigate the casualties. Any chances of capturing the perpetrators will be greatly reduced.

There are no proven simple, automated, real-time biological detectors available at this time, although there are several under development. Those under development will require frequent routine maintenance including restocking of reagents.

The crucial need in the biological area is the development of an inexpensive, automated biological detector that is characterized by minimal maintenance, good sensitivity, and can differentiate between active (native) toxins and biologically inactivated toxins. Ideally, such a detector would be sensitive to pathogens without interference from innocuous organisms, although such generic capability is hard to achieve. At a minimum, such a detector should be able to detect and identify the most likely threat agents. Such a detector needs to be linked with a warning and reporting system to ensure prompt response.

At the present time, the only DoD systems capable of detecting biological attack are the BIDS for ground forces, the M-94 long-range Biological Stand-off Detection System, and the IBADS naval system. None of these is suitable for long-term protection of civilian assets. Sensors under development, such as the Port/Airfield sensor, are more automated and could provide protection for a few key assets, but are too expensive and require too much logistic support for wide-scale deployment.

Bio-chips (BW) (FP & Civ)

The ideal would be a biological material somehow coupled to a solid state device that produces an electronic signal that is easily detected and that can produce an alarm. Such devices are now at the forefront of existing technology, but are becoming feasible and could be developed within the next ten years. These are the "smoke alarms" of the bio detector family.

Mass spectrometers for biological analysis (BW) (FP & Civ)

Some effort exists to develop mass spectrometers that detect and identify microorganisms; however, such practical instruments are not yet available. Though such an instrument would not be cheap, it would provide confirmation and specify the type of microorganism used without having to test sequentially for agents.

Protection Existing or Under Development
DoD Capabilities Early Warning for High Value High Risk Facilities.

- Protection of buildings
  - Overpressurization of buildings
  - Filter systems for air intakes

Overpressurization of buildings (CW & BW) (FP & Civ)

A standard technique used in chemical laboratories is to adjust the differential atmospheric pressure between interior and exterior of buildings and portions of buildings to control the direction of air flow within the building. For some high risk facilities such as command posts, headquarters, communication centers, etc. such investments would be warranted. It should be noted that toxic labs are designed to keep toxic materials inside. In our case, the pressure should be adjusted to keep toxic materials out.

Filter systems for air intakes (CW) (FP & Civ)

The Army has developed charcoal filters that can filter air intakes to high priority buildings. It might be possible to impregnate filters with enzymes that selectively bind specific chemical agents. High Efficiency Particulate (HEPA) filters are available for biological materials, and these are used in biological buildings including BL-4 facilities along with pressure controls.

Protection
Existing or Under Development DoD Capabilities
Predeployment of Protective Equipment and Medical Supplies

- Predeployment of 2-PAM and atropine
- Vaccines

Predeployment of 2-PAM and atropine (CW) (FP & Civ)

In the event of a chemical agent incident, a large supply of treatments such as atropine and 2-PAM chloride will be required. However, it is doubtful at this time it there is a sufficient quantity of these treatments if a massive incident occurred. It should also be noted that raw atropine is only available from foreign sources. (Bulgaria for the most part.) Also, delivering them in a timely manner will be a problem unless they are stored throughout the country. Autoinjectors have a limited shelf and must be replaced regularly.

Vaccines (BW) (FP & Civ)

USAMRIID is the only organization in DoD developing vaccines against the common biological microorganisms of military significance. However, due to funding restriction and the high cost, they can only develop a few of these vaccines at any one time. (The Army at Walter Reed also has the responsibility to develop vaccines against endemic diseases of military significance to which our war fighters would be exposed.) The contract costs are high for production, perhaps, but the S&T investments are modest. The whole idea of only doing a few at a time is a matter of prioritizing the work.

A more important bottle neck to consider is that there are limited facilities available to do the GLP testing to obtain FDA approval. Currently, USAMRIID is doing near GLP-quality studies. These validation studies in animal models are critical to the DoD as we develop candidate vaccines for some of the bio threats. Since we can not do efficacy testing in man, we will have to rely on the data from the animal studies- and they must be done well! Obviously, BL3 facilities are needed, but equally important is the ability to create aerosols of the bio threat agents. So, finding a place that can do aerosol generation, has BL3 (or BL4) labs, and can meet the requirements for Good Laboratory Practices is important- and expensive too.

Protection
Existing or Under Development DoD Capabilities
Consequence Management

- Biomasks --Civilian masks
- Quick effective (some standard) decontamination methods
- Rapid diagnostic methods for biological incidents
- Rapid detection methods for BW agents and exposure
- Voice emitters for masked personnel
- Airflow models

Bio-masks — Civilian masks (CW & BW) (FP & Civ)
Simple effective (to some standard) masks for casualties to prevent further contamination and exposure to agents. DoD mask are only designed to fit the warfighter physique. Thus, masks are not available for children. The Israelis have designed a family of masks for the general population.

Quick effective decontamination methods (CW & BW) (FP & Civ)
Quick decontamination methods for both chemical and biological incidences are required, but do not exist. Foams containing enzymes that detoxify catalytically would be a significant advance.

Analytical methods (CW) (FP & Civ)
Analytical methods are needed to determine the type and extent of the threat as rapidly as possible. Symptoms will be the first sign of an attack, The symptoms may not identify the exact threat agent. For example, if a nerve agent is used, the decontamination and casualty handling techniques and procedures for a nonpersistent or a persistent agent are not the same. Little decontamination of a nonpersistent agent is required, but full physical decontamination of VX or TGD would be necessary. A portable mass spectrometer such as those already developed for the ERDEC would be satisfactory for this application except that once used to identify an agent they become contaminated and their disposition is tenuous. The actual solution now being used is sending the ERDEC Treaty Lab to major events in case of a chemical attack.

Rapid diagnostic methods for biological incidents (BW) (FP & Civ)
Rapid detection methods for biological agents are needed to identify the threat (or a hoax) and to decide on the proper treatment for casualties and facilities quickly, while potentially infected personnel are still on the scene. Simple ID tickets with ticket reader specific for only one agent or Fiber-Optic Waveguide (FOWG) devices may be more useful.

Communication devices (BW & CW) (Civ)
The ability of Hazardous Materials (HAZMAT) units to communicate when in protective clothing and masks is nearly impossible at this time. Built-in communication devices for protective masks should be integrated into existing masks.

In the past ERDEC has developed simple voice emitters for masks. These have not been adopted by the military because the power supplies do not last long enough for field operations. However, these devices would have a long enough life for the typical HAZMAT incident or could be rapidly replaced.

Airflow models (BW & CW) (FP & Civ)
Both DoD and DOE have developed airflow models of different complexity to model the transport of biological and chemical agents through the atmosphere. Two types of models are desirable. Simplified models that run on laptop computers and that have minimal data input requirements would be useful to help identify possibly contaminated areas to support responders to biological and chemical incidents. More complex models could assist training of responders to develop intuition regarding the behavior of agent both inside and outside of structures, as well as, to provide remote expert assessment to the first responders.

Decontamination
Existing or Under Development DoD Capabilities
Interception

- Nondestructive analysis
- Decontamination foams

Nondestructive analysis (CW & BW) (FP & Civ)
For chemical treaty verification, the DOE labs have developed various devices such as PINS which will do elemental analysis by bombarding a target with neutrons of selected energies. By detecting the gamma rays and doing an energy analysis of the emitted radiation, the presence of certain elements can be detected through the packaging. (Such devices are now used in airport baggage rooms to screen luggage for explosives. The presence of phosphorus and sulfur would be indicative of a nerve agent or of mustard. (These two elements are also indicative of biological material)

Decontamination foams (CW & BW) (FP & Civ)
Decontamination foams with enzymes for the containment and decontamination of chemical and biological devices are under investigation.

Decontamination
Existing or under development DoD Capabilities
Consequence management

- Wide area decontamination
- Decontamination techniques for sensitive equipment

Wide area decontamination (CW & BW) (FP & Civ)
Wide area decontamination systems for both chemical and biological agents may be necessary for persistent chemical agents and for environmentally resistant biological agents such as anthrax spores.

Decontamination techniques (CW & BW) (FP & Civ)
Equipment and procedures for decontamination inside of buildings are needed to ensure restoration of facilities.

(CW & BW) (FP & Civ) Decontamination techniques for sensitive equipment such as communications and other equipment.
Re-occupation of buildings and the re-use of equipment is a vital requirement.

Decontamination

- Standards for decontamination for both chem and bio

How clean is clean enough?

How clean is clean? There are no existing standards for determining when an item is properly decontaminated. The present DoD standards used in demilitarization are called 3X and 5X. The 3X standard is achieved by bagging an item. If upon monitoring the air in the bag after a predetermined duration, the concentration of vapor agent is below the TWA, then the item is declared to be 3X. The 5X standard requires heating an item to 100°F for 15 minutes. These standards are for the release of equipment to the general public or for transportation between government facilities.

Neither of these is satisfactory for decontaminating civilian facilities and personnel from terrorist attacks. Some better standard must be developed.

Because certification of decontamination is a local responsibility, these standards must be applied throughout the federal and local public health system.

REPORT OF THE COMPETENCY PANEL ON PHYSICAL, LAUNCHED, AND UNCONVENTIONAL MEANS (PLUM)

Panel Chairs
Mr. Milt Finger
MG William Garrison, USA (Ret)

Panel Members
Mr. Jack Bachkosky
Mr. Paul W. Cooper
Dr. Terry Gudaitis
Mr. Jeff Harris
COL Paul Hutton III, USA (Ret)
Mr. Ira Kuhn

Government Advisors
Dr. Al Brandenstein
Dr. R. Stephen Day
Mr. Robert Doheny
Mr. Donald Henry
Dr. Lyle Malotky
Dr. Randy Murch
Mr. Ed Phillips
Mr. Raymond Polcha
Mr. Chuck Sieber
Mr. Rick Strobel
Dr. Pat Vail
Mr. Kevin Wong

INTRODUCTION AND SUMMARY

This report of the Physical, Launched and Unconventional Methods (PLUM) Competency Panel on future "(Un)Conventional Threats" (threats using conventional explosives and weapons with unconventional methods), addresses threats not classified as chemical, biological, nuclear or under the umbrella of information/electronic warfare.

The PLUM panel examined threats from ranging from stationary implanted explosives such as letter bombs, mines, truck-size bombs conventional weapons such as mortars and man portable air defense systems (MANPADS), and a spectrum of other means. It also included attack of infrastructures using incapacitating electromagnetic weapons, carbon fiber conductors, cloggants of engines, and combined effect and directed energy weapons. Of these various threats only stationary explosives have been used against US targets, although surface-to-air missiles have been used against non-US aircraft abroad. It is recognized that a determined foe will seek out the weak points of an "enemy" and exploit those means using attack methods that are the easiest to employ, are likely to give the desired effect, and have low risk.

The PLUM panel, after examining a wide spectrum of alternative threats including kinematic weapons, system incapacitators, combined effect attacks and directed energy weapons, focused it's study on explosives, either in bulk or launched. As stated in volume one of this study, the trend in transitional threat incidents is toward larger incidents designed to cause large numbers of casualties. Conventional explosives are now the most widespread weapon of choice for transnational threat actions and will remain the most likely threat to the US population and interests at home or abroad.

Specific threats included in this panel report are listed below. Other possible threats outside the scope of the PLUM panel are addressed in volumes one and three of the Study. As stated above, the PLUM panel focused its energies on examination of chemical explosives. Kinematic weapons, System Incapacitators, Combined effects attacks, and Directed energy weapons are discussed in the methodology section of this report.

PLUM threats include:

- Stationary or Mobile Explosives (Truck-sized bombs, Mines, Package-sized bombs, Letter bombs)
- Kinematic Weapons (Direct-fire ballistic, Indirect fire ballistic, Guided, Aircraft delivered)
- System Incapacitators (Electromagnetic pulse {EMP}, Carbon conductors, Cloggants/corroders)
- Combined effects (Explosive/incendiaries, Explosive/CBR agents)
- Directed Energy Weapons (Lasers, High Power Microwaves)

THREATS

The US needs a wide range of responses to deny, disrupt, disable, defeat, and interdict transnational threats.

We have assumed that the Transnational Threat goal is to cause a transforming event with attendant societal impact. Single large events such as the World Trade Center, Khobar Towers and Oklahoma City fall into this category. However, there also have been transnational threat group plans revealed that included a campaign of events such as the follow on attacks planned by Ramzi Yousef on New York City infrastructure and commercial air that were interdicted. The goal of a transforming event is aided and abetted by the "CNN effect"; that is, the instant and widespread coverage of an event.

The history of large stationary and vehicle bombs in the US goes back to the turn of the century with the carriage black powder bombings of J. P. Morgan's mansion in New York. Later events involving bombs in excess of 1000 pounds of explosives include those at the University of Wisconsin in the seventies, Harvey's Casino in 1980, the World Trade Center in 1993, the Murrah Building in 1995, the US Embassy and Marine Barracks in Beirut, both in 1983 and Khobar Towers in 1996.

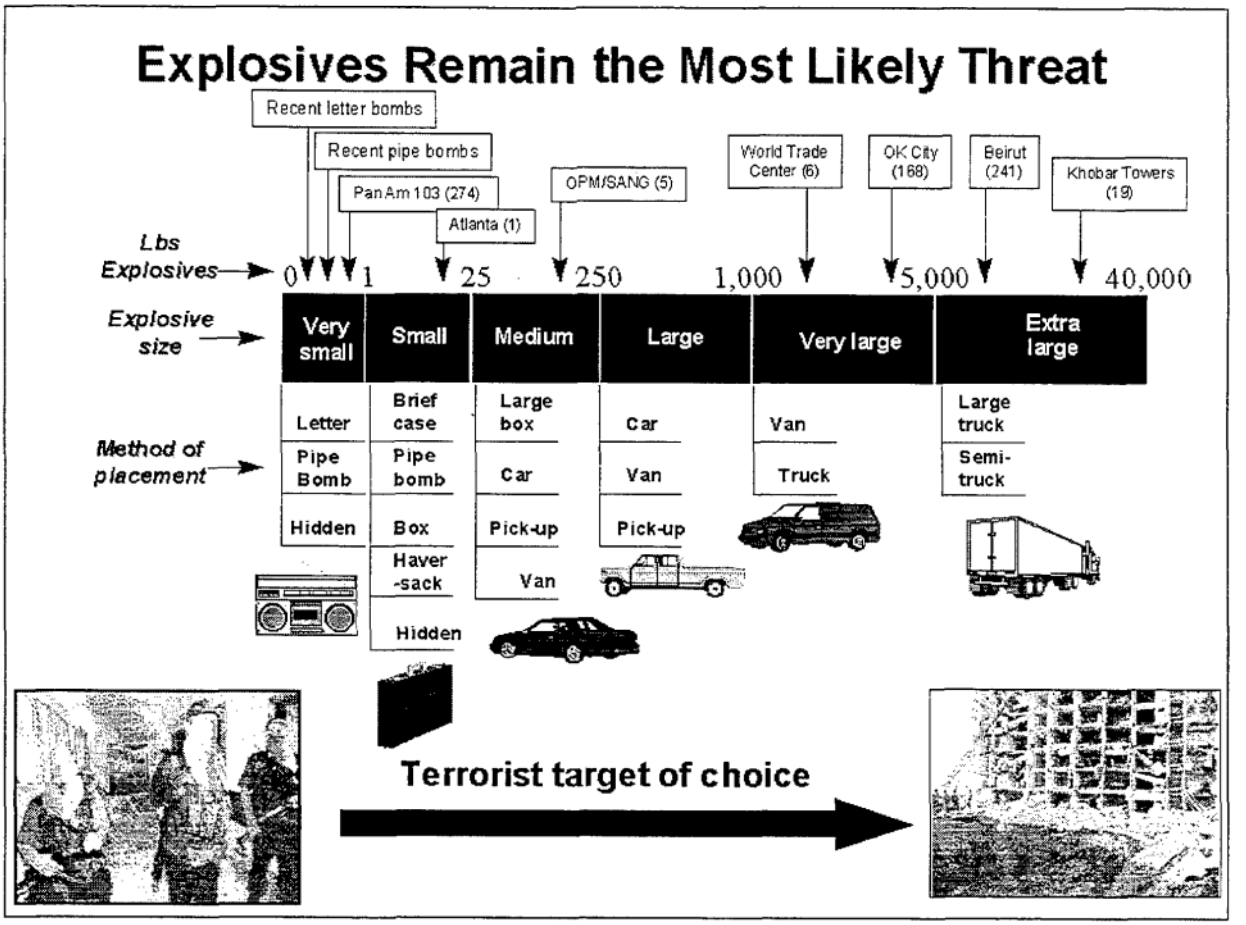
There is obviously a precedent set for multi-event or serial bombing campaigns for transnational threat groups. As transnational threat groups come to realize that size really counts, larger and more devastating effects will become more common. An example of the threats from US based groups is the VANPAK case where four package bombs were sent through the US mail to two judges and two civil rights workers, one killing one of the judges. A truly transnational campaign, the LETBOMB series was conducted late last year by mailing 18 letter bombs to perceived anti-Muslim individuals in the US and eight to others in the US, sent by Islamic fundamentalists. The Beirut incident occurred over a relatively short period, with the US Marine and French barracks bombings happening within hours of each other. Ramsey Yousef, the mastermind behind the World Trade Center bombings, stated that he would have liked to cause 250,000 casualties. Other aborted threats included potential bombings of New York tunnels, bridges, and the United Nations building. Examples of such Multi-Event Campaigns are noted below:

- Executed in or at US facilities
  - 1949-55: New York Mad Bomber
  - 1985-87: Airline Bombs
  - 1979-96: Unibomb Series
  - 1983-84: Beirut (US and Israeli embassies, US and French Barracks)
  - 1993: US World Trade Center (planned follow on attacks on NY infrastructure)
  - 1989: VANPAK Bombs
  - 1996: LETBOMB Series
- Aborted US and Other
  - DATE: Chicago gang members interdicted before using MANPADS to shoot down domestic airliners
  - 1994: New York Infrastructure (tunnels, bridges, UN, and Federal Buildings)

- 1997: 11 separate Airline bombs on Philippine carriers

FINDINGS

Finding 1. Conventional explosives will remain the most likely threat.



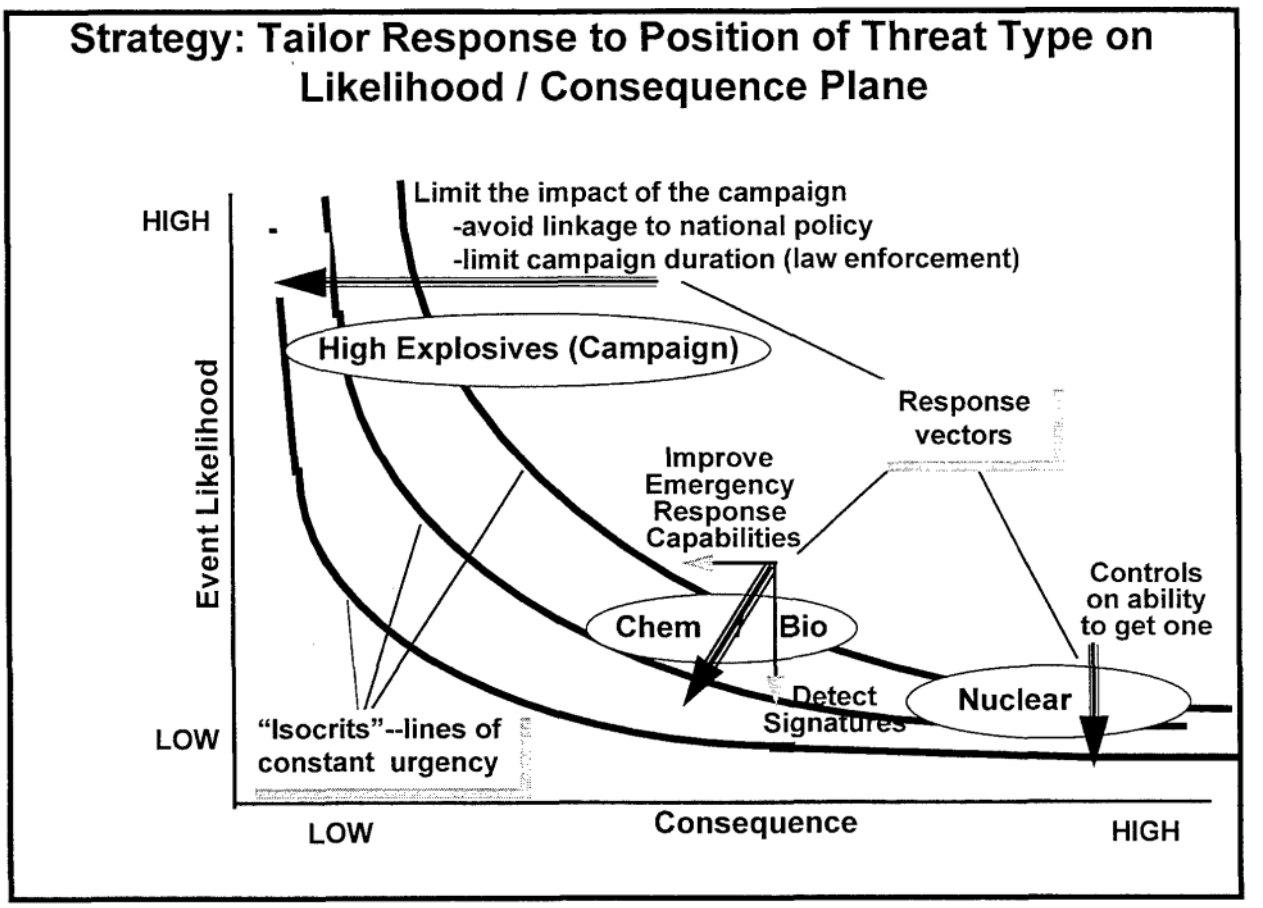
Historical precedent, ease of access, and the flexibility of delivery will keep explosives high on the transnational threat weapons list. Individual firearms and drive-by-shootings are still of concern but are more localized and have less collateral damage, perhaps on the same order as small pipe or satchel bombs. The tendency is toward large truck bombs and potential use of surface-to-air missiles and mortars.

Finding 2. There is a spectrum of defenses and responses

There are many choices listed below that can be made for applying resources of time, personnel, and budget to alleviate the transnational threats. These are described in more detail in Annex A, "Methodology".

- Strategic Prevention
  - intelligence

  - weapon acquisition inhibition
  - border enforcement
- Target Protection
  - warning
  - isolation
  - hardening
  - crowd control
  - kinematic weapon defeat
- Consequence Management
  - reaction training, exercises, and equipment
  - emergency medical capability
  - rapid event characterization
  - secondary effects suppression
  - communications
  - reconstitution resources
- Post Attack Investigation
  - intelligence
  - attack area surveillance
  - damage event forensics
- Other Response Actions:
  - policy and regulation
  - training, exercises, and behavior
  - operations and procedures
  - information access and perception management
  - equipment, systems, and communications
  - technology development



When the consequence of potential terrorist events is plotted against the likelihood of occurrence, it is clear that policy and resources need to be guided by the levels of constant urgency. For example, because the consequences of any nuclear event would be catastrophic and cannot be mitigated, US effort should focus on reducing their likelihood (i.e., intelligence/interdiction). By contrast, because the likelihood of conventional explosive events is so high and cannot be easily lowered, US efforts might focus on reducing the consequences (i.e., force protection).

RECOMMENDATIONS

Managing the problem

The frequency and severity level of transnational threats is likely to escalate. Therefore, we recommend an increased investment of US resources to attempt to ameliorate these threats. Underlying these recommendations are political considerations such as developing procedures that will allow federal agencies to work more closely with the civilian sector to accelerate appropriate technology transfer while safeguarding US security interests.

- Make selected DoD resources available to civilian infrastructure
  - Use Chemical Warfare/Biological Warfare (CW/BW) approach with the National Guard as point of departure

- Near term opportunities
  - Enhanced area surveillance of fixed facilities
  - Implement "Gore Report" on civilian aircraft
  - Establish "red teams" to provide realistic evaluation
- Research and Development (R&D) Program based on assessment studies, likely outcome:
  - Inexpensive but sophisticated surveillance of facilities
  - Fast and accurate explosive device detection
  - Aircraft self-protection
  - Advanced mitigation technologies
- Establish force/civil protection test-bed to support R&D and evaluate operational concepts

Training

Efficiency in training via interactive training tools and the sharing of these tools with local civilian authorities via distance learning will be vitally important. A significant role of the National Guard is of paramount urgency to enable these initiatives.

- Develop interactive training tools to prevent/manage crises and share with local authorities
- Improve crisis management interface with local authorities
- Develop decision theory approach to countermeasure/protection funding
- Develop weighted risk analysis with metrics
- Increase role of National Guard to assist and support First Responders in consequence management

Technology

Several technical capabilities for assisting with civil protection exist in military programs. Further development and/or exploration of these technologies for application by US civil authorities in counter terrorism activities is required while still protecting the aspects that have a high military sensitivity and that help preserve our military superiority. Some of these recommendations are underway, but must be further emphasized.

- Develop technology to safely stop vehicles remotely
- Develop systems to tag / track / locate
  - equipment items
  - individuals

- Develop improved surveillance systems for extensive wide area coverage of critical assets and surrounding environments in both CONUS and OCONUS with automated monitoring "aides"

- Develop multi-technology sensor suites for discriminating control of equipment and personnel flow around identified critical assets
- Support development of less-than-lethal tools / tactics
- Surface-to-Air Missile (SAM) countermeasures
  - Develop an investment strategy for outfitting Civil Reserve Air Fleet (CRAF) with Infrared Counter Measure (IRCM) capability
  - Support R&D to reduce power/weight/cost of missile CM systems
- Support R&D in robotic and covert micro-miniaturized surveillance systems
- Support developments for
  - Improved personnel identification (ID)
  - Remote ID including bomb sensing
  - Render Safe for explosive devices
- Mandate future architectural designs to enhance critical facilities protection from high explosive effects

Policy

There are significant cost implications associated with these recommendations. Various options and priority items need to be determined along with program plans and milestones so that cost/benefit implications can be assessed.

- Support additional investment in intelligence and open source information evaluation and dissemination
- Extend force protection analysis and assessment to other high value potential targets
  - DoD to expand its participation (analysis, training, recovery tools) with civil authorities to improve overall survivability of integrated infrastructure
- Periodic review of "Gore Report" findings and support implementation of recommendations
- Integrate Public Affairs/Media Policy
  - Develop media "management" strategy
- Raise perception of US being prepared for any contingency

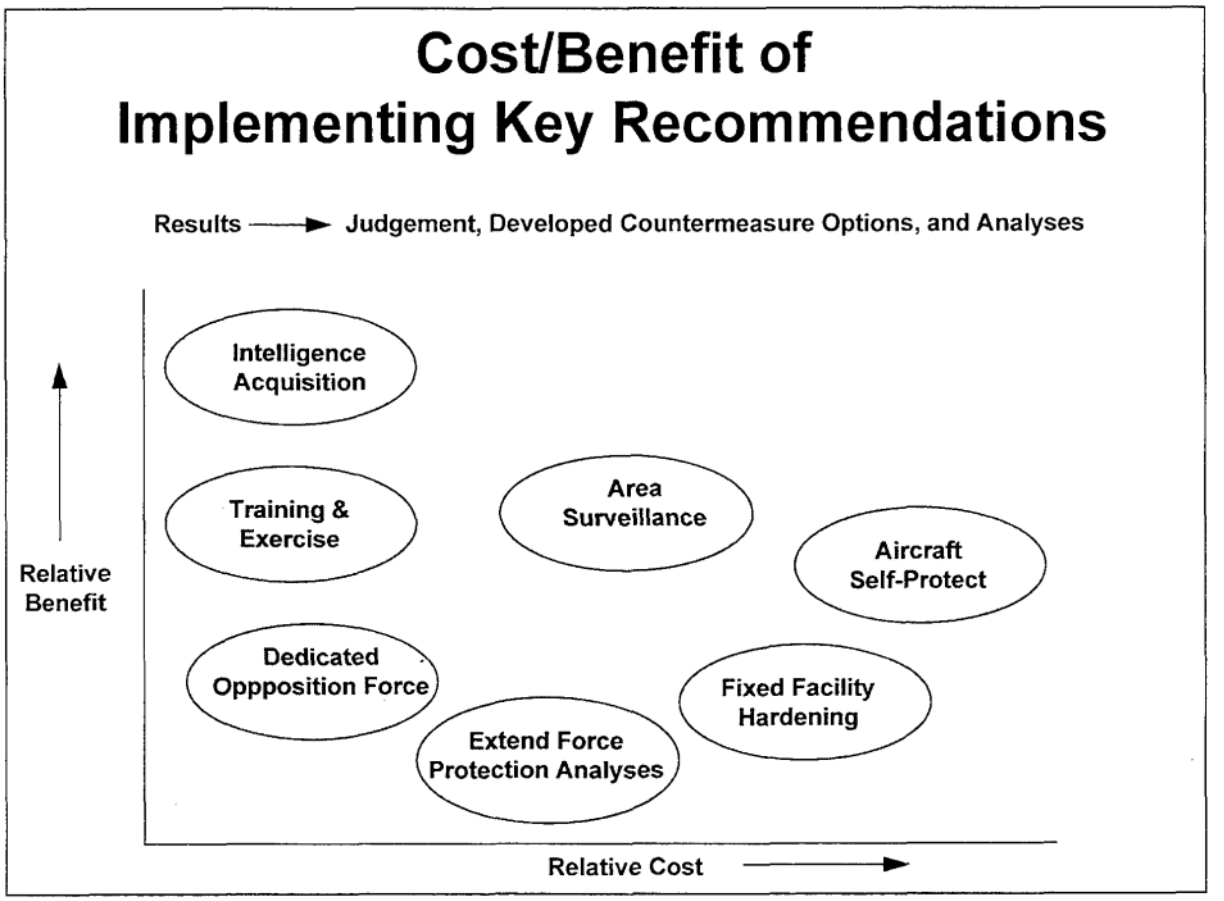
The panel makes these recommendations in light of:

- DoD dependence on civil infrastructure at all-time high and growing
- Civil infrastructure is a good terrorist target in its own right.

- Protection of all high value targets is impracticable.
- Failure analysis of critical infrastructure will yield improved design that is more robust and failure tolerant.

Many of these policy issues will have to be implemented in concert with other government agencies. DoD involvement with other government agencies and civilian authorities should increase the perception of greater US preparedness and therefore reduce the transnational threat incentives for taking hostile actions.

Treating transnational threats as criminal activities requires that policy makers carefully define the limits of which transnational threat events exceed the level of a criminal act and should be considered a national security issue.



Through the development of preventive/protective options, we can be poised to make intelligent investments. Knowing what can be done if needed will allow appropriate allocation of limited resources to high risk, high consequence situations. A selected set of investment options is depicted in terms of their benefit versus cost.

We have an immediate threat — still growing — of transnational threat group use of explosives. We need to ramp up rapidly to meet it, and then be able to maintain reasonable defenses with modest new investment. The relative need for US investments and focus to defend against explosive threats requires the highest levels of current/near term investment.

A time phased balanced approach will husband our limited resources while providing significant prevention/protection against the spectrum of transnational threats.

ANNEX A:

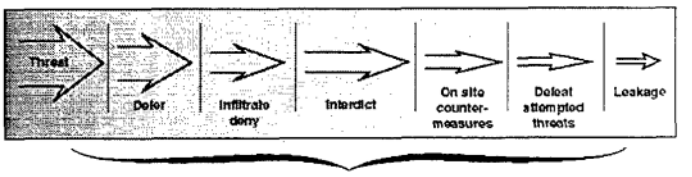
Methodology

The methodology used to determine the spectrum of possible threats and responses is outlined below:

- Identification of all possible threats
- Consider time span of +5 years and +25 years
- Rank ordering in respect to
  - History
  - Likelihood of future occurrence
  - Likelihood of knowledge prior to event
  - Likelihood of mitigation/interdiction
  - Motivation (recognition, influence, decisions, money, spiritual)
  - Opportunity
- Policy issues
- Assessing role of DoD
- Science and technology needs
- Societal issues
- Considering some case studies/scenarios (~5)

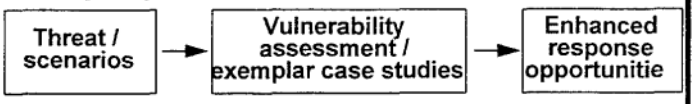
Assessment methodology

Mitigating the threat will continue to require a multi-tiered architecture (‰system of systems‰)

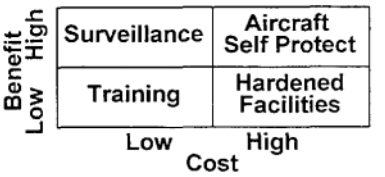


- Balancing opportunities (cost / benefit / consequences)
- Constrained by socio-political issues (risk / intrusion)
- Countering military capitalism

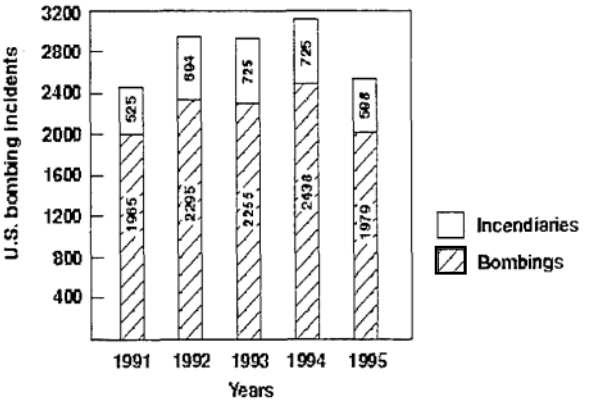
- **Assessment process**



- **Cost / benefit**



Historical examples



Fatalites	27	26	49	31	193
Injured	46	349	1323	308	744

As a background to establishing our methodology we reviewed historical bombings in the US as depicted above. While the number of bombings is nominally at a level plateau, we believe the severity and lethal effects of the bombings have significantly risen.

Scope of PLUM Analysis

Threats	Targets	Defenses	Responses
Stationary or Mobile Explosives • truck-sized • mines • package-sized • letter-sized Kinematic Weapons • direct-fire ballistic • indirect-fire ballistic • guided • aircraft delivered System Incapacitators • EMP • carbon conductors • cloggants Combined Effects • explosive/incendiaries • explosive/CBR agents Directed Energy Weapons • lasers • microwave	Structures and Facilities • large • hazardous • terminal / ports • choke points Utilities • communications • power sources & distribution • gas pipelines • water supplies Vehicles • ground • sea • air Humans • groups • individuals • vehicle drivers/pilots	Strategic Prevention • intelligence • weapon acquisition inhibition • border enforcement • OPSEC • Internet abuse • restrict critical data Target Protection • warning • isolation • hardening • crowd control • kinematic weapon defeat Consequence Management • reaction training, exercises, and equipment • emergency medical capability • rapid event characterization • secondary effects suppression • communications • reconstitution resources Post Attack Investigation • intelligence • attack area surveillance damage event forensics	Policy and Regulation Training, Exercises, and Behavior Operations and Procedures Information Access and Perception Management Equipment, Systems, and Comms. Technology Development

To define the scope of transnational terrorist threats using physical, launched and unconventional means (PLUM) and to differentiate these threats from those being covered by other DSB "competency panels," the table above lays out five categories of threat:

- stationary or ground mobile explosives of various sizes
- kinematic weapons, both precision and non-precision
- target-specific incapacitators
- combined effects weapons designed to amplify damage or lethality or to frustrate rescue and consequence management
- directed energy weapons

Because the threats are generally tailored to the type of target and because the appropriate defense must account for both the threat character and the target type/setting, four representative target categories are listed above:

- structures and facilities (large, hazardous, terminal/ports, choke points)
- utilities (communications, power, gas, water)

- vehicles (land, sea, air)
- humans (groups, individuals, vehicle controllers)

A threat type vs. target type matrix is shown as an applicability check below.

Threats vs. Targets

TARGETS / THREATS	Structures & Facilities			Utilities			Vehicles				Humans	
	Large or Haz-ardous	Ports or Choke Points	Com-munica tions	Power Sources & Distri-bution	Gas Pipe-lines	Water Sup-plies	Ground	Sea	Air	Groups	Indi-viduals	Vehicle Drivers / Pilots
Stationary or Mobile Explosives												
Truck-Sized	X	X				X						
Mines		X					X	X				
Package-Sized			X	X	X				X	X		
Letter-Sized											X	
Kinematic Weapons												
Direct-Fire Ballistic	X	X	X	X			X				X	X
Indirect-Fire Ballistic	X	X										
Guided	X	X	X	X					X			
Aircraft Delivered	X	X	X	X								
System Incapacitators												
EMP			X	X								
Carbon Conductors			X	X								
Cloggants			X	X		X						
Combined Effects												
Explosive/Incendiaries	X	X										
Explosive/CBR Agents	X	X										
Directed Energy Weapons												
Lasers												X
Microwave			X									

The "Scope" figure above also lists four general categories of "defense measures" which would logically be mounted against the terrorists and their weapons. These measures are time-sequenced in terms of their application:

- strategic prevention
- local area target protection
- post-attack consequence management
- post-attack investigation.

The list on the next page elaborates this "defense measures" list to identify a wide range of potential coping strategies. Note that several options among these measures serve to combat threats addressed by other "competency panels," and in that sense, some of these defense techniques posses a generalized across-the-board value.

Elements of Defense

Strategic Prevention

- Intelligence
  - HUMINT
  - SIGINT
  - MASINT
- Weapon acquisition inhibition
  - precursor regulation
  - trade barriers
  - economic sanctions
  - non-proliferation treaties
  - non-use treaties
  - anti-harboring actions
  - ingrained tagging
  - controllable/inhibitable functionality
- Border enforcement

Target Protection

- Warning
  - area and perimeter surveillance
  - perpetrator tracking
  - activity tracking
  - activity pattern recognition
  - weapon/agent signature detection
  - alarms
- Isolation
  - access control
  - standoff
  - environmental decoupling and/or filtering
  - safe zones
  - behavioral training
- Hardening
  - structural materials and design
  - strap-on armor
  - utility redundancy and backup
  - secondary effect suppression
- Crowd control
  - hold back
  - dispersal
  - incapacitation
  - capture
- Kinematic weapon defeat
  - detection/track/source localization
  - guidance defeat
  - warhead nullification
  - trajectory disruption

Consequence Management

- Reaction training, exercising and equipment
  - remote national teams
  - official local responders
  - target population
- Emergency medical capability
  - on-site
  - mobile
  - community
- Rapid event characterization
  - damage agent identification
  - lethality and geographic extent measurement
- Secondary effects suppression
  - booby trap or sequential event detection/localization/diagnosis
  - explosive disposal
  - explosive device containment
  - reaction personnel protection
  - unmanned vehicles
  - decontamination
- Communications
  - secure emergency network
  - media relations
- Reconstitution resources

Post Attack Investigation

- Intelligence
  - follow-up SIGINT
  - follow-up HUMINT
- Attack area surveillance
  - archiving pre-event activity
  - data compression
- Damage event forensics
  - testing for residues and taggents
  - event reconstruction and analysis

The "competency panel" recommended response actions, as seen in the right-most column of the "Scope" figure, are means of mechanizing the coping strategies and fall into five categories:

- policy and regulation
- training, exercise, and behavior
- operations and procedures
- information access and perception management
- equipment, systems, and communications
- technology development

Naturally, DOD can contribute to only parts of the solution set.

The threat evaluation matrix shown on the next page serves to prune down the threats to be addressed. Following are descriptions of what is meant by column and row headings.

We have identified 12 factors along one axis of the Threat Evaluation Matrix. These describe the characteristics of the specific threats arrayed across the other axis. These factors can be grouped in terms of DoD responses by associating the factors with one of 3 overall objectives, namely to:

- Reduce the probability of an event:
  1. Historical record/likelihood. This factor is somewhat ambiguous. The historical record is unique in that it can't be influenced by anything we do. It is useful as the baseline from which we infer the likelihood that is something we can influence.
  2. Motivation of groups (intent)
  3. Sophistication of technology/capability/availability. This is the factor we get at with controls on commerce, either by export/import controls, or by domestic regulation.
  4. Likelihood of prior knowledge. Speaks directly to the intelligence function, like other criminal activity.
  5. Likelihood of interdiction. Closely related to #4, a combination of intelligence and the capability to act on it.
  6. Opportunity. This is what we address with concerns for physical security, or in the current special case force protection.

Within the traditional law-enforcement framework of means/motive/opportunity: #3 speaks to means, #2 to motive, and #4, 5, and 6 to opportunity. Prevention can address any or all of these factors.

- Deal with the tactical effect of an event, i.e., the extent of casualties and property damage:

    7. Likelihood of mitigation/response. Depending on the threat, this could be an issue of equipping.

    8. Training issues.

This is principally the concern of local civilian authorities, both law-enforcement and emergency response agencies. The DoD role is one of technical and logistic support.

- Deal with the strategic effect, i.e., the impact on US national security interests:

    9. Likelihood of attribution/retribution (seen as deterrence, has potential relationship to #2 Motive, above)

    10. Impact. Count of bodies or property damage not relevant until it reaches a threshold that changes something. Oklahoma City was still likely below the line.

    11. Policy issues (retaliation position, disproportionate response)

    12. Public awareness

DoD interests as a principal player and our focus in the study should be here in the strategic considerations.

Threat Evaluation Matrix

Threat Type / Factors	What "Red" means (1)	Explosives/Incendiaries			Sequen-tial Devices	Unusual CBR (2)	Com-bined effect(3)	Laser Dazzle or Blind
		Bulk	Small IEDs	Standoff Deliver				
1. Historical record/likelihood	Likely	**Red**	**Red**	**Yellow/ Red**	**Red**	**Yellow**	**Yellow**	**Yellow**
2. Motivation of groups (intent) (4)	Consistent	**Red**	**Red**	**Yellow**	**Red**	**Yellow**	**Yellow**	**Yellow**
3. Sophistication of technology / capability / availability	Unsophis-ticated	**Red**	**Red**	**Red**	**Red**	**Red**	**Red**	**Red**
4. Likelihood of prior knowledge	Not likely	**Red**	**Red**	**Red**	**Red**	**Red**	**Red**	**Red**
5. Likelihood of interdiction	Not likely	**Red**	**Yellow**	**Yellow**	**Red**	**Red**	**Red**	**Red**
6. Likelihood of mitigation / response	Not likely	**Yellow**	**Yellow**	**Yellow**	**Red**	**Red**	**Red**	**Red**
7. Likelihood of attribution / retribution	Not likely	**Yellow**	**Yellow**	**Yellow**	**Yellow**	**Yellow**	**Yellow**	**Red**
8. Opportunity	high	**Yellow**	**Red**	**Red**	**Yellow**	**Red**	**Yellow**	**Yellow**
9. Impact (5)	Strategic	**Red**	**Green**	**Yellow**	**Red**	**Red**	**Red**	**Green**
10. Policy Issues (retaliation position, disproportionate response)	Not resolved	**Red**	**Red**	**Red**	**Red**	**Red**	**Red**	**Red**
11. Training issues	Stressing	**Red**	**Red**	**Red**	**Red**	**Red**	**Red**	**Red**
12. Public awareness	Very aware	**Red**	**Green**	**Red**	**Yellow**	**Yellow**	**Green**	**Green**

Notes: (1) In general "Red" is bad for DoD, "Green" is good, and "Yellow" is in between.
(2) Includes use of industrial chemicals, attack crops, etc.
(3) Add gasoline to fire/explosion, attack pipeline, tanker, ammo magazine, fuel farm
(4) Motivation: elevate status of group & recognition, influence decision makers, economic, ideological
(5) Includes political/socio-economic & diplomatic impact, the CNN effect, and the "Pearl Harbor" threshold

IEDs - Improvised Explosive Devices (IEDs) including mines, letter bombs, etc.
CBR - Chemical, biological, Radiological

REPORT OF THE COMPETENCY PANEL ON INFORMATION WARFARE / ELECTRONIC WARFARE

Panel Chairs
Mr. John Stenbit
Mr. Larry Wright

Panel Members
Mr. Duane Andrews
Mr. Jeffrey Cooper
Dr. Curtis Davis
Dr. Michael Frankel
Mr. John Grimes
Mr. William Howard, Jr.
Mr. Bruce M. Lawlor
Dr. Robert Mueller
Dr. Prasanna Mulgaonkar
Mr. Dennis Murray
Mr. Robert Nesbit
Mr. Mark Silverman
Mr. Robert Stein
VADM Jerry Tuttle, USN (Ret)
Mr. Sam Varnado
Dr. Abe Wagner

Government Advisors
Ms. Mary Dunham
Col(s) John Collier, USAF
COL Brian Fredericks, USA
Mr. Tom Handel
BrigGen Dave Nagy, USAF
Mr. Marion Oliver
LtCol Jim Rodgers, USAF
Mr. Howard Sequine

INFORMATION WARFARE (IW) THREAT ASSESSMENT

Without exception, investigations into the security of DoD networks by the individual Services and DISA have concluded that our networks are vulnerable to unauthorized access. Tools and techniques for penetrating networks illicitly are rapidly becoming more sophisticated and varied, the associated software is easily available on the internet, with instructions for its use, and there is a community eager to share and exploit these tools.

Many of the currently available network protections are aimed at improving perimeter defenses, keeping the outsider out (this includes firewalls and improved user authentication techniques). Such defenses will take care of a large number of penetrations, particularly nuisance penetrations by casual hackers. However, perimeter defenses are not enough. Even with perfect perimeter barriers, a serious threat remains from the "insider," someone who formerly or currently has rightful access to network systems, but has been recruited, planted, or duped by a group with malicious intent. Such a person could perform a destructive act directly, or create a pathway enabling outside entry. The insider can compromise classified systems which otherwise would be considered very secure.

In many cases the techniques for unauthorized entry are well known and though simple measures (typically involving perimeter defenses) are also known to defeat them, these measures have not been implemented. If implemented, the currently available protective measures will make efforts to penetrate DoD networks more difficult. The commercial networks may then offer the "path of least resistance" and also provide an attractive target in that money, goods, and services are available for theft. (The presence of these monetary assets is another motivating factor thta leads to the development of sophisticated hacking tools.) The vulnerability of commercial systems is important since the DoD relies heavily on their services (e.g. utilities, communications). A means for improving the protection of commercial services that support DoD functions must be pursued.

The intended effects of an IW attack by a Transnational probably will not be subtle. The surreptitious compromise of computer networks requires a long-term dedicated effort of the sort most likely to be mounted by nation states or organized crime. Nation states whose motivation is intelligence gathering have the resources, patience, and finesse required. In the near term, Transnational organizations could buy information from these sources but would not have an interactive capability. In the longer term, however, it is expected that the motivated Transnational will develop a more sophisticated IW capability.

In the near term, the impact on networks that the Transnational Threat will be able to achieve will be disruptive (typically denial of service) but will be temporary in nature. Most DoD computer networks generally possess a redundancy and resiliency that reduces the likelihood of long term interruption of service. Examples of possible disruption are the corruption of data through a time-delayed virus, disruption of commercial electrical power via control system (SCADA) dial-up access, or the disabling of 911 or other telephone services to impede and confuse the response to emergencies. The Transnational is attracted to the IW approach because it can implement these measures remotely, with no physical presence at the scene of the disruption.

Though the effect of a single attack is assessed to be temporary, a carefully orchestrated IW campaign can deliver sequential shocks to a system (or to multiple systems at once) extending the impact of the attack, and creating cascading effects.

Because the potential impact of Transnational IW attacks by themselves is considered to be temporary in nature, the central thrust of a significant attack will probably entail high explosives, chemical, biological, or nuclear weapons. The IW dimension, if used, acts as an adjunct to impede emergency services and increase panic. The IW component can serve to amplify the psychological impact of other actions taken.

CURRENT NETWORK SECURITY POSTURE

The current network security posture is largely inadequate despite the fact that DoD unclassified networks have been compromised on a number of occasions. The known intrusions to date have been considered an annoyance or embarrassment rather than a threat, perceived as coming from amateur hackers. The transition has not been made to a consideration of those with more malign intent, or from concern about an isolated incident to concern about a campaign of attacks with a directed purpose. Consequently, network security has not been treated as a readiness issue, even though the reliance on networks for communication and logistics has become pervasive. Contributing to the lax posture is the popular feeling that network hacking is a prank rather than a serious crime, and that there is no apparent accountability. This is further exacerbated by the DoD's general inability to identify and take action against perpetrators, due to a lack of preparation, tools, and a perception that there are legal restrictions against taking action against the perpetrators.

There is no consistent reporting of incidents — malicious, accidental, or otherwise. Hence the fact that the intelligence and defense communities have not detected an information warfare "campaign" — as opposed to discrete probes — is cold comfort. We can only respond to the attacks we know about. Moreover, knowing that one is under a campaign-level attack requires, in addition to the data capturing events and the methods for categorizing them, analytical tools for distinguishing patterns in space and time among thousands of trillions of network events. At present there is, in short, no way for the DoD to measure the health of its own network, or even know its true topology!

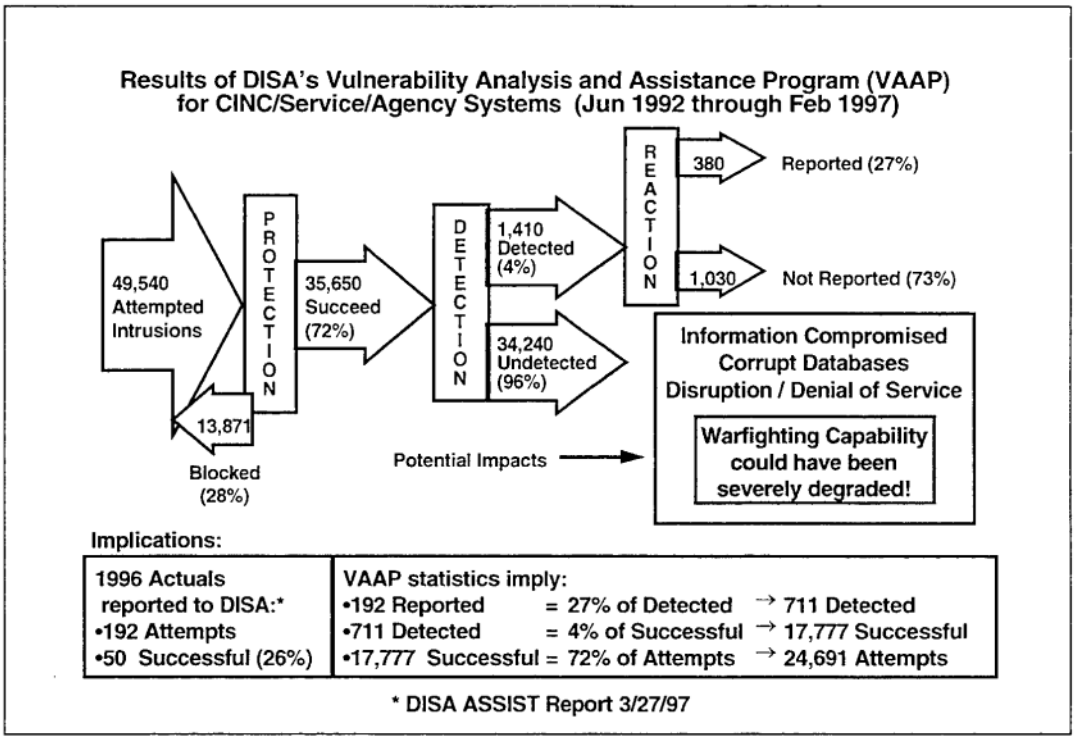
A basic need is to be able to recognize directed network attacks when they occur. This requires a process that is fueled by a flow of incident reports which are collected and analyzed for their specific character and for longer term trends of activity. The routine detection and recognition of network penetrations is not generally possible because there is no "culture of incident reporting" of anomalous incidents (and no clear definitions of what should be reported). There is no organized common repository for collection nor analysis of incident reports within the DoD. Despite an increasingly critical reliance by the DoD on commercial services, there is no process for receiving information on threat incidents from the commercial organizations.

The DoD is in a position to make progress towards bringing network security and IW readiness to a uniformly high level. Though there are many examples of poor readiness and awareness, there are pockets of expertise in IW in the DoD community, particularly in the Offensive Information Operations area. Because of the diffuse nature of possible threats it is important to process information from a broad range of sources both inside and outside the DoD. The DoD already has existing avenues for obtaining relevant information from and collaborating with sources outside the DoD. Within the capabilities and organizations that already exist, the DoD has the means to begin to assemble a viable IW response capability.

The Quadrennial Defense Review reports that "current capabilities are adequate to defend against existing information operations threats; but more robust capability is needed as we approach the 21st century."

This assessment seems to be at odds with results reported through the Defense Information System Agency's (DISA's) Vulnerability Analysis and Assessment Program (VAAP). In that program, DISA tests the security of information systems throughout the Services, Commands and Agencies. The organization being tested knows DISA is trying to penetrate their systems.

DISA only uses techniques which are openly available and which have been previously called to the organization's attention, and for which they have been given advice on how to close the vulnerability.



In 5 years of testing, DISA has attempted 49,540 intrusions. Of those attempts 35,650 got through the protection and 34,240 or 96% of those are never detected. These could potentially have severe impact on the target information system. Four percent of the successful penetrations are detected. Of those detected, 27% are reported as required.

Not counting DISA's VAAP testing, several hundred actual intrusions of DoD systems are reported to DISA each year. In 1996, 192 attempts were reported. Since such a small percentage of actual penetrations are reported, there were likely many more attempted intrusions than 192. In fact, if one uses the experience from the VAAP testing as a guide, the 192 reported intrusions would translate to 24,691 attempts of which 17,777 were successful and 17,066 went undetected. Even if these estimates are off by an order of magnitude (which is quite unlikely), the results imply that current capabilities are far from adequate against existing threats.

POLICY GOALS

While Transnational Threats present no new specific threats to DoD information systems, DoD must address and solve the already existing IW vulnerabilities that could interfere with its other functions and responses concerned with Transnational Threats. Moreover, widespread global information systems also present significant new opportunities that could assist the U.S. Government in dealing effectively with these new problems. All DoD operations — both essential combat and important business applications — now rest on a foundation of critical

information resources and processes. Indeed, Joint Strategic Vision 2010, the current military strategy underlying U.S. doctrine and operational concepts, demands Information Dominance as a core capability. However, this critical information infrastructure is no longer limited only to DoD controlled networks and resources (e.g., the Defense Information Infrastructure (DII)); but DoD is increasingly reliant on the unclassified commercial national information infrastructure (NII) and the entire global information infrastructure (GII) for much of its crucial capability, including transmitting and distributing key classified data. Therefore, serious attention to these issues is warranted.

In light of the numerous information incidents and attacks that both government and private networks have experienced, this increasing dependence on the information infrastructure should highlight the likelihood that these networks, systems, and databases will be the subject of malign attacks or even concerted IW campaigns. The technology and knowledge exists in the public domain, and knowledge of these capabilities is widespread, to support a wide range of attacks of different types and degrees of impact on critical DoD and civil functions. Therefore, DoD would be derelict if it were not prepared to address these potential threats with the serious attention and vigorous responses that they deserve. DoD must develop an appropriate culture for living in an information-dominated age in which dependence on information systems cannot be avoided. The capability to operate in stressed IW environments must become a core Force Protection and Operational Readiness measure and must be inculcated as an integral element of procedures and operations; preparedness and responsibility for appropriate behavior must be part of every operational commanders critical task list.

Given the relative ease of carrying out malign actions against crucial information targets and the numbers of potential Bad Actors who could generate huge numbers of incidents, it is important to establish methods of reducing the overall number of incidents and therefore easing the problem of recognizing signal from noise, discriminating serious directed attacks from accidents, pranks, or low-level malicious actions. This type of filtering is essential for constructing an effective indications and warning (I&W) system that would allow affected parties to distinguish truly serious attacks or IW campaigns and take appropriate actions through heightened information condition (InfoCON) states. "Raising the Bar" is designed to forestall the bulk of low-level incidents by changing standards of behavior and creating both technical and procedural barriers to easy malign activities. Doing this requires not just the imposition of technical measures and barriers but, more fundamentally, the creation of a culture that does not tolerate these activities even if they are merely annoying rather than severely damaging.

It also implies that all potential Bad Actors understand that they will be identified and dealt with aggressively; pranks and malicious behavior will be prosecuted so that a culture is created that understands that these standards of conduct need to be obeyed. Certainty of appropriate and calibrated retribution for all unsanctioned activities against information systems will communicate to all parties the costs of malign activities; such a policy, if successfully implemented, and especially in concert with raising the bar against low-level incidents, would deter substantial numbers of potential problems.

This also implies holding those who own, operate, and use information systems to standards of behavior and appropriate procedures so that systems and networks are employed in a safe manner. In order to assure the ability to operate under conditions where users are critically

dependent on information systems, a policy of strict accountability must be established that makes operability of information systems and the key functions they support a command responsibility throughout the chain of command, not just a problem for the system administrators and information infrastructure providers. Strict accountability must include mandatory reporting of incidents, enforcement of procedures, effective forensics to allow attribution, and appropriate prosecution are all equally important in changing the prevailing culture and creating a climate in which information systems can be employed as robust, dependable assets.

To ensure adherence to proper procedures by users and operators, including the crucial incident reporting function, Red Teams will conduct unannounced penetration attempts on a frequent, but unscheduled basis using a wide range of techniques and capabilities. To ensure that malign activities are not risk or cost-free for the perpetrators, a policy of both aggressive "counter-attacks" and vigorous prosecution will be instituted. To facilitate these new initiatives, DoD will seek aggressive interpretations of legal and regulatory constraints on its information protection activities.

DoD must build the capability to improve its information protection abilities faster than the threats can create new methods for attack; this requires that processes for continuous improvement and organizational learning be an integral part of any DoD information assurance program. Information assurance standards or procedures that merely adopt best practices in existence at the time they are promulgated cannot maintain the needed degree of effectiveness in the dynamic environment presented by modern information systems and technologies. Learning from experience and iteratively improving practices, procedures, and systems is essential; continuous updating and refinement based on lessons learned from Red Team and forensic activities must be integrated into a dynamic set of information protection practices and become part of the operational and organizational culture.

Finally, DoD must understand that it is not alone; it exists within an increasingly seamless web of interconnected systems and users. Merely fixing its own internal systems by building perimeter defenses would not guarantee that DoD systems were secure from attack; multiple entry points to critical external functions and insider threats would still exist. And, moreover, this narrow focus would provide no assurance that its critical suppliers, other government agencies, allied forces, or the national information infrastructure on which many of its activities depend would continue to function; these would remain vulnerable and also provide opportunities for denial-of-service attacks against critical DoD functions. DoD must, therefore, create structures that enable it to cooperate and share information with other government agencies, the private sector, and Allied governments in addressing information assurance concerns.

RESPONDING TO IW THREATS

A process fueled by reports of suspicious network activity is needed to provide indicators of the security status of the networks. If the DoD's ability to recognize and detect unauthorized accesses is inadequate, a false sense of security arises which may color the thinking of decision makers when responding to a crisis, as a result of the use of information from a compromised system. The current volume of anomalous activity on networks is typically so great as to discourage reporting; as a consequence little or no detection and reporting is routinely performed. Despite this, an essential aspect of the approach being recommended is to have a fairly broad set of detection criteria to lower the probability that a "real" threat goes undetected.

The first component in dealing with the high volume of reports is to evolve, through experience, a set of threat templates and report filtering techniques to reduce the level of innocuous anomalous activity. This will be an iterative process, evolving as a better understanding of what constitutes threatening behavior is developed.

As a superficial example of a "threat template," three wrong password attempts might be considered non-threatening but a series of N attempts from the same source within a certain period of time could trigger a report. As another example, within the network some operations might in themselves trigger reports, such as accesses to certain protected directories or files, or achieving "super user" or root access from a remote log-in connection.

The incident reports will be the forcing function that feeds analysis and triggers action. An anomalous activity report (or series of reports) will trigger the action of response teams who:

- look for previous similar events, correlated events elsewhere in the system, and correlated events in other systems,
- initiate defensive reactions and restoration of network security, and
- locate and identify the offender for retribution.

The process will generate an assessment of the threat characteristics, leading to improved threat templates, alerts to other users concerning the threat, and the development of new defensive measures (patches, bug fixes, procedure changes).

The process allows the defense to rapidly react to threat events, keep pace with the threat tool set, and potentially recognize IW campaign efforts distributed over time and multiple systems. As new hacking tools appear on the scene, fixes can be developed and disseminated. Rather than lag behind the threat, Red Team efforts can probe vulnerabilities and lead to fixes before the vulnerabilities are exploited maliciously.

The implementation of this process leads to a dynamic, adaptive process for providing readiness and maintaining security against IW threats.

OVERALL IW STRATEGY: CONTINUALLY "RAISE THE BAR"

The overall strategy for Information Warfare is simple and easily implemented — put in place what we know how to do now; improve our capabilities over time; and recognize that transnational threat campaigns, as opposed to individual incidents, are particularly important to identify as they are emerging. The notion underlying this strategy is one of "continually raising the bar," making it increasingly difficult for would-be attackers to penetrate or do harm to our information systems as knowledge, technology and funding allow.

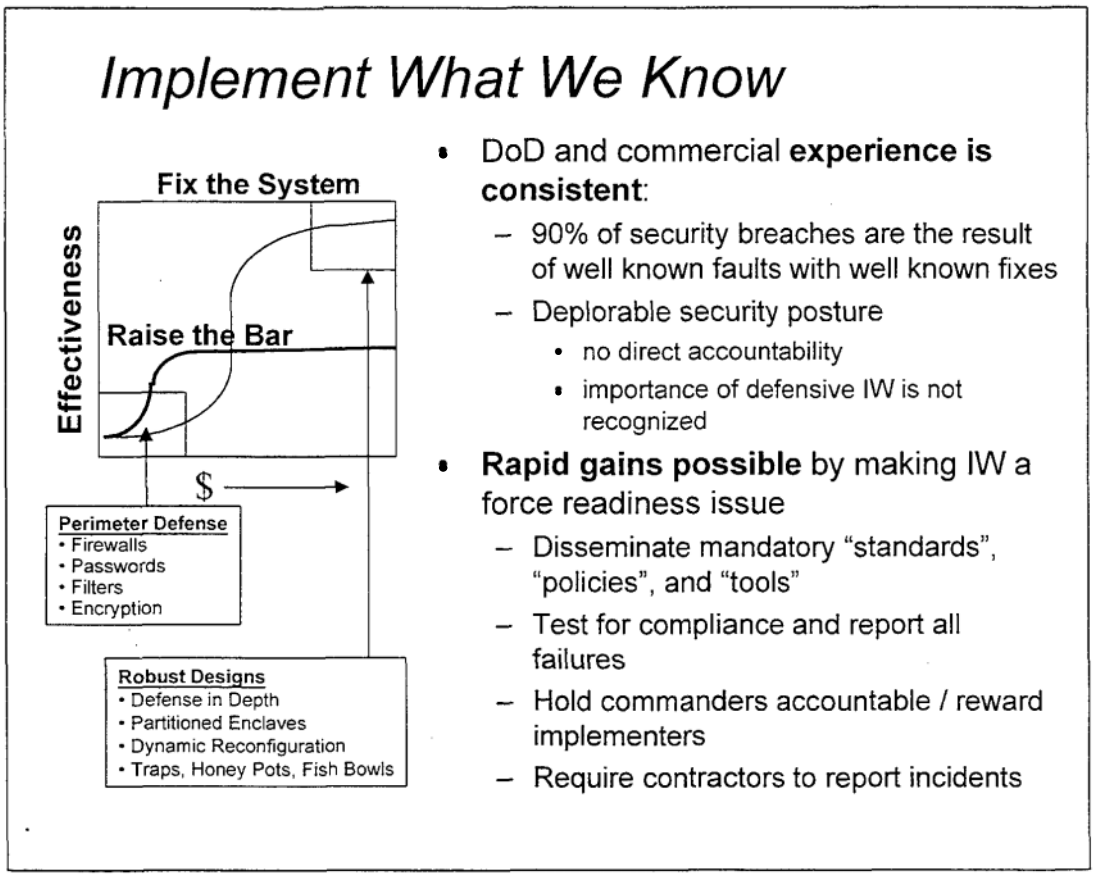
Taking the initial step of implementing those measures that we know how to do today will put a step function of improvement into our information systems, with a minimal expenditure of effort or funds. Procedures are already in place to do much of what is initially needed, but the enforcement of these procedures (things like changing passwords, removing manufacturers' defaults, etc.) is either weak or non-existent. By some estimates, strong enforcement will eliminate up to 90% of today's unauthorized intrusions into DoD networks, thereby improving the situation significantly in itself and having the corollary benefit of making the other 10%, the more sophisticated intrusions, easier to detect. Enforcement will not happen, however, without

accountability and strong incentives and disincentives. In this regard we believe that information assurance and the protection of the information infrastructure must be treated as a readiness issue, just like the protection of critical physical assets.

Beyond this initial step, our capabilities must improve over time to not only stay ahead of the threat, but to continually increase our marginal gain. This will require policy changes, the incorporation of new technologies as they emerge, and the implementation of lessons learned. The "System of System" architecture that we recommend in the following pages we believe will accomplish this. The architecture is fundamentally "report" driven, i.e., it depends upon timely aggressive generation and collection of reports of intrusions, openly encourages them, responds to them, learns from them, and institutionalizes the lessons learned from them. For this to happen, reports must be publicized, not hidden, and in that regard we have recommended policies that mandate such reports both within DoD and from DoD's supplier base through innovative contract clauses. The recommended architecture is fashioned to cross traditional "stove-pipe" disciplines to take advantage of all IW learning, however disparate and from whatever source.

Despite all precautionary measures, we recognize that transnational threats (both multimodal campaigns and isolated incidents) will occur. The third leg of our strategy recognizes that we must prepare for this inevitability. Three specific approaches that we propose involve:

- accelerated research into defensive techniques that can address the last 10% of the threat;
- leveraging commercial off-the-shelf (COTS) security solutions to the extent possible; and
- provision for creating a minimal essential information infrastructure that can be used by the DoD and the primary responder communities when the primary structures are under attack or are disabled.



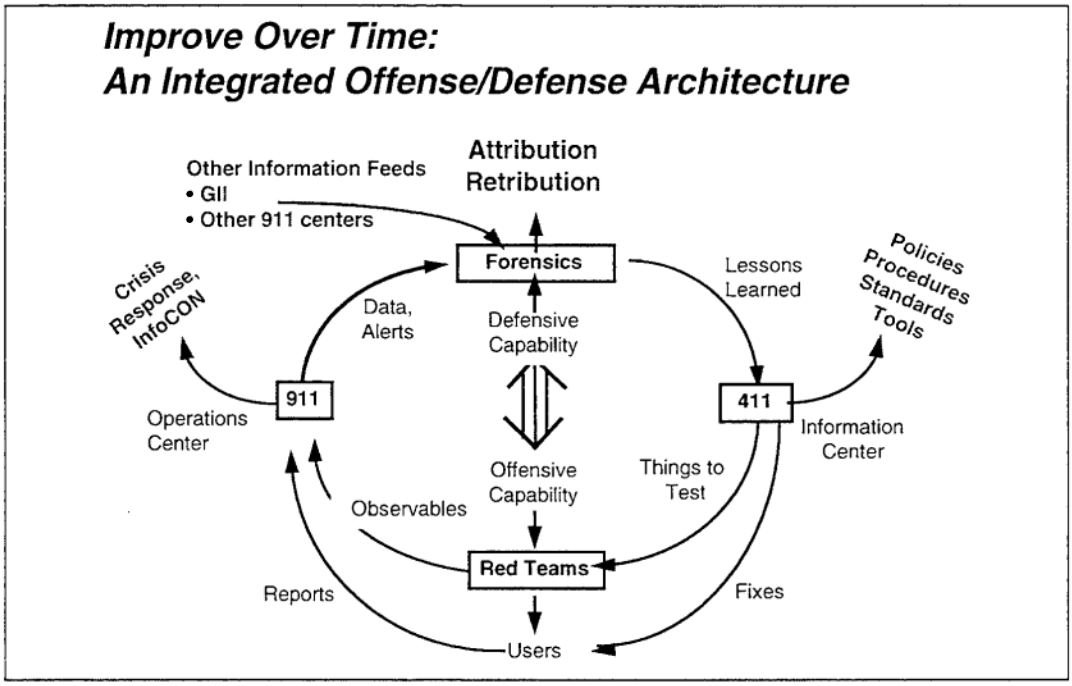
IMPLEMENT WHAT WE KNOW

The first step in improving our IW defensive capabilities is to implement a series of simple fixes – fixes that require no inventions, no new systems, no new technologies and no significant infusion of funds. From everything that we have heard from both the DoD and the commercial sector, the experience with security breaches is consistent – 90% are due to well known faults with well known and established fixes. The fact that this 90% is allowed to exist in the face of what is known today is the result of what can only be called a deplorable information security posture with no direct or even indirect accountability and no serious recognition of the importance of protecting the integrity of information, the ability to collect it and the ability to disseminate it. Such a situation would not be tolerated within the DoD with regard to physical security.

Thus, simple adherence and enforcement of known techniques and information assurance (IA) procedures have the potential of improving the current situation by an order of magnitude, removing 90% of the penetrations and allowing the system, its experts and its administrators to focus on the remaining 10% and its far more serious long term implications. Key to rapidly gaining this order of magnitude improvement is to make IW a force readiness issue, against which commanders will be held accountable, implementers will be rewarded and violations will be disincentivized. For this to be consistently implemented, the requirement to generate intrusion reports for all detected incidents must be vigorously adhered to. The recommended

approach that follows literally encourages the reporting of violations from existing sources such as external attempts to penetrate DoD networks from the outside, inside attempts from formally organized Red Teams and even from the contractor community via new contract requirement clauses regarding incident reporting within contractor networks.

As the graphic on the side of the chart above suggests, this initial step will improve effectiveness significantly at little marginal cost, but will not totally "fix" the system. The remainder of this section outlines our recommendations aimed at providing more robust capabilities and solutions for the long term.



IW OFFENSIVE / DEFENSIVE ARCHITECTURE

The critical recommendation of the panel is the integration of existing functions into an architecture that can iteratively improve security over time. As observed earlier, the problems with information security are not just technical. They are driven by human issues:

- awareness of the need for security,
- well defined standards and an unambiguous requirement to follow the standards,
- testing to ensure compliance, and
- the ability to deter bad actors by definite consequences.

The architecture is driven by incident reports, and has three main outputs:

1. standards published by the 411 and available to the entire user community (DoD and its suppliers),

2. crisis response (including alert levels, and indications and warnings) provided by the 911 operations center, and
3. attribution (leading to retribution) that results from the forensics activities.

KEY ELEMENTS OF THIS SECURITY ARCHITECTURE

The architecture proposed above, also points to a key requirement for continual improvement — the close integration of offensive and defensive technology development efforts. Today, the offensive IW and defensive IW communities are disjoint. Offensive efforts are mostly classified, and defensive efforts are distributed over a large, diverse community. Our recommended architectural approach provides close coupling between the two communities to ensure that the defense has knowledge of all the tools available to the offense.

It should be noted that the architecture is general. It can be implemented with little change for tackling biological, chemical, or nuclear warfare or other conventional forms of terrorist activities. Indeed, it is the committee's observation, that forming such "domain-specific" 411-911-forensic teams, and coupling these in a cross disciplinary manner (through close collaboration between the forensics teams) will create the ability to recognize transnational campaigns that span multiple warfare modalities.

APPROACH: SYSTEM OF SYSTEMS (1)

1. The DoD shall assign a center ("411") and a process that will
    a. Define procedures, policies, standards, incident/threat templates, and technology, focused on information security
    b. Focus on continual refinement and dissemination of these procedures and solutions
2. The DoD shall promulgate a policy that
    a. Mandates implementation of these procedures as part of force protection, and force readiness
    b. Holds commanders accountable for failures
    c. Rewards compliance
    d. Requires reporting of all security incidents

One of the first activities of the defensive IW information center (411) should be to collect, document and publish the best-of-breed defensive IW processes, procedures, policies, and standards. This information should be widely disseminated to the user communities within the DoD as well as to related communities such (e.g., Department of Justice). Selection among these standards will allow implementation of solutions with different risk/reward characteristics. It must be recognized that as DoD information infrastructures evolve into a highly interconnected network-of-networks, the vulnerability of the entire enterprise devolves to the vulnerability of

the weakest link. In selecting the security standards to be used, risk management of the collective system is a goal, and ignoring this collective risk is forbidden. This will serve to establish a baseline for security.

The second element of the approach will mandate DoD information system compliance with these standards and require reporting of all information security related incidents to the 911 operations center. The key is the accountability for compliance. We recommend that operational commanders be accountable for compliance with the mandatory standards published by the information center. Failure to comply places the information infrastructure at jeopardy. In its Joint Vision 2010, the DoD has declared Information Dominance as one of the key pillars of the US warfighting strategy. Vulnerabilities of the information infrastructure should be treated on par with vulnerabilities of the physical infrastructure (i.e., bases, weapon systems, etc.), and commanders should be held accountable just as they are for force protection and readiness. Failure to protect this infrastructure should be an offense on par with the failure to protect forces against physical attack.

As new information on vulnerabilities (due to technology evolution, or discovery of new threats) becomes available through the iterative process defined earlier, 411 will publish updated standards and procedures resulting (through the implementation mandate) improvements in our information security.

APPROACH: SYSTEM OF SYSTEMS (2)

3. The DoD shall create and task a Red Team structure that:
   a. performs random and unannounced testing of the information infrastructure to:
      - ensure compliance with current standards disseminated by the 411
      - explore new ways to challenge the information systems
   b. has the legal authority to monitor and test DoD information systems and assets across service boundaries
   c. reports on findings ("readiness reports") at a minimum to the
      - owner(s) of the infrastructure
      - designated elements of the command chain(s)
      - the 911 center
   d. utilizes the best-of-breed commercial, DoD, and underworld information warfare tools and techniques with no holds barred within the Rules of Engagement (ROE) of the specific attacks

The Red Teams are the most critical aspect of the recommended approach. Implementation of 411 standards will be tested by random, unannounced tests conducted by independent Red Teams. These teams will be equipped with the best tools available and chartered to operate across the DoD network-of-networks.

The Red Team's probing of the systems will have three goals:

1. to establish compliance with mandated standards,
2. to determine adequacy of these standards over time,
3. to exercise and document new vulnerabilities as they are discovered by the offensive warfare and threat communities in general.

The first case, (failure to comply with mandates) will be treated as serious (career impacting) offenses on the part of the commanders with direct infrastructure responsibility. In the latter two cases, the information will feed the continuous process improvement through the 911, forensics, and 411 processes.

In all cases, the Red Team shall have well defined rules of engagement that will define the goals of each attack and the reporting process. We recognize at this stage, that the reports from the Red Team activities will only be preliminary and would have to be augmented with 911 observations and forensics analysis to provide an in-depth appraisal of each system's true security posture. To facilitate this analysis, the Red Team will provide the 911 center with detailed plans, timelines, and expected indicators in advance, and follow up with actual observed results after the testing.

APPROACH: SYSTEM OF SYSTEMS (3)

4. The DoD shall assign and task an operations center ("911") that:
All security incidents are reported to:
   a. Performs triage on the incidents and defines corrective action (crisis response) based all available information including status from other 911 centers activates forensic teams to further analyze the incidents
   b. Maintains a knowledge base of incidents and makes it available to the users, and to the defensive and offensive IW technology development communities.
   c. Summarizes the security status and posture in a continually updated InfoCON
   d. Correlates responses with expected red-team attacks and reports results to appropriate entities defined in the red-team ROE

Whenever there is any unusual activity detected in an information system, the system operators are required to report the incidents to 911. The 911 operations center is modeled after the 911 centers used in civilian crisis. Their main function is to provide rapid assessment of unusual activities on the network and determine the appropriate first response. Just as a civil 911 activity then tasks fire, police, or medical teams, the IW 911 will task specialized teams to react as appropriate. When the incidents point to new or complex vulnerabilities, the 911 will activate forensic teams and provide them the detailed information and support necessary to perform their functions.

Over time, the operations center will become a repository for the corporate knowledge base on incidents (their severity, frequency, observables, etc.) This information will be made available to the research communities developing offensive and defensive IW technologies. This knowledge base will also enable policy makers to understand the true extent and severity of the IW threat and compare the instantaneous severity of the threat against historical precedents. This

comparison will be summarized by the 911 center as an InfoCON level (similar in nature to the Defense Condition (DefCON) level that the DoD has used for many years: see the Information Warfare Defense DSB report, November 1996), which becomes a key input to an I&W process.

Since reporting of incidents to 911 is mandatory, the 911 center will be able to evaluate the users response to red-team attacks. Users who fail to generate timely reports that correlate with Red Team penetrations will be documented and these reports will be made available to the appropriate command authorities as determined by the ROE of the Red Team. As described earlier, this is a key mechanism for forcing compliance with mandatory reporting requirements.

APPROACH: SYSTEM OF SYSTEMS (4)

5. The DoD shall assign a center of excellence in IW forensics that
   a. Analyzes incidents to determine attribution for eventual prosecution or retribution
   b. Uses techniques that preserve the "chain of evidence" and prevent corruption of the "attribution trail" whenever possible
   c. Uses the most aggressive legal interpretations possible to ensure that the attribution and retribution goals are met
   d. Integrates incidents from multiple domain-specific forensic teams to detect spatial and temporal patterns indicative of transnational threat campaigns
   e. Provides feedback to the 411 centers (lessons learned, improved threat templates) that enable improvements in security to be broadly disseminated

One of the critical shortcomings of today's DoD information systems is the lack of a well defined center of excellence in information forensics. The zero-tolerance policy cannot be upheld unless there is a clearly defined, legally supportable chain of evidence that can attribute malfeasance to bad actors. Once such attribution can be made, retribution (ranging from offensive information warfare to physical attacks) can (and should) follow.

Accomplishing this requires aggressive favorable interpretation of legal constraints. Several inputs to our deliberations have indicated that the legal interpretations required to do the required forensics are within the current structure of the law. We strongly recommend that wherever there are gray areas of the law, they be aggressively pursued with the goal of enabling forensics rather than hindering.

Tight integration between different forensic teams focused on multiple warfare modalities (IW, biological warfare (BW), chemical warfare (CW), nuclear warfare (NW), etc.) is an essential element of detecting coordinated transnational campaigns. Our threat analysis observed that IW would most likely be used by transnational threats to magnify the effect of other (typically conventional) acts. Therefore, incidents reported by other 911 centers and interactions with other forensic teams is likely to improve the detection of campaigns.

The output of the forensic teams (in the form of lessons learned) will be then fed into the 411 operations where it will be folded into the continually updated standards, processes, and policies and become part of the mandated defensive IW posture.

CREATE A GLOBAL CULTURE OF INCIDENT REPORTING

There is an urgent need to gather substantially more data about the many and varied penetration attempts and attacks on all manner of systems which support the DoD and Federal Government. Today, reporting ranges from spotty to non-existent.

Thus policies that require and foster comprehensive reporting from within DoD are an important first step to gathering the data from which we can begin to conduct needed assessments to

improve our knowledge and planning. This reporting requirement is needed immediately. Furthermore, given the pervasive dependencies of DoD on commercial infrastructures, a method is needed to extract information from the private sector about attacks on its infrastructure. The DoD should use contractual clauses to induce suppliers to provide such information to a central repository, such as a 911 center.

Numerous briefings to this DSB have described the large numbers of apparent penetrations of DoD systems by unauthorized persons. At the same time it became clear that we have "bunches of data" and not much information about the real threat to DoD systems, or about the numbers and magnitude of attacks on extant DoD systems. Furthermore, we have no real understanding about the degree to which our National Information Infrastructure has been attacked or is vulnerable.

Additionally the ubiquitous Global Information Infrastructure offers the opportunity to elicit information from across the world about threats to our infrastructures. Not only does it provide potential access to millions of people, it can also provide a medium by which the US could offer rewards for information on transnational threats which might induce persons with knowledge of planned attacks to come forward if their anonymity could be protected. Furthermore, we should plan to gather information from and about intruders through the intelligent use of forensic tools such as Fish Bowls, intelligent redirection of attacks and participation in chat groups.

DEFENSIVE IW IS NOT TOO HARD

Many of our vulnerabilities are known but ignored. We should harvest the power of "simple" improvements such as improved filters and firewalls, dynamic passwords, replacing default passwords, use of commercial encryption on unclassified systems, and a series of information security threat conditions to heighten our defenses when DoD systems are under attack. By preventing most of the "intrusions" we have been seeing to date, DoD could reduce significantly (separate the wheat from the chaff) its data analysis requirements, presumably thereby focusing on or identifying potentially more dangerous threats.

Elimination of 90% of the penetrations should not be cause for comfort, but a result which permits DoD to focus on the more important threats. It is the identification of these presumably fewer, but potentially lethal threats that should have DoD's highest priority.

Detection, classification and response to sophisticated attacks and campaigns is simultaneously the most difficult and most important task. Raising the bar will not resolve this issue per se; and detection of such attacks in real time will require tools and techniques not yet available. But there is much that can be accomplished as stated earlier through the creation and use of 411, 911 and forensic capabilities.

The private sector is and will develop many tools and techniques that will improve DoD information technology environments. Object Oriented Data Bases, software based security tools for the internet, increased power densities, and smaller and faster chips are all examples of technologies most likely to emerge from the private sector.

The DoD has needs for computing capabilities and security which are beyond the needs of most commercial enterprise, and technologies to support these issues may need to come from within DoD. The remaining 10% of attacks on DoD systems arguably represent the most difficult to

detect and characterize and therefore require some special attention. Complex adaptive systems are needed which can detect and react to intrusions in smart ways.

Clearly our perimeter defense paradigm is inadequate in this new networked world, and a defense-in-depth approach must acknowledge that once the perimeter is breached the system is highly vulnerable. Dynamic "protected" enclaves could significantly increase DoD's ability to continue critical operations while under IW attack.

DARPA's ongoing programs are in the forefront of research to develop "defense-in-depth" technologies and these programs warrant strong support from the Secretary of Defense. Methodologies to identify the signature of and detect attack are required to detect network intrusions. The smart integration of COTS with technologies developed in DoD warrants early and constant attention to harness the power of each in a way that enhances the robustness and resiliency of critical DoD systems and networks.

In addition to continued focus on defensive IW technology, the panel recommends that DoD, through DARPA, initiate an aggressive program to create and disseminate forensic tools capable of tracking security penetrations to the source. There is clear need for tools that can be used by moderately skilled individuals to perform forensic analyses while protecting the evidence trail and avoiding detection.

In addition, most defensive IW research has focused on protection of information and the infrastructure. We believe that extending these techniques by focusing on active deception that can evaluate the actions of bad actors and respond appropriately, could help future forensic analysis.

COTS ALONE IS INSUFFICIENT

The commercial sector has begun to respond to nascent demand for better security tools, but by itself COTS technology will not be sufficient. First, although COTS is much more dynamic and more net-based than government-proprietary security tools developed over the past ten years — and for that reason more appropriate to mass market needs — demand has been weak, and physical and human attacks on infrastructure are still seen as more significant threats than cyber threats. Absent other incentives the commercial sector is not inclined to build into a product costly features that the consumer does not (or thinks he does not) want.

Security is not just a hardware or software tool — it's a complex system of measures, an integrated end-to-end infrastructure — to include

- secure software and operating systems,
- intelligent network design,
- effective day-to-day administration,
- a set of policies and procedures consistent with the "good" being protected, and with the level of liability and risk that the owner of the good is willing to accept given competitive pressures, and
    - responsible and competent Internet service and backbone providers (an ever-increasing requirement).

No single business is capable of providing this range of services for itself, and no single provider is working on such an integrated solution!

For businesses, investment in security is an optimization of the last 10% of the "cost of doing business," and is directly related to the competitive situation and the state of trust relationships in a society. Too often government intervention in security tools has led to making security/authentication more complicated and costly, less marketable, less user friendly, more likely to be outdated when it hit the market, etc.

DoD Must Provide Minimum Essential Information Infrastructure

The DoD needs to do more thorough planning and provisioning to mitigate the effects of IW/EW attacks on its own infrastructures, as well as the supporting civil infrastructures, and to provide better support for civil first responders. In particular it needs to define a minimum essential information architecture, and implement that architecture over time. Key elements of that architecture are outlined as follows.

DoD must plan and provide for a means to reconstitute essential communications capabilities in response to IW or physical attacks on its elements, or natural disasters. This capacity must be provided in a secure way independent of the public switched networks. There are probably many ways to achieve this goal, and we encourage the analysis of the possibilities. Milstar could provide secure, protected links for reconstitution of essential communications via an "order-wire" system needing modest bandwidth channels if the appropriate planning, procedures, and training are put in place and exercised by both military and civilian users.

DoD must achieve a much higher level of interoperability with civil first responders at early stages of an emergency. This interoperability could become quite elaborate, involving assets like the Air Force Airborne Command and Control Center (ABCCC) airborne command posts, but must at least provide interoperable radios to the forces likely to be involved with first responders. Thus DoD should procure a few commercial radios compliant with the Association of Public-Safety Communication Officials (APCO-25) standard for public safety communications, and deploy these to units most likely to be used for first responder support.

RECOMMENDATIONS

Recommendation 1.

The IW part of the end-to-end operational concept recommended in the main Summer Study should include the integrated offense / defense architecture and the system-of-systems solution elements described in this report

- The foundation of the recommendations is an architecture approach that uses a feedback mechanism for dynamic improvement; therefore, all elements of the architecture must be implemented to accomplish the full benefits.
- We believe this architecture directly fits the IW domain and that this construct is applicable to other transnational threat domains

Who: Secretary of Defense and the Joint Chiefs of Staff

Where: Entire communities of interest

RECOMMENDATION 2.

Consistent with the general DSB Summer Study recommendation for readiness, IW readiness should be included in the process

- Definition of readiness should be based upon a set of standards and metrics developed by the 411 center
- IW readiness, per se, should be tested, measured, evaluated, and reported as part of the normal Joint Chiefs of Staff (JCS) readiness reporting system (refer to DSB report on Information Warfare Defense, November 1996)

Who: JCS

RECOMMENDATION 3

For IW architecture elements the following reorganization of existing assignments and responsibilities should occur:

- 911 Center assigned to JCS
- While DISA currently has part of this assignment and might be the basis for expansion, the task force does not believe they are capable of doing this even with major augmentation
- Forensics assigned to Information Operations Technical Center (IOTC) located at Fort Meade, MD.
- Specialized talents needed to perform forensics will be scarce and must be gathered from wherever they reside, including defensive IW, Air Force/Office of Special Investigations, other NSA, and the Computer Incident Response Teams (CIRTs).
- 411 assigned to IOTC
- Requires IOTC to embrace and implement defense IW as a priority
- Red Team leadership assigned to JCS (J-3)
- Populate team from NSA, Joint Command and Control Warfare Center (JC2WC), etc.

These organizational elements can be created within current funding levels via reassignment and reprioritization of responsibilities

RECOMMENDATION 4

Include in all contracts and requests for proposals (RFP's) a requirement to report, using the suppliers own systems, all attacks on its information systems to the 911 and to describe in the proposals its detection capabilities and what reports the 911 should expect.

- The effectiveness of suppliers capabilities at detecting and reporting IW incidents can be used as an evaluation discriminator
- Suppliers should be permitted, and encouraged, to use the 411 center

Who: USD - Acquisition & Technology

Where: All DoD Acquisitions

RECOMMENDATION 5

DoD and supporting information systems should move away from a perimeter defense concept for defensive IW towards a "distributed partitioned secure enclave concept"

Who: Assistant Secretary of Defense (C3I)

RECOMMENDATION 6

Enhanced Interface with State / Local "First Responders"

Task DISA to assemble, equip, train, test and maintain order wire

- Allow first responder to establish communications
- Requires procurement of Public Safety Standard Radios (APCO-25)
- Makes use of MILSTAR
- Should include deployable local area network/wide area network (LAN/WAN)

When: Now

Where: Deployable

REPORT OF THE COMPETENCY PANEL ON CIVIL INTEGRATION AND RESPONSE

Panel Chairs

Mr. Michael Hopmeier
Mr. David Paulison

Panel Members

Mr. Jeff Abraham
Mr. Carlos Castillo
Mr. Phillip Chovan
Mr. Henry Christen
Mr. James Denney
Mr. Louis Guzzi, MD
Mr. Paul Maniscalco
Ms. Annette Sobel, MD

Government Advisors

Maj Gen Paul Carlton
CAPT Rob Carnes, USN
Mr. Christian Cupp
BG John Parker
Mr. Ray Polcha
Mr. Bob Ruth
Dr. Pat Vail

TABLE OF CONTENTS

EXECUTIVE SUMMARY i

CIVIL INTEGRATION AND RESPONSE 1

Background 1
What is First Response? 2
Definition of an Incident 3
The Civil Incident Management System (IMS) 3
Incident Managers 5
Military Doctrine and Technology vs. Civilian Needs 5
When does the Federal Government Get Involved? 6
Different Response Classes 8

OBSERVATIONS 12

RECOMMENDATIONS 15

ANNEX A: CIVIL INTEGRATION AND RESPONSE PANEL MEMBERSHIP

EXECUTIVE SUMMARY

The Defense Science Board completed the formal portion of its summer study, Defense Responses to Transnational Threats in mid-August. As part of the study, each competency panel prepared a written summary of its findings and recommendations.

One of the competency panels, the Civil Integration and Response Panel, focused on issues related to the federal/civil interface in response to transnational threats. The panel was made up principally from professional in the fields of firefighting, emergency medicine, paramedic response and law enforcement. These representatives came almost exclusively from the civilian sector and all had extensive and significant experience as well as being senior personnel and executives in their respective communities.

The panel had three principal missions:

- Educate the DoD on issues dealing with the civil sector in response to threats
- Learn from the DSB and briefers what the Federal response capability and policy is
- Make recommendations as to how the defense and civil communities can better interact in response to transnational threats.

The panel made the following observations:

- A significant difference exists between civil and military training/exercises and experience.
- The overwhelming majority of defense effort is focused on pre-incident and, to a slightly lesser extent, on crisis management with minimal national effort on consequence management.
- Transnational threats will involve non-military assets and targets to an unprecedented level.
- Many military and defense technologies do not map directly to civilian needs.
- Consequence management is independent of cause.

Further, after considering the entire spectrum of potential responses and threats, the panel determined that the civilian community should have three principal responses in dealing with the continuum of possible responses to an unconventional threat[1]:

1. Recognize that a threat exists
2. Notify the proper authorities and begin to obtain advice on response to the threat

[1] An "Unconventional Threat," is of a magnitude or type where local communities require assistance. The definition is focused in those transnational groups that may employ chemical, biological or nuclear related capabilities.

3. Stabilize the situation by minimizing the threat and damage to life and property until specialized assets can arrive to assist with the situation.

In summary, the recommendations of the panel were:

- Implement a standing panel to act as representatives of the first response community to the Federal, Civil, and Intergovernmental Agency Communities.
- Implement a system to disseminate critical information and provide for first responder access to classified Federal data especially as it applies to threat warning.
- Establish a single Point of Contact (POC) for access to information and support from the Federal Government for the First Response Community.
- Accept the Civil Community Incident Management System (IMS) as the standard for federal assistance to first responders and provide training to relevant military personnel in the IMS.
- Resolve conflict between various federal agencies, as well as internal to DoD, on issues of leadership, support, training and response.
- Implement an aggressive technology transfer program from DoD, DOE, and other Agencies allowing for both development and deployment of relevant technologies and equipment.
- Provide for a single, integrated training methodology focused on institutionalizing Federal and Civil training within the first responder community.
- Institute a program for providing experts and advisors to local communities as and when needed for the formulation of plans, programs, technology and advice on training and exercises.
- Provide standardized, realistic training information and goals for first responders: The First Response Handbook.
- Where practical, obtain certification and approval for use in civilian environments of military equipment and personnel.
- Provide a straightforward, consolidated and rational method of Federal monetary support for first responder training, preparedness and response.
- For the Federal Government to take greater advantage of potential information resource in first responder community.
- Task the DoD Defense Science Board (DSB) to perform a study of how technology can be harnessed to support the medical mission.

CIVIL INTEGRATION AND RESPONSE

BACKGROUND

At the beginning of the Defense Science Board Summer Study, it was recognized that a significant part of the effort involved in combating Transnational Threats would involve a closer and deeper reliance and cooperation with local, civil assets than had heretofore ever been considered. As a result, a competency panel was formed to specifically address this issue, the Civil Integration and Response (CIR) Panel, co-chaired by Mr. Michael Hopmeier and Mr. David Paulison*.

The mission of the CIR panel was to bring into the study information, experience and representation of the first responder (fire, police, paramedic, emergency medicine) communities. The CIR panel had three specific goals:

- Educate the DoD participants on issues dealing with the civil sector in response to transnational threats
- Learn from the DSB and others what the Federal response capability and policy is and make this information available to the first responder community
- Make recommendations as to how the defense and civil communities can better interact in response to transnational threats.

Unlike many of the other competency panels, a major aspect of the CIR Panel was interaction with the other panels for the express purpose of providing insight into the public safety community. Also unique was the extent to which the goals, skills and knowledge embodied in the CIR panel had impact and relevance on the other panels' studies. This impact was felt by and effected the other panels deliberations and conclusions to an unprecedented level.

Also of import was the ability for the members of the CIR panel to interact and effect the conclusions, views and operations of a broad-based community, the civil first responders. All the members of the panel have used the information and insight gained as a result of their exposure to the federal/defense community to effect not only the actions and policies of their own respective organizations but also to influence other communities and groups as well. As is well known, the US Army Chemical/Biological Defense Command (CBDCOM) has the mission to provide training to many of the metropolitan communities but this training is not always fully absorbed at the institutional level. Insight gained by the CIR panel members was and is already having an effect on plans and preparedness in many communities.

The final portion of the CIR Panel mission is embodied in this report and the final briefing. Recommendations and suggestions, as well as observations, are enumerated here and present the feelings of a broad, capable and very knowledgeable cross section of the civil responder community. While they may not represent 100% of the community they certainly provide guidelines and a solid basis for further action and study. As in any large community, many different opinions and feelings on almost every issue abound. However, it was intended by the make up of

[2] Panel membership is at Appendix A

this panel that the opinions and findings presented here be considered as representative and reliable for the public safety community as a whole.

WHAT IS FIRST RESPONSE?

A variety of definitions abound for what a first responder is and what is first response. An almost equal number of misconceptions also exist.

In general, first response may be considered the first *organized* group of people to arrive at the scene of an incident and provide assistance, coordination, direction or action. This is usually some combination of fire, police and paramedic personnel, normally notified by a call to 911.

It should be noted that considerable discussion has occurred over issues associated with an occurrence on or in a federal agency versus in a civilian area. The example normally cited is the Oklahoma City incident with the Murrah Federal Building. While some have pointed out that the response was modified because this was a federal facility, in all ways that mattered this is incorrect.

All military commanders have the authority to deploy personnel and assets domestically in support of crises if this is needed to reduce loss of life or damage to property. This authority is limited as to time it can be utilized without authority of higher command but exists nonetheless (see Annex D, Volume I for an overview of statutory and of regulatory requirements and constraints.)

What this means in real terms is that the same response from the federal authorities would have occurred whether it was a federal building or a private structure. Any local commander would have immediately had authority to provide support.

Also of note is the response of civilian public safety agencies. In almost every case in the United States, and in many cases overseas, a federal/military installation has some sort of mutual aid agreement with local authorities to provide assistance in times of crisis (this agreement works both ways and there are numerous examples of local military installations providing specialized assistance such as air transportation and medical support to local authorities).

One of the best examples of local authorities augmenting a military crisis is the air crash that occurred in 1992 at Pope AFB in North Carolina. An F-16 collided with a C-130 transport while trying to land at Pope AFB. The C-130 touched down safely, the F-16 pilots ejected and the fighter crashed into a parked C-141 Starlifter. The resulting impact sent metal and 55,000 gallons of burning fuel through a staging area where paratroopers were preparing for airborne operations. The resulting fireball burned and/or severely injured more than 160 personnel. The military medical support was soon overwhelmed and required assistance from the local community. Almost immediately following the incident the local public safety personnel were notified and responded exactly as they would have had the incident occurred at the local airport as opposed to on a military installation. This response included fire and emergency medical support as well as police to assist in coordination and direction of assets. Most of the casualties were eventually evacuated to San Antonio where they were treated and eventually released. However, without the immediate intervention and support of local authorities this catastrophe would have had a much higher number of fatalities.

One further consideration in evaluating overall response to unconventional threats; while local and

even regional public safety officials are engaged in dealing with an incident other tasks and incidents will still occur. During the World Trade Center response and the Murrah Federal Building operation there were still motor vehicle accidents, shoplifting and baby's being born. It is not practical, or even possible, to focus all effort on a single incident to the exclusion of all other responsibilities.

DEFINITION OF AN INCIDENT

Any incident, regardless of type or cause, can be broken into three distinct sets of activity: Pre-incident to provide preparedness, crisis management during the event and consequence management during and after the event.

As is illustrated below, these sets of activity are not strictly sequential but overlap to form a continuum.

Activities include:

- Pre-Incident – all those efforts, actions or resources identified prior to an event to prepare for an incident. These include, but are not limited to, Research & Development (R&D), education, training, intelligence, exercises, preparedness, policy development, pre-positioning of equipment, infrastructure development, and generation of skills and knowledge base.
- Crisis Management – the event itself and the time immediately prior to and immediately after the event. This phase involves direct intervention/involvement in the event and usually entails considerable confusion as well as reactive application of available resources as opposed to planned resources and responses. The crisis is typified by highly reactive responses as opposed to planned proactive actions. Normally, the crisis itself has the shortest duration of the three aspects of the event.
- Consequence Management – the mitigation, containment, decontamination and information management of the event. This phase is generally the longest in duration and includes everything from mitigation of further damage to assessment and attribution of the event. In the case of mass casualties, this is the phase where definitive medical care and transportation is provided. In other events the analysis, clean up and summation of the event will occur in this phase.

THE CIVIL INCIDENT MANAGEMENT SYSTEM

The civilian Incident Management System (IMS) was previously called the Incident Command System (ICS). The system was developed in California in the 1970's as a response to multi-agency problems encountered in major wildland fires.

This Civil Command, Control and Communications system was developed by a group of engineers with defense industry backgrounds. The system addressed the following major needs:

- Common terminology and communications interoperability

- Coordination mechanisms between diverse agencies
- Effective multi-agency coordination through the incident management and staff
- Coordinated allocation of scarce resources
- Adherence to the principles of chain of command, unity of command, and span of control.
- A system of status keeping and planning

The IMS is now a standard template in Emergency Management System (EMS) mass casualty operations and fire/rescue operations. The system is also mandated by several national standards. For example, the National Fire Protection Association (NFPA) mandates an incident management system for hazardous materials operations, structural and wildland fire fighting, confined space rescue operations, etc.

The IMS consists of an incident manager (with a management staff), and four functional sections called operations, logistics, plans, and administration. The sections are further divided into branches. For example, a common format is a medical branch, fire/rescue branch, and Hazardous Materials (HAZMAT) branch. The medical branch is then divided into the sectors of triage, treatment, and transport.

A key issue in response to unconventional threats is the integration of management/command/control when federal assets arrive and attempt to coordinate with the on-scene civil responders.

It is not practical for any federal agency to assume the duties of incident manager. Nor is it practical to assume that a DoD/DoJ agency would be subordinate to a civilian commander. The solution is unified management, where civilian and federal managers operate jointly. Individual sections of both systems would then coordinate at their respective levels. For example, the civilian medical branch would integrate with a DoD medical unit. The IMS model has evolved into an all risk management system (not just fires) for other emergency response agencies such as emergency management, and to a limited extent, law enforcement.

A mass casualty event is not a common incident. Most medical incidents are treated/transported by a two-person team. These units can be described as "free lance" providers, working within a common system. Multi-unit coordination is common in the fire services, but infrequent in EMS. However, a mass casualty event can only be managed by an effective EMS/IMS. The functions of decontamination, triage, treatment, and transport can only be coordinated by an efficient system. When it is considered that such events will be regional in scope, and will consume logistics at an alarming rate, command/control/communications become crucial.

Lastly, these events will require federal assistance from DoD and non-DoD agencies and special response teams. Coordination, liaison, and communications will be essential.

The civilian Emergency Management System is composed of multiple agencies in multiple jurisdictions and is derived from the following supporting infrastructure:

- **State Emergency Plan** (or similar title): The State Emergency Plan is the primary document guiding the State's response during emergencies. It defines emergency roles and responsibilities of State agencies.
- **Multi-Hazard Functional Planning Guidelines** (MHFP) (or similar title): The MHFP

provides local emergency planning guidance in the form of a model plan. Most jurisdictions have used the MHFP as the basis for their emergency plan. The MHFP is organized around key emergency response functions.

- **Mutual Aid Plans and Support Documents:** Several documents generally describe the structure and function of mutual aid in each region and may include a Master Mutual Aid Agreement index, Mutual Aid Handbook, and discipline specific mutual aid plans such as fire, law enforcement, medical and EMS.
- **An Operational Area Satellite Information System** (OASIS) (or similar title): An OASIS guideline describes an information and resource tracking system for operational areas. It defines data and formats for reporting on key functions that include the MHFP functions.

INCIDENT MANAGERS

A key leadership position in a mass casualty terrorism event is the incident manager. In many cases, there are not clear guidelines at the state/local level specifying who is in charge. Historically, well-meaning but competing agencies or command confusion caused by separate EMS, fire, and law enforcement command posts has compromised incidents. In a mass casualty terrorist incident, the management issue is more confusing because the event is a crime scene, a mass casualty medical emergency, and/or a fire/rescue incident.

If management challenges exists at the local level, the problem exacerbates when state resources arrive, and becomes much more complex when federal agencies and/or DoD teams arrive.

In some states, legislation specifies who the incident manager should be. Usually it is the fire chief in mass casualty incidents, the emergency manager in disasters, and the police chief/Sheriff in law enforcement incidents. In other states, there is no legislation, with the matter being left to local preferences, historical in nature, and often unwritten (None of the legislation or informal rules relate to terrorist events.)

When a myriad of federal agencies enter the picture, the challenges of scene management increases. The Presidential Decision Directive-39 (PDD-39) legislation specifies that the FBI is the lead federal agency for crisis management. The FBI has extensive crime scene management experience, and has exercised extensively with DoD and DOE to deal with possible crises that might involve nuclear devices, biological or chemical agents or high explosives (which may be "salted" with radiological material). For post-incident consequence management, PDD-39 specifies that FEMA is the lead federal agency.

MILITARY DOCTRINE AND TECHNOLOGY VS. CIVILIAN NEEDS

Military systems and doctrine are designed to meet unique military needs. Doctrine, technology, and training focus specifically on functioning in and countering incidents in a military/combat environment. In a chemical or biological unconventional incident, for example, this generally includes extensive training on the part of all personnel within the affected area, special equipment and materiel designed specifically for this type of threat. The goal of this training is successful

achievement of mission objectives, which includes threat neutralization with the lowest attainable morbidity/mortality rates and collateral damage.

Consider the simple case of trying to transport a casualty contaminated with chemical or biological agents. In combat, the person is triaged, secured in protective gear (if not already in use), decontaminated, and transported in a military vehicle to the receiving medical facility. Subsequently the vehicle is decontaminated. All personnel are functioning in protective gear and the medical care facility is sufficiently prepared to handle the incident. The entire surrounding environment is probably contaminated and, more importantly, considered unrecoverable. Information flow is tightly controlled in this scenario.

The civilian environment is vastly different in many respects. Essentially none of the surrounding population is protected, none of the environment or infrastructure is expendable (it is generally considered unacceptable to burn office buildings or use caustic decontamination substances in downtown areas) and control of the situation is, at best, marginal (information flow is less restricted due to media access). Constraints include the absolute necessity for limiting further environmental and personnel contamination, whatever the cost. Further, while some military vehicles and materiel are designed with the potential need for decontamination in mind, that is not the case in a civilian environment. Decontamination of a Greyhound bus or ambulance or fleet of fire trucks with conventional equipment presents a significant challenge.

A second issue is the question of doctrine and response. The military has a standardized set of procedures for dealing with almost any contingency, including unconventional incident attack. Operational military units participate in annual Ability To Survive and Operate - (ATSO) exercises that address the unconventional incident threat environment response. In contrast the civilian authorities do not use this routine training approach. This situation is further exacerbated when the federal and civilian agencies must interact as a team to jointly address all aspects of consequence management.

One of the greatest anticipated challenges by both the Unconventional Incident Response Force and the Center for Disease Control (CDC) National Center For Environmental Health is a General Emergency Cell with the ability to integrate with on-scene assets and stabilize the situation. This activity will require varying amounts of time and resources as there is no standard mechanism of response in the civilian community, even assuming early warning, detection and situational (threat) recognition. Consequently, the first responder community response will be based upon individual community unit doctrine. As a result, no consistent, anticipated response baseline and command structure will be implemented for integration with federal response.

One of the first steps in alleviating these problems will be to provide accurate, timely information to the first responder community so they can recognize a situation of this nature, and provide appropriate, directed training so that an actual response will be consistent, effective, and seamless with other, higher level (i.e. State and Federal) assets.

WHEN DOES THE FEDERAL GOVERNMENT GET INVOLVED?

As noted earlier, numerous different Federal Agencies have overlapping jurisdiction for responding to incidents, and further, the methods for involving them also vary greatly. However, as a general

rule of thumb, most agencies will self-initiate involvement based upon information and notification from a variety of unofficial, ad-hoc sources of information (personal phone calls from colleagues, watching an event occur on CNN). The involvement (agency, resources, level of preparation and readiness, etc.) is situation and incident dependent and there is no universal norm. There are a set of potential situations where the federal authorities are already present and prepared such as a transnational group threatening to use a nuclear device that has been uncovered by intelligence or law enforcement agencies. These more prepared crisis responses generally result either from intelligence data indicating a credible threat or a high profile situation such as the G8 in Denver; however, these situations are not the norm.

The point at which Federal Agencies become involved is usually when: 1) an unconventional threat has occurred and 2) the local authorities are unable to deal with the threat either as a result of being inundated and available resources become drastically insufficient or because no resources exist as a result of the incident being unique. In either case it is generally not until several hours into an event that coordinated, knowledgeable and responsive support form Federal Authorities occurs. Up to that point, response and assistance is based upon individual initiative of local and/or qualified (i.e. resources and trained) commanders to determine what level, if any, of response and assistance should be provided. For example, in the World Trade Center incident no DoD resources were involved.

DIFFERENT RESPONSE CLASSES

It must be realized that, from the point of view of the first responder, the cause of the incident is secondary. Whether manmade or accidental the first responder must react. Further, given the typical "fog of war" associated with most emergencies, that reaction will be based on incomplete, inaccurate and potentially contradictory information. Even if intelligence data prior to an event indicates when that event may be immanent, any crisis response will almost universally result in at least partial confusion. As a result, the first responder will create a generalized response pattern that is designed to address any contingency minimally, though not necessarily optimized for that particular incident (i.e. responding with a fire company, Emergency Medical Technician (EMT) unit and police car to every call). It should be noted that circumstances will sometimes modify this protocol. For example, lack of funds or significant burden on the system (large number of fires or riots) may reduce the level or immediate type of response.

As a result, the response class is independent of the cause of the incident. Consequently, response initiatives will, in almost all cases, consist of one or more (usually more) of the following classes of incidents:

- Explosive Detonations
- HAZMAT (to include chemical, biological and nuclear)
- Mass Casualty from any cause
- Supporting Infrastructure Degradation or Destruction- Telephone, Power, Water, Utilities

Whether responding to a nuclear explosion (all four classes) or the Oklahoma City event (blast, mass casualty), a biological attack (HAZMAT, mass casualty) or an industrial chemical accident similar to Bhopal, India (HAZMAT, Mass Casualty), the incidents will always be some combination of the above four classes.

Infrastructure attack is somewhat unique in that it involves, in general, a more subtle form of attack. It is considered to range from destruction/interruption of power substations to jamming 911 lines. While not generally specifically destructive, these attacks could be used in combination with another attack to heighten effects and create greater confusion and casualties.

All these classes of attack will be addressed in generally the same way with details varying in the assessment, entry, casualty gathering, casualty transport and medical support provided.

Each class of the above events occurs, not just on a daily but in some large municipalities on an hourly basis. What distinguishes events of interest to this study versus every day events is the scope or scale. If the event is beyond the capabilities of the local community (i.e. more casualties than available medical support, requirements for special decontamination or equipment, etc.) than it falls in to the category of *unconventional* and outside assets (outside the local community) will be required. These assets may be as minimal as a neighboring jurisdiction providing assistance in covering a community to a full-scale deployment of federal assets consisting of thousands of personnel and support equipment. Whatever the cause and for whatever reason, assistance would be required.

HAZMAT

HAZMAT (Hazardous Materials) describes a class of response involving some form of agent (liquid, gaseous, solid or other) that is inimical to human health and safety. Among other things, chemical, biological and radionucleides all fall in to this category. The public safety community has dealt with HAZMATs for years and has a variety of training and certification programs designed to provide the skills and equipment needed to deal with HAZMAT incidents.

Traditionally, most HAZMAT incident have either consisted of fuels (gas, diesel, oil) or common industrial compounds (chlorine, ammonia). However, over the past twenty years several conditions have been combining to broaden out these classes of "normal" HAZMATs.

First, growth and diversification of heavy industry, both domestically and overseas, has created a greater need for a wider ranging number of industrial compounds. As an example, in World Wars I and II phosgene gas was used as a chemical warfare agent. Today, it is used for several different industrial processes and is shipped all over the world by land, sea and air.

Second, the modes of transportation have diversified. No longer are small quantities shipped via special courier but instead large quantities of numerous different agents are regularly shipped throughout the country. Further, as a result of changing industrial processes, numerous new compounds and various environmental wastes and hazards are being developed daily.

All of this required that the first responder be prepared to deal with a vast array of different agents, both singly and in combination. For example, when a train derails and tanks leak, the various compounds are not segregated as to type or class, they all mix, usually under environmental stress (i.e. fire or explosion). Further, in many cases the paperwork associated with these agents is unavailable, inaccurate or maliciously changed (illegal transport and dumping of hazardous waste has become a large market in the US).

As was noted earlier, seldom are any of these classes encountered in isolation. A HAZMAT incident could (and probably would) be found in association with some form of accident or catastrophe. This could be a motor vehicle accident, an industrial explosion, a train derailment, a terrorist incident or a combination of these. Also, in many cases, these incidents will also involve mass evacuation and the concomitant shelter and health care needs associated with such an incident.

In general, the first responder must be prepared for, and deals with, a much greater number of HAZMATs and HAZMAT incidents than any military unit. Further, the military maintains much better accountability for its HAZMATs so in many cases these incidents are easier to deal with in a military setting than in a civilian one.

Finally, and perhaps most importantly, first responders are generally prepared to deal with any HAZMAT, at least initially, whether a chem/bio warfare agent or an industrial accident (in many cases they are one in the same). However, to the casualties and victims it matters little whether they are injured or die from an ammonia tank car derailment or a terrorist attack with Sarin. This must be considered when scenarios are evaluated since it may be easier (and potentially more effective) to steal a tank car of chlorine and blow it up in the middle of a city than create a quantity of nerve gas.

Civilian HAZMAT capability varies from jurisdiction to jurisdiction and can be minimal to advanced. Training encompasses awareness through the operational level. Operational and technical training is usually provided to specialized units within an organization. Equipment includes self-contained level 1-3 (HAZMAT protective) entry suits in limited numbers with limited

decontamination capability. The treating of victims is currently limited to specific antidotes and decontamination for operators and open decontamination for the civilian population. Preparedness includes mandated training in a recognized Incident Management System.

High Explosives

In many cases, high explosive incidents also involve one or more of the other noted classes (HAZMAT, Mass Casualty, Infrastructure). High explosive incidents have traditionally been the weapon of choice of the terrorist as well as being quite common in industrial accidents and natural disasters.

Also associated with high explosive blast is the high probability of structural damage and wide spread dispersion of shrapnel. High temperature combustion of incendiary products may also be associated with a blast. The first responder must be prepared to deal with all of these results.

Particularly troublesome is the recent use of binary/multiple devices designed to lure-in and trap/disable first responders. This is a relatively new, and very disconcerting development. Traditionally (at least in this country) the first responders (fire and paramedic) have been considered neutrals and not actually targets of attack. This recently changed with the Atlanta double bombing and the planned armored car robbery in Texas. In both these cases, incidents were designed and implemented with the clear goal of attracting and incapacitating/killing the first response force. Not only does this effect the response to the initial incident but it also changes the method of approach to future incidents.

Mass Casualty

The definition of mass casualty varies based on municipality, type of casualty and even time of year. Also, extenuating circumstances also change the definition. As a working definition, mass casualty may be considered any situation in which the initial response and readily available first tier (local responders immediately available without recalling or depending on mutual aid) is not sufficient to care for the casualties.

This situation falls into two general categories; overload in quantity and overload in type. In the former case, a mass casualty incident whereby hundreds or thousands of people are burned and have crush injury or massive trauma (two jumbo jets collide over a busy airport and flaming wreckage falls into a subdivision or on a passenger terminal); here local medical authorities can care for and treat the casualties as they would in any other incident but they are overwhelmed by shear numbers. The latter case is where the skills and/or resources simply don't exist; a chemical agent incident (whether intentional such as Tokyo or accidental such as Bhopal) can overwhelm local authorities with only a handful of cases. Dealing with the effect from biological agents can be much worse.

Nonetheless, whether overwhelmed by numbers or types the local EMS will respond by escalating levels of resources and coordinating response as best as possible. Most municipalities have some plan for a "conventional" mass casualty incident and practice them at least annually. Few, if any, ever practice escalation to the point where resources beyond the immediate community mutual aid agreements extend.

Fire and EMS First Responder mass casualty plans are incorporated into the Incident Management System and are inclusive of medical emergency, rapid intervention and triage components (Triage, Treatment and Transportation), patient care components, morgue operations and air operations.

There is no current capability to treat large numbers (hundreds, thousands or tens of thousands) of radiological, chemical or biological exposures anywhere in the United States.

The hospital receiving system is currently no better prepared than the first responder to treat radiological, chemical or biological patients. Nationally, the receiving hospital system is brittle, vulnerable and may likely be incapacitated by any mass casualty convergence.

Infrastructure: Communications, Power, Water, Global Navigation System and Other Support

One of the most complex, and poorly understood, threats to emerge in recent years is that of infrastructure attack. This threat, wherein the infrastructure of a community is attacked, is potentially one of the most insidious that may have to be dealt with.

Examples of this type of attack include jamming the 911 system, knocking out power substations and/or telecommunications nodes, causing traffic jams at key locations coupled to false reports of incidents or items of public interest and even infiltrating the Emergency Alert System with false but authenticated reports. Jamming or simulating radio communications providing information and coordination to public safety professional might be particularly effective. All of these, many based on advanced technology and/or "cyber-attack" represent a new and potentially deadly threat that most local communities, and even most federal agencies, are unprepared for.

The goal of many of these attacks is to disrupt the existing response system, a system that might potentially be tenuous in the event of a major incident. This disruption and attack, while not necessarily resulting in casualties directly could potentially result in significant secondary problems.

In general, it is believed that these infrastructure attacks would occur in combination with other, more direct attacks and be designed to augment and enhance their effects. However, this need not be the case.

To prepare for these types of incidents, efforts should be made to make all infrastructure systems as redundant and robust as possible. The recently completed Presidential Commission on Infrastructure Protection study addresses these significant challenges.

OBSERVATIONS

A significant difference exists between Civil and Military training/exercises and experience. Within the military the focus is on training, preparedness and exercises, designed to provide for the pinnacle of performance should any of these resources and/or skills be required. In general (with the exception of the special operations communities that maintain one of the highest operational tempos in the military) very little real world experience is gained.

In contrast to this, however, is the first responder community which exists at the opposite end of the spectrum. With first responders, the majority of their training occurs on the job performing the duties in reality, not in exercises. Further, the small amount of training time that is available is overtaxed as it is. The majority of the training for first responders occurs almost as an apprentice program where they learn on the job.

This dichotomy in performance, attitude and, most especially, available resources causes considerable consternation and confusion between these two disparate communities. While they share some common ground, significant differences still exist.

In the military, redundancy and excess capacity exists in many areas because sufficient resources must be maintained to perform the defense mission. The infrastructure available to support military operations (R&D, planning, training and exercise facilities, long range planning) do not exist within the civilian first responder community. Even the largest departments (New York City, Los Angeles, Chicago) have no R&D department or funds for these efforts.

However, all this being said it must be noted that in the areas of public safety and emergency response there is no comparison between the experience that the first responder community has and that of the military. To put things in perspective, a typical battalion chief in a major metropolitan community (approximately equivalent to an O-3/Captain in the Army) may fight two to three structure fires in a day. A chief on a major military installation might not have that many in a year or even a career. The same comparison holds true for other incidents.

Of particular note is the emergency medical arena. In general, emergency physicians do added duty in civilian ERs because that is the only way they can maintain appropriate levels of skill. In an inner city an ER may have 1-3 high velocity gun shot wounds a night, many using standard military weapons. Therefore, in order to maintain the skills needed to treat combat injuries ER physicians work and function with their civilian counterparts.

There is an analogous but somewhat different problem with medical corpsman. While military physicians are licensed to practice anywhere in the country, corpsman and medics are not. The military does not encourage obtaining EMT certifications and the civilian community does not recognize military medic training. As a result, this important occupation in the military has a great deal of difficulty maintaining sufficient practical experience. This problem is being addressed, however, by the special operations medical community in that they are now implementing, as part of their core curricula, a training program in which the students spend several months riding with civilian EMTs in cities so they can gain this valuable real world experience.

The overwhelming majority of defense effort is focused on pre-incident and, to a slightly lesser extent, on crisis management with minimal national effort on consequence management.

In general, the military and Federal Agencies view their role in combating transnational threats as focused on either the prevention of the threat from carrying out an operation or the direct intercession for crisis management following the incident. Issues such as training, intelligence, R&D, technology evaluation and deployment, doctrinal development and periodic exercises are all performed in preparation for or attempting to prevent an incident. During the incident, defense and federal intervention normally takes the form of direct action (hostage rescue, force of arms, perimeter security) or support (transportation, communications, etc.). Most of the consequence management aspects are confined to provision of supplies (food, pharmaceuticals, blankets, shelter) and skilled personnel (medical support, combat and civil engineers).

Unfortunately, in many of the anticipated transnational threat scenarios the local communities and public safety organizations will still be left to handle long term issues such as longer term life support that they are currently unequipped to handle. Further, destruction or neutralization of significant amounts of equipment is also a very real potential. It is probable that significant portions of the infrastructure (fire engines and ambulances, water supplies and even entire hospitals) could be rendered unusable in a chem/bio incident. This would not, however, alleviate the existing needs and missions assigned to this equipment and infrastructure.

Transnational threats will involve non-military assets and targets to an unprecedented level

Traditionally, at least domestically, civilian targets and infrastructure have generally been safe from most forms of political terrorism; it has mostly been constrained to military and/or government targets. However, today's changing geo-political climate, societal viewpoints and increase in transnational threats is based on simply causing destruction to draw attention as opposed to having better focused targets for aggression. These factors are changing traditional concepts. Further, a new class of threat, the economically driven, takes a much broader viewpoint of target viability.

The lack of a single coherent, well-defined and coordinated threat (i.e. the former Soviet Union) has resulted in significant DoD downsizing and reduction of assets and resources, especially in the support arena such as firefighting and emergency medicine. This reduction is resulting in greater reliance on non-traditional forms of support i.e. domestic first responders in proximity to military installations and federal facilities. Almost without exception every domestic military installation, and many overseas, have mutual aid agreements with the surrounding communities. This is due in part to the need for added support during incidents as well as the recognition that the communities and installations are mutually interdependent.

Many military and defense technologies do not map directly to civilian needs

Despite the seeming similarity of many military and civilian missions, significant differences nonetheless exist. These differences, while sometimes subtle can have very drastic and significant impact on the operation and integration of technologies and doctrine into operations.

As just one example, the demographics of the typical military population is basically personnel from 18-40 years of age in peek physical condition who receive regular medical care and are always up to date on various inoculations and required medications. However, in the typical urban community children, the old and physically handicapped are not merely anomalies but the norm.

For that reason, pharmaceuticals that are prepackaged and dosed (i.e. atropine and tupam autoinjectors), safety gear (masks) and other items cannot be directly used from military stocks on civilian populations. An equally important and applicable scenario exists with the USMC currently who now regularly deploy with stocks of insulin, diapers, baby formula and pediatricians due to the high incidence of dependent evacuations during their missions.

Another example deals with the issue of certification of equipment. Generally the Defense Department does not obtain Occupational Safety and Health Administration (OSHA) or National Institute of Occupational Safety and Health (HIOSH) certification for its equipment. As an example, OSHA does not recognize military chemical protection equipment, Military Oriented Protective Posture, Level 4 (MOPP4) gear, as being acceptable for civilian use. Yet nonetheless it is planned to provide this gear to public safety personnel in times of crisis. While they will use it during an incident, because of the lack of certification this gear will not be used for training and exercises due to the fact that any injuries may leave the community open to lawsuits for using unapproved equipment. This argument applies to a wide array of other items.

Consequence management is independent of cause.

Considerable discussion has occurred surrounding terrorist incidents and attribution. The most significant chemical incident in the last twenty years was the Union Carbide accident in Bhopal India in 1984 where more than 2000 people died in the first 24 hours, eventual fatalities totaled over 15,000 with a total of nearly 500,000 injured. While an industrial accident, it was nonetheless handled in exactly the same way as if it had been an intentional act (it should be noted that the same plant exists today in Virginia).

What this means in real terms is that while much of the discussions center around attribution and proper response, from the point of view of the first responder this is secondary; the consequences of the actions must be dealt with first.

RECOMMENDATIONS

Implement a standing panel to act as representative of the first response community to the Federal, Civil and Intergovernmental Agency Communities.

Currently, only one portion of the first responder community, law enforcement, is even loosely represented at senior levels of the federal government responsible for setting national policy and integration with the civil community. This occurs through the Department of Justice and the FBI. Neither the firefighting nor emergency medical communities have comparable representation, and even the law enforcement representation does not necessarily meet all of the requirements.

With the advent of the transnational threat and the concomitant realization that almost any response involving federal assets will involve local assets first, consideration and representation of the needs and environment of the first responder *must* be factored into further efforts. An example of what happens when this is not done can be seen in the difficulties in the implementation of the Nunn-Lugar-Domenici Program where, early in its implementation the goal of supporting the first responder was lost and emphasis was instead placed upon developing a federal infrastructure divorced from the realities of the first responder needs.

The Civil-Federal integration panel should consist of representatives from the various first responder communities (fire, law enforcement, emergency medicine). These members would be recognized experts from throughout the operational community with actual operational experience. Every effort should be made to avoid populating the panel with personnel who, while they may hold positions of authority in this community lack operational and relevant experience and knowledge.

The tasking of the panel would be to assist senior state and federal policy makers and agencies in the crafting and employment of legislation and policies designed to assist the first responder community. The goal would be to improve the application of effort and resources at the federal level to ensure that it truly meets the needs of the first responder community where needed.

Ex-officio members should include; the Commander, Director of Military Support, Director, Emergency Management Institute, Director, Occupational Safety and Health Administration and other members form government agencies that may have either interest or relevant experience. The committee should exist within the executive branch and provide support to all departments. The committee should be a de-facto member of any federal program having impact on the operations of the first responder community.

Implement a system to disseminate critical information and provide for first responder access to classified Federal data especially as it applies to threat warning.

On many occasions in the past, situations have arisen where the federal government had information that indicated the possibility of an event but, because it was classified only vague references could be made about it to the local public safety officials. This resulted in considerable frustration, consternation and outright anger on the part of the public safety officials. Consequently, a reticence to prepare for an incident as opposed to a heightened state of alert was sometimes engendered. While certainly important and not to be overlooked, national security and classification should not be an impediment to the protection and support of the American people.

A system should be implemented whereby public safety senior personnel (2-3 per community) would be issued federal security clearances so that they could selectively access classified material when needed. Since it is impractical to clear each one of their facilities nor expect them to access classified material sufficiently often to remain cognizant and knowledgeable of all the various procedures, their access would be strictly limited to material which would be accessed at cleared facilities (i.e. local FBI, Secret Service, US Marshall's, military and other qualified installations) and every time they access the material they would receive a briefing on its handling, safeguarding and care.

Public safety personnel would be notified of the need to review classified threat analyses either by personal visits from local agents or by unclassified e-mails or messages telling them to report to their local POC and access a particular piece of information that would be transmitted via secure means to their contact.

MOUs would be initiated between each local community and its cognizant support office defining how they could contact each other and agreeing to provide support. Personnel given clearances would be senior public safety personnel responsible for planning and direction of public safety effort but NOT political leaders (i.e. mayors, city councilmen, etc.) unless they had DIRECT oversight and responsibility for this mission. When each individual retires or otherwise leaves his position his clearance would automatically be terminated.

These clearances would need to be provided to approximately 120 different municipalities (the 120 largest in the country account for about 80% of the population) with an average of 3-5 people per municipality. Total estimated number of clearances would be less than 1000. This number is sufficiently small that existing programs for clearance investigation and granting could be used without undue impact on operations or cost. A new Presidential Decision Directive (PDD) would likely need to be drafted, and approved, by the executive branch with specifics on administering the information sharing program. In the event that multiple qualified federal offices exist in a given municipality and they cannot agree among themselves who should have the responsibility, the decision will fall to the FBI as to which office in any given area will provide support. FEMA could maintain a database of all communities, personnel and local agencies participating in this program and be responsible for ensuring that records are maintained and updated. FEMA could also be responsible for dissemination of information notifications but not for the classified material which will be the responsibility of the originating agency. FEMA will not necessarily have automatic access to the information provided.

Establish a single Point of Contact (POC) for access to information and support from the Federal Government for the First Response Community.

Currently almost every Federal Agency has an established program to deal with emergencies and crises, many of which directly impact the first responder. Further, many agencies have multiple programs, many mutually ignorant of others. Finally, considerable misinformation exists throughout the emergency management community as to proper responses plus "experts" continue to pop up almost daily.

To ensure the most accurate, timely and effective dissemination of information a single point of contact for first responders to call should be created. This POC would provide day to day information via a web site backed up by a 24 hour special hotline (suggestions for exercises technologies, recommended sources of pharmaceuticals, available resources) as well as providing a

validated, reliable source for emergency information (proper methods of decontamination, plume dispersal data, agent identification). Finally, this single POC would also act as liaison between the various federal response agencies and assets and the incident personnel. FEMA might be a good choice for the Federal point of contact

It is vital that during a crisis a single source of information exists and further, that the responsibility for coordinating the various federal assets be left to the federal government and trained personnel, not placed on the backs of already overburdened responder personnel on site at the incident.

Accept the Civil Community Incident Management System (IMS) as the standard for federal assistance to first responders and provide training to relevant military personnel in the IMS.

Currently, the Incident Management System (IMS) is the closest thing to an available standard that exists in the national public safety community. The IMS, as noted earlier, was developed as a result of the wild fires in California. It has since grown into an all-hazard method of coordinating and deploying various and disparate resources from a large number of sources including federal assets, state level resources and surrounding, though unconnected, communities.

The IMS will, by default, be the civil community C3 system that is used during a crisis by the local first responders. As such, it will be the system in place that the federal assets must adapt to and be able to function with. Unfortunately, little knowledge of this system exists within the military and federal assets that would directly support an incident.

To alleviate this lack of knowledge, any and all federal personnel, both military and non-military, who will be tasked to assist and coordinate response to a domestic emergency should be trained in IMS and it should be adopted as the doctrine for those resources directly tasked with supporting first responders. The system should be taught in the same program and concurrently with current training so that federal commanders will be able to interact with their civilian counter-parts, thereby improving operating efficiency during times of crisis.

A number of classes and programs, not to mention books and texts, exist on the IMS. These classes are taught throughout the country at various academies as well as by federal agencies such as the Emergency Management Institute within FEMA. The classes can be standardized and provided via distance learning through any of a number of different systems including the Veterans Administration, National Guard, and Active Reserves in DoD.

Implement an aggressive technology transfer program from DoD, DOE and other Agencies allowing for both development and deployment of relevant technologies and equipment.

Current regulations make it difficult to transfer equipment to local communities and first responders from federal or military stockpiles. Agencies tasked with directly supporting local responders have minimal understanding or input into the DoD Research, Development and Acquisition system. Consequently, development and deployment of technologies to support first responders is not optimized.

A formal method across the federal government to assess and provide for the input of government technology needs of the first responder should be set in place so that, where not in contradiction to the core missions of the national security community, these needs can be considered and implemented in the federal process. In many cases this input can benefit both the first responder and

the federal community as, in issues of public safety, the first responder community has vastly more experience than the federal agencies. Further, in the event that technologies and systems are deployed that meet the needs of the first responder they will very likely be adopted commercially. This will result in lower per unit costs, enhanced ability to provide support and logistics and also assist in the strategic goals of greater reliance on Commercial off-the-shelf (COTS) technology.

The National Security Community (primarily DoD) should implement a policy to actively seek out and obtain input and assistance from the first responder community, on a national level, to provide guidance, input and advice on Research Development and Acquisition activities that may have an impact on the first responders and their colleagues in the federal community. Further, every effort should be made to involve the first responder community in the Test and Evaluation (T&E) of new systems as there insight and resources could prove valuable for the federal community.

Once technologies are developed and deployed, or in the event that they are stockpiled by the military or other federal agencies, it is not practical for local communities to also stockpile. A formal methodology for the transfer of federal resources should be implemented. FEMA (with DoD assistance) should be given the responsibility to develop an efficient method of transferring or otherwise making available capabilities to respond to major crises. They have a sufficiently large base of administrative and bureaucratic personnel as well as having contact with many of the civil infrastructure organizations designed to provide this type of support.

Provide for a single, integrated training methodology focused on institutionalizing federal and civil training within the first responder community.

Current Federal policy, managed by the US Army Chemical/Biological Defense Command (CBDCOM), is focused at creating and directly providing specialized chemical and biological defense training to and within the first responder community. In spite of all the money spent to date, this role is still not being effectively fulfilled in large part due to a vast gulf between the training needs of the first responder and the training capabilities of CBDCOM.

Further, CBDCOM and the DoD in general, are unable, nor should they be required, to provide regular evaluation and standardization of training, periodic exercises and maintenance of performance and training records for the first responder community. Based on the current system, after initial training and a single follow up review approximately one year later the entire federal program for each city is fully completed and no plan exists for future federal training. If personnel are transferred or retire or a significant period of time goes by without retraining and exercises then the effort and money will have been largely wasted since any minimal capability will have been lost.

Instead, an effort should be made to institutionalize training to and within the first responder community. In accepting and embracing continually updated standards and institutionalizing this new skill set as part of their basic repertoire of skills and equipment, the civil first responders community readiness could be strongly enhanced. The defense community should focus on development of basic technologies, standards and curricula as well as providing specialized support and specific training, in areas such as dealing with weapons of mass destruction and consequence management.

To make this effective it is necessary to create some method by which the public safety community not only accepts but embraces and supports the need for specialized training and capability to deal

with unique, unconventional threats.

Another method is the thoughtful and planned provision of federal funds, coupled to a well thought out and implementable, long range, civil community strategy. Along these lines, adoption of an incentive program for the creation of new standards and capabilities within the civil community is one possibility.

Incentives could be provided in the DoD Tri-Care system for private contractor health care providers to maintain minimum skill and resource sets to meet the needs of unconventional crises. These requirements would include maintaining minimum numbers of staff meeting special training standards (similar to physicians being boarded and requiring continuing education units and regular updated training). This would be a minor modification and augmentation of the already existing system to verify and ensure proper training and that credentials are maintained. By having the existing system embrace this new training and certification methodology it becomes institutionalized and a regular part of the operational community and its day to day procedures. By leveraging existing capabilities and focusing effort and resources on augmentation and enhancement, much could be accomplished at reduced costs.

Once this system is accepted by the medical community it can be extrapolated, at the civil community level, to the fire and law enforcement arenas. The role of DoD in this would be as the conduit for incentive provision (through the Tri-Care Program) as well as providing basic information and standards for dissemination to the user community *through its own channels*. Once institutionalized and accepted, this process could continue with a minimum of support and funding.

Institute a program for providing experts and advisors to local communities as and when needed for the formulation of plans, programs, technology and advice on training and exercises.

With the new emphasis and public recognition of the threat posed by chemical and biological weapons, not to mention the increase in publicity associated with bombings and other acts of terrorism, we have witnessed an overnight abundance of "experts" on issues of counter-terrorism and domestic preparation. This sudden increase in overnight experts has been occasioned in large part to the large quantities of money that are being made available primarily through various federal programs.

The Federal Government should provide a cadre of experts and a method of validating credentials, at least those of former federal employees, so that local communities can be assured of receiving accurate, timely and expert advice. Further, a capability should be made available which allows local communities to access expert information and consulting from professionals in the fields of public safety and counter-terrorism. These must be experts who have passed rigorous training requirements the federal government should impose as well as having gained experience in real world crisis situations.

The consulting would include assistance in preparation of emergency response plans, planning of exercises and review of performance. Assistance in identification of competent, qualified professional services and information as well as providing on-site assistance and evaluation would also be incorporated.

The key would be to provide some form of assurance as to the validity and accuracy of the information provided to the communities to ensure that it is, in fact, the best and most accurate data

available and that the plans are based on reality and supported by validated information and intelligence.

Provide standardized, realistic training information and goals for first responders: The First Responders Handbook.

As a result of the sudden burgeoning interest, shortage of accurate, reliable and useful crisis response information has recently occurred. In just one recent example, the Atlanta/Fulton County Fire Rescue Department recently conducted an experiment and exercise where they were trying to define what is required to perform successful and effective chemical decontamination of mass casualties. In this experiment they set up several fire trucks with various arrays and configurations of water supply and flow and had people walk through them; the goal was to determine the most effective and expedient manner to perform chemical agent decontamination on large numbers of people. Georgia red clay (that the volunteers rolled around in) was used as the chemical stimulant.

While very obvious and readily available (at least in Georgia), red clay is not necessarily the best stimulant for VX or Sarin to determine the effectiveness of a decontamination method. Nor should individual departments and communities be required to determine on their own what methods are or are not effective.

A handbook and database of lessons learned and factual and/or validated information should be generated and widely disseminated to the first responder community. This handbook should be reasonably short and specific and designed to provide basic information that a first responder might require in responding to an incident. It should include data on the three basic tasks that the first responder must perform in responding to an unconventional incident:

- Recognition that an unconventional incident is underway
- Immediate notification of proper authorities to provide assistance in dealing with the incident
- Skills, techniques and available or field expedient technologies and resources to help maintain the safety of responding personnel, reduce or prevent loss of life and minimize destruction to property

Information in the handbook might include (but not be limited to);

- Early warning signs for detection and human exposure to chemical or biological agents
- Recognition signs that an unusual situation may exist at some facility (growth vats usually found in facilities to produce beer, large quantities of chemicals, special hardware, etc.)
- Expedient and effective means of both chemical and biological agent decontamination
- Considerations in responding to incidents such as near real time detection and classification of chemical or biological agents
- Other considerations such as dealing with potentially hundreds to thousands of exposed individuals.
- Points of contact for the sources and/or experts associated with unusual chemical,

biological or radiological agents

- Dealing with large masses of refugees for extended periods of time

The handbook and related database updates might be made available on an internet web site so that it can be distributed to appropriate users.

Further, a means for different agencies and cities to share lessons learned, experience and questions could also be provided. Both civilian and federal agencies have vast amounts of experience and knowledge that, for a variety of reasons, is not yet being effectively disseminated.

It is recommended that the USMC Chemical/Biological Incident Response Force (CBIRF) take the lead, in coordination with the U.S. Army CBDCOM, in the development of this handbook since they are both currently very knowledgeable in field operations dealing with joint military/civilian situations as well as having developed an effective rapport with the civilian public safety community. This effort could be coordinated with various relevant professional organizations (i.e. International Association of Fire Chiefs (IAFC)) to ensure that information is relevant, useful and usable by the first responder community.

Resolve conflicts between various federal agencies, as well as internal to DoD, on issues of leadership, support, training and response.

On some city training occasions, the internal conflict between various federal agencies, most notably within Defense, has spilled over into the joint and coordinated operations with first responders. It is patently obvious that there is still considerable turmoil within the federal government on how to deal with this nation-wide training, awareness and readiness effort.

This turmoil is directly effecting the capability and readiness of federal resources to support first responders as well as creating a significant and negative perception of the capability of the federal government to assist, protect and serve its people. The issues of who is in charge, what their missions are and how they will be employed must be resolved and steps taken to see to it that the internecine bickering ceases once and for all.

Sources of confusion seem to reside in two principal areas; the debate between the Director of Military Support (DOMS), CBDCOM and CBIRF and the issue of roles and missions between the FBI and everyone else. DOMS, CBDCOM and CBIRF need to develop an effective working relationship. Similar problems exist in the R&D and acquisition aspects as well. Several different agencies are working on similar or parallel efforts to address the protection, sensing and response needs of the nation. These difficulties also exist between agencies.

Where practical, obtain certification and approval for use in civilian environments of military equipment and personnel.

While it is generally recognized that during times of crisis any action required to safeguard the lives of people will be taken this does not necessarily apply in time of exercise and training. This dichotomy results in the possibly that equipment, skills and resources will be applied during a crisis and no experience in their employment will be have been realized on the side of the civil first responder or the state/federal responders.

As one example, constant discussion occurs about providing DoD chemical protective equipment to first responders for their use. However, this protective equipment (e.g. MOPP4 suits) is not approved by either OSHA or NIOSH. Consequently, in the event that communities try and use the DoD gear during a real event and someone is injured, or worse, they may be subject to costly and lengthy litigation. Nonetheless, this DoD equipment *will* be used in a crisis should it be available.

This same situation occurs in the realm of skills and expertise. Currently, military medics are not certified by any of the professional certification organizations that are recognized by various state and local governments. As a result they are unable to practice or exercise with their civilian counterparts. Nonetheless they will be employed in a mass casualty incident should they be needed.

The FEMA might issue a broad order which stipulates that any equipment procured by the federal government that might possibly be used in times of crisis to support joint civil/military operations must be evaluated for its ability to be certified by relevant civil certification and standards agencies so that it can be safely and legally used in training as well as time of crisis. The same should be applied to medical and related skill areas.

Provide a straightforward, consolidated and rational method of monetary support for first responder training, preparedness and response.

Currently a myriad of different programs exist, with concomitant funding, to provide assistance to first responders. The preponderance of these programs, many under the heading of counter-terrorism, are so extensive that in a recent GAO report[*] it was found that an accurate accounting could not even be made of the number of programs, their costs or effectiveness.

A single federal program management agent for the support of first responders needs to be designated to coordinate all efforts directed at this area. While it will not change the fact that, as a result of the extremely broad nature of the mission many different agencies will be involved, some attempt at coordinating these efforts must be made.

While FEMA has not traditionally performed this mission they are nonetheless the obvious and, with proper guidance and oversight, potentially most effective agency. The National Institute of Justice currently performs this service for the law enforcement community, along with the Department of Justice but they have little or no knowledge of either the firefighting or emergency medical communities. These efforts need to be focused and should have the assistance of the advisory board discussed earlier.

Take greater advantage of potential information resource in first responder community.

Today's changing global political climate has had a significant impact on many aspects of modern society. In one of the most drastic, the enhanced and more readily accessible global internet communications system and infrastructure has resulted in a closer and smaller world, information wise, that at any time in history. Further, this coming together in information sharing is accelerating at an astronomical rate. This has resulted in more diverse and geographically distributed businesses and organizations and has made it possible to coordinate truly world spanning efforts by ever smaller organizations and entities. While a positive change in many ways, it has also resulted in the

[3] Combating Terrorism: Spending on Government wide Programs Requires Better Management and Coordination (Letter Report, 12/01/97, GAO/NSIAD-98-39)

ability of smaller and smaller, less sophisticated entities to engage in global crime, narcotics and terrorism. Geographic distance and unreliable communications are no longer a burden to today's criminal and terrorist.

As a result, non-traditional sources of information can now be utilized to provide insight and early indications of potential criminal acts. One of these sources is the local public safety agency, especially law enforcement. The law enforcement community has an extremely well developed and effective human intelligence capability, one larger, broader and more experienced by far than many realize. While the domestic human intelligence system is focused primarily on domestic crimes, as a result of the ever integrating and diverse international groups in the United States, much information of an international scope can be developed through the use of domestic assets.

A program should be implemented to provide training to all public safety personnel on the important warning indicators or other information that may have a potential impact in local communities. This information training should be provided to all public safety personnel. Concomitant with this should be the implementation of a central clearinghouse for domestic intelligence so that data may be correlated, compared and factored into intelligence and situational analysis. *No efforts to gather intelligence beyond what occurs in normal day to day operations currently will be pursued but the data will be analyzed and correlated in a different and more effective manner to hopefully provide new warnings and insights.*

Very strict controls and safeguards must be put in place on this effort to ensure that constitutional rights and legal implications are properly respected.

Task the DoD Defense Science Board to perform a study of how technology can be harnessed to support the medical mission

The importance of medical support and technology, while acknowledged, is seldom given the priority or consideration it deserves. In the final analysis, the only important aspect of any crisis response and the subsequent consequence management is the number of lives saved. In this, given that a situation does occur, the medical intervention phase of the response will always be key.

Specifically, it is recommended that a study by a DoD Defense Science Board (DSB) advisory panel be performed to evaluate the current state of defense medical preparedness, available resources, existing strategy for future employment and R&D and technology to meet these needs. Concomitant with this should be an evaluation of the doctrine for employing new technologies and resources and how that will support the overall mission of military medicine.

The study would have two purposes; first, to identify where deficiencies exist and what changes should be made to current policy and second, to elevate the importance of the military medical mission so it is on par with the other aspects of military intervention and response. The study should be performed outside of the military medical hierarchy to ensure credibility and objective evaluation of the relevant points.

REPORT OF THE COMPETENCY PANEL ON CIVIL INTEGRATION AND RESPONSE

Panel Chairs

Mr. Michael Hopmeier
Mr. David Paulison

Panel Members

Mr. Jeff Abraham
Mr. Carlos Castillo
Mr. Phillip Chovan
Mr. Henry Christen
Mr. James Denney
Mr. Louis Guzzi, MD
Mr. Paul Maniscalco
Ms. Annette Sobel, MD

Government Advisors

Maj Gen Paul Carlton
CAPT Rob Carnes, USN
Mr. Christian Cupp
BG John Parker
Mr. Ray Polcha
Mr. Bob Ruth
Dr. Pat Vail

ANNEX A:
CIVIL INTEGRATION AND RESPONSE (CIR) PANEL MEMBERSHIP

The CIR panel was made up of respected professionals from the various civilian first response communities. These members included:

Michael Hopmeier, is currently the Chief, Innovative and Unconventional Concepts, Unconventional Concepts, Inc. He has spent the last 10 years of his career as both a technology analyst and high value program troubleshooter for a wide array of government agencies. His specialties include special operations/low intensity conflict, counter-terrorism, law enforcement, bio-medical technology and unconventional programs. He currently serves as the Director, Defense Technologies, Defense Alliance for Advanced Medical Technology, Operational Advisor to the DARPA Biological Warfare Defense and Mine Location Programs and Science Advisor to the USMC Chemical Biological Incident Response Force. He is currently collaborating on several programs to assist public safety community on addressing unconventional threats

Chief David Paulison, Metro-Dade Fire Rescue and Past President of the International Association of Fire Chiefs. Chief Paulison is Chief of one of the largest metropolitan fire and rescue services in the United States and an internationally recognized expert in the field of public safety. Chief Paulison has in his organization one of two internationally deployable Urban Search and Rescue Teams in the country as well as being one of the most vocal advocates for advanced technology and long range planning for the public safety community.

Mr. Jeff Abraham, Research Scientist in the Safe Guards and Security Technology Division of the Pacific Northwest National Laboratory as well as being a deputy sheriff with the Benton County Sheriff's office. Mr. Abraham has extensive experience in law enforcement, customs inspection and perimeter control, special operations law enforcement training and operational law enforcement issues. He is also a recognized expert on issues of special nuclear material trafficking and terrorism.

Assistant Fire Chief Carlos J. Castillo, Metro Dade Fire Rescue. Chief Castillo is currently the Assistant Chief for Operations in Metro-Dade and, as such, is responsible for managing and directing the departments operations. This includes Miami International Airport, the number two most heavily used international airport in the world. Chief Castillo has coordinated the department's involvement in the development of the system and procedures for international disaster response for the Office of U.S. Foreign Disaster Assistance and is a member of the International Search and Rescue Advisory Group under the auspices of the United Nations Disaster Relief Coordinators Office (UNDRO). Among other things, Chief Castillo helped to coordinate the disaster response to the Oklahoma City Bombing by being one of the first people activated by FEMA to assist in the management of this effort.

Deputy Chief Philip Chovan, City of Marietta Fire Department. Chief Chovan, aside from his duties as a Fire Chief in a major metropolitan fire department is also an expert in hazardous material response and has extensive experience in generation of protocols involving chemical, biological and nuclear materials and terrorist attacks. Chief Chovan was also one of the principal planners for

emergency response for the 96 Summer Olympics in Atlanta.

Henry T. Christen, Director, Emergency Services, Okaloosa County, FL. Mr. Christen, aside from having been a battalion chief and Chief of Training for the Atlanta Fire Department is currently responsible for emergency management and coordination activities with Eglin Air Force Base, one of the largest military installations in the world. Besides having extensive experience in planning for and responding to mass casualty events (hurricanes) Mr. Christen also creates and implements several joint operations plans for dealing with HAZMAT, terrorist and military emergencies in coordination with Eglin and the area military installations. He is currently co-authoring the definitive text on the Incident Command System.

James P. Denney, Senior Executive, Los Angeles Bureau of Human Resources. Mr. Denney has worked his way up through the ranks of the Los Angeles Public Safety system with experience as a deputy sheriff, emergency medical technician, Rescue Company Commander, Emergency Medical System District Commander and as a staff officer, Bureau of Emergency Medical Services and finally as a senior staff officer in the Bureau of Human Resources. Mr. Denney is a recognized expert on emergency response and planning and has been involved in numerous joint federal/local operations, both live and exercises. Being involved in the planning and implementation of programs for one of the largest metropolitan areas in the country, Mr. Denney has developed an international reputation in the field of emergency planning and public safety.

Louis Guzzi, M.D., Dr. Guzzi is a triple-boarded in the fields of anesthesiology, critical care and internal medicine. Dr. Guzzi is also an internationally recognized expert in the fields of emergency medicine and medical response to terrorist/HAZMAT incidents. During his time in the Army Dr. Guzzi was a senior medical advisor, and technology and protocol developer, for US Special Operations Forces. Dr. Guzzi has extensive and unparalleled experience and field operations background in combat and emergency medicine, military as well as civilian. Dr. Guzzi has regularly been involved in the development and implementation of medical plans for unconventional threats and is deeply familiar with the issues associated with joint operations among the military services and the civilian community.

Paul M. Maniscalco, is a Deputy Chief with New York City Fire Department, Bureau of EMS. He has been Commander of the 8th Division (Brooklyn South and Staten Island), Commanding Officer, Special Operations Division and filled many operational posts in his career. Chief Maniscalco was the EMS Incident Commander at the World Trade Center bombing as well as having been involved in almost every major terrorist and major medical emergency in New York City in the last 19 years. He is also a Past President of the National Association of Emergency Medical Technicians. Chief Maniscalco is an internationally recognized expert in the fields of emergency response & planning, emergency management and public safety with special expertise in unconventional and terrorist operations implementation and planning. He is currently co-author of the definitive text on the Incident Management System.

Annette L. Sobel, MD, MS, FAAFP, COL, MC, USAFR. Dr. Sobel is currently a Senior Researcher at Sandia National Laboratories specializing in training and medical issues associated with terrorism and weapons of mass destruction. Dr. Sobel has extensive experience in emergency medicine, training and special operations. She has been a flight surgeon, occupational health researcher and specialist in human factors. Dr. Sobel initiated the Air National Guard's Care Force Team concept in New Mexico, designed to provide direct support to civilian disaster response. Dr.

Sobel is nationally recognized as an expert in emergency medical and terrorist response as well as having worked extensively in the preparation and employment of various training protocols designed to support the civilian public safety community.

ADVISORS

Aside from the actual members of the panel, the CIR was also supported by an excellent cross section of military and government advisors. Included among this auspicious group were:

Major General Paul K. Carlton, USAF, Commander, 59 MDW. General Carlton is a leader in the field of military emergency medicine and is currently refining the medical support capability for emergency civilian support within the USAF. He is also supporting the development of new protocols and operational concepts for response to HAZMAT incidents.

Mr. Bob Ruth, Emergency Medical Preparedness Office, Veterans Administration, Major General, USAR. Mr. Ruth has been involved in the planning and implementation of the VA response to medical emergencies, both military and civilian.

Brigadier General John Parker, USA, Director of Operations, Office of the Surgeon General. General Parker has extensive experience in the deployment and operation of medical and emergency personnel in a variety of circumstances, both purely military and joint military/civilian situations.

CAPT Rob Carnes, MD, USN, USMC Commandant's Warfighting Laboratory. CAPT Carnes is one of the principal advisors to CBIRF and leading several efforts to develop chem/bio detection technologies for use in field/domestic operations.

Mr. Chris Cupp, Director, Research and Resources, Defense Technical Information Center. Mr. Cupp is an expert on information dissemination and research, two key areas in supporting the first responder community.

Mr. Ray Polcha, Naval Surface Warfare Center/OPNAV N-89.

Dr. Pat Vail, US Air Force Research Laboratory. Dr. Pat Vail is an expert on innovative technology application as well as being a leader in the field of directed energy technology and (.-Uubiquitous