Research Challenges in Combating Terrorist Use of Explosives in the United States

Subcommittee on Domestic Improvised Explosive Devices

December 2008

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
DEC 2008		**00-00-2008 to 00-00-2008**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Research Challenges in Combating Terrorist Use of Explosives in the United States	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **National Science & Technology Council,Subcommittee on Domestic Improvised Explosive Devices,Washington,DC,20502**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

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

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**48**	

About the National Science and Technology Council

The National Science and Technology Council (NSTC) is a Cabinet-Level body established by Executive Order on November 23, 1993, to serve as the principal instrument within the executive branch for coordinating science and technology policy across the diverse entities that make up the Federal research and development enterprise. Chaired by the President, the NSTC also includes the Vice President, the Director of the Office of Science & Technology Policy (OSTP), Cabinet Secretaries and Agency Heads with significant science and technology responsibilities, and other White House officials.

A primary objective of the NSTC is the establishment of clear national goals for Federal science and technology investments across a broad array of topics spanning virtually all the mission areas of the executive branch. The Council prepares research and development strategies that are coordinated across Federal agencies to shape investment packages aimed at fulfilling multiple national goals.

The purpose of the Subcommittee on Domestic Improvised Explosive Devices is to advise and assist the Committee on Homeland and National Security and NSTC on policies, procedures, and plans for Federally sponsored technologies to combat the domestic use of improvised explosive devices (IEDs) by terrorists. The scope of the Subcommittee encompasses assessment of technologies, standards, and science and technology policies of the entire counter-explosives domain: deterrence, prevention, detection, protection and response. The work of the subcommittee also serves to meet the research, development, testing and evaluation (RDT&E) coordination function assigned to the Secretary of Homeland Security in Homeland Security Presidential Directive 19 (HSPD-19), paragraph 9.

About this Report

IEDs are generally easy to develop, difficult to combat, and cause disproportionate harm (physical and psychological) to the citizenry. RDT&E options to assist in domestic IED efforts are plentiful, easily overwhelming the ability of government and industry to fund. This report outlines ten challenge areas where concentrated research can be most beneficial in combating IED use in the homeland, and is a summation of interagency efforts to analyze operational capabilities and gaps, as well as their associated research needs.

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF SCIENCE AND TECHNOLOGY POLICY
WASHINGTON, D.C. 20502

January 9, 2009

Dear Colleagues:

Terrorists have repeatedly shown their willingness and ability to use explosives as weapons worldwide, and ample evidence exists to support the conclusion that they will continue to use such devices to inflict harm.

In acknowledgement of this threat, the President issued Homeland Security Presidential Directive 19 (HSPD-19), "Combating Terrorist Use of Explosives in the United States," to deter, prevent, detect, protect against, and respond to terrorist use of explosives in the United States. Technology plays a crucial role in supporting each of these efforts, and has been a research focus for the federal government for several years.

This report, prepared by the National Science and Technology Council (NSTC) Subcommittee on Domestic Improvised Explosive Devices, outlines ten challenge areas where concentrated research can be most beneficial in combating IED use in the homeland. It is a summation of interagency efforts to analyze operational capabilities and gaps, as well as their associated research needs. By developing a common planning focus for departments and agencies, we will be able to advance counter-IED technologies at a far greater pace than would otherwise be possible.

Federal and private investment on these priority topics will provide the greatest benefits to our first responder community as they work to keep us safe in our daily lives.

Sincerely,

John H. Marburger, III
Director

Executive Summary

Terrorists have repeatedly shown their willingness and ability to use explosives as weapons worldwide and there is ample evidence to support the conclusion that they will continue to use such devices to inflict harm. In acknowledgement of this threat, the President issued Homeland Security Presidential Directive 19 (HSPD-19), "Combating Terrorist Use of Explosives in the United States," which establishes overall national policy, and calls for the development of a national strategy and an implementation plan to deter, prevent, detect, protect against, and respond to terrorist use of explosives in the United States. The Department of Justice (DOJ) and the Department of Homeland Security (DHS), in coordination with the Department of Defense (DoD) and other interagency partners, developed the National Strategy to Combat Terrorist Use of Explosives in the United States and the HSPD-19 Implementation Plan, which provide a way forward.

Both the National Strategy and the Implementation Plan highlight the importance of a coordinated approach to a counter-IED (C-IED) RDT&E program. The co-chairs of the NSTC CHNS, with concurrence from the Office of Science and Technology Policy (OSTP) and the Homeland Security Council (HSC), established the Subcommittee on Domestic IEDs (D-IED SC) to serve as the formal mechanism for this coordination. The membership of the D-IED SC comprises representatives of the organizations in the Federal government that have responsibilities in the area of countering the terrorist use of IEDs.

The D-IED SC developed this report to describe the high priority science and technology challenges to be addressed. The operational needs identified by the DHS Office for Bombing Prevention (OBP) within the Office of Infrastructure Protection (IP) as part of the development of the HSPD-19 Implementation Plan, and supplemented by input from the members of the D-IED SC, formed the starting point for gap identification.

The D-IED SC recognizes that part of the solution to improving our security relative to IEDs lies in changes to tactics, techniques, and procedures (TTPs), or policy. Furthermore, many of the needs identified are already being addressed in other interagency coordination bodies, such as the NSTC Subcommittee on Biometrics and Identity Management. The D-IED SC members focused on needs that can be met by development of scientific and technological solutions. Each of the needs in the consolidated list was assigned one of the following priorities:

- Critical: Must do and time critical
- Necessary: Needed but not time critical
- Recommended: Value added feature or enhancement

Ten needs were determined by the D-IED SC to fall into the Critical category.

- C-IED Network Attack and Analysis
- Detection of Homemade Explosives
- Standoff Rapid Detection of Person Borne IEDs
- Vehicle-borne IED Detection
- IED Access and Defeat
- Radio Controlled IED Countermeasures
- IED Assessment and Diagnostics
- Waterborne IED Detect and Defeat Systems
- IED Warnings
- IED Threat Characterization and Signatures

The descriptions of the needs contained herein form the basis upon which the Federal agencies with responsibilities in the C-IED effort will build their programs. This report will also serve to focus the government partners in academia, private industry and other governmental entities on the development of science and technology to meet these needs and will foster interagency collaboration and partnering.

Table of Contents

Introduction

The United States is a nation at risk from new and evolving threats. The new, and not so new, forces engaged in terrorism have studied our approaches to security and have developed strategies designed to take advantage of our security shortfalls. Terrorists have repeatedly shown their willingness and ability to use explosives as weapons worldwide, and there is ample evidence to support the conclusion that they will continue to use such devices to inflict harm. The threat of explosives attacks in the United States is of great concern considering terrorists' demonstrated ability to make, obtain, and use explosives; the ready availability of components used in the construction of Improvised Explosive Devices (IEDs); the relative technological ease with which an IED can be fashioned; and the nature of our free society.

Homeland Security Presidential Directive 19 (HSPD-19), "Combating Terrorist Use of Explosives in the United States," establishes the overall national policy, and calls for the development of a national strategy and an implementation plan for the deterrence, prevention and detection of, protection against, and response to terrorist use of explosives in the United States. The Department of Justice (DOJ) and the Department of Homeland Security (DHS), in coordination with the Department of Defense (DoD) and other interagency partners, developed the National Strategy to Combat Terrorist Use of Explosives in the United States and the HSPD-19 Implementation Plan, which provide a way forward that streamlines and enhances current activities, thereby reducing conflict, confusion, and duplication of effort among interagency partners.

HSPD-19 designates DHS as the lead agency for coordination of research, development, testing, and evaluation (RDT&E) projects related to combating terrorist use of explosives and IEDs in the homeland, and the Implementation Plan appoints DHS Science and Technology Directorate (S&T) to coordinate interagency advancement of priority technology capabilities.

Both the National Strategy and the Implementation Plan highlight the importance of a coordinated approach to a counter-IED (C-IED) RDT&E program. The co-chairs of the National Science and Technology Council (NSTC) Committee on Homeland and National Security (CHNS), with concurrence from the Office of Science & Technology Policy (OSTP) and the Homeland Security Council (HSC), established the Domestic Improvised Explosive Devices (D-IED) Subcommittee (SC) to serve as the formal mechanism for this coordination.

The D-IED SC is co-chaired by Dr. Ruth Doherty (DHS S&T), Mr. Jeffrey David (Technical Support Working Group (TSWG)) and Mr. Duane Blackburn (OSTP). The membership of the D-IED SC comprises representatives of the organizations in the Federal government that have responsibilities in the area of countering the terrorist use of IEDs. The following organizations have been actively participating in the work of the D-IED SC:

Department of Commerce (DOC):
- National Oceanic and Atmospheric Administration (NOAA)

Department of Defense (DoD):
- Army Asymmetric Warfare Office (AAWO)
- Army Research, Development and Engineering Command (RDECOM)
- Joint Improvised Explosive Device Defeat Organization (JIEDDO)
- Office of Naval Research (ONR)

Department of Homeland Security (DHS)
- Customs and Border Protection (CBP)
- National Protection and Programs Directorate, Office of Infrastructure Protection (IP), Office for Bombing Prevention (OBP)
- Science and Technology Directorate (S&T)
- Transportation Security Administration (TSA)
- Transportation Security Laboratory (TSL)

Department of Justice (DOJ)
- Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF)
- Federal Bureau of Investigation (FBI)
- National Institute of Justice (NIJ)

Department of State (DOS)
Intelligence Community (IC)
Office of Science and Technology Policy (OSTP)
Technical Support Working Group (TSWG)
U. S. Postal Inspection Service (USPIS)

Operational Needs: Prioritization Process

One of the first activities undertaken by the D-IED SC was the prioritization of operational requirements or needs. The process employed and the results are presented below.

The D-IED SC started with results of the DHS OBP effort, conducted as part of the development of HSPD-19, to identify and prioritize operational requirements for C-IED science and technology consideration.

OBP gathered operational requirements from numerous sources including:

- DHS OBP-led capability analyses, conducted nationwide, to identify gaps in C IED capabilities of public safety bomb squads, public safety dive teams, explosives detection canine teams, and SWAT teams. The National Capabilities Analysis Database (NCAD) captures the results of these assessments, which provide an on-going measure of counter-IED capability improvements and often reveal gaps in technology or research requirements;
- Requirements submitted by other DHS components, including CBP, S&T, and TSA ;
- JIEDDO capability gaps;
- Input from subject matter experts in leadership positions, such as the National Bomb Squad Commanders Advisory Board (NBSCAB) and the Scientific Working Group on Dog and Orthogonal detection Guidelines (SWGDOG); and
- TSWG broad-agency announcements gathered through their interagency requirements process.

The examination of these sources yielded a list of approximately 180 operational needs, described with varying degrees of specificity. Subsequently the D-IED SC combined many of the similar technology needs and removed those that were not related to RDT&E (e.g., needs that were mainly related to tactics, techniques, and procedures (TTPs) or policy matters), or were already being addressed in other interagency coordination bodies, thus reducing the total number under consideration to 36. The D-IED SC members reviewed the consolidated list and assigned priorities to the needs. The allowable priorities were restricted to three categories:

- Category A (Critical) – Must do and time critical
- Category B (Necessary) – Needed but not time critical
- Category C (Recommended) – Value added feature or enhancement

Priority rankings of the list of 36 needs were submitted by the following organizations: AAWO, ATF, CBP, FBI, JIEDDO, NIJ, OBP, ONR, TSA and USPIS. The consensus of the D-IED SC was that ten of the needs belonged to Category A.

Appendix C provides the SC's consensus ranking for all 36 needs by Critical, Necessary, and Recommended priority.

Grand Challenges: A Framework for Action

The members of the D-IED SC identified the following 10 operational needs as the most critical priorities:

- C-IED Network Attack and Analysis
- Detection of Homemade Explosives
- Standoff Rapid Detection of Person-borne IEDs
- Vehicle-borne IED Detection
- IED Access and Defeat
- Radio Controlled IED Countermeasures
- IED Assessment and Diagnostics
- Waterborne IED Detect and Defeat Systems
- IED Warnings
- IED Threat Characterization and Signatures

Once addressed, the key contributions in science and technology outlined here can help achieve these needs for the Federal, State, local, tribal and territorial communities. These Grand Challenges require sustained Federal investment in research, testing, and the effective application of technology. They further outline the overall scope that scientists and engineers must address as they develop the technologies needed to combat the domestic use of explosives by terrorists.

The overall Grand Challenge in countering the terrorist use of IEDs can be summarized as providing the science and technology required to break the chain of events leading up to an attack and to deal with the aftermath, should an attack succeed. The challenges that follow are organized in the order shown in the lower half of Figure 1. The order does not reflect relative priorities.

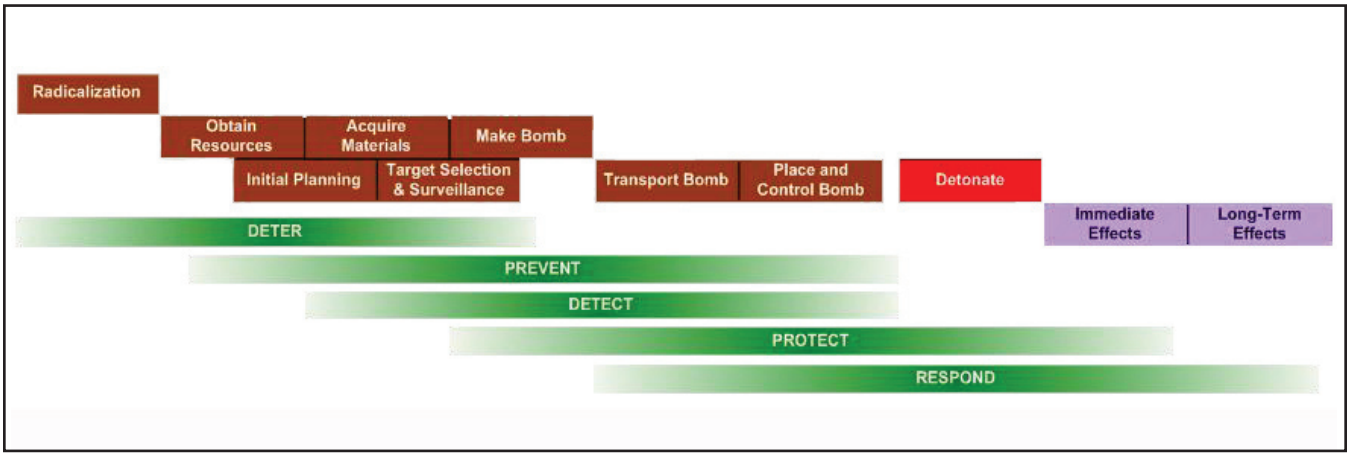


Figure 1: Interrupting the Terrorist Attack Sequence

Figure 1 illustrates the high level sequence of events involved in the planning and execution of a terrorist IED attack (top) as well as the government's response (bottom).

1 DETER & PREDICT

Counter IED Network Attack & Analysis

There is currently not an effective ability to identify active radicalized individuals or groups, or terrorist support networks within the United States, or reliably recognize activities that indicate preparations are underway for an IED attack.

An improved understanding and anticipation of IED threats will enable the United States authorities to predict potential actors, behaviors, targets, and timing more accurately for the purposes of interdiction, prevention, and protection.

Worldwide intelligence gathering activities and investigations of IED events have generated volumes of data related to the activities involved in planning for terrorist attacks, and to the tactics, techniques, and procedures (TTPs) used to execute bombings. We must draw on this abundance of information to improve our ability to identify the operational signatures of individuals, groups, or networks and predict potential targets and staging areas consistent with applicable law, including those laws relating to privacy and confidentiality of personal data.

To deploy our limited resources most efficiently, we must study the enemy as thoroughly as he has studied us, and strive to develop an ability to identify behaviors and TTPs that radicalized individuals or groups, and networks, might take under various conditions. This requires the development of models that reflect our adversary's behavior, capturing elements from radicalization to acts of terrorism, and including detailed patterns of behavior ranging from group formation through dissolution.

Challenges:

Today's analytical tools are based largely upon static models and lack a dynamic ontology or associated taxonomy. On the international stage, our adversary's agile and adaptive TTPs have succeeded repeatedly against this static approach. A dynamic computational framework that employs a science-based social and behavioral analytical approach is essential to understanding and anticipating better the IED threat.

The domestic environment is an open, complex, multi-cultural setting for which no fundamental baseline description of the society, based on sound social and behavioral scientific principles, has been established. The applicability of approaches used in foreign settings has not yet been demonstrated within the United States.

There is a need to improve analytical tools to better predict and prevent the enemy's successful use of IED threats.

Key Operational Considerations:

A robust predictive capability must support the following near real-time capabilities:

1. Recognition of radicalization-related indications and warnings through social science-based pattern extraction, analysis, and visualization;
2. Prediction of cultural- and adversary-based target and staging areas based upon CONUS and OCONUS patterns of adversary specific behaviors and TTP; and
3. Prioritization of intelligence, surveillance, and reconnaissance (ISR) assets through formulation and testing of customized hypotheses, given particular attack variables.

The capabilities should be flexible and scalable to ensure that the resulting tools and information are usable throughout the IED community of interest

including Federal, State, local, tribal, and territorial responders and policy makers. These capabilities should integrate privacy protections in all phases of design, development, and deployment.

Key Science and Technology Contributions:

The following science and technology efforts can contribute to the development of a computational framework that better reflects the adversary's agile and adaptive behavior:

Recognition of radicalization-related indications and warnings through social science-based pattern extraction, analysis, and visualization will require the development of:

- A data structure that integrates individual, group, and community-level indicators of radicalization and incorporates multiple modeling, simulation, and visualization techniques;
- Validated radicalization models that span the group formation life-cycle; and
- Radicalization-related data extraction and content analysis technologies.

Prediction of cultural and adversary-based target and staging areas, adapted from CONUS and OCONUS patterns of adversary specific behaviors and TTP, will require:

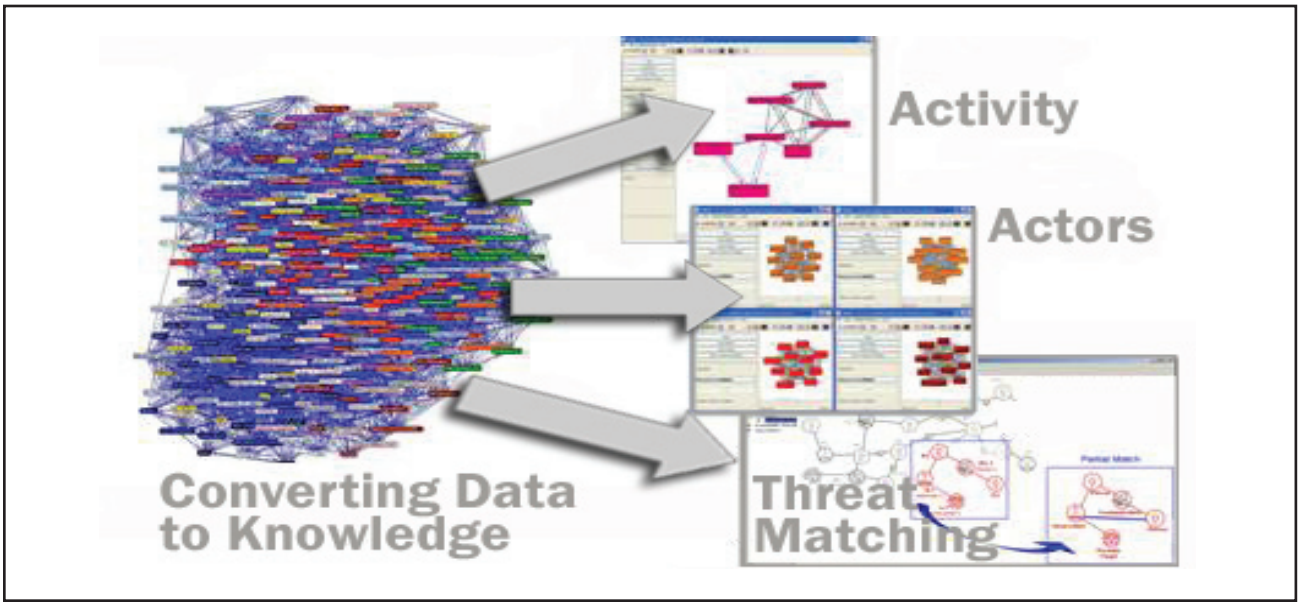
- A data structure that integrates behavioral, demographic, and cultural factors with traditional geospatial and network analysis;
- Validated targeting models (group, culture, and tactic specific);
- Validated staging areas models (group, culture, and tactic specific); and
- Near real-time capability to integrate and analyze emerging geospatial and behavioral data.

Prioritization of ISR assets through customized hypothesis formulation and testing will require:

- An interactive interface to support hypothesis generation, analysis, and visualization, of threat patterns, and to prioritize intelligence, surveillance, and reconnaissance assets;
- An ability to leverage the near real-time geo-behavioral analytical capability referenced above.

References:

a. HSPD-19, paragraphs, 4 (a), 5 (f), 7, 8



2 DETECT & DEFEAT

Detection of Homemade Explosives

The terrorist threat facing our nation's critical infrastructure can take many forms, including HMEs. In fact, for over 20 years, terrorists have used HMEs to target U.S. interests with notable success and devastating consequences. Considering likely events based on available intelligence and past experiences, HMEs will continue to be used by terrorist groups against U.S. interests due primarily to the wide availability of improvised bomb making materials, the ability to conceal large amounts of explosives, the ease of getting the IED to the target, the proliferation of bomb making instructions, and the history of success, which increases repetition and imitation.

The detection of the wide range of materials that can be used in constructing HMEs is challenging, and a successful solution may require multiple technologies. The integration of multiple technologies into a system that can give comprehensive coverage against known threats and be adaptable to cover new threats as they emerge will require a strong systems architecture approach from the start.

The term HME has been used to cover a wide range of materials from pure explosive compounds, such as TATP, that can be synthesized from readily available articles of commerce to home-made variants of explosives, such as ANFO, that are used in very large commercial blasting operations. The former is a very sensitive material, and so ordinarily is not made in large quantities. The latter is relatively insensitive, and can be made in very large quantities. In non-transportation applications, the detection of the precursors of the explosives in a way that allows discrimination between legitimate use of those precursors and illegal use to make explosives is extremely challenging.

There is a need for a means to detect Homemade Explosives (HMEs, historically known as Improvised Explosives [IEs[2]]) and their precursors in both screening and standoff applications in order to alert an operator or responder to the presence of materials in sufficient quantities to be a significant threat.

Challenges

The diversity of materials that can potentially be used to devise HMEs, and their normal presence in streams of commerce make detection of these materials a particularly difficult problem. Improvised explosive devices (IEDs) can be constructed from bottles of liquid medical essentials, flammables, industrial gases, explosives, or reactive/energetic chemicals. The main challenge for finding a solution to the detection problem is that the only common thread for these materials may be their energetic/reactive nature.

While DHS, ATF, and the FBI have agreed on nine explosives chemical precursors[C] as having the largest quantities in unregulated distribution, as well as the highest destructive potential, the detection of HME and their precursors cannot be limited to this set.

Key Operational Considerations

The solution must provide a capability to detect HMEs and their precursors in a variety of venues and situations. For use at a security checkpoint where inspection of persons is conducted, the envisioned users will be security personnel who are non-scientists, so the technology must be adaptable for use by people who have not been technically trained.

However, the need for HME detection goes far beyond screening in a transportation venue. There is also the need to detect HME precursors and their relative quantities in other environments in such a way as to allow a decision to be made regarding what action should be taken to protect the first responders and others in the vicinity.

At this time there is no stand-off or remote detection of classes of liquid explosives or flammables for use in screening and portal environments. There is also a need in security and operational law enforcement environments to detect explosives, including HMEs, from a safe standoff distance for a given quantity of explosives.

Sampling and detection methods are needed that are able to screen at a fast rate (nominally <5 sec) while maintaining a low false alarm rate (false positives) and a high enough rate of detection (true positives) to deter terrorist use of HMEs.

Ideally the sampling and detection methods should be useable in various modes of employment, with an emphasis on transportation (air) checkpoints (most critical due to the small amount of explosive needed to create catastrophic damage), but also for screening at large crowd venues, such as sports events. It would be preferable to have both a fixed and portable version of the equipment with real time response for screening people and baggage.

The need is immediate but the envisioned time horizon for the technology should be adaptable to meeting changing and emerging threats of the future.

Key Science and Technology Contributions

The introduction of the technological solution should enable the end user to maintain current tactics, techniques and procedures without major changes to their current practices. The deliverable sought for this requirement gap should include the following:

1. Underlying science for the sampling and detection of HMEs and their precursors that are applicable under a wide range of environmental conditions at stand-off and screening checkpoints
2. Systems architecture capable of addressing the known HME threats and extendable to new materials and/or classes of HMEs in the future.
3. Comprehensive characterization data on the relevant characteristics of vapor and surface contamination from known or expected HMEs to enable development of the sampling and detection methods.
4. A listing of materials and chemical classes the technological solution addresses and could be expanded to in the future.

References

a. HSPD-19: Sections 4b and 5e.
b. National Strategic Plan for U.S. Bomb Squads, December 2007, National Bomb Squad Commanders' Advisory Board, page 19, Section 7
c. Containing the Threat from Illegal Bombings: An Integrated National Strategy for Marking, Tagging, Rendering Inert, and Licensing Explosives and Their Precursors, National Academies Press 1998.

[2] The term Improvised Explosive (IE) has been used extensively in the explosives scientific community and the field of law enforcement to describe explosives that are formulated from readily available ingredients. It has also been extensively utilized in the historical underground, or anarchist, literature. Homemade Explosive (HME) has recently come into usage to describe the same types of materials, i.e., readily available materials, but places greater emphasis on the simplicity of fabrication methods. It is included in the WTI Lexicon and has gained international currency, so the term HME will be used here, but should be understood to include those materials also referred to as IEs.

3 DETECT & DEFEAT

Standoff Rapid Detection of Person-Borne Improvised Explosive Devices (PBIEDs)

PBIEDs are not new to the United States. In 1997, police in Brooklyn thwarted a double suicide bombing of the New York City subway system. Countering PBIEDs is a particularly difficult problem in a free and open society such as ours, where individuals are free to travel without leave or hindrance, and where the Fourth Amendment to our Constitution guarantees protection from unreasonable searches and seizures. Fourth Amendment rights pose particular challenges in the context of protecting the public from PBIEDs in a public venue, where they are most likely to be used.

Portal-based solutions to PBIED detection require proximity to the suspected bomber and the cooperation of the individuals going through the portal, thereby impeding traffic flow and causing people to collect in a relatively small area, making them potential targets for PBIEDs. Increased range for the detection of PBIEDS, either remotely or at standoff distances, is desirable to minimize the accumulation of people and to give additional time to react to a detected threat.

to handguns, with instantaneous effect. The problem is further complicated by the fact that PBIEDs are usually concealed, so the detection methodology must be able to cope with clothing or other cover as well as the possibility that the aspect presented to the detector may hide the device or other materials being probed.

PBIEDs are terror weapons that are typically employed in venues where large concentrations of individuals congregate, such as at major sporting events or in airports or shopping malls. The presence of a crowd makes the detection problem more difficult due to clutter and possible interferences.

Since they can have minimal metal content, PBIEDs are hard to detect with technologies that presume the presence of metallic components and rely on that feature for positive detection.

There is a need for a means to detect improvised explosive devices concealed on an individual's person at a sufficient distance, and in sufficient time, to allow actions to be taken to safely deal with the threat posed by that device.

Challenges:

The main challenges associated with PBIEDs are the need for detection before the bomber is in a position to carry out his mission and with enough time to allow an effective response once the PBIED is detected. PBIEDs can have a large lethal radius, much more than the 15 meters nominally assigned

Response to a PBIED is a significantly more complex undertaking, particularly for domestic law enforcement agencies, than dealing with other types of deadly force situations, such as those involving handguns. The PBIED is ordinarily concealed under clothing or other cover, and may not be exposed before the device is detonated. Whatever approach is taken to identification of a PBIED and subsequent incapacitation of the bomber must have a degree of certainty that is legally sufficient to justify the use of whatever means of incapacitation is employed, up to and including deadly force.

Key Operational Considerations:

A solution is needed that provides security personnel the ability to detect PBIEDs at a sufficient distance, to a reasonable degree of certainty, and in sufficient time, to allow reasoned decisions to be made and effective actions to be taken to safely deal with the threat posed by that device in a public venue.

That solution must be unobtrusive, because if the bomber knows that they are being observed, they are likely to detonate, causing as much damage as possible. Ideally, that solution will require no cooperation from the subjects under observation.

Many of the venues in which detection of PBIEDs will be done are outdoors and do not have controls over environmental conditions (temperature, humidity, precipitation, dust, etc.). Any proposed solution must be able to detect PBIEDs that have minimal metal content under a variety of clothing, in all weather, day or night, outdoors, and that may contain a variety of different types of explosives.

When the individual carrying an IED is in a crowd, the solution must be able to detect the device without impeding pedestrian traffic flow.

The solution must have a high probability of detection and low false alarm rate. False positives–an indication that there is a PBIED when there is not one–are acceptable within limits. False negatives–an indication that there is not a PBIED when there is one–are not.

The solution may provide stationary, portable or mobile adaptations, preferably all three.

The solution must be easy to use, require minimum training, and be cost effective.

Key Science and Technology Contributions:

Science and Technology should develop the stand-off capability described through a prototype stage, using an open competitive process to take maximum advantage of our nation's science and technology infrastructure. Industry should be encouraged to participate and team with other members of industry and with the Federal government, to ensure that this capability is commercialized and available to the local and State responder community, our first line of defense.

References:

a. HSPD-19 Requirement 5(d): Improving Capabilities to Combat Terrorist Use of Explosives within the United States.
b. High Priority Technology Needs, June 2008, Science and Technology Directorate, Department of Homeland Security, page 10, Counter-IED.
c. National Strategic Plan for U.S. Bomb Squads, December 2007, National Bomb Squad Commanders' Advisory Board, page 12, Section. 5.1.1; page 19, Section 7.

4 DETECT & DEFEAT

Vehicle-Borne Improvised Explosive Devices (VBIED) Detection

Over the last two decades, terrorists have used VBIED tactics (sometimes in sophisticated simultaneous attacks) to target global suppliers of critical resources and U.S. interests around the world. This tactic has impacted our government's ability to protect its citizens and workers of host nations, provide vital services, and has created the potential for using system disruption tactics as a method of strategic warfare. Gauging by the number of casualties and amount of property damage, VBIEDs have been the most successful means of terrorist attack both domestically and internationally, except for the September 11, 2001 attacks. Available intelligence based on global events and terrorist trends and past experiences, such as the bombing of the Murrah Federal Building, suggests that terrorist networks will most likely use VBIED tactics to attack our homeland. Factors contributing to the popularity of VBIEDs among terrorists are the wide availability of materials used to make IEDs; the ability to conceal large amounts of explosives; the ease of getting the vehicle to the target; the proliferation of bomb-making instructions; and a history of extensive experience and success, which increases repetition and imitation.

The problem of VBIED detection can be split into two operational categories: (a) checkpoint screening applications, wherein the detection system occupies a fixed location and observes all vehicles passing through the checkpoint for evidence of the presence of a VBIED; and (b) mobile or portable applications that may be needed to determine from a distance whether or not a suspicious vehicle is a VBIED. The applicable technologies for these two categories may be the same or different, but the implementation will differ based on operational considerations.

Challenges:

All existing solutions to remotely confirming the presence of a VBIED require proximity. No existing solutions provide the ability to detect a VBIED, with any reasonable degree of assurance, at a sufficient distance, and in sufficient time, to allow actions to be taken to safely deal with the threat posed by that device. A sufficient distance depends on the size and nature of the explosive device(s) carried in the vehicle, but can safely be assumed to be on the order of 100s of meters.

Bomb squads rely on visual confirmation, with either a bomb technician or, preferably, a robot, in close proximity to a vehicle. Confirmation will often require punching a hole in the vehicle and inserting a probe, risking premature detonation and placing the bomb technician in great danger.

There is a need for a non-invasive capability to detect vehicle-borne improvised explosive devices (VBIEDs) at a sufficient distance, and in sufficient time, to allow actions to be taken to safely deal with the threat posed by those devices.

There are numerous challenges associated with detecting VBIEDs. One challenge is that there is not a standard type of vehicle associated with VBIEDs. Thus any proposed solution must be applicable to

any of the types of vehicles likely to be encountered where the detection system is deployed. Vehicle selection usually depends on several factors:

- Ability of the vehicle to blend in with the normal traffic at the target
- Vehicle availability
- The security surrounding the intended target

For instance, "hardened" facilities with good physical security measures (including barriers to ensure significant standoff distances) may require the terrorist to use trucks with large, enclosed cargo areas. A vehicle of this size provides increased explosives capacities capable of generating damaging air blast effects over a large distance.

Secondly, there are no standard explosives associated with VBIEDs. If the proposed solution focuses on detection of the explosives rather than device components (e.g., wires, batteries, other electronic components), then the explosives detection technologies must be able to detect a spectrum of threats including HMEs. Additionally, these technologies must possess standoff detection capabilities in a fast-paced environment with dynamic backgrounds, and must be able to achieve low false alarm rates. Furthermore, detection systems cannot be static. They must include the capability to easily upgrade system algorithms to respond to new explosives threats and background conditions, as well as threats actively attempting to defeat the system and security measures.

Other challenges in detecting VBIEDs with explosive detection technologies:

1. The reduction of false alarm rates while maintaining detection capability is central to a solution for this need. Insufficient signal to noise on the detector, and interference with detection capabilities from frequently carried commodities, cause high false alarm rates and have the capability to obscure explosive threats. High false alarm rates can result in operators clearing or ignoring alarms, and have the potential to cause major delays to ground transportation.
2. Explosives with low vapor pressures may be particularly difficult to detect, depending on the basis of the detection technology.
3. Vehicle checkpoint throughput rates are low and detection technologies are not able to rapidly screen vehicles of various sizes (ranging from cars to trucks.)
4. There are difficulties in penetrating various materials/commodities to screen concealment areas in vehicles.
5. Depending upon the technology, passengers may not be able to stay inside the vehicle while it is being screened because of safety concerns. Furthermore, exclusion areas are required for equipment operators, vehicle occupants and the general public; this requires a large operational footprint.
6. Detection technologies tend to be expensive to purchase, operate, and maintain.

X-ray imaging systems are much less susceptible to false alarms than explosive detection technologies, but share many of their other limitations, including safety and high cost. They also tend to be large and cumbersome.

Key Operational Considerations:

The desired VBIED detection solution:

- Must provide rapid, non-invasive, standoff explosives detection capabilities across the threat spectrum, in a noisy environment, in sufficient time (minutes if not seconds,) for effective action to be taken to neutralize the threat at a sufficient distance to place the operator and target outside of the hazard zone for that category of device. Optimally, it also will identify the location of the explosives within the vehicle.

4 DETECT & DEFEAT

Vehicle-Borne Improvised Explosive Devices (VBIED) Detection

- For mobile applications should be compact enough to be transported on a bomb squad response vehicle or trailer, require minimal effort to set-up and operate, and have a small footprint. Ideally would be handheld or at least small and light enough to be deployed by a robot, or carried and set-up by an individual wearing a bomb suit.
- Should require minimal training to operate and maintain.
- Should be able to quickly screen suspect vehicles without having to scan each side of the vehicle separately.
- Must be able to quickly adjust screening capabilities to accommodate any size vehicle.
- Must not be affected by: the physical condition of the vehicle; emissions that are given off from the subject vehicle or any other vehicles in the vicinity; elements such as water, salt, dirt, sand and other grime that is commonly found on vehicles. It must be able to operate in all environments and weather conditions.
- Must not pose an unacceptable safety risk to the operator, bystanders or occupants of the vehicle being surveyed. Safety considerations, both with regard to operation and disposal of nuclear materials, would seem to make nuclear-based solutions unsuitable for use by State and local agencies.
- Must be cost effective.

Key Science and Technology Contributions

Science and technology should support the development and testing of VBIED explosives detection solu-

tions to standards that meet the minimum requirements of end users. Among the key contributions that may be provided by investments in S&T are

- development of concepts for rapid and non-intrusive imaging of the contents of a vehicle,
- approaches to standoff detection of IED components through electromagnetic signatures or other characteristics of the initiation system,
- development of methods of access that are minimally disruptive and have a low probability of initiating an IED accidentally,
- standoff methods of detecting explosives residues deposited on the vehicle,
- characterization of the likely distribution and quantity of explosives residues on vehicles bearing IEDs.

This is not an exclusive list and other S&T approaches are welcome.

References:

a. HSPD-19 Requirement 5(d): Improving Capabilities to Combat Terrorist Use of Explosives within the United States.
b. High Priority Technology Needs, June 2008, Science and Technology Directorate, Department of Homeland Security, page 10, Counter-IED.
c. National Strategic Plan for U.S. Bomb Squads, December 2007, National Bomb Squad Commanders' Advisory Board, page 12, Section. 5.1.2.; page 19, Section 7.

5 DETECT & DEFEAT

IED Access and Defeat

IED design is largely unpredictable, and IED defeat operations do not follow rigid courses of action. Today's devices, and those developed by future bomb makers, will likely contain not only a high explosive charge and improvised initiator, but a power source and activation mechanism that reflects state-of-the-art technology. However, as newer and more technologically advanced devices emerge, the simple device consisting of readily obtainable low explosive or pyrotechnic materials and a rudimentary firing mechanism will remain a deadly variant in the bombers arsenal. Therefore response technologies must address the entire spectrum of possible threats, not just the latest devices design and employment strategy.

Gaining access to critical components and materials is an integral part of the render safe procedure. This requires that IED defeat operators receive standardized training and equipment in order to access and perform render-safe procedures on all types of IEDs, including VBIEDs and RCIEDs.

Key Operational Considerations

Preservation of human life is paramount in conducting IED defeat operations. To the greatest extent possible, IED access and render-safe procedures are performed remotely in order to reduce risk of harm to personnel. In most instances, this is accomplished through the use of robotic platforms which are controlled by either radio or fiber-optic cables. However, the use of non-RF methods of remote control for robots and other EOD tools is required to address the RCIED threat.

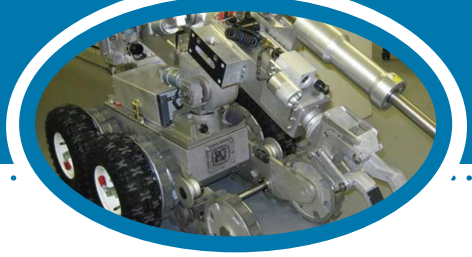
There is a need for technologies to access and defeat IEDs in a way that ensures the safety of IED defeat operators and first responders involved in bomb disposal operations.

Challenges

Bomb technicians and other IED defeat operators must penetrate the barrier materials or structures surrounding or containing the item of primary concern (gain access to), as well as the contents and components of suspect packages, in order to decide upon the selection of appropriate tools to disrupt or disable the device without causing the device to function as designed.

The range of IEDs that may be encountered is very broad, from tens of pounds of explosive that might be found in a leave-behind IED to thousands of pounds that might be present in a VBIED. The energetic materials used in the devices also range in sensitivity from fairly insensitive (e.g., ANFO) to extremely sensitive (e.g., TATP). Approaches to defeating one of these materials might initiate the other. A variety of tools applicable to the range of IEDs is needed.

Due to the potential for creation of an infinite number and variety of IEDs, bomb technicians require a wide range of tools in order to be prepared for all possible scenarios. These tools range from simple hand tools, to radiographic equipment, and in some cases, disruption charges that weigh hundreds of pounds when assembled. Therefore, in addition to remotely operated tools, IED defeat operators need the ability to quickly and easily transport tools, equipment, and the technician themselves to the incident site and subsequently down range. This is especially true for larger tools such as those used for VBIEDs.



Threats identified in urban areas, or areas where a high-order detonation would not be warranted, require careful planning for access and defeat. Every IED defeat operation carries some risk of a high-order detonation, but proper training of bomb disposal personnel help mitigate this potential. However, training alone may not ensure that IED defeat operators are able to quickly and easily select the most appropriate tool to render safe a given device, depending on the sophistication of the device; the complexity of the tool; and the experience level of the technician. Because of this, access and defeat tools should be sufficiently characterized to allow operators to select the appropriate tool based on the devices construction and its placement.

Key Science and Technology Contributions

Science and technology can contribute to the problem of access and defeat of IEDs in a number of areas by developing

1. approaches to access the device that are minimally disruptive and hence unlikely to cause unintended initiation of the IED.
2. approaches to protecting operators who must approach the IED to do manual defeat
3. methods of mitigating blast when defeat must be done in a location where collateral damage must be minimized (e.g., in an urban setting)
4. tools that can function in the presence of, and interoperable with ECM equipment.
5. defeat techniques that do not require substantial amounts of explosive (which carries with it a hazard of its own) or water (which may not be readily available in large quantities at the site).

References

a. HSPD-19 4 (b, c, d), 9; HSPD-19 I-Plan (Draft) Task Ref: 3.2.1, 3.2.2, 3.2.3, 3.2.4, 3.2.5
b. National Guidelines for Bomb Technicians (Revised 4/06)
c. National Strategy for U.S. Bomb Squads (December 2007) page 19, Section 7.
d. FBI Special Technicians Bulletin 2007-3: Vehicle Borne Improvised Explosive Device Response Bomb Squad Readiness.
e. Bomb Squad Response to Suicide Bombers and Vehicle Borne Improvised Explosive Devices: Categories of Situations and Strategies for Each Category

6 DETECT & DEFEAT

Radio Controlled Improvised Explosive Device (RCIED) Countermeasures

The RCIED (Radio Controlled Improvised Explosive Device) is a very real and formidable terrorist threat facing our homeland, as was demonstrated in the attack on a women's clinic in Birmingham, AL in 1998, among others. Radio Frequency (RF) has been used in a number of ways to trigger conventional IED(s) and VBIEDs. Electronic Counter Measures (ECM) systems to jam RCIEDs, which were developed initially for the military, are a necessary tool in accessing and defeating RCIEDs. The efficacy of ECM systems is continually challenged as terrorists are forever reinventing and redeveloping RCIED technology.

There is a need for improved means to jam radio-controlled improvised explosive devices (RCIEDs) within a meaningful radius of operation, to allow actions to be taken to safely deal with the threat posed by that device.

Challenges:

The RCIED threat continuously proliferates for several reasons. One being the wide range of commercially available radio-controlled equipment readily available and adaptable to IED triggers, another being the stand-off distance the RCIED gives to the terrorist. It is a technical challenge to meet the changing and evolving domestic and global RF threats. The domestic use of any ECM system must be in compliance with applicable laws and regulations. With each technical modification, responding to or anticipating a change in the RCIED threat, the potential exists to run afoul of regulatory constraints. Regulatory responsibility for the radio spectrum is divided between the Federal Communications Commission (FCC) and the National Telecommunications and Information Administration (NTIA). The FCC, an independent regulatory agency, is assigned responsibility for the regulation of non-government interstate and foreign telecommunications. The Presidential authority for Federal government RF spectrum use has been delegated to the Administrator of the NTIA, an operating unit within the Department of Commerce. Several other Federal Spectrum Stake Holders such as: FAA, NASA, and DoD also have concerns when it comes to the RF jamming.

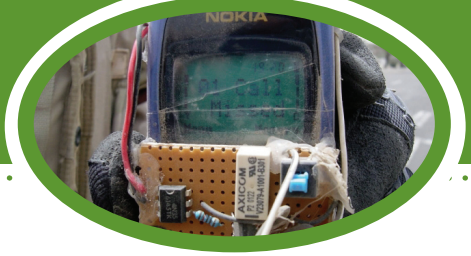
Key Operational Considerations:

The solution to this need must be deployable by the majority of medium bomb robots deployed with U.S. bomb squads, and, if need be, must be capable of being carried to the scene and emplaced by a bomb technician.

It must be able to preclude the radio control device from initiating a detonation within a meaningful radius of operation, without affecting radio frequencies outside of that radius to a high degree of certainty.

It must allow communication with deployed bomb robots and, if required, bomb technicians, operating within that radius of operation.

The solution must have meaningful mission duration, be cost effective and compliant with applicable regulations.



It must require minimal training and be easily employed by the average public safety bomb technician.

Key Science and Technology Contributions:

S&T contributions to RCIED Countermeasures include:

1) Optimization and characterization of the current ECM system on the standardized platform with the current antenna technologies. A hurdle in this effort to bring this capability to future cities is the confidence in the performance of the system. To properly build this confidence in federal spectrum stakeholders, sufficient data is needed in the characterization of the current ECM platform used by Public Safety Bomb Squads. Characterization, combined with new antenna technologies on the standardized vehicle platform will help expedite the ECM capability to future bomb squads.
2) Development of alternative approaches to interfering with the ability of terrorists to control the initiation of IEDs with electromagnetic radiation. This may involve more highly targeted intervention with the specific devices of interest, rather than jamming.

References:

a. HSPD-19 Requirement 5(d): Improving Capabilities to Combat Terrorist Use of Explosives within the United States.
b. 28 U.S.C. § 533; 28 C.F.R., § 0.85(l). DOJ/ FBI Counterintelligence and Counterterrorism Authority.
c. Executive Order 12333 – United States Intelligence Activities (December 4, 1981) (E.O. 12333).
d. PPD-39 – U.S. Policy on Counterterrorism (June 21, 1995).
e. National Strategic Plan for U.S. Bomb Squads, December 2007, National Bomb Squad Commanders' Advisory Board, page 13, Section. 5.1.3

7 DETECT & DEFEAT

IED Assessment and Diagnostics

Improvised explosive devices are not the product of logic, but of evolution; an inelegant process. Bomb makers do not choose the logically best design to meet their needs; they adapt what already exists. Because of this, being able to analyze IED firing systems and circuitry (diagnostics), and evaluate not only the potential for destruction, but likelihood of detonation (assessment), are critical to developing appropriate IED response plans and render safe procedures. Technologies for assessment and diagnostics performed on IEDs must undergo a sustained development, testing, evaluation, and improvement process in order to mitigate the impact of new and emerging IED threats, and offset the technological adaptations and defeat countermeasures developed by the enemy.

Key Operational Considerations

Assessment and diagnostic procedures should be performed outside the blast and fragmentation range of the IED in order to keep bomb technicians out of harms way. Technologies and techniques that require the technician to approach the device should allow the operator to safely collect useful information while minimizing the time required being in close proximity to the device. Furthermore, for a technology to be useable near an IED, consideration must be given to its functionality in an ECM environment.

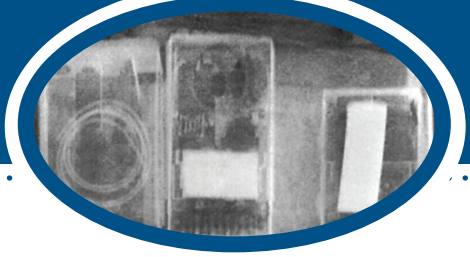
The personal protective equipment necessary for working near an IED limits not only movement, but vision and hearing as well. All equipment should be easy to operate while the technician/operator is in a bomb suit regardless of proximity to the device. The logistical burden associated with the tools and techniques for assessment and diagnosis of the IED should be kept to a minimum.

There is a need for technologies that can assess and diagnose new and emerging IED threats.

Challenges

The makeup of an IED is no longer limited to conventional explosives such as TNT. Devices designed and built by bomb makers today can incorporate improvised explosives and detonators, modified ordnance, and hazardous materials such as industrial toxic chemical, radiological materials, or substances that enhance the effect of the explosive materials. In addition, IED designs may span the range of simple pressure-plate devices to systems which use microprocessor controlled sensor circuitry. Assessment and diagnostic tools that provide qualitative and quantitative information on the threat is critical for planning access and defeat procedures.

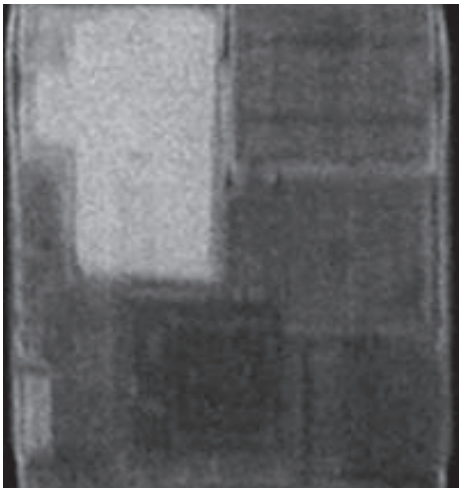
With respect to the detection of potential explosives contained within a device, special consideration should be given to identification of improvised explosives because of their potential sensitivity to influences such as heat, shock, friction, and static discharge.

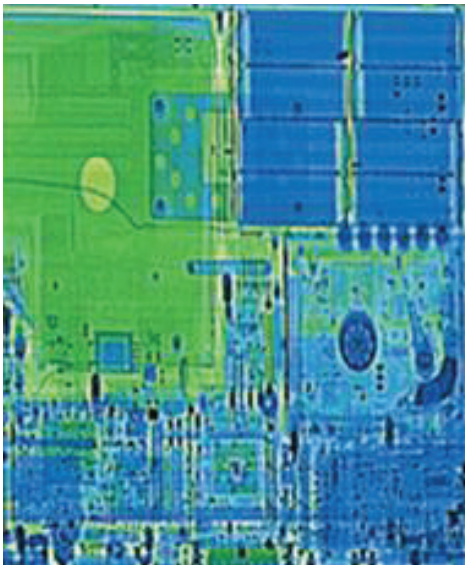


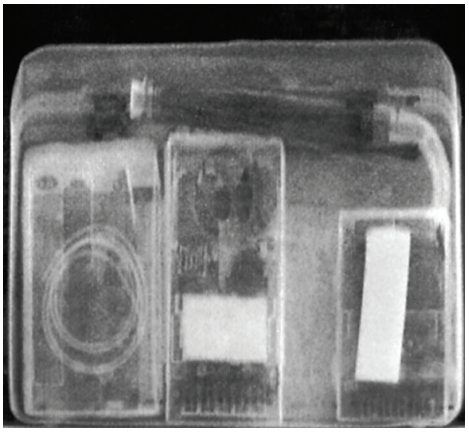
Key Science and Technology Contributions

Science and technology can contribute to the development of advanced assessment and diagnostic tools and techniques in the following areas:

- Novel imaging approaches to identify the precise location of IEDs whether by detection of the explosive filler, energized or un-energized circuitry, or some other yet to be identified signature.
- Approaches to stand-off diagnostics.
- Identification of characteristics of IEDs that provide information that can be used in the selection of an approach for defeating the IED.
- Approaches to assessment and diagnosis suitable for use by responders who may not have the scientific or technical background to interpret quantitative data, and will therefore be dependent on qualitative information.







References:

a. HSPD-19, paragraphs 4 (b, c, d), 9;
b. HSPD-19 I-Plan Tasks: 3.2.1, 3.2.2, 3.2.3, 3.2.4, 3.2.5
c. National Guidelines for Bomb Technicians (Revised 4/06)
d. National Strategy for U.S. Bomb Squads (December 2007), page 13, Section 7.
e. FBI Special Technicians Bulletin 2007-3: Vehicle Borne Improvised Explosive Device Response Bomb Squad Readiness
f. Bomb Squad Response to Suicide Bombers and Vehicle Borne Improvised Explosive Devices: Categories of Situations and Strategies for Each Category

8 DETECT & DEFEAT

Waterborne IED Detect and Defeat Systems

The terrorist threat facing our nation's critical infrastructure can take many forms including bombs used in a maritime environment. Over the last two decades, terrorists have used WBIEDs to target U.S. interests with notable success and devastating consequences, including the deadly suicide bombings of the USS Cole and a French oil tanker off the coast of Yemen. Considering likely events based on available intelligence and experience, terrorist groups will continue to use WBIEDs, on land and in a maritime environment, against U.S. interests.

Over two billion tons of domestic cargo move through U.S. ports annually, and a significant portion of domestically produced commodities and products are shipped by water. Nearly two-thirds of all U.S. wheat and wheat flour, one-third of soybean and rice, and almost two-fifths of domestic cotton production is exported via U.S. ports. Records indicate that approximately 4.2 million passenger cars, vans, SUVs and light trucks pass through U.S. seaports annually.

More than four million Americans work in port-related jobs that generate $44 billion in annual personal income and $16.1 billion in Federal, State, and local taxes. Port activity also contributes more than $723 billion annually to the Gross Domestic Product. Additionally, public ports serve national security functions. The DoD routinely uses public ports for the mobilization, deployment, and re-supply of U.S. armed forces. Many naval installations are based in U.S. ports, creating a unique set of cross-sector challenges.

Accessibility by water as well as land, proximity to vast metropolitan centers, and inherent integration into transportation hubs present additional multi-faceted security challenges for ports. We know that drug smugglers use divers as a means of attaching and retrieving contraband, and it is not a far stretch for us to recognize that terrorist combat swimmers and boat operators may act alone or in teams to attach explosive devices or limpet mines to ship hulls, bridge supports, dams, levees, locks, or oil rigs. Recently the Sri Lankan government was targeted successfully by a suicide SCUBA diver who wore, placed, and detonated a device against the hull of a fast patrol boat in Trincomalee Harbor, resulting in its sinking.

Challenges:

In the maritime environment, our ability to detect the presence of explosives or explosive devices, locate the explosive or device precisely, diagnose the device to determine its components and how they function, and defeat the device using the best tool to eliminate the threat is made more difficult by the water environment. Not only may there be more variables to consider than in a non-maritime environment, the presence of the water changes the implications of variables that are part of our understanding developed on land.

Within the Public Safety Dive Teams (PSDT) community there is a lack of national standards in both the equipment and training necessary to provide an effective response throughout U.S. ports, which puts both the diver and port at risk. A response must be successful in adverse operational conditions that may include unstable vessels or platforms, cold water, offshore locations, poor visibility, and the possibility that a device or hazard is entirely submerged.

Each of the various conditions under which bomb technician divers operate requires them to possess specific skills, tools, and standard operating procedures that currently do not exist nationally. To complicate this mission further, many PSDTs are created as a collateral duty responsibility, and therefore divers are often multi-tasked within their respective departments.

Recognized standards for tools and operating procedures do exist nationally for bomb technicians involved in non-waterborne render-safe procedures.

The development of those tools and procedures falls under the purview of the staff at the Federal Bureau of Investigation's (FBI) Hazardous Devices School (HDS). While HDS staff work in coordination with the Department of Defense and the NBSCAB to set standards, develop tools, and train render-safe personnel, this is the only such school or organization with responsibility for this function within the entire United States.

In recognition of the value of this existing set of national tools and standards, which are rare in any other public service, the FBI has initiated a process to begin to assess the training or actual deployment techniques currently being used by bomb squad divers across the United States. The FBI, in collaboration with DHS, has simultaneously developed and implemented a nationally consistent training process to equip PSDTs with the skills and procedures they need to operate more safely in the WBIED environment and to seamlessly integrate with bomb squad assets during a WBIED event.

To develop a national standard for WBIED operations, there is a need to develop a set of tools and operating standards that may become the subject of enhanced training for bomb squad divers at the FBI's HDS. This new set of tools and procedures will be integrated with existing and/or enhanced training for public safety dive teams in order to provide a single, vertically integrated approach to WBIED incidents in U.S. ports or other maritime infrastructure.

Key Operational Considerations:

U.S. Navy EOD technicians are currently the only personnel properly trained and qualified to render safe an underwater hazardous device (UHD). However, domestic response is not U.S. Navy EOD's primary mission, and nearly 70% of its forces are currently deployed in support of the Global War on Terrorism, reducing domestically stationed detachments to the minimum manning levels permissible to maintain operational status.

There is a need to protect our ports and waterways by being able to detect the presence of explosives or explosive devices, locate the explosive or device precisely, diagnose the device to determine its components and how they function, and defeat the device using the best tool to eliminate the threat.

The USCG is the Federal organization most responsible for domestic, maritime security. In addition to its normal shore stations, USCG maintains thirteen terrorism-focused Maritime Safety and Security Teams, established through the Maritime Transportation Security Act, that possess explosives detection canine teams, and has consolidated its diving resources into two Deployable Operations Groups (DOG), located in Norfolk, VA, and San Diego, CA. The USCG has some UHD search capability, but limited maritime or underwater explosive device preparedness and response capability.

In a number of areas of the country, public safety dive teams (PSDT) and their bomb squad counterparts have moved to develop local solutions to the capability gap represented by the issues previously

Waterborne IED Detect and Defeat Systems

described. Today, none of those programs has produced the capability that can replace a U.S. Navy EOD team in the WBIED render-safe role. Further, the responsibility for render-safe of waterborne military ordnance will likely continue to reside primarily with the U.S. Navy.

The response community in the maritime domain today expands to include those who have the daily responsibility for port security diving; their bomb technician diver counterparts who have ultimate local responsibility for handling render-safe issues within their areas of operation; and the U.S. Navy EOD technicians who will likely always remain the ultimate reach-back capability for WBIED response.

We must develop technology and associated training for public safety divers, bomb technician divers, and other dive resources who may respond to domestic UHDs, since we cannot expect U.S. Navy EOD technicians to continue as the sole providers of assistance to conventional dive teams possessing minimal render-safe capabilities. The ability to locate and validate possible threats is the minimum acceptable level of response.

Key Science and Technology Contributions:

Desired solution(s) will provide capabilities to detect, diagnose, and disrupt or disable IEDs, by remote, semi-remote, or manual means, in a maritime environment. Solution(s) must address IEDs attached to ship hulls at depth and devices attached to small crafts afloat that may be used themselves as explosive devices.

Where such IED placements affect maritime traffic, including shipping and passenger cruise ships, CIKR, national security activities, etc., solutions must address devices emplaced where the presence of water changes the buried or ground-emplaced characteristics of a classic device, e.g., in drainage conduits, wetlands, shallow areas of fresh or saltwater, on bridge supports, etc.

Solution development should provide material for developing threat characterizations, tool performance testing, and standards.

A plan for transition of DoD technology for State and local use will be included.

Related Requirements:

Maritime Operational Threat Response (MOTR) for the National Strategy for Maritime Security:

"DHS will plan for the prevention and detection of sea mining and swimmer operations in waters subject to the jurisdiction of the United States."

References:

a. HSPD-19 4 (b, c, d), 9
b. HSPD-19 I-Plan (Draft) Task Ref: 3.2.2
c. National Strategy for Maritime Security. September 2005

8

9 MITIGATE

IED Warnings

The terrorist threat facing our nation's critical and civic infrastructure can take many forms including vehicle bombs, suicide attacks, or combinations thereof. This includes attacks such as those seen in the Beslan School or the Moscow Theater, which combine armed attackers, hostages, and IEDs. In the event that IED attacks were to occur – or worse, that a campaign of terrorist use of explosives, employing such methods, were to be launched on U.S. soil – authorities must quickly provide the American people with accurate information about the nature of the threat. Authorities also must provide guidance on protective actions and precautions that Americans might take to improve security in their communities and reduce the risks to them and their families.

The United States has very little experience in dealing with an immediate threat of attack that could affect individual American citizens in their own communities. Likewise, civic officials have very little awareness or training in how to instruct the public properly regarding the safety measures they should take during terrorist attacks or similar extraordinary events. Officials' experience is generally centered on managing public information and security during serial murders or kidnappings; civil unrest, gang violence, and inner city crime waves; and rare events exemplified by the 1979 Three Mile Island event, the Unabomber attacks from 1978 to 1995, and the anthrax and sniper attacks in the Washington, D.C., metropolitan area in 2001 and 2002, respectively. Criminologists or terrorism experts serving local law enforcement or the FBI have formulated most instructions to the public, and senior law enforcement officials have issued them.

If terrorists stage a coordinated attack, or multiple attacks against the American people using IEDs, VBIEDs, or suicide bombers against targets within communities and public gathering places, the problems presented will be significantly more complex and will likely have national implications. In a free and open society, it is impossible to ensure the constant safety of people and the certain protection of targets against terrorist attacks. Nevertheless, there are clearly steps that authorities can and should take at the local, regional, and national levels to inform the public, and manage the security problem posed by terrorism. The ability to provide information quickly and accurately is critical to preserving public confidence at the local level and generating awareness, cooperation, and support of the public in identifying abnormal or suspicious events that might indicate imminent danger or precursor activities to an IED attack.

Challenges:

There are two challenges involved in this effort:

- Protecting the public from initial and successive IED events, especially in the face of a general lack of official knowledge of the unfolding scenario, and
- Maintaining public confidence in the face of potential threats. Public confidence is important in preserving public conviction at the local level and generating awareness, cooperation, and support of the public at the local level in identifying abnormal or suspicious events that might indicate imminent danger or precursor activities to an IED attack.

Key Operational Considerations:

The threat of IED attack is shared almost universally by U.S. communities and citizens, private sector enterprises and public sector agencies, and across the 18 sectors of the nation's critical infrastructure and key resources, and its private and public sector managers and operators. Consequently, the community of interest for this research effort includes public officials and agency leads across the range of U.S. jurisdictions and communities from the Federal, State, regional, and local levels.

The results of this project should prepare government officials, civic leaders, media representatives, law enforcement officials, and emergency managers to properly delineate and issue hazard and risk warnings to

the public, prior to an imminent or suspected IED attack, and provide appropriate protective actions and post-attack instructions.

Specific stakeholders in the results of this research effort include:

- Office of the President and White House Staff;
- Department of Homeland Security;
- DHS/FEMA;
- Department of Justice;
- Equivalent agency heads at the State, regional and local levels;
- Governors' offices nationwide;
- Local elected officials, e.g., Mayors and County Executives; and
- Local law enforcement, public safety, and emergency management officials.

- Consistent and repeatable methods to inform and employ the public in identifying suspicious circumstances or abnormal conditions in local communities that could serve as warnings to local authorities of terrorist attack planning or potential IED events;
- Development and testing of guidelines for government and civic leaders in issuing effective emergency communications in the event of an IED attack;
- Technology that rapidly will provide accurate status information from forensic and law enforcement agencies to government officials and leadership, and public safety and security personnel, with near real-time updates;
- Pre-planned responses and messages that have been crafted, analyzed, tested, and rehearsed by civic officials and members of the media and press corps to provide accurate instructions and reassurances to the public;
- Development of local models and simulation-based games to exercise first responders and local government leaders in potential scenarios and test courses of action to support and protect local populations;
- Development of simulations to analyze effects on transportation and public infrastructures, local economies, and tempo of civic life in the event of an IED attack or terrorist campaign employing IEDs, and to analyze and test alternate approaches to managing the consequences.

There is a need to identify effective methods to guide public officials quickly and to inform the American public accurately during conditions of heightened U.S. threat alert.

Key Science and Technology Contributions:

Research to support this need will focus on development of a data structure and analysis program (and accompanying training materials) that will support Federal, State, local, tribal, and private sector partners having specific roles and responsibilities within their communities for public safety and security against IED attack. Development of hazard and risk warnings to the public in imminent threat of, or immediately after, a terrorist IED attack will incorporate the following requirements:

- Detailed responses and methodologies to appropriately inform and protect the public during terrorist explosive attacks. This should involve members of professional press and media with local officials and emergency managers;

References:

a. HSPD-19 Section 4(a, d)
b. HSPD-19 Implementation Plan (draft) Task Ref: 2.3.4, 3.

10 CROSS-CUTTING

IED Threat Characterization and Signatures

We are devoting considerable effort and resources to addressing a great variety of capability gaps in relation to IEDs. Our contributions will yield a greater level of effectiveness if we build from a knowledge base of IED characteristics and of the consequences of their use under known conditions.

To develop the capability to counter IED attacks, we must integrate our understanding of two aspects of the threat – the actor and the tool. Despite the worldwide proliferation of IED attacks, little standardized data exists that can be used to characterize the construction of the IEDs, or the resulting blast effects under various conditions and methods of delivery. There is no commonly accepted set of test criteria on IED detonations or a database of recent performance data.

The IED community requires an ability to obtain, access, and analyze detailed and authoritative performance data on IED threat devices, based on the design, assembly, and detonation of IED threat devices in a laboratory and/or testing environment.

Challenges:

The following challenges limit our ability to characterize and understand the nature of IED threats:

1. Lack of unrestricted access to fully instrumented explosives test ranges has limited the capability to conduct multiple tests of IED devices under controlled conditions and to collect well-understood data.
2. The lack of a common lexicon and data standards for defining measurements, and storing and analyzing data, prevents us from comparing and using test results and analyzing previous, current, and future test data to determine overall effectiveness of C-IED solutions.

Key Operational Considerations:

Our ability to analyze IED threats requires common definitions and lexicon, a detailed process for testing and characterizing the performance of IEDs and IED countermeasures, the ability to simulate IED threats, and the development of IED threat models.

A repository of data, obtained under controlled conditions, is necessary to conduct the analysis required for this characterization and modeling. Collecting data on vehicles used as devices, and on devices in vehicles (person-borne, placed, etc.), will require a standard set of procedures for surface sampling to characterize the extent of surface contamination occurring during the IED construction process and an instrumented range to test small vehicles, with progression toward larger vehicles.

Results at all levels will drive current and future projects involving all partners with a stake in the IED Kill Chain

Analysis of test data will provide an understanding of why and how various components can be used in device construction, as well as measurements of the effects of blasts conducted under different physical configurations.

Key Science and Technology Contributions:

Threat characterization requires analytic tools that incorporate prediction and pattern assessment.

Science and technology can contribute to developing a comprehensive body of common standards by searching out the standards that may exist, evaluating their effectiveness, ensuring their consistency, and using them to develop additional necessary standards that are missing.

Scientific analysis of accumulated test data can provide an understanding of why and how various components can be used in device construction. Measurements of the effects of blasts conducted under different physical configurations can be used to model the consequences of IED blasts.

Correlation of standardized characterizations to post-event forensics and real-time event data will assist in identification of ongoing planning activities by the enemy.

The C-IED community requires an ability to obtain, access, and analyze detailed and authoritative performance data on IED threat devices, based on the design, assembly, and detonation of IED threat devices in a laboratory and/or testing environment.

Science and technology can contribute comprehensive instrumentation and instrumentation protocols and standards for existing testing facilities to provide reliable and well-understood characterizations.

References:

a. HSPD-19 I-Plan (Draft) Tasks: 3.1.2
b. HSPD-19, Paragraphs 8, 9

Conclusion

DHS Secretary Michael Chertoff recently noted that "When we prioritize IEDs as a focus, we are prioritizing what is far and away the greatest threat in the West with respect to terrorist attacks." The capability we have at our disposal today is limited, but science and technology can contribute to closing the existing gaps. The critical needs identified in this document will serve to focus the public-private discussion on the areas most in need of attention, and will foster through cooperation and collaboration the growth of a community dedicated to improving the security of our nation.

Appendix A: HSPD-19

February 12, 2007

Homeland Security Presidential Directive/HSPD-19

Subject: Combating Terrorist Use of Explosives in the United States

Purpose

(1) This directive establishes a national policy, and calls for the development of a national strategy and implementation plan, on the prevention and detection of, protection against, and response to terrorist use of explosives in the United States.

Definitions

(2) In this directive:

(a) "agencies" means those executive departments enumerated in 5 U.S.C. 101, independent establishments as defined by 5 U.S.C. 104(1), Government corporations as defined by 5 U.S.C. 103(1), and the United States Postal Service;

(b) "explosive attack" means an act of terrorism in the United States using an explosive;

(c) "explosive" means any chemical compound mixture, or device, the primary or common purpose of which is to function by explosion, including improvised explosive devices, but excluding nuclear and radiological devices;

(d) "improvised explosive device" or "IED" means an explosive device that is fabricated in an improvised manner incorporating explosives or other destructive, lethal, pyrotechnic, or incendiary chemicals;

(e) "NIPP" means the National Infrastructure Protection Plan developed pursuant to Homeland Security Presidential Directive 7 of December 17, 2003 (Critical Infrastructure Identification, Prioritization, and Protection)(HSPD 7); and

(f) "risk" means the product of credible threat, consequence, and vulnerability, as defined in the NIPP.

Background

(3) Terrorists have repeatedly shown their willingness and ability to use explosives as weapons worldwide, and there is ample intelligence to support the conclusion that they will continue to use such devices to inflict harm. The threat of explosive attacks in the United States is of great concern considering terrorists' ability to make, obtain, and use explosives, the ready availability of components used in IED construction, the relative technological ease with which an IED can be fashioned, and the nature of our free society.

Policy

(4) It is the policy of the United States to counter the threat of explosive attacks aggressively by coordinating Federal, State, local, territorial, and tribal government efforts and collaborating with the owners and operators of critical infrastructure and key resources to deter, prevent, detect, protect against, and respond to explosive attacks, including the following:

(a) applying techniques of psychological and behavioral sciences in the analysis of potential threats of explosive attack;

(b) using the most effective technologies, capabilities, and explosives search procedures, and applications thereof, to detect, locate, and render safe explosives before they detonate or function as part of an explosive attack, including detection of explosive materials and precursor chemicals used to make improvised explosive or incendiary mixtures;

(c) applying all appropriate resources to pre-blast or pre functioning search and explosives render-safe procedures, and to post-blast or post-functioning investigatory and search activities, in order to detect secondary and tertiary explosives and for the purposes of attribution;

(d) employing effective capabilities, technologies, and methodologies, including blast mitigation techniques, to mitigate or neutralize the physical effects of an explosive attack on human life, critical infrastructure, and key resources; and

(e) clarifying specific roles and responsibilities of agencies and heads of agencies through all phases of incident management from prevention and protection through response and recovery.

Implementation Actions

(5) As soon as practicable and not later than 150 days after the effective date of this directive, the Attorney General, in coordination with the Secretary of Homeland Security and the heads of other Sector-Specific Agencies (as defined in HSPD 7) and agencies that conduct explosive attack detection, prevention, protection, or response activities, shall submit to the President for approval, through the Assistant to the President for Homeland Security and Counterterrorism, a report, including a national strategy and recommendations, on how more effectively to deter, prevent, detect, protect against, and respond to explosive attacks, including the coordination of Federal Government efforts with State, local, territorial, and tribal governments, first responders, and private sector organizations. The report shall include the following:

(a) a descriptive list of all Federal statutes, regulations, policies, and guidance that (i) set forth agency authorities and responsibilities relating to the prevention or detection of, protection against, or response to explosive attacks, or (ii) govern the use of the assets and capabilities described in paragraph (b) of this section;

(b) an inventory and description of all current Federal Government assets and capabilities specifically relating to the detection of explosives or the protection against or response to explosive attacks, catalogued by geographic location, including the asset's transportability and, to the extent feasible, similar assets and capabilities of State, local, territorial, and tribal governments;

(c) an inventory and description of current research, development, testing, and evaluation initiatives relating to the detection of and protection against explosives and anticipated advances in capabilities for reducing the threat of explosive attacks, and recommendations for the best means of disseminating the results of such initiatives to and among Federal, State, local, territorial, and tribal governments and first responders, as appropriate;

(d) for the purpose of identifying needed improvements in our homeland security posture, an assessment of our ability to deter, prevent, detect, protect against, and respond to an explosive attack based on a review of risk and the list, inven¬tories, and descriptions developed pursuant to paragraphs (a), (b), and (c) of this section, and recommendations to address any such needed improvements;

(e) recommendations for improved detection of explosive chemical compounds, precursor chemicals used to make improvised explosive chemical compounds, and explosive device components;

(f) recommendations for developing a comprehensive understanding of terrorist training and construction methods relating to explosive attacks and the production of explosive and incendiary materials;

(g) recommendations for protecting critical infrastructure and key resources against an explosive attack that can be used to inform sector-specific plans developed pursuant to the NIPP, including specific actions applicable to each of the critical infrastructure and key resources sectors;

(h) a recommended draft incident annex to the National Response Plan developed pursuant to Homeland Security Presidential Directive 5 of February 28, 2003 (Management of Domestic Incidents), for explosive attacks, detailing specific roles and responsibilities of agencies and heads of agencies through all phases of incident management from prevention and protection through response and recovery;

(i) an assessment of the effectiveness of, and, as necessary, recommendations for improving Federal Government training and education initiatives relating to explosive attack detection, including canine training and performance standards;

(j) recommended components of a national public awareness and vigilance campaign regarding explosive attacks; and

(k) a recommendation on whether any additional Federal Government entity should be established to coordinate Federal Government explosive attack prevention, detection, protection, and response efforts and collaboration with State, local, territorial, and tribal government officials, first responders, and private sector organizations.

(6) Not later than 90 days after the President approves the report, the Attorney General, in coordination with the Secretaries of Defense and Homeland Security and the heads of other Sector-Specific Agencies (as defined in HSPD 7) and agencies that conduct explosive attack detection, prevention, protection, or response activities, shall develop an implemen¬tation plan. The implemen¬tation plan shall implement the policy set forth in this directive and any recommendations in the report that are approved by the President, and shall include measures to (a) coordinate the efforts of Federal, State, local, territorial, and tribal government entities to develop related capabilities, (b) allocate Federal grant funds effectively, (c) coordinate training and exercise activities, and (d) incorporate, and strengthen as appro¬priate, existing plans and procedures to communicate accurate, coordinated, and timely information regarding a potential or actual explosive attack to the public, the media, and the private sector. The implementation plan shall include an implementation timetable, shall be effective upon the approval of the plan by the Attorney General, and shall be implemented by the heads of agencies as specified in the plan.

Roles and Responsibilities

(7) The Attorney General, in coordination with the Secretary of Homeland Security and the Director of National Intelligence, shall maintain and make available to Federal, State, local, territorial, and tribal law enforcement entities, and other first responders at the discretion of the Attorney General, a web based secure portal that includes information on incidents involving the suspected criminal misuse of explosives, including those voluntarily reported by State, local, territorial, and tribal authorities.

(8) The Secretary of Homeland Security, in coordination with the Attorney General, the Director of National Intelligence, and the Secretaries of State and Defense, shall maintain secure information-sharing systems that make available to law enforcement agencies, and other first responders at the discretion of the Secretary of Homeland Security, information, including lessons learned and best practices, concerning the use of explosives as a terrorist weapon and related insurgent war fighting tactics, both domestically and internationally, for use in enhancing the preparedness of Federal, State, local, territorial, and tribal government personnel to deter, prevent, detect, protect against, and respond to explosive attacks in the United States.

(9) The Secretary of Homeland Security, in coordination with the Attorney General, the Secretary of Defense, and the Director of the Office of Science and Technology Policy, shall coordinate Federal Government research, development, testing, and evaluation activities relating to the detection and prevention of, protection against, and response to explosive attacks and the development of explosives render-safe tools and technologies. The heads of all other agencies that conduct such activities shall cooperate with the Secretary of Homeland Security in carrying out such responsibility.

General Provisions

(10) This directive:

(a) shall be implemented consistent with applicable law and the authorities of agencies, or heads of agencies, vested by law, and subject to the availability of appropriations;

(b) shall not be construed to impair or otherwise affect the functions of the Director of the Office of Management and Budget relating to budget, administrative, and legislative proposals; and

(c) is not intended to, and does not, create any rights or benefits, substantive or procedural, enforceable at law or in equity by a party against the United States, its agencies, instrumentalities, or entities, its officers, employees, or agents, or any other person.

Appendix B: Domestic-IED Signed Charter

CHARTER
of the
SUBCOMMITTEE ON DOMESTIC IMPROVISED EXPLOSIVE DEVICES
COMMITTEE ON HOMELAND & NATIONAL SECURITY
NATIONAL SCIENCE AND TECHNOLOGY COUNCIL

A. Official Designation

The Subcommittee on Domestic Improvised Explosive Devices (IEDs) (Subcommittee) is hereby established by action of the National Science and Technology Council (NSTC) Committee on Homeland & National Security (CHNS).

B. Background

Terrorists have repeatedly shown their willingness and ability to use explosives as weapons worldwide and there is ample intelligence to support the conclusion that the IED is now and will continue to be the weapon of choice for terrorists because of its ability to cause harm, but, more importantly, to create fear among a wide audience, effectively becoming a weapon of mass influence. The threat of explosive attacks in the United States is of great concern considering terrorists' ability to make, obtain, and use explosives, the ready availability of components used in IED construction, the relative technological ease with which an IED can be fashioned, and the nature of our free society.

Homeland Security Presidential Directive 19 (HSPD-19), "Combating Terrorist Use of Explosives in the United States," establishes the overall national policy, and calls for the development of a national strategy and implementation plan, on the deterrence, prevention and detection of, protection against, and response to terrorist use of explosives in the United States. Science and technology play a significant role in the national strategy, and the Department of Homeland Security (DHS) Science and Technology Directorate (S&T) has been appointed in HSPD-19 to coordinate interagency advancement of priority technology capabilities. The co-chairs of the NSTC CHNS, with concurrence from the Office of Science and Technology Policy (OSTP) and the Homeland Security Council (HSC), have agreed to establish this Subcommittee to serve as the formal mechanism for this coordination.

C. Purpose and Scope

The purpose of the Subcommittee is to advise and assist the CHNS and NSTC on policies, procedures and plans for federally-sponsored technologies to combat the domestic use of explosives by terrorists. The scope of the Subcommittee encompasses assessment of technologies, standards, and S&T policies of the entire counter-explosives domain:

- Deterrence – cumulative effect of all mission areas to discourage or restrain terrorists from attacking a target.
- Prevention – efforts to uncover, track, and stop terrorist explosives plots before an attack.
- Detection – efforts to identify or confirm the existence of explosive related materials or activity.
- Protection – activities that mitigate the risk and impact of terrorist use of explosives against critical infrastructure and soft targets.
- Response – efforts to stop imminent explosive threats and activities conducted after an attack occurs.

The work of the Subcommittee will be conducted in close collaboration and partnership with the HSC-led HSPD-19 process. Specifically,

1. The DHS Office for Bombing Prevention (OBP), working with and through the HSC, will lead an interagency effort to identify and prioritize operational requirements. This information will serve as an input to the Subcommittee's deliberative activities to identify and prioritize research activities.
2. Budget requirements and information developed through the Subcommittee will be integrated into the overall HSPD-19 budget plan by HSC, thus allowing OMB and agencies a complete vision of explosives activities and priorities.

D. Tasking

The Subcommittee serves as part of the internal deliberative process of the NSTC. Reporting to and directed by the CHNS, the Subcommittee will:

- Coordinate RDT&E plans among the federal agencies involved in this area;
  - o Review prioritized operational requirements developed by OBP
  - o Identify current capabilities (COTS and GOTS) and current RDT&E plans in federal agencies
  - o Analyze needs against capabilities/plans (gap analysis)
  - o Coordinate interagency RDT&E to address identified technology gaps
  - o Identify needed standards for explosive technologies and work to develop them in the appropriate standards bodies
- Identify and expound on RDT&E recommendations in the HSPD-19 report that could pro-

vide an order of magnitude or paradigm shift in countering domestic IEDs;
- Ensure a consistent message about domestic counter IED technologies and related government research initiatives when agencies interact with Congress, the press and the public;
- Recommend a multi-agency investment strategy that advances domestic counter-IED RDT&E activities to meet public and private needs and focuses S&T funds on technologies that will have the greatest impact preventing terrorist use of explosives in the domestic environment;
- Strengthen international and public sector partnerships to foster the advancement of domestic counter-IED technologies;
- Coordinate technology transfer programs to ensure rapid fielding of new explosives-related capabilities; and
- Recommend government-wide policies for explosives technologies where required.
- Identify necessary improvements in personal protective equipment and training for responders.

The Subcommittee Co-Chairs, with the CHNS endorsement, will recommend action on major issues to the Director, Office of Science and Technology Policy for approval.

E. Membership

The following NSTC departments and agencies are represented on the Subcommittee:

Department of Defense
Department of Energy
Department of Health and Human Services
Department of Homeland Security
Department of Justice
Department of State
Department of Transportation
Environmental Protection Agency
Intelligence Community
National Science Foundation
Technical Support Working Group

The following organizations in the Executive Office of the President shall also be represented on the Subcommittee:

Homeland Security Council
National Security Council
Office of Management and Budget
Office of Science and Technology Policy

Appendix B: Domestic-IED Signed Charter

Cooperating departments and agencies shall include such other Executive organizations, departments and agencies as the co-chairs may, from time to time, designate.

F. Private Sector Interface

The Subcommittee may seek advice from members of the President's Council of Advisors on Science and Technology and will recommend to the Director, Office of Science and Technology Policy the nature of additional private sector advice needed to accomplish its mission. The Subcommittee may also interact with and receive ad hoc advice from various private-sector groups as consistent with the Federal Advisory Committee Act.

G. Termination Date

Unless renewed by the Chairman of NSTC prior to its expiration, the Subcommittee shall terminate no later than March 31, 2009.

H. Determination

I hereby determine that the formation of the Subcommittee on Domestic IEDs is in the public interest in connection with the performance of duties imposed on the Executive Branch by law, and that such duties can best be performed through the advice and counsel of such a group.

Approved:

Stanley Sokul, Office of Science and Technology Policy
Co-chair, Committee on Homeland and National Security

4/14/08
Date

for

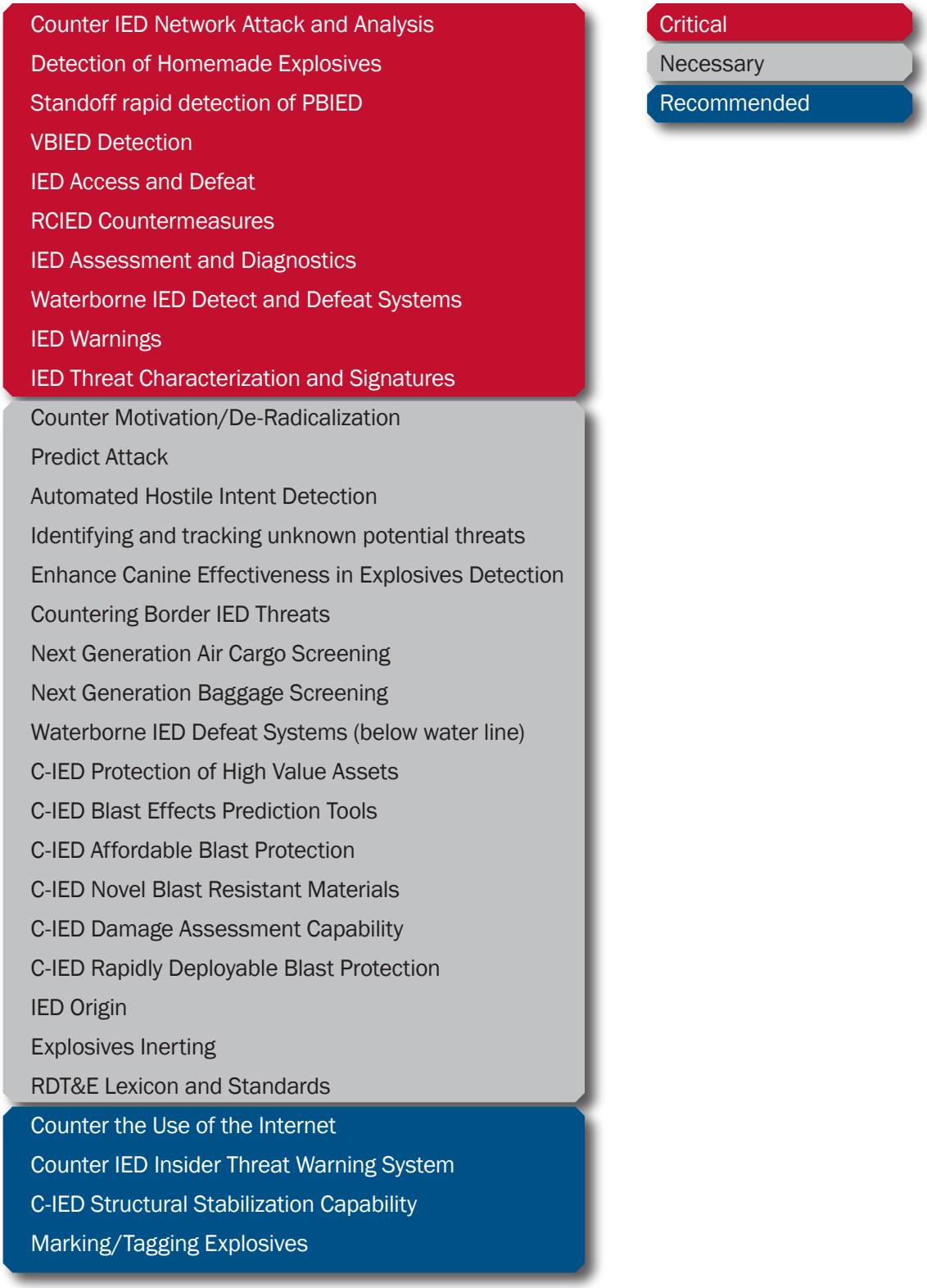
John J. Young, Jr., Department of Defense
Co-chair, Committee on Homeland and National Security

26 June 08
Date

Jay M. Cohen, Department of Homeland Security
Co-chair, Committee on Homeland and National Security

7/7/08
Date

Appendix C: Grouped Operational Needs



Appendix D: List of Acronyms

AAWO	Army Asymmetric Warfare Office
ATF	Bureau of Alcohol, Tobacco, Firearms and Explosives
CBP	Customs and Border Protection
CHNS	Committee on Homeland & National Security
C-IED	Counter Improvised Explosive Device
CIKR	Critical Infrastructure and Key Resources
CONUS	Continental United States
COTS	Commercial Off-the-Shelf
DHS	Department of Homeland Security
D-IED	Domestic Improvised Explosive Device
DoD	Department of Defense
DOJ	Department of Justice
DOS	Department of State
ECM	Electronic Countermeasures
EOD	Explosive Ordnance Disposal
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FEMA	Federal Emergency Management Agency
GOTS	Government Off-the-Shelf
HDS	Hazardous Devices School
HME	Homemade Explosives
HSC	Homeland Security Council
HSPD	Homeland Security Presidential Directive
IE	Improvised Explosive
IED	Improvised Explosive Device
IR	Infrared
ISR	Intelligence, Surveillance, and Reconnaissance
JIEDDO	Joint Improvised Explosive Device Defeat Organization
MOTR	Maritime Operational Threat Response
NASA	National Aeronautics and Space Administration
NBSCAB	National Bomb Squad Commanders Advisory Board
NCAD	National Capabilities Analysis Database
NIJ	National Institute of Justice
NIPP	National Infrastructure Protection Plan
NSTC	National Science and Technology Council
NTIA	National Telecommunications and Information Administration
OBP	Office for Bombing Prevention
OCONUS	Outside Continental United States
OMB	Office of Management and Budget
ONR	Office of Naval Research
OSTP	Office of Science and Technology Policy
PBIED	Person-borne Improvised Explosive Devices
RCIED	Radio Controlled Improvised Explosive Devices
RDECOM	Army Research, Development and Engineering Command
RDT&E	Research, Development, Test, and Evaluation

Appendix D: Glossary

RF	Radio Frequency
S&T	DHS Science and Technology Directorate
SC	Subcommittee
SWAT	Special Weapons and Tactics
SWGDOG	Scientific Working Group on Dog and Orthogonal detector Guidelines
TSA	Transportation Security Administration
TSL	Transportation Security Laboratory
TSWG	Technical Support Working Group
TTP	Tactics, Techniques, and Procedures
UHD	Underwater Hazardous Device
USCG	United States Coast Guard
USPIS	U. S. Postal Inspection Service
VBIED	Vehicle-borne Improvised Explosive Devices
WBIED	Waterborne Improvised Explosive Device