

CRITICAL RESEARCH/INNOVATION FOCUS AREA DOCUMENT

Deter and Predict Counter Improvised Explosive Devices (C-IED) Network Attack and Analysis

**Dr. Ruth Doherty
Counter Improvised Explosive Devices (C-IED)
U.S. Department of Homeland Security, Science and
Technology (S&T) Directorate**

**May 4, 2009
Version 1.0**

Please note that as more details are available, DHS will post updated research/innovation focus area overviews on the FutureTECH website. This is a pre-decisional draft document of the NSTC Subcommittee on Domestic IEDs. Please contact Dr. Ruth Doherty, ruth.doherty@dhs.gov for more information.

Who?

Identify any DHS component stakeholders that contain or represent potential end users. Also name any Capstone IPT (refer to http://www.dhs.gov/xres/programs/gc_1234200779149.shtm and the article entitled "Making it Easier to Work with DHS"), if any, which identified a capability gap related to this research/innovation focus area.

The U.S. Department of Homeland Security (DHS) leads for CIEDs are the Office for Bombing Prevention and United States Secret Service (USSS). The corresponding DHS Science and Technology (S&T) Capstone IPT that identified capability gaps related to this focus area is entitled "Counter-IED."

What?

Describe a required technology/capability. Describe how a technology will provide the capabilities and functional improvements needed to address the DHS need. Do not describe a specific technical solution. Instead, describe a conceptual technology for illustrative purposes. Define typical missions that the proposed technology could be utilized to accomplish.

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 tactics, techniques and procedures (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 better understanding and anticipating the IED threat.

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 contiguous United States (CONUS) and outside the contiguous United States (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.

A computational framework that better reflects the adversary's agile and adaptive behavior is needed. 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

Please note that as more details are available, DHS will post updated research/innovation focus 2 area overviews on the FutureTECH website. This is a pre-decisional draft document of the NSTC Subcommittee on Domestic IEDs. Please contact Dr. Ruth Doherty, ruth.doherty@dhs.gov for more information.

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

Why?

Describe the analysis and rationale for requiring a new technology/capability. Describe why existing technologies cannot meet current or projected requirements. Describe what new technologies/capabilities are needed to address the gap between current capabilities and required capabilities.

Currently, there is 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.

DHS must draw on this abundance of information to improve the 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 they have studied us and strive to develop an ability to identify behaviors and TTPs that radicalized individuals/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.

When?

If a technology/capability is intended as a countermeasure to a threat, summarize the threat to be countered and how the technology could be used (i.e., concept of operations). If applicable, provide a schedule/timeframe to capture when the technology/capability is needed in order to address the DHS gap.

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 TTPs used to execute bombings.

Please note that as more details are available, DHS will post updated research/innovation focus 3 area overviews on the FutureTECH website. This is a pre-decisional draft document of the NSTC Subcommittee on Domestic IEDs. Please contact Dr. Ruth Doherty, ruth.doherty@dhs.gov for more information.

Where?

Describe the projected threat environment in which the technology/capability may be potentially deployed.

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.

Please note that as more details are available, DHS will post updated research/innovation focus 4 area overviews on the FutureTECH website. This is a pre-decisional draft document of the NSTC Subcommittee on Domestic IEDs. Please contact Dr. Ruth Doherty, ruth.doherty@dhs.gov for more information.