

COMBATING TERRORISM
TECHNICAL SUPPORT OFFICE



2012 REVIEW BOOK



A CTTSO HISTORY TIMELINE

The Combating Terrorism Technical Support Office (CTTTSO) is charged with providing a forum for interagency and international users to discuss mission requirements to combat terrorism, prioritize those requirements, fund and manage solutions, and deliver capabilities. The CTTTSO is the Department of Defense organization that currently oversees the Technical Support Working Group (TSWG), the Explosive Ordnance Disposal/Low-Intensity Conflict Program, and the Irregular Warfare Support Program.

The Technical Support Working Group (TSWG) is the U.S. national forum that identifies, prioritizes, and coordinates interagency and international research and development requirements for combating terrorism. TSWG membership includes representatives from more than 100 government organizations. Participation is open not only to federal departments and agencies, but also to first responders and appropriate representatives from state and local governments and international agencies. These departments and agencies work together by participating in one or more subgroups.

The TSWG is currently comprised of nine subgroups, each chaired by senior representatives from federal agencies with special expertise in those functional areas.

The subgroups are:

- Advanced Analytic Capabilities (AAC)
- Chemical, Biological, Radiological, Nuclear, and Explosives (CBRNE)
- Improvised Device Defeat (IDD)
- Investigative Support and Forensics (ISF)
- Personnel Protection (PP)
- Physical Security (PS)
- Surveillance, Collection, and Operations Support (SCOS)
- Tactical Operations Support (TOS)
- Training Technology Development (TTD)



Technical Support Working Group (TSWG) formalized

1986

World Trade Center bombed

1993

Oklahoma City bombing

1995

1999

Combating Terrorism Technical Support Office created

Terrorist attack on the USS Cole in Yemen

2000

Bali bombings

Explosive Ordnance Disposal/Low-Intensity Conflict moved to CTTTSO

2002

Madrid train bombings

2004

Irregular Warfare Support Program formally created and funded as a separate program

July 7th attacks on the London Underground

2005

2007

Mumbai attacks

2008

A terrorist attack kills the U.S. Ambassador to Libya and three other Americans

2012

More than \$1B was spent to ensure that the London Olympics were terrorism-free



1983

Bombing of U.S. Embassy and Marine Corps barracks in Beirut, Lebanon

1988

Bombing of Pan Am Flight 103

1998

Bombing of U.S. Embassies in Kenya and Tanzania

Presidential Decision Directive (PDD) 62 is signed, defining U.S. policy on combating terrorism

2001

September 11th attacks
The U.S. enters Operation Enduring Freedom
TSWG organizes a BAA for the Department of Defense

2003

The U.S. enters Operation Iraqi Freedom
Saddam Hussein is overthrown
Capture of Saddam Hussein by U.S. special operations forces

2006

Special Operations Forces (SOF) support thrust begins in CTTTSO

Attempted underwear bomber aboard Northwest Airlines Flight 253

2009

2011

Killing of Osama bin Laden by a team of U.S. Navy SEALs



New ways to wage war – and to wage terror – promise both small and large changes in established assumptions. But whether that technique is a new explosive mixture, a computer virus, or a disinformation campaign, it always goes back to the same assumptions. The attacker is always trying to get by the defender, and the defender is trying to deploy the right countermove. New threats require new strategies. Innovation enables the United States to increase our own defenses, identify weaknesses in those who attack us and our allies, and change the rules in our favor.

Innovation has many forms. It ranges from basic research – technology that will not be available for decades but that promises to truly alter how we understand and interact with the world – to small, but key, innovations, to current equipment with delivery schedules measured in days, weeks, or months. All are essential, and all must work in concert.

In a time when innovation often comes from new and emerging companies, it is interesting to look at an organization that has been involved with innovation for more than 25 years. The Combating Terrorism Technical Support Office (CTTSO) doesn't just pursue innovation for the sake of innovation – it pursues innovation to meet the needs of its diverse user base. A new way to build blast-resistant buildings is one thing, but it only becomes powerful when directly meeting the needs of the people who live and work in those buildings. CTTSO acts as a matchmaker, ensuring that those on the front lines of the fight against terrorism get what they need to do their job just a little easier, and that the people who build those things reap the rewards.

“Therefore, just as water retains no constant shape, so in warfare, there are no constant conditions.”

*Sun Tzu,
The Art of War*



“... I believe I’m chairman at a time that seems less dangerous but it’s actually more dangerous. That’s the essence of what I describe as a security paradox. Although geopolitical trends are ushering in greater levels of peace and stability worldwide, destructive technologies are available to a wider and more disparate pool of adversaries. Highly accurate ballistic missiles are prevalent in every theater. Bombs made out of fertilizer can defeat and destroy our toughest mine-resistant vehicles. A cyberattack could stop this society in its tracks. And these are real threats that we face today.”

*General Martin A. Dempsey, Chairman of the Joint Chiefs of Staff,
April 12, 2012, Boston, Massachusetts*



Two such examples that have been provided to the users who needed them are the Enhanced Mortar Targeting System, which is a better mortar system for soldiers operating from remote, austere sites, and the Mass Alert Emergency Mobile Responding System, which warns large groups in crisis situations and is currently deployed with Customs and Border Protection along the Arizona border. And this year, the Advanced Diver Mask Mounted Display and the Parachute Simulator promise to continue the tradition of requirements going to end users who need them. The Advanced Diver Mask Mounted Display is the result of a requirement from those diving in pitch-black water that allows them to clearly see what they are doing, whether looking for mines, scanning for intruders, inspecting ship hulls, searching for evidence, or recovering a body. The Parachute Simulator is being developed to train special operations forces on parachute jumps to significantly improve operational skills without danger or risk of training injury.

This year has been one of significant change, and it is expected that 2013 will be no different. In such turbulent times, it is natural to take refuge in places with a history of success. No matter what changes the future brings, whether big or small, CTTSO will continue to be there to do its part in supporting the combating terrorism mission.

“Nothing endures
but change.”

Heraclitus





Preface



Table of Contents

The Combating Terrorism Technical Support Office

- 8 Organization
- 9 International Program

Technical Support Working Group

- 12 History and Mission
- 12 Organization and Structure

The Technical Support Working Group Subgroups

- 16 Advanced Analytic Capabilities
- 28 Chemical, Biological, Radiological, Nuclear, and Explosives
- 40 Improvised Device Defeat
- 50 Investigative Support and Forensics
- 60 Personnel Protection
- 70 Physical Security
- 82 Surveillance, Collection, and Operations Support
- 88 Tactical Operations Support
- 100 Training Technology Development

Explosive Ordnance Disposal/Low-Intensity Conflict

- 110 Organization, Funding, and Program Information

Irregular Warfare Support

- 118 Organization, Funding, and Program Information

Appendix

- 130 CTTSO Technology Transition Office
- 132 BAA Information Delivery System (BIDS)
- 134 2012 Membership
- 146 2012 Performers
- 154 Glossary of Acronyms

The background of the page is a faded, high-angle view of the American flag, showing the stars and stripes in a soft, golden-brown color palette.

Combating Terrorism Technical Support Office

Vision

Identify requirements to combat terrorism and provide solutions to war fighters, first responders, and other front-line users as rapidly as possible.

Mission

Identify and prioritize the needs of the interagency community charged with combating terrorism. Deliver capabilities to those on the front lines through rapid research, development, test, evaluation, and operational support. Incorporate available expertise and experience from government, commercial, private, and academic sources throughout the United States and the world.





The Combating Terrorism Technical Support Office (CTTSO) is charged with providing a forum for interagency and international users to discuss mission requirements to combat terrorism, prioritize those requirements, fund and manage solutions, and deliver capabilities. The CTTSO accomplishes these objectives through rapid prototyping of novel solutions developed and field-tested before the traditional acquisition systems are fully engaged. This low-risk approach encourages interdepartmental and interagency collaboration, thereby reducing duplication, eliminating capability gaps, and stretching development dollars.

Organization

The Assistant Secretary of Defense for Special Operations/Low-Intensity Conflict (ASD (SO/LIC)) established CTTSO in 1999 to consolidate its research and development programs previously administered by the Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence). The research and development effort that supports the interagency





Technical Support Working Group (TSWG) was the first program to transition to CTTSO. The Explosive Ordnance Disposal/Low-Intensity Conflict (EOD/LIC) Program, which develops advanced technologies for Joint Service EOD and Special Operations Forces (SOF) missions, transitioned in 2001. In 2007, the Irregular Warfare Support (IWS) Program was initiated to satisfy a growing need to improve the capacity of the United States to counter insurgencies and fight an irregular war.

International Program

International cooperation allows CTTSO to leverage foreign experience, expertise, resources, and infrastructure in a unified approach against terrorism for the benefit of all. Therefore, in addition to its domestic interagency efforts, CTTSO directly manages bilateral agreements with five partner countries (Australia, Canada, Israel, Singapore, and the United Kingdom) and cooperates when appropriate with countries and organizations around the world. Dozens of operational capabilities developed with CTTSO partners are currently in service with a variety of personnel both throughout the United States and around the world.



The background of the page is a faded, high-angle view of the United States flag, showing the stars and stripes in a soft, light tone. The text is overlaid on the left side of this background.

Technical Support Working Group



DoD photo by Tech. Sgt. Manuel J. Martinez, U.S. Air Force. (Released)



History and Mission

In April 1982, the National Security Decision Directive 30 assigned responsibility for the development of an overall U.S. policy on terrorism to the Interdepartmental Group on Terrorism (IG/T), chaired by the Department of State (DOS). TSWG was an original subgroup of the IG/T, which later became the Interagency Working Group on Counterterrorism. In its February 1986 report, a cabinet level Task Force on Counterterrorism – led by then Vice-President Bush – cited TSWG as assuring “the development of appropriate counterterrorism technological efforts.”

Today, TSWG still performs that counterterrorism technology development function as a stand-alone interagency working group. TSWG’s mission is to identify and prioritize the needs of the national interagency community through research and development programs for combating terrorism requirements. TSWG delivers capabilities to those on the front lines through rapid research and development and testing and evaluation, while providing operational support. TSWG incorporates available expertise and experience from government, commercial, private, and academic sources throughout the United States and the world.

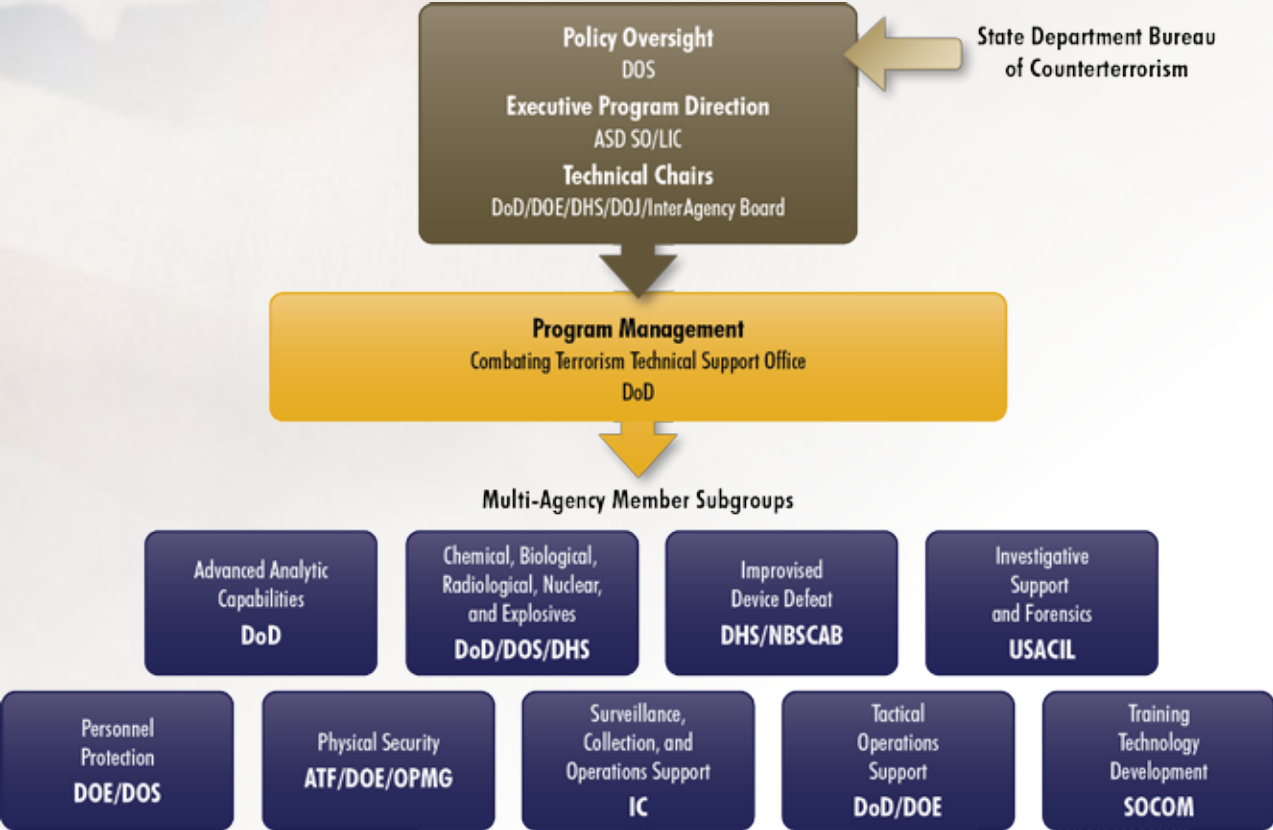
TSWG initiates efforts to influence longer-term research and development initiatives; and, reflecting the shift to a more offensive strategy, balances its technology and capability development efforts among the four pillars of combating terrorism: antiterrorism, counterterrorism, intelligence support, and consequence management.

Organization and Structure

TSWG operates under the policy oversight of the Department of State Coordinator for Counterterrorism and the management and technical oversight of the Department of Defense Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict. While TSWG’s core funds are derived principally from CTTSO and DOS, other departments and agencies contribute additional funds and provide personnel to act as project managers and technical advisors. TSWG has successfully transitioned capabilities to the Departments of Agriculture, Defense, Homeland Security, Justice, State, and the Treasury; the Public Health Service; and many other departments and agencies. Additionally, TSWG has transitioned many systems to state and local law enforcement. TSWG membership includes representatives from more than 100 government organizations. Participation is open not only to federal departments and agencies, but also to first responders and appropriate representatives from state and local governments and international agencies. These departments and agencies work together by participating in one or more subgroups. A comprehensive listing of member organizations is provided in the appendix.



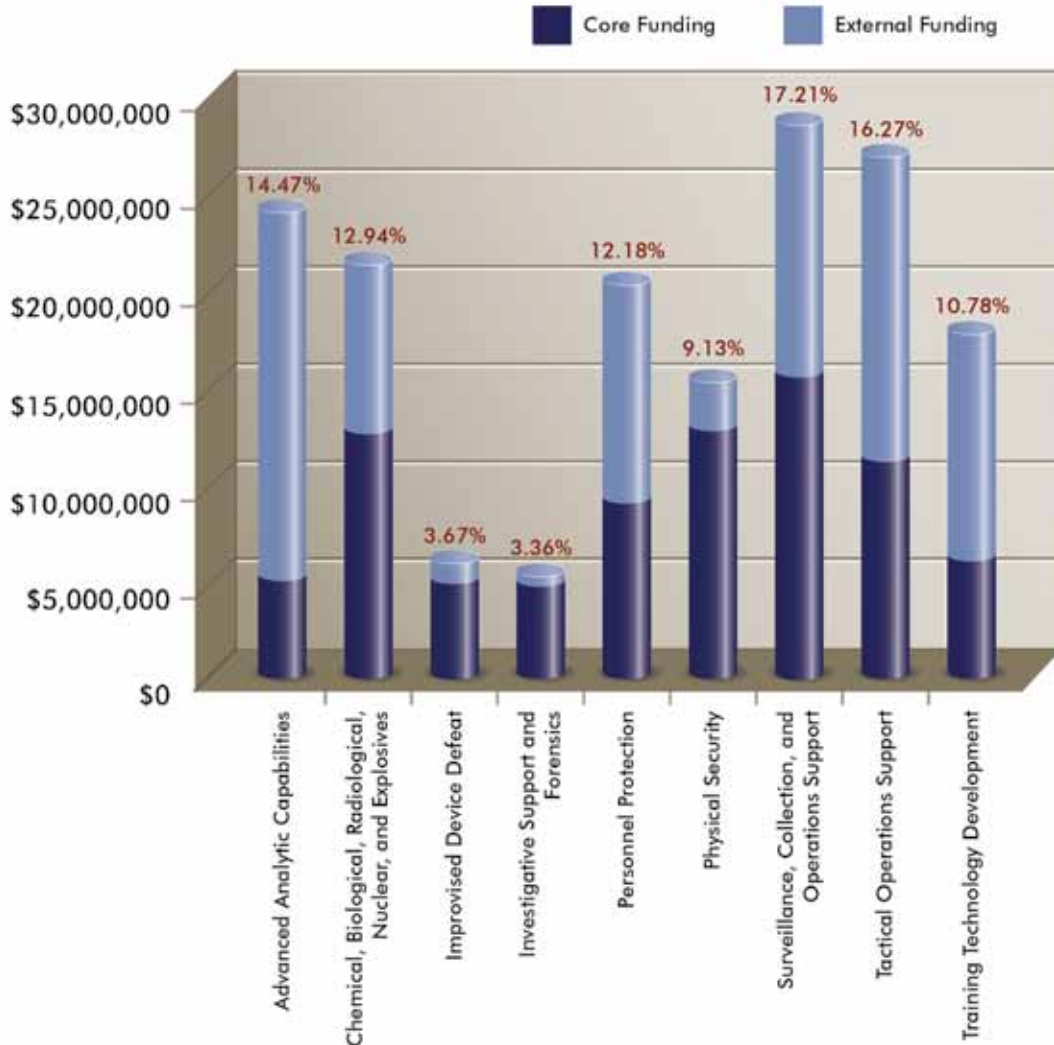
TSWG’s subgroups are chaired by senior representatives from federal agencies with special expertise in those functional areas. Chairmanship of nine subgroups is shared as indicated in the organizational chart below.



State Department Bureau of Counterterrorism



TSWG FY 2012 Project Funding (\$164.3 Million)





The background of the page is a faded American flag, showing the stars and stripes in a light, semi-transparent manner.

Advanced Analytic Capabilities

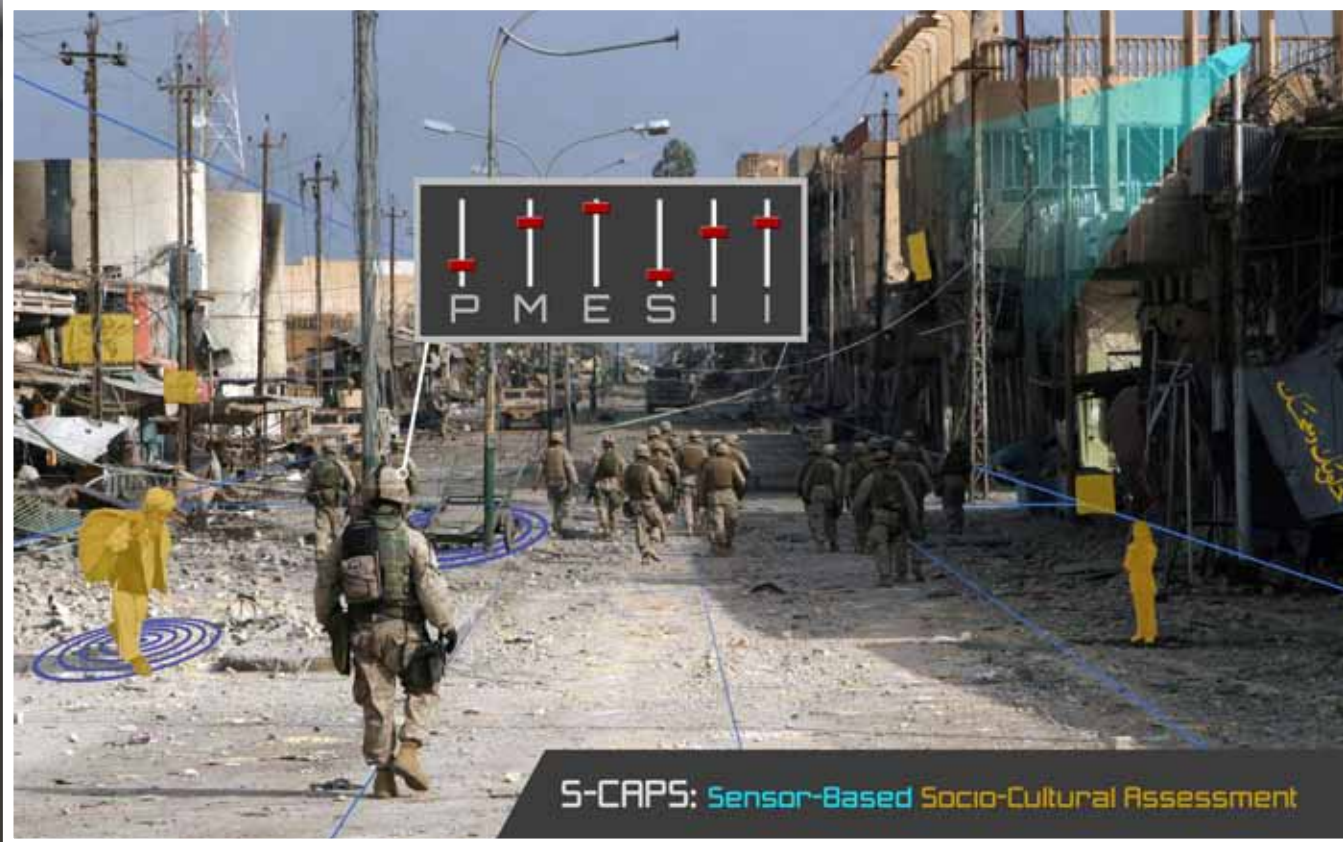
Mission

Identify, prioritize, and execute research and development projects that satisfy interagency requirements to improve sense-making, decision-making, and data management for counterterrorism, counterinsurgency, stabilization/re-construction missions, and cyber defense. Focus on the development and integration of analytic tools and associated processes at the tactical level to include operational level interface.

The Advanced Analytic Capabilities (AAC) Subgroup prioritizes multi-agency user requirements and seeks new user-friendly capabilities to counter terrorism that enable war fighters to make better and faster decisions. One specific focus area is developing integrated platforms for model-enabled analysis at the operational and tactical levels that also enhance the interface between operators and intelligence analysts. AAC's work also includes specialized development in cyber defense. Current efforts within the subgroup involve developing more secure System Control and Data Acquisition (SCADA) devices.

Contact Information

aacsubgroup@cttso.gov





Focus Areas

Integrated Analytic Platforms

Develop and deploy robust integrated platforms to enhance analysis of diverse and disparate data sources to support decision-making and planning. These platforms shall enable a variety of analytic tools and methods to be readily interoperable with each other and with supporting data sources. Integrate analytic tools into existing military operational platforms, both forward deployed and reach-back capabilities, to facilitate the appropriate interaction, exploration, and visualization of key elements. Develop infrastructure to facilitate secure collaboration and fusion among and between analysts and forward deployed operators in real time.

Decision, Planning, and Analytical Tools

Develop tools and models that provide analytic rigor to the military and interagency planning and decision-making process for counterinsurgency and counterterrorism operations and campaigns. This includes decision-support tools that will enable operators and planners at the operational and tactical levels to better understand the operational environment, evaluate first and higher order effects of alternate courses of action, and enable near real-time decisions within the context of the mission.

Cyber Defense Applications

Support sustained operations through development and fielding of enhanced layered defensive capabilities by anticipating and avoiding threats through understanding the cyber situation, anticipating adversarial actions, assessing potential impacts, and by implementing defensive methodologies.

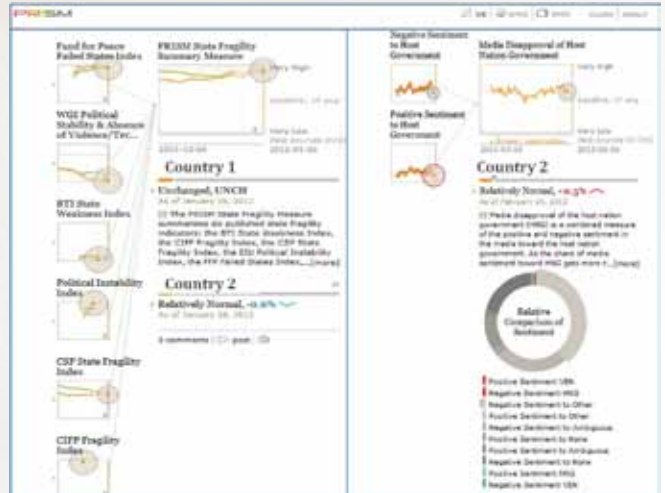


Integrated Analytic Platforms

Monitoring Social Trends

Completed

Special operations planners required continual, robust monitoring of the attitudes of foreign populations toward different violent extremist groups and toward their own host government officials. The trends of these measurements over time provide insight into threat levels and the context for potential future threats. A media monitoring capability named PRISM (Planning, Research, and Intelligence Scalable Modeling) monitors large numbers of Web-based media sources in selected countries to aggregate, estimate, and track the attitudes expressed in the media. A cognitive task analysis was conducted to develop an analytic methodology and a processing pipeline to provide trend data from foreign media. PRISM integrated Web media extraction, foreign language machine translation (including French, Urdu, and Arabic), sentiment estimation, statistical modeling, and visualization components to deliver trend data to analysts and planners. In addition, PRISM provided access to an extensive database of related social and cultural contextual data trends on the countries studied. A prototype PRISM capability was developed, installed on a network, and evaluated in the joint planning cell within special operations.



Integrated Fusion and Analysis Platform

Current

U.S. intelligence analysts in Afghanistan lacked analytic tools to properly support analysis of massive amounts of data in order to provide their commanders with a comprehensive understanding of the highly complex and dynamic counterinsurgency (COIN) environment within which they operate. Key pieces of critical information were lost in the reams of data and omitted from assessments, resulting in a lack of full understanding of the operational environment and enemy.

Palantir is the commercially developed software technology that



was selected and is currently used by major financial institutions, industry, and several government agencies for a variety of applications. Palantir combines several analytical functions (data-mining/research, link-analysis, geospatial, and temporal context) into one platform. It does this with a user interface that is intuitive, easy to learn, and easy to use, even by inexperienced operators in austere environments. The CTTSO worked with several organizations to deploy a system in theater that incorporated disconnected laptops at the lowest tactical level; regional nodes; and reach-back for training and intelligence support in the contiguous United States while allowing data to be transferred to all parties in a collaborative environment. A ruggedized expeditionary version was also field tested. United States Marine Corps and Special Operations Forces users report significant time savings in their analytical workflows due to Palantir. CTTSO is now evaluating the Integrated Fusion and Analysis Platform capabilities with U.S. forces deployed in various geographic areas, to include U.S. Marine forces deployed on Naval vessels and Expeditionary forces operating where information is sparse and often unclassified.

Decision, Planning, and Analytical Tools

Susceptibility and Vulnerability Analysis Tool

Completed

For a number of years, the CTTSO has been involved with the Susceptibility and Vulnerability Analysis Tool (SAVANT), a software application that assists members of the influence operations community as they conduct planning and analysis for their missions. SAVANT is being trained to all new active and reserve influence operations soldiers, and has been brought into theater in Afghanistan. The application is being incorporated into a Program of



Record. Over the past year, the developer has been building a new Web-based version of the SAVANT application. The CTTSO has provided support to facilitate the incorporation of data from third-party systems into the Web-based SAVANT application in such a way that access to those data providers, and the results obtained from the providers, is tailored to answer specific questions that soldiers may have as they conduct the workflow of their doctrinal process.



When information is obtained from the third-party systems, it is also accompanied by links that provide details into the third-party system, as well as bibliographic information that identifies the source and authorship of the material. Soldiers appreciate the automatic references provided by the data integration feature, as well as the ability for this feature to facilitate continuity of information during relief-in-place/transfer of authority. The CTTSO has supported both the development of the infrastructure that allows data from third-party systems to be incorporated into SAVANT, as well as integration with a specific third-party data source, the Cultural Depot, a wiki that allows soldiers to capture and share their knowledge of an area of operation. The initial operating capability of the Web-based version of SAVANT is expected in August 2013.

OE-SGT Integration with Integrated Fusion and Analysis Platform

Current

The Operational Environment Scenario Generation Tool (OE-SGT) is a Political, Military, Economic, Social, Information, and Infrastructure (PMESII) scenario creation tool kit. With OE-SGT, users are able to rapidly incorporate public news sources and classified intelligence data into their human terrain scenarios. This helps analysts more accurately predict the impact of potential courses of action on civilian quality of life and cooperation levels.

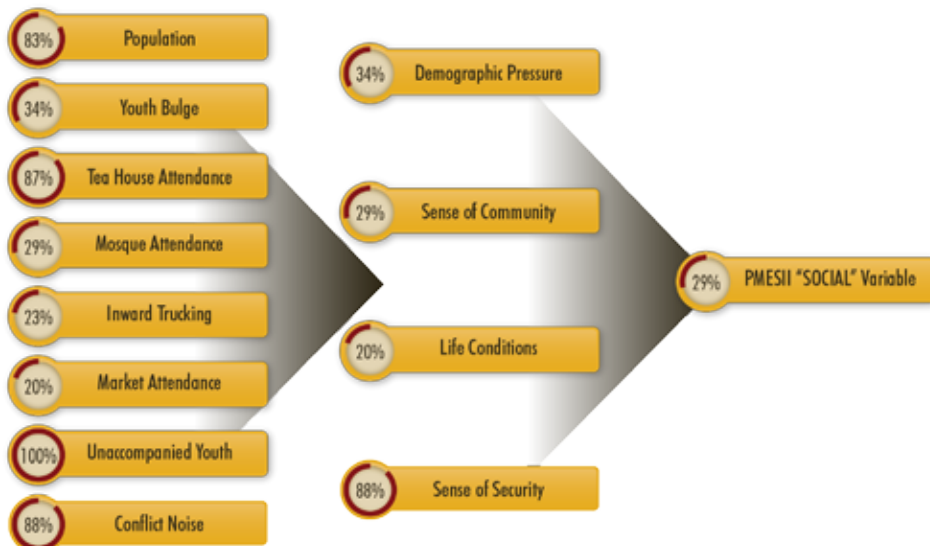


Originally developed to support the U.S. Army's One Semi-Automated Force program, the OE-SGT has been extended to import Integrated Fusion and Analysis Platform data from the Palantir intelligence system and export scenarios compatible with the Athena Stability and Recovery Operations Simulation. OE-SGT reduces the time and effort needed to create stability operation scenarios, helping to improve both the quality and cost-effectiveness of simulation-based PMESII analysis as an operational decision support tool.

Social Cultural Assessment from Passive Sensing

Current

A need exists for social cultural intelligence in stabilization/reconstruction, counterterrorism, and counterinsurgency missions, particularly in austere and denied areas of operations (AO). Existing intelligence, surveillance, and reconnaissance (ISR) technologies and techniques are insufficient for this purpose. Sensor systems and automated analysis tools are optimized today for traditional kinetic environments or high-value individual tracking, and human source alternatives to manually collect poll and survey data are in short supply and lead to dangerous situations. As a result, social cultural changes too often go unnoticed, undetected, or inaccurately assessed. The Social Cultural Assessment from Passive Sensing (S-CAPS) project will provide a proof of concept by assessing



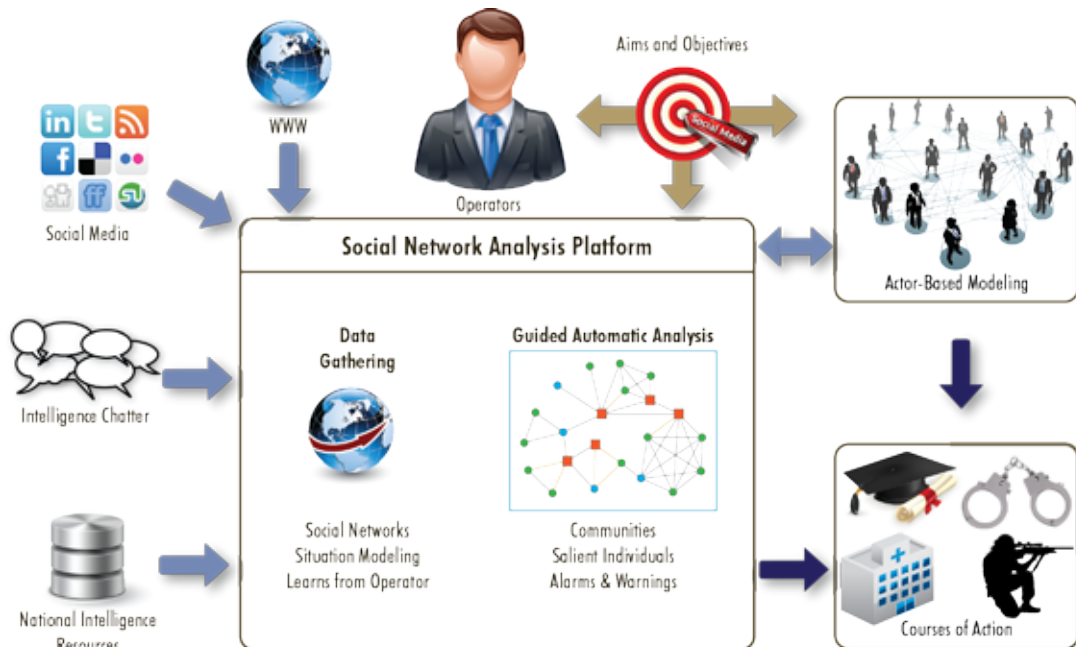


patterns of life, establishing baselines for “atmospherics”, and monitoring trends with limited sensor data. While social cultural models today are primarily strategic and used for simulation and planning, S-CAPS uses model-based analysis of sensor data to develop timely, local social cultural model baselines and to detect anomalies. S-CAPS employs Technology Readiness Level 9 multimodal unattended ground sensors to collect and wirelessly exfiltrate low-resolution video, seismic, and acoustic data. Soft-biometric and anthropometric parameters, time-labeled foot/vehicle/animal traffic flow, acoustic signatures, and micro-demographic measurement variables are derived from this sensor data. These low-level measurement variables are used as inputs to the model, leading to intermediate proxy variables (e.g., sense of community, demographic pressure, life conditions), and eventually to higher-level PMESII variables. The ultimate result will be a timely, local summary of the civil operating picture in terms of PMESII variables, temporal pattern of life changes, and sense of well being in the AO.

Social Network Analysis Platform

Current

Social Network Analysis Platform (SNAP) will enable analysts and commanders to rapidly gain and maintain situational awareness in irregular warfare by assisting them with assimilating the most relevant and actionable information. It aims to facilitate speedy and effective planning, preparation, and support of missions. SNAP is built around the Sintelix system and gathers, extracts, and links





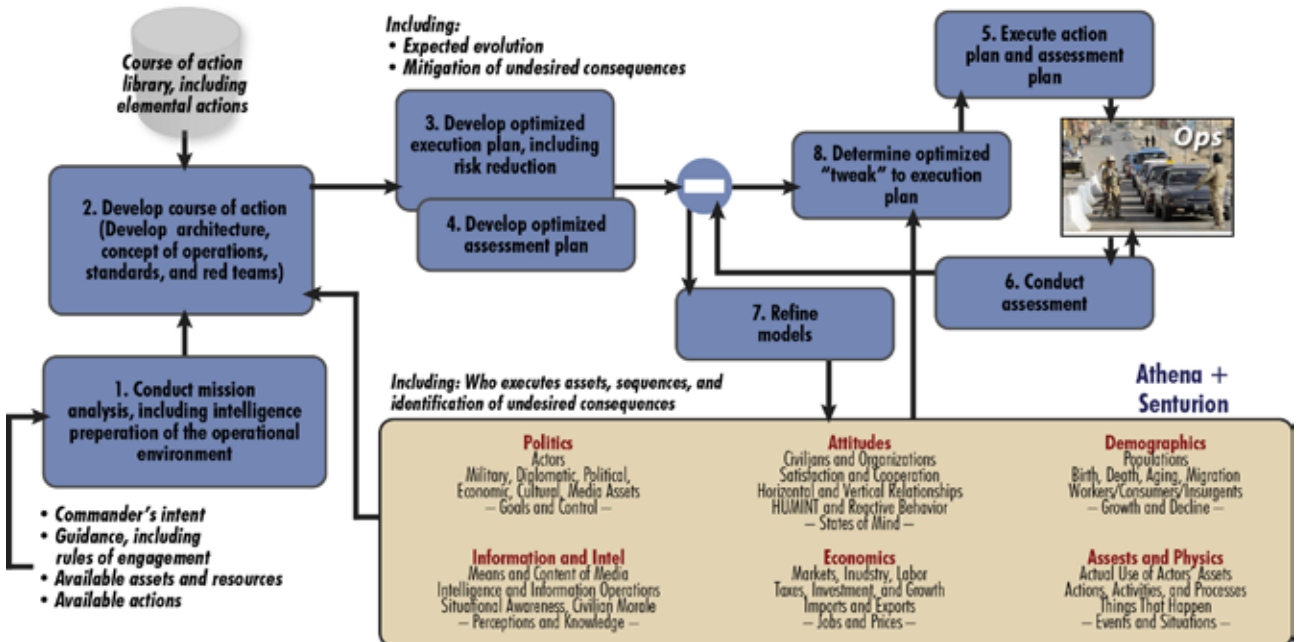
data drawn from classified sources, the Web, and social media. It provides the information it extracts via interactive dashboards, network visualizations, semantic search, and hyperlinked source documents.

Sintelix provides very high quality automatic extraction and linking, and substantially avoids pollution from errors and misses and performs as well as human analysts. The unique focus of the project is creating the capability for SNAP to learn from its users during the normal course of their work and to progressively improve its accuracy and value. SNAP automatically creates rich networks that not only include information on social relationships, but also about relationships between people, organizations, locations, and many other entity types. When complete, given the raw data about a situation, SNAP will be able to identify the key players; their roles, relationships, and power bases; the key social groupings and cleavages; the key players' and groups' motivations, strengths, weaknesses, threats, and capabilities; and to generate alarms and warnings. Evaluation of the performance will be assessed with real-world data and compared to other techniques.

Model Predictive Controller

Current

The Advanced Analytic Capabilities Subgroup is actively engaged in the development of capabilities that can improve the creation and execution of complex diplomatic, information, military, and economic and PMESII campaigns. One of these activities, Model Predictive Controller (MPC), pursues this goal by establishing a





protocol that permits users to employ models, estimates, and assumptions — even seemingly poor ones — to their maximum benefit. Technically, MPC is a sophisticated engineering discipline that draws upon well-established principles of modeling, estimation theory, and control theory. Operationally, however, it is a straightforward, easily taught mechanism that can be cost-effectively implemented and effectively employed by the current generation of campaigners.

MPC holds promise for alleviating many of today's planning and execution shortfalls. It will improve the analytical capability of planners and controllers by increasing the role of model-enabled tools for what-if analyses, sensitivity analysis, and unintended/unexpected consequence identification. MPC will bring to bear state-of-the-art optimization techniques, as it improves planning and execution responsiveness, efficiency, and effectiveness. Finally, by providing analysts and decision makers with comprehensive insight into the underpinning model-enabled processes, it will allay the lack of understanding of models, and in turn, the lack of trust in model-based results.

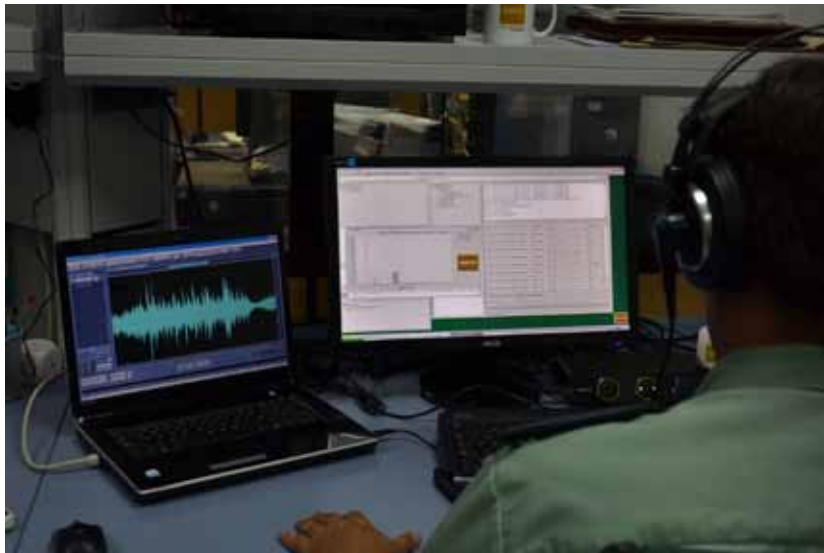
Cyber Defense Applications

Voice Biometrics

Current

This project was selected as a winner of the Global Security Challenge and addresses two key requirements for adapting voice biometrics to mobile systems, including response time (now 15 seconds) and the need to reduce the CPU and memory requirements.

Voice biometrics (speaker recognition) is a highly accurate and easy to use way to identify and authenticate speakers. Just as a person's fingerprints are unique to that person, so is the voice.

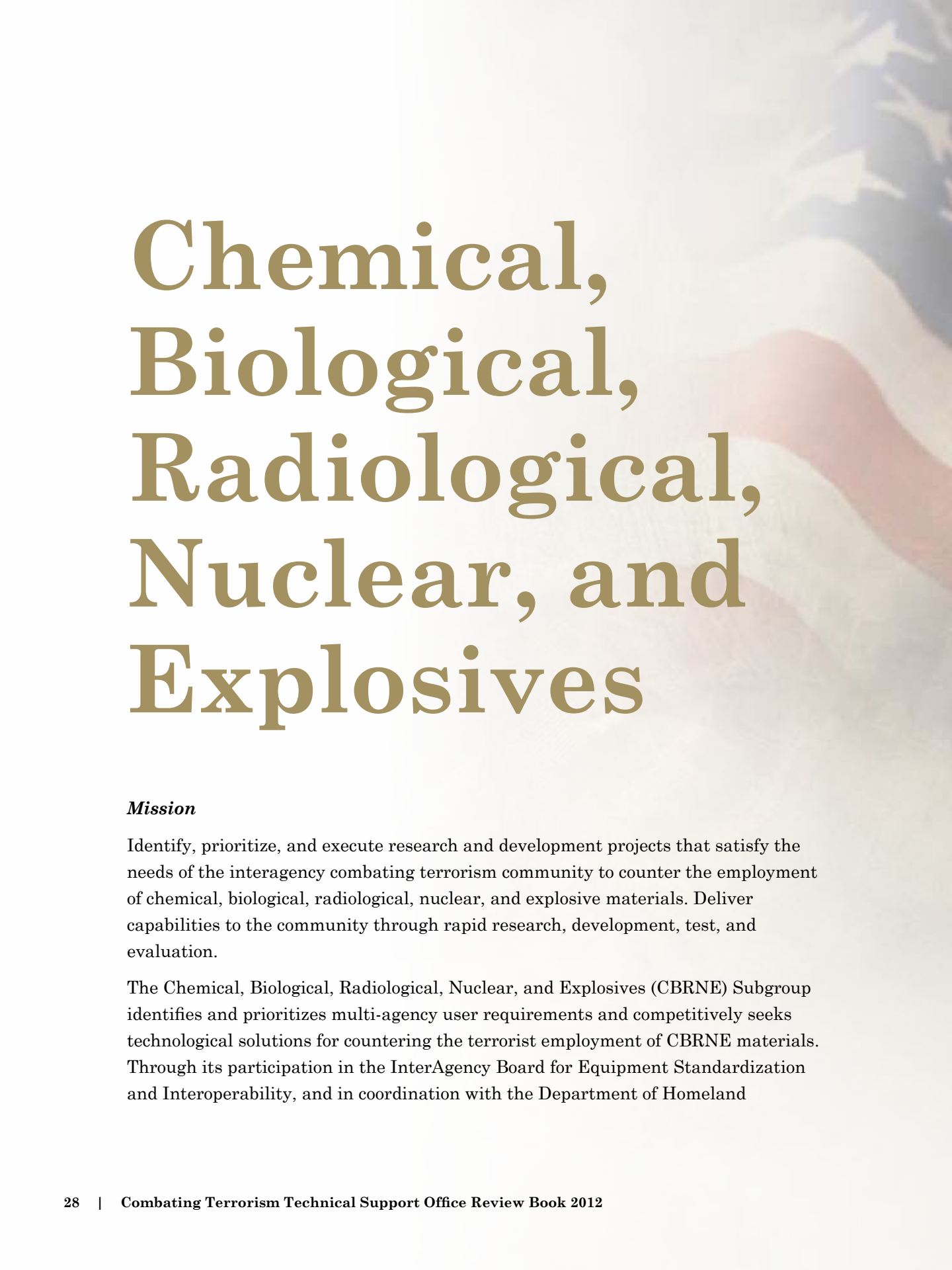




Speaker recognition is used worldwide in intelligence, law enforcement, and homeland and financial security applications. In the law enforcement arena, the accuracy of the technology allows it to be used as evidence in court. Voice is a “standoff” biometric, which means identification of a person can be made without his or her knowledge. This makes it a powerful tool and is the reason for its broad acceptance.

The initial proof of concept has been completed, and discussions are under way to evaluate the tactical deployment of the mobile applications of this technology.





Chemical, Biological, Radiological, Nuclear, and Explosives

Mission

Identify, prioritize, and execute research and development projects that satisfy the needs of the interagency combating terrorism community to counter the employment of chemical, biological, radiological, nuclear, and explosive materials. Deliver capabilities to the community through rapid research, development, test, and evaluation.

The Chemical, Biological, Radiological, Nuclear, and Explosives (CBRNE) Subgroup identifies and prioritizes multi-agency user requirements and competitively seeks technological solutions for countering the terrorist employment of CBRNE materials. Through its participation in the InterAgency Board for Equipment Standardization and Interoperability, and in coordination with the Department of Homeland



Security, the National Institutes of Justice, the Environmental Protection Agency, and other Department of Defense components, the CBRNE Subgroup integrates technology requirements from the fire, hazardous materials, explosives detection, law enforcement, and emergency medical services communities into its process.

Contact Information

cbrnesubgroup@cttso.gov



Focus Areas

Threat Characterization and Attribution

Investigate the unique physical and chemical characteristics of threat materials, develop tools to determine the origin of a piece of CBRNE evidence, evaluate clandestine methods of CBRNE production, and assess the effects of decontamination on CBRNE evidence.

Consequence Management

Develop equipment to counter the intentional and unintentional releases of CBRNE materials, to include decontamination and restoration.

Information Resources

Integrate shared information management tools to provide on-scene situational awareness.

Protection

Operationally enhance individual and collective protection performance while reducing cost. Develop decision support tools to allow operators to make protective equipment decisions based on field-generated physiological data.

Trace Detection

Develop enabling technologies to detect threat materials and their precursors at trace levels.

Bulk Detection

Develop enabling technologies to detect threat materials and their precursors at bulk levels.

Proximity and Standoff Detection

Develop enabling technologies to detect threat materials and their precursors at proximity and standoff distances.



Threat Characterization and Attribution

CB Indicators and Warnings

Completed

Open sourced improvised chemical and biological agent production literature has proliferated extensively. The Chemical and Biological (CB) Indicators and Warnings handbook provides information about general indicators and warnings, production setups, and end products that are representative of plausible improvised production methods of chemical and biological agents following methods found in openly available improvised production literature. The handbooks (For Official Use Only and Secret) provide operators with the ability to potentially identify components of, or whole laboratory setups, for improvised chem/bio laboratories. The handbook and the training aid in improving situational awareness when entering potentially dangerous makeshift labs. More than 35,000 copies of version 2.0 have been delivered to the user community. In December 2011, an updated 3.0 version was released.



Information Resources

Explosives Detection Evaluation Guide

Completed

The Navy Explosives Ordnance Disposal Technology Division (NAVEODTECHDIV) has tested approximately 100 different explosives detection systems in support of military and law enforcement operators. The NAVTECHDIV team developed a comprehensive guidebook, providing a “thumbnail” view of



FirstDefender RM (ver. 1.1.6)
Thermo Scientific (Formerly Alamo)

System Description
The FirstDefender RM is a handheld identification system capable of identifying a wide variety of organic, inorganic, solids or liquids. The instrument is for walk-out use.

Size/Weight
7.6"
1.6" x 4.2" x 1.2"

Expendables
Sample Size: 250 µl/µg
Sample Storage: 8000
Battery Life: 1 yr / 7 hrs

Performance

Min. Sample Size (µg)	Min. Sample Size (µl)	Identification Effectiveness	Min. Time (min)	Max. Time (min)
100	100	99%	30	30
10	10	99%	30	30
1	1	99%	30	30
0.1	0.1	99%	30	30
0.01	0.01	99%	30	30
0.001	0.001	99%	30	30
0.0001	0.0001	99%	30	30
0.00001	0.00001	99%	30	30
0.000001	0.000001	99%	30	30
0.0000001	0.0000001	99%	30	30
0.00000001	0.00000001	99%	30	30
0.000000001	0.000000001	99%	30	30
0.0000000001	0.0000000001	99%	30	30
0.00000000001	0.00000000001	99%	30	30
0.000000000001	0.000000000001	99%	30	30
0.0000000000001	0.0000000000001	99%	30	30
0.00000000000001	0.00000000000001	99%	30	30
0.000000000000001	0.000000000000001	99%	30	30
0.0000000000000001	0.0000000000000001	99%	30	30
0.00000000000000001	0.00000000000000001	99%	30	30
0.000000000000000001	0.000000000000000001	99%	30	30
0.0000000000000000001	0.0000000000000000001	99%	30	30
0.00000000000000000001	0.00000000000000000001	99%	30	30
0.000000000000000000001	0.000000000000000000001	99%	30	30

Notes
*Optional CR123 disposable batteries or rechargeable batteries.
All equipment represented are from a manufacturer of data available.
1. When using primary sampling mode as a laboratory setting if the data is available, then field data was substituted.
Library version listed: 100

References FirstDefender RM and RMX Report published in 2010

62 different systems. The book is divided into systems for trace detection, small bulk detection, and bulk detection. Each specific product is further divided into operation overview and system description, strengths, limitations, system performance, technology, size/weight, cost, battery life, consumables, and specific manufacturers' data. This guide, classified as For Official Use Only, will be useful as an unbiased aid in purchasing equipment, and to help determine if the equipment fits the overall operational need.

Protection

Next Generation CB Garment

Completed



Due to the current operating environment, the need exists for a personal protective ensemble providing reduced thermal burden at the weight of current CB protective ensembles that will enable the users to more effectively conduct missions while continuing to maintain percutaneous protection against chemical warfare agents and toxic industrial chemicals (TICs) in traditional and catastrophic environments. The new garments are necessary to maximize operational performance, individual protective capability, and effectiveness by minimizing the effects of physiological stressors associated with sustained operations with strenuous physical activity while wearing protective garments. Associated increased mobility, increased environmental contaminant performance, and enhanced individual endurance is facilitated by reduced garment weight, bulk, and thermal burden.

W. L. Gore and Associates, in partnership with Lion Apparel, developed a garment that provides National Fire Protection



Association (NFPA) 1994, Class 3 protection while providing a reduction in thermal burden similar to that provided by a standard station/combat uniform. The garment is capable of being worn unobtrusively. The garment is certified to the 2012 edition of NFPA 1994, Class 3 when worn with the appropriate protective gloves, socks, boots, breathing apparatus, and mask to ensure whole-body protection. The garment design does not interfere with the performance of routine and emergency mission duties. The material solution is capable of operating in temperature and humidity extremes and is capable of withstanding salt spray, rain, sand, dust, sweat, oil, and other contaminants.

Noise Filtering SCBA

Completed

The CBRNE subgroup, working with Sound Innovations, recently completed the development of a wireless earpiece capable of providing in-ear voice pickup and communication delivery and the associated printed circuit board (PCB) for incorporation into the communication systems of self-contained breathing apparatus (SCBA) manufacturers. The PCB supplements the existing SCBA microphone signal with the in-ear microphone signal to provide the highest-intelligibility signal possible. Current SCBA systems are hampered by poor intelligibility of the speech signal. The resultant product bridges the gap between limitations in communications. These limitations present a significant safety hazard for first responders and military personnel operating in environments where SCBA use is necessary.

Modular CBRN Hose System

Completed

The traditional approach to CBRN respiratory protection forces operators to select a specific type of equipment for a known threat scenario. An SCBA delivers clean air in an unknown/hazardous environment, but wear duration is typically limited to 30 minutes. The use of a CBRN Powered Air Purifying Respirator (PAPR) extends wear duration significantly (by several hours) with less user burden; however, they cannot be used in unknown or high risk environments. Therefore, the specialist community accepts a number of performance tradeoffs. This leads to a less than optimum tactical approach to missions and increased user risk. Avon Protection Systems, Inc. integrated its existing SCBA Compact Demand Valve technology with new PAPR methodology to deliver a universal hose connection system. This provides a standard interface connection for both SCBA and PAPR systems to be used in combination for increased protection and mission time. In addition, the development delivers a unique low profile connection with air purifying respirators with an optional connection for a heads-up display for greater



situational awareness. The modular hose provides interoperability between existing equipment. It is a universal hose able to combine different systems and provides the ability to change protection modes, depending on the environment.



Universal Mask - XM55

Current

Avon Protection Systems Inc. is developing an improved prototype universal application field protective mask (XM55) capable of providing respiratory and ocular protection from chemical warfare agents, toxic industrial chemicals, toxic industrial materials, biological agent aerosols, and other emerging threats. The M53 mask was originally developed by Avon Protection Systems and was the first mask that was capable of being used in positive and negative pressure modes.

Following extensive field use, end users identified potential enhancements to the original design that would further improve the mask's performance. Avon Protection Systems will substantially evolve the existing M53 mask platform by integrating novel design features to eliminate internal liquid buildup, to improve robustness of the hydration connection, to improve speech clarity, and to increase face seal to suit interface performance.

Trace Detection

HME Trace Detector

Current

The use of agricultural fertilizers as precursors to homemade explosives (HME) used for improvised explosive devices (IEDs) is of great concern to the U.S. military, first responders, law enforcement, and security forces. Most common fertilizers contain nitrogen. It is the nature of the nitrogen-containing compounds that determines whether a fertilizer can be reasonably processed into an explosive. Ammonium nitrate (AN) and urea are explosive precursors; however, AN requires only simply mixing with a fuel to be easily processed and used in an IED. On the other hand, converting urea into an explosive urea nitrate is more difficult to process, making



it less of a threat. An urgent need exists for in-field technology that provides high accuracy, low level detection with low false positives to distinguish between these precursors and harmless compounds.

Quantum Magnetics is developing a robust lightweight handheld explosives detector capable of analyzing particulate inorganic HME threats such as nitrates, chlorates, perchlorates, and permanganates at a limit of detection of less than one microgram while retaining the ability to detect particulate commercial and military threats. The handheld HME trace detector will provide a reliable, low maintenance, simple device capable of operating in diverse environmental conditions to meet customer needs in the field.

Bulk Detection

Countering Improvised Explosive Laboratories

Completed

Clearing insurgent laboratories producing homemade explosives poses a problem of dealing with largely variable materials in terms of sensitivity, physical appearance, chemical, and other properties. A need exists for efficient methods for the detection, identification, and neutralization/desensitization of the improvised explosive laboratories, with minimal collateral damage and minimal interference with troop operations.



Untreated Explosive Detonation



Treated Explosive Detonation



This program demonstrated the feasibility of detecting tri-acetone tri-peroxide (TATP) based explosives in the field through the development of a simple wet chemistry colorimetric kit. To answer the desensitization/neutralization aspect of the effort, a two-part gelation kit was developed that can be applied to a suspect powdered explosive, or explosive precursors, that allows for safe handling of the suspect powder, and subsequent detonation or disposal.

Flash Portal

Current

Arktis Radiation Detectors Ltd is designing and testing a demonstrator using a panel of Helium-4 scintillation-based fast neutron detectors to trigger the readout of gamma detectors, thereby substantially decreasing signal to noise and significantly improving the operational performance of passive detection radiation monitoring portals for the detection of Special Nuclear Materials (SNM). The potential benefits of such a demonstration include an increased sensitivity for passively detecting shielded SNM, a decreased susceptibility to nuisance alarms, and the capability to easily upgrade existing radiation portal monitors to achieve the goals above. This is one element in a multi-layered defensive strategy for countering nuclear terrorism and for counter-proliferation operations. The ability in the field to reliably detect small amounts of SNM in transit will strengthen the security of the United States, its allies, and major United States facilities and bases overseas. This program is being performed in coordination with the UK Atomic Weapons Establishment, the European Commission's Joint Research Centre, and the U.S. Department of Homeland Security's Domestic Nuclear Detection Office.

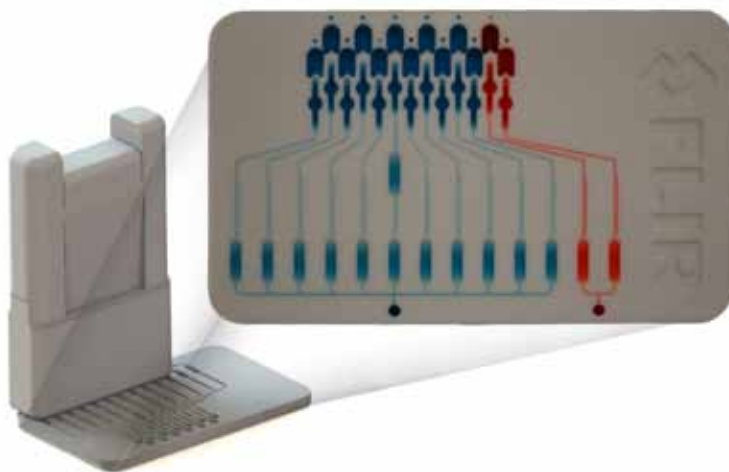




Colorimetric Barcode

Current

The rapid detection and identification of HME precursors is vitally important in military, homeland security, humanitarian, and environmental applications. Colorimetric approaches are valuable due to their relatively low cost, excellent sensitivity, fast speed, portability, and simple operational requirements (no additional power, equipment, or training necessary, enabling rapid deployment in remote areas). While colorimetric approaches for HME precursor detection already exist, they are prone to false positives. A need exists for the development of low-cost, single-use tests to rapidly identify unknown materials. These disposable devices provide enhanced HME precursor detection capabilities in a user-friendly format with lower false positive rates.



FLIR is developing a seamlessly integrated, single-use test kit—sampling device and analysis cassette—for the identification and differentiation of precursors of homemade explosives based on colorimetric detection. The system has demonstrated class-level detection of nitroaromatics, nitrate esters and nitramines, inorganic nitrates, chlorates, and peroxide-based explosives; differentiation between inorganic chlorates and perchlorates, and differentiation of inorganic nitrates and metals.

Proximity and Standoff Detection

Advanced Multi-Antenna Imaging Radar for Suicide Bomber Detection

Current

An active gigahertz microwave imaging sensor system with an extended range of at least 10 meters is being developed. The system will have the capability to detect, assess, and alert on metallic



threat objects such as guns, knives, and non-metallic objects with dielectric constants in the normal range of commercial, military, and homemade explosives concealed under clothing, hand-carried items, and in backpacks.

The current improvements to the Buckler-Davies Consulting Ltd system will allow for the simultaneous processing of at least four people. These developments will provide the capability to process crowds moving through venues in a discreet manner with minimal time delay. The imaging system will include a real-time display with enough fidelity to discern threats immediately. Indicated alerts will be recorded with an optical video image indicating the alert location on the person and the type of threat.



The background of the page is a faded, light-colored American flag, showing the stars and stripes. The title is centered over this background.

Improvised Device Defeat

Mission

Identify, prioritize, and execute projects that satisfy mission critical needs and address interagency requirements for advanced technologies to safely and effectively defeat improvised terrorist devices.

The Improvised Device Defeat (IDD) Subgroup delivers advanced technologies, tools, and information to increase the operational capabilities of the U.S. military explosive ordnance disposal (EOD) community and federal, state, and local bomb squads to defeat and neutralize terrorist devices. In collaboration with military, federal, state, and local agencies, the IDD Subgroup identifies and prioritizes multi-agency user requirements through joint working groups and thorough validation processes.

Contact Information

iddsubgroup@cttso.gov





Focus Areas

Device Defeat

Develop advanced technologies to defeat the broad spectrum of improvised terrorist devices to include IEDs, vehicle-borne improvised explosive devices (VBIEDs), person-borne IEDs (PBIEDs), and enhanced hazard devices containing chemical, biological, or radiological materials. Develop innovative, cost-effective disruption and precision render-safe solutions that increase standoff distance, reduce collateral damage, and decrease risk to the improvised devices defeat operator. Improve neutralization techniques for both sensitive and insensitive explosives and enhanced payloads such as flammable liquids and gases.

Access and Diagnostics

Develop reliable, precise, and cost-effective advanced technical solutions and procedures to improve military and civilian bomb squad technicians' diagnostic analysis of IEDs. Develop and advance technologies that identify and locate the IED, explosive or enhanced fillers, and key fuzing and firing components. Develop testing methodologies and protocols that define and confirm the access, diagnostic tool, or procedure's ability to satisfy expected design and operational parameters.

Emerging Threats

Advance production of effective countermeasures to neutralize or defeat radio-controlled IEDs and provide safe environments for improvised device defeat operators. Develop, characterize, and test technology solutions to effectively render safe improvised devices using novel fuzing systems that incorporate such items as electronic sensors, microcontrollers, or mechatronic¹ components.

¹-Mechatronics adds intelligence to a mechanical design or replaces a mechanical design with an intelligent electronic solution. An example of a mechatronic component is the digital thermostat, which has replaced the much more inefficient mechanical thermostat. Digital thermostats are more accurate and are typically programmable, allowing for increased efficiency.



Remote Procedures

Develop advanced application systems to remotely access, diagnose, and defeat improvised devices. Advance development of manufacturer- and model-independent products and robotics with plug and play interface. Develop open architecture, navigation, communication, and operator controls for robotic platforms, tools, and sensors.

Tool Characterization and Information Resources

Improve performance evaluation methodologies, test procedures, and tool characterization models for improvised device defeat technologies. Conduct ongoing evaluation and improvement of tools, methods, and protocols for confirming the accuracy of detection equipment, reliability of diagnostic tools, and completeness of neutralization and render safe techniques. Advance training concepts and information delivery systems that promote the tactical and operational response readiness required to effectively, safely, and efficiently counter improvised devices and emerging terrorist threats.

Maritime Security

Develop technologies to protect ships, boats, docking facilities, offshore platforms, shoreside loading facilities, power plants, bridges, and marine cables and pipelines from any form of terrorist attack, including water-borne and underwater IEDs. Develop and test technologies to include manned or unmanned long- and short-range sensors for detection and tracking; physical barriers and stopping devices; unmanned surface, underwater, and air vehicles; weapons; armor; life support; diving and underwater systems; and mammal systems.



Device Defeat

Vehicle-Borne Improvised Explosive Device Tool Kit

Completed

Vehicle-borne improvised explosive devices (VBIEDs) are devastating terrorist tools that must be effectively and efficiently mitigated by bomb squads. The IDD Subgroup, in cooperation with the Israel National Police, developed a robotically employed standardized tool kit to address a VBIED. The Vehicle-Borne Improvised Explosive Device Tool Kit (VBIEDTK) is delivered and operated on robotic systems utilized by U.S. federal, state, and local bomb squads and military explosive ordnance disposal teams. The tools address commonly encountered obstacles in order to access, penetrate, hold in place, remove large bulks, and reach difficult locations inside and under the vehicle. The tool kit is an assembly of five item kits that include an extender kit, an extended gripper, a vehicle lift, power tools, and a remote X-ray bracket. The tool kit was designed by bomb technicians based on their experience and operational needs in rendering safe VBIEDs utilizing robots. Additionally, the tool kit has been evaluated in partnership with the Department of Homeland Security Science and Technology Directorate. The VBIEDTK will be available in the near future through commercial vendors.

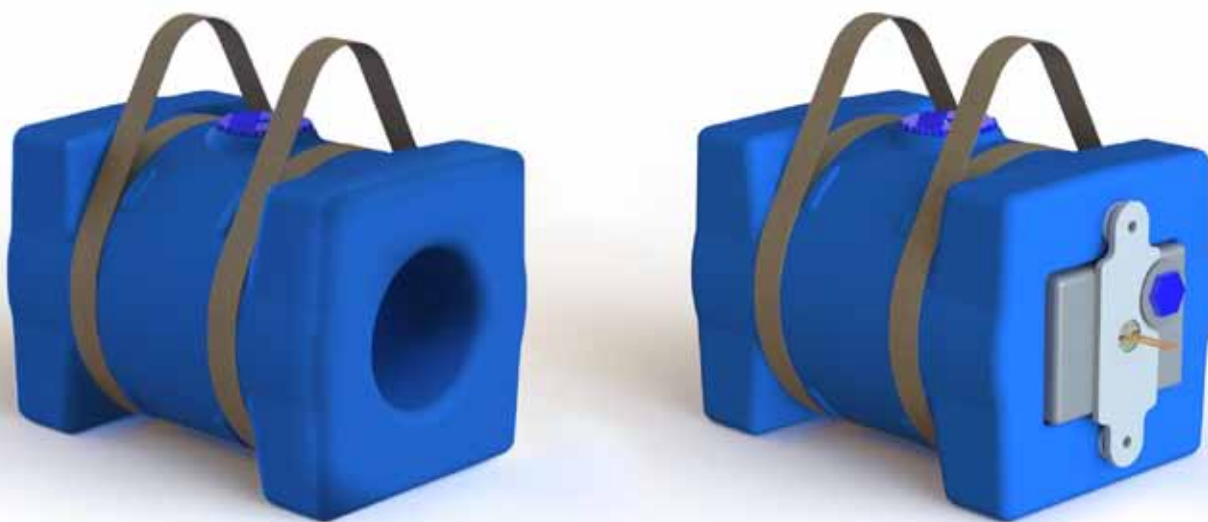




Commercialization of SIDD

Current

The Scalable Improvised Device Defeat (SIDD) system is an explosively-driven water-jet disrupter system that offers tactical flexibility to deal with a variety of vehicle-borne and other static threats while minimizing collateral damage and cost. Applied Research Associates, Inc. has developed the SIDD as a response to a need for an affordable VBIED disruption device that exhibits minimal collateral damage. The SIDD system is a tested tool for military EOD units and civilian bomb squads, with two previous generations of technical advancement under TSWG's management. This next generation development effort retained the critical geometry and performance capabilities of the previous generation design, while improving the deployability and operational features of the overall system. The SIDD features non-fragmenting, non-metallic construction with ideal geometric dimensions for disruption capability and has demonstrated highly effective penetration during field testing using C4 drivers. The 5, 15, and 30 gallon SIDD systems can be rapidly deployed manually or with robotic or remotely-operated vehicles. The initial manufacturing run will be 150 units (50 of each size) for field evaluation by various end users. In the future, the plastic injection mold designs for all sizes will be in place. The systems will be fully manufacturable in any quantity needed, and end users will be able to acquire additional SIDD units at lower cost.





Remote Procedures

Body Bomb Tool Kit

Completed

The Improvised Device Defeat Subgroup, in cooperation with the Israel National Police, developed a robotically employed Body Bomb Tool Kit (BBTK). The BBTK consists of various tools to efficiently and successfully remove and render safe a person-borne improvised explosive device (PBIED). The tools are designed to allow the robot to change tools remotely while at the crisis site without having to return to the safe area, thereby saving time and conserving robot battery power. The BBTK consists of a tool mount and 15 assorted tools, including knives, grippers, scissors, car door openers, and tools for piercing and tearing. The tool kit was designed by bomb technicians based on their experience and operational needs in rendering safe body bombs using robots. Additionally, the tool kit has been evaluated in partnership with the Department of Homeland Security Science and Technology Directorate. The BBTK will be available in the near future through commercial vendors.



iLIVE Video Enhancement System

Current

A current shortfall of many unmanned ground vehicle cameras is that their optics are not designed for maximum efficiency in all lighting conditions. The inLine Instant Video Enhancement (iLive) System provides an enhanced viewing capability for camera operators in low light conditions. Using the Lightweight Enhanced Night/Day Vision System software library, the iLIVE system can turn



night into day and offer enhanced viewing and targeting for EOD robotics and remote cameras. The iLIVE is compatible with analog or digital video inputs and can deliver the enhanced images to any video display system chosen by the user. The iLIVE system leverages existing camera systems using a highly innovative software library implemented on a multimedia digital signal processing chip, giving the user unprecedented viewing and usability and targeting functions. The iLIVE's small footprint and power requirements enable mounting to many remotely-operated vehicles on sea, land or air, as well as to fixed camera assets, with little to no impact on the performance of the chosen vehicle or system.



Tool Characterization and Information Resources

Bomb Technician Wiki

Current

Bomb squads are investing in 21st Century technology to keep abreast of the threats and information that have an effect on their day-to-day responses. The Bomb Tech wikipedia (wiki) will provide state and local bomb squads with an unclassified, collaboratively edited, Internet encyclopedia reference wiki. The bomb technician will be able to post information to the wiki that can be expanded upon by other bomb technicians and provide an easily accessible repository of useful, unclassified information in one place. More than 460 accredited bomb squads exist throughout the U.S., and they are diverse in geography and experience. TSWG has funded development of the wiki, which will be hosted on the National Bomb Squad Commander's Advisory Board's Web site with appropriate security. The community-driven wiki will use industry standard software. The wiki will be a repository for useful reference material for all accredited bomb technicians. Material on the wiki will be a useful mix of references, guides, and definitions covering policy, operations, training, equipment, technical, and historical matters. The wiki will be able to be accessed, and contributed to, by more than 3,000 personnel in the community.

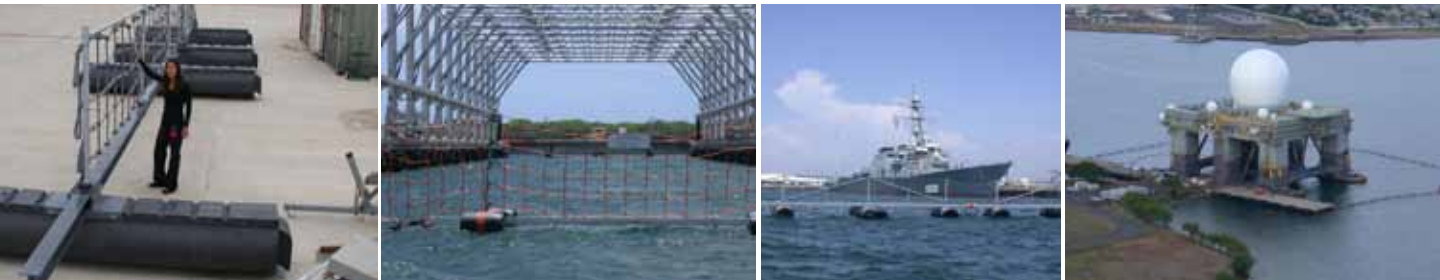


Maritime Security

Mobile Port Security Barrier

Completed

Water-borne improvised explosive devices (WBIEDs) are a viable threat to maritime interests overseas and in U.S. ports. The Navy must protect infrastructure and platforms worth upwards of billions of dollars each. Waterfront boat barriers can significantly reduce the WBIED threat by marking restricted waters, discouraging attack, establishing “temper and intent”, and stopping or delaying attackers. A study concluded that existing Navy barrier systems could be downsized to achieve significant reductions in barrier weight and cost and make the system that much easier to ship, store, deploy, and recover. The IDD Subgroup and the Navy Facilities Engineering Support Center have developed a rapidly deployable and recoverable Mobile Port Security Barrier system (PSB-X) that can be deployed from land or sea vessel and provide protection against WBIEDs. The expeditionary system is mobile and lightweight to allow easy transport and storage in 40-foot shipping containers as well as rapid deployment and recovery for pierside and harbor anchorages. The PSB-X system will be used in defining perimeters, such as a desired safe zone around a vessel, for supplemental maritime security, and for temporary area denial.



Advanced Diver Mask Mounted Display

Completed

The Advanced Diver Mask-Mounted Display (MMD) provides Navy divers with significantly clearer vision while underwater. The diver binocular MMD was initially developed by Naval Surface Warfare Center Panama City Division (NSWC PCD) several years ago, and NSWC PCD subsequently obtained a government-owned patent for



the system. With subsequent interest in the MMD system from the United Kingdom, NSWC PCD initiated a partnership and licensing agreement with Sound Metrics Corporation through a Cooperative Research and Development Agreement to transition the technology to production manufacturing. Sound Metrics Corporation is also the developer of the Dual-Imaging Digital Sonar-Diver Held (DIDSOH-DH). Sound Metrics is now manufacturing and marketing the Navy design as a commercial product available to military and civilian divers and marketing the MMD as a portable, high-data content (sonar, video), standard interface data display that can be purchased individually or integrated with the DIDSOH-DH. The transformational flip-up, flip-down device allows divers to clearly see what they are doing, whether looking for mines, scanning for intruders, inspecting ship hulls, searching for evidence, or recovering a body.



The background of the page is a faded, high-angle view of the United States flag, showing the stars and stripes in a soft, light tone.

Investigative Support and Forensics

Mission

Identify, prioritize, and execute research and development projects of multi-agency interest that provide investigative and forensic support to terrorist-related counteraction, investigations, and analysis.

The Investigative Support and Forensics (ISF) Subgroup executes wide-ranging research and development to advance investigative and forensic science. The subgroup emphasizes the areas of crime scene response, forensic intelligence, individual identification techniques, and electronic evidence analysis. ISF works with a diverse group of federal and state law enforcement agencies as well as the Department of Defense and Intelligence Community to produce advanced and new technology that improves their mission capabilities for combating terrorism. The subgroup's work has been groundbreaking and has affected forensics throughout the law enforcement world and the military.

Contact Information

isfsubgroup@cttso.gov





Focus Areas

Crime Scene Response

Improve the quality of recognition, documentation, collection, and preservation of evidence as well as the safety of first responders at a scene. Improve the capability of first responders and forensic examiners to process and record terrorist incident scenes for future prosecution.

Criminalistics

Advance the capability to identify and evaluate physical evidence by the application of physical and natural sciences and technology. Improve the efficiency and speed of the analysis and evaluation of physical evidence and the reporting of results to end users. Develop new and more efficient traditional forensic capabilities.

Electronic Evidence

Develop computer forensic hardware, software, decryption tools, and digital methods to investigate terrorism. Identify computer systems and media used by terrorists, and acquire from them the maximum amount of evidence. Develop advanced methods to extract and enhance audio recordings and video images from surveillance sources. Improve techniques for the analysis of electronic devices to obtain the most forensic information.

Forensic Intelligence

Develop advanced and new multi-disciplinary forensic and scientific techniques to perform sensitive site exploitation and process incident scenes to acquire, collate, analyze, and disseminate law enforcement and tactical actionable intelligence and information. Develop improved interrogation, interviewing, and credibility assessment methods. Improve law enforcement related technical surveillance methods.

Identity Knowledge

Develop new scientific technology for the specific identification of individuals who have committed or are associated with terrorist acts. Improve the capability to use physical evidence to individualize or classify subjects or persons of interest.



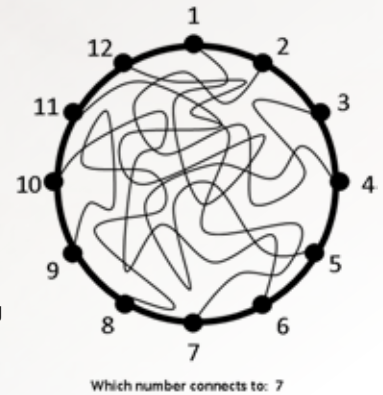
Criminalistics



Scientific Review of Friction Ridge Examination Protocols and Procedures

Completed

Fingerprint examinations still result in more successful identifications of criminals and terrorists than any other forensic method. However, the methods and protocols for fingerprint analysis and examinations have been less scrutinized for scientific validity than DNA procedures. This project, performed by Cognitive Consultants International Ltd. examined the fingerprinting procedures presently being used by forensic laboratories to determine their efficiency and scientific validity. The effect of biases was also critically analyzed. The research developed some standardized guidelines to promote consistent implementation of industry-accepted scientific standards for the examination processes. These standards were then tested, revised, and disseminated through the forensic community.



Thermal Ribbon Analysis Platform

Current

Fraudulent and counterfeit documents are an essential tool for terrorists and criminals when they engage in many activities such as illegal border crossings, credit card fraud, financial crimes, and unauthorized entry of facilities. When high quality, commercial-type images are required, the documents are most often produced on printers with thermal ribbons. Any given portion of a thermal ribbon is only used one time, so it retains a latent image of what it printed. Locating these images and synchronizing the images





of the different colored ribbons can produce a complete image of what was printed. This will positively identify the specific printer used for a given document as well as determine exactly what was printed when the counterfeit document is unavailable. Quantum Signal LLC is developing a hardware-software system that rapidly identifies and extracts the latent images on thermal ribbons and then reproduces an image of the document or graphics. The system will allow for the enhancement of recovered images and will track the entire forensic process to ensure admissibility in court. The hardware will easily fit on a bench or countertop and will require a minimal amount of training time to operate. The end result will be an efficient comprehensive tool to identify what printer created a document or image without actually reconstituting the document.

Electronic Evidence

Digital Video Player Library Link

Completed

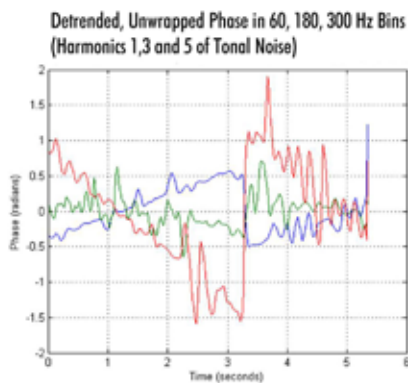
With digital video cameras being frequently used for surveillance and security purposes, recordings related to terrorist and criminal activities are frequently collected as evidence. The lack of standardization and the large number of proprietary formats create a severe challenge when they are forensically examined or analyzed. The examiner may spend much effort and time to gather technical data about the specific equipment that was used. Signalscape Inc. is setting up a video library link on an FBI Web site to overcome these difficulties. The Web site is available to law enforcement and combating terrorism agencies. The site includes information about the software required to play back the recorded evidence along with technical data about the equipment. Images of players and their components, easily searchable databases, and links to the manufacturers are available. The library link contains a searchable database that connects video file extensions to their specific players. The library link directs investigators to a manufacturer Web site to download the appropriate software or links them to an archive where the software can be downloaded when available. The library also provides manufacturer points of contact, making it possible for investigators to directly connect with the manufacturers when necessary.



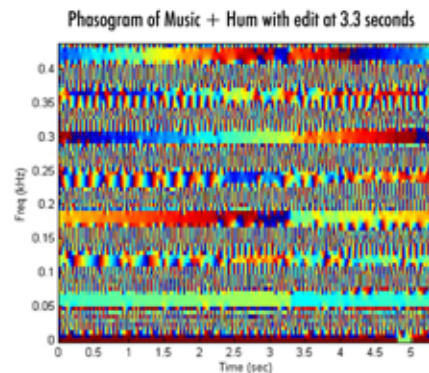
Validating Phase Discontinuity as Authentication Indicator

Completed

During counterterrorism and criminal investigations, forensic examiners must often determine if audio tracks in digital recordings have been tampered with or altered. As the terrorists and criminals have gained more expertise in this area, better and more sophisticated technology is needed to identify alterations. Southwest Research Institute developed a new forensic technique to better verify tampering or altering in audio recordings by examining phase discontinuity of various signals within the recordings. Many different tones and signals may be present on a recording. When altering and tampering occurs, some of these are likely to show phase discontinuity. Likewise, when the recording has many signals that all show continuity, no tampering has likely occurred. This method can not only show if altering of the recording has occurred, but it can also show the specific location. Additionally, a corpus of recordings was produced that included multiple variables such as sources and levels of usable tones, noise, distortions, and confounding factors. The corpus can be used to determine the effects the variables have on the developed forensic techniques. The final product also includes the best ways to apply the techniques in forensic examinations.



A more quantitative representation of the way the phase discontinuity detection algorithm would work is shown here, where coincident phase jumps in three different harmonics of the tonal noise signal are shown. Coincidence detection will improve the accuracy of the algorithm but may require user input to provide a rough guess as to the fundamental frequency of the tonal noise.



Validating Phase Discontinuity as Authentication Indicator involves analyzing signals having embedded tonal noise such as the one shown here, which has speech with 60-Hz hum in the background. The algorithm used looks for abrupt changes in the color of the 180-Hz band near the middle of the frame as being indicative of an edit.



Data Recovery from Memory Components

Current

Although electronic equipment and instruments such as mobile computing devices, smartphones, portable GPS navigators, cameras, portable audio and video recorders, and automotive engine control and safety systems are readily destroyed during explosions and transportation crashes, the memory components often survive intact. The data within these components can provide a wealth of intelligence and evidence about the related incident. General Dynamics Information Technology is developing a software tool capable of extracting, interpreting, and saving the digital data recovered from the memory components of damaged electronic devices. The tool will use a graphical user interface based software tool that is capable of advanced data mining techniques to enable the exploration of raw binary data that has been imaged directly from the original memory component. It will provide visualization to assist in the identification of patterns in the raw data indicative of useful information. The system will run on PC-based systems and will be fully capable of exporting the data and files to other storage media as well as fully documenting the performed processes.

Forensic Intelligence

Automated Facial Expression Recognition System Next Generation

Completed

The automated facial expression recognition system, previously developed in a CTTSO project, helped determine credibility by the analysis of facial micro-expressions. These expressions are less than a tenth of a second in duration and not usually observed, nor are people aware that they make them. The expressions, which reveal seven different emotions, have been found to be consistent in all cultures and can be used to determine credibility. This project, performed by Platinum Solutions, advanced the technology level to make an operational system with more capabilities than the previous version. Besides video recording the face and audio during an interview to identify the micro-expressions, the next



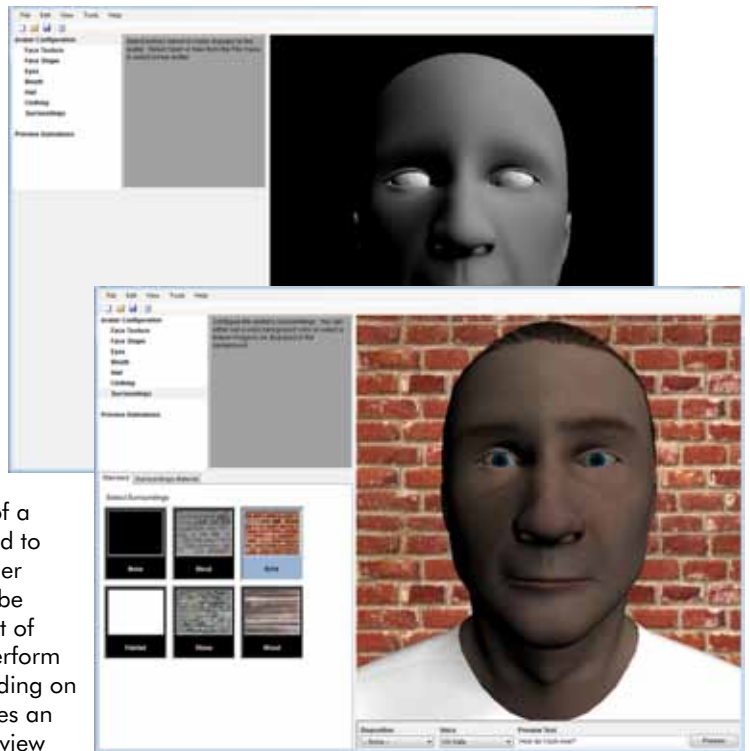


generation version provides a number of new capabilities. One capability is a speech-to-text feature that distinguishes between the interviewer and the interviewee as well as fully synchronizes the text with the audio. Another new capability is a searchable database of the interview recordings that is part of an overall case management system. This version operates much faster and is ruggedized, compact, and weighs less than 20 pounds, including the case.

Avatar

Completed

Many factors affect the amount and quality of information during interviews. Research has shown that a person will relate better to the questioner and provide more information when they belong to the same racial, ethnic, and gender categories. Another factor that produces better results is when the questions and the process are standardized. The Avatar system was designed and built to capitalize on these factors. Avatar can create a computer image of the head and shoulders of a male or female that can be adjusted to match the race, ethnicity, and gender of the interviewee. The system can be programmed for a standardized set of questions that can automatically perform some follow-up questioning depending on the answers provided. Avatar creates an audio and video record of the interview with a written transcript that makes extensive post-interview analysis possible. The records are easily searchable and can be merged into other files. Avatar also allows the operator to key in changes or edits to their responses for better accuracy.



Digital Communication Analysis for Insider Threat

Current

Protecting against a threat to an organization from within its own ranks is difficult and easy to miss. An attack from inside has the potential for causing more physical, financial, and psychological damage than an external attack. Within any organization, large amounts of digital text communications exist that can reveal a profile of the psychological, mental, and emotional states of the author.



Charles River Analytics is developing an assessment software tool that automatically analyzes digital communications such as e-mails to detect disgruntlement, anger, psychological states, attitudes, and personal characteristics of the persons within the organization. The assessments will produce a prediction of the likelihood of physical violence, espionage, sabotage, and information theft by the author of the messages. The software tool will be insertable at various levels into communication systems and their databases. After searching and analyzing the messages for specific words, patterns of words, linguistic traits, tendencies, and other information that can identify persons who have specific risk factors, it will produce a relative index of the likelihood of certain future behaviors. The index will allow investigators and security personnel to focus their efforts for follow-up action on those most likely to be an insider threat.

Head Mounted Credibility Assessment System

Current

U.S. military, law enforcement, and intelligence personnel have a need for a screening credibility assessment system for their combating terrorism operations. The system needs to be accurate, efficient, and have a low inconclusive rate as well as be quick and easy to employ and require a minimal amount of training to operate. Azimuth Incorporated is developing the Head Mounted Credibility Assessment Screening System that will provide U.S. forces with these capabilities. This new system will exploit pupillary response, electro-dermal activity (skin moisture), and heartbeat as its primary physiological traits. The sensors will be positioned in a head-mounted device and will collect their signals in a non-obtrusive manner. Algorithms in an attached computer tablet will process the signals and provide numerical values to the operator for a real-time determination of credibility of the interviewee. The system will function for four hours on rechargeable batteries and will be lightweight, rugged, and highly portable.

Identity Knowledge

Separation of Complex DNA Mixtures

Current

Terrorists and criminals frequently leave DNA evidence at crime scenes or other locations that can be used to identify them and where they have been. The DNA identification techniques are now



so powerful and sensitive that multiple sources of DNA often are found in a sample. This usually prevents a positive identification of any of the persons who are a source of the DNA in the mixture. If the DNA can be separated and then analyzed, these mixed samples can provide an incredible amount of evidence and intelligence value. The Bode Technology Group is developing a procedure that separates samples with multiple sources of DNA. The process will then allow individual DNA profiles to be obtained for each of the different sources. The procedure will work on samples with as many as seven different DNA sources and have a relatively rapid turnaround. Computational analysis methods will be included in the overall process to provide greater resolving power. The project will also ensure that the procedures developed will meet the Daubert legal standards to make the results admissible in court.



Personnel Protection

Mission

Identify, prioritize, and execute research and development projects that will provide advanced tools, techniques, and guidelines to satisfy interagency requirements for enhanced personnel security.

The Personnel Protection (PP) Subgroup develops new equipment, reference tools, and standards to improve the protection of high-risk personnel (HRP). Projects focus on putting innovative tools such as automated information management systems, communication devices, mobile surveillance systems, as well as personnel and vehicle protection equipment, in the hands of those tasked with the safety of HRP. The subgroup delivers new technologies to military, federal, state, and local law enforcement protection details.

Contact Information

ppsubgroup@cttso.gov





Focus Areas

Communications, Surveillance, and Reconnaissance

Develop technology that provides military and law enforcement personnel with a greater capability of covertly communicating and collecting surveillance data to identify and mitigate terrorist threats against personnel. Provide personnel with tools to tag, track, and locate mission critical personnel. Develop technology that enhances situational awareness of mission operations.

Individual Protection and Survivability

Enhance the protection of personnel during blast and ballistic events. Develop technology that increases the performance of body armor by reducing weight and optimizing material performance. Develop test devices and procedures that provide more biofidelic responses during blast and ballistic testing events in order to mitigate the probability of personnel injury. Quantify the effects of conventional and enhanced blast damage mechanisms to the human body.

Information Resources

Develop reference materials, information management systems, and analytical tools to improve mission preparation, facilitate decision making, and advance incident response capabilities. Enhance software tools to more efficiently exploit intelligence and surveillance data. Generate tools that will augment the detection of networks, relationship resolution, and tracking of terrorists through large amounts of data.

Mobile Security

Enhance personnel protection during vehicular, marine, and air transportation. Develop techniques to increase protection against blast and ballistic threats during transit. Conduct performance evaluations and studies to assess the protection capabilities of transport mechanisms, and generate solutions to optimize protection.



Communications, Surveillance, and Reconnaissance

Instant Eye

Current

Today's war fighter is often operating in small units far from support elements, including unmanned aerial system (UAS) assets. A stealthy overhead intelligence, surveillance, and reconnaissance asset that can be launched from behind cover to gain situational awareness will allow soldiers to more effectively and safely conduct their missions. Physical Sciences, Inc. is developing Instant Eye, a small unmanned aerial system that provides the individual soldier with instantaneous overhead video surveillance on demand. The Instant Eye would be launched by a soldier and directed to position where its onboard video cameras can view the targeted area. It was designed to operate effectively in stressing combat environments, with autonomous features that enable the UAS to hold position until repositioned, recalled, or discarded. This system requires less than 30 minutes of training to be able to fly the Instant Eye for a basic surveillance mission.

Special Forces soldiers will evaluate Instant Eye for rooftop, doorway, and culvert clearance, as well as general surveillance and reconnaissance capabilities. The Mk-2 Instant Eye, delivered in August 2012, is packaged in a ruggedized container and is comprised of one game controller-like ground control system and two UASs, as well as spare parts. The UAS weighs just under one pound and features forward and downward looking electro-optical cameras, downward infrared illuminators, digital communication with a range of 1,000 meters line-of-sight, video range of 1,000 meters line-of-sight, and ruggedized propellers that are impervious to grass and minor crashes. The Mk-2 Instant Eye is inaudible at 100 feet, can sustain up to 25 mile per hour winds, has a max speed of 55 miles per hour, and a max altitude of 15,000 feet, and a 20 minute battery life. Up to four Instant Eye systems can operate within the same mission space. The Mk-3 Instant Eye planned for fiscal year 13 will improve the current flight duration, wind performance, and overall durability and have an Android compatible control system.





Mobile Surveillance Platform Gen4

Current

The government previously developed a mobile surveillance system that simultaneously captured, recorded, encrypted, and streamed multichannel video and audio with associated GPS position

information and other metadata. Video, audio, and metadata is acquired using a low-footprint, custom-designed encoder that captures high-quality video and audio directly to internal storage for later retrieval, while simultaneously streaming secured, medium-quality video and audio over the cellular network to a single head-end server located in a Command Center. The head-end server then makes all video, audio, GPS positioning, and other metadata available to the end user on a local area network through a proprietary desktop application. This capability was very useful, except that it was limited on the ability to directly be modified or integrated with other government systems.



Cybernet Systems Corporation is developing the Mobile Surveillance Platform (MSP) Gen4, an improved version of the previous system with a well documented application programming interface. The MSP Gen4 will function over low-bandwidth high-jitter networks with more robust hardware at a reduced size. The system will allow users to capture surveillance data in both mobile and fixed site tactical scenarios.

Individual Protection and Survivability



Multi-Threat Concealable Body Armor

Completed

The threats faced by federal law enforcement officers are varied and include both ballistic attacks as well as stabbing attacks from cutting and puncturing weapons. Many of these officers rely on their protective equipment being undetectable to potential armed attackers. Previously available multi-threat body armor systems failed to achieve the requisite level of concealability; therefore, a truly concealable multi-threat body armor system that provides



both ballistic protection and knife and spike protection was needed. ArmorWorks designed and developed a Multi-Threat Concealable Body Armor (MTCBA) system that combines a lightweight and modular hybrid soft armor package with a low-profile, form-fitting, yet breathable carrier. The MTCBA system was designed to meet NIJ Level II ballistic requirements and NIJ Level I Spike and P1 Knife protection classes. The MTCBA is available to law enforcement customers through direct sale with ArmorWorks.



Ballistic Blunt Trauma Test Rig

Completed

Current methods used to assess injury probability from behind armor blunt trauma (BABT) is by shooting body armor with a soft clay backing, which measures the indentation created by the deformation of the non-penetrating ballistic impact. BABT is determined by the depth of penetration in clay. If the deformation in the clay exceeds 44 millimeters, the body armor fails. Although this method has been an inexpensive reliable standard for estimating injury, it does not provide the ability to estimate the internal injury probability based on the dynamic deflection of a non-penetrating round. The original Ballistic Blunt Trauma Test Rig (BTTR) was initially developed by Biokinetics but needed further optimization to ensure the accuracy in determining the probability and severity of BABT from a non-penetrating ballistic impact. The improvements that Biokinetics made to the BTTR improved its usability and reliability without affecting its overall response. The membrane deflection was maintained within the biofidelity corridors, and the variability between impact locations has been vastly improved over the previous BTTR version. Test rigs have been provided to the National Institute of Standards and Technology for test and evaluation for potential modifications to the testing and qualification of body armor.



Behind Armor Blunt Trauma Recreations Study

Completed

Behind armor blunt trauma from a ballistic event has the potential to result in severe incapacitating injuries. In order to test and qualify that armor protects against injury from BABT, current testing is performed where body armor is applied to a backing of Roma Plastilina Clay. The body armor is tested so that when the depth of penetration in clay exceeds 44 millimeters as a result of non-penetrating impact, the body armor fails. Clay has been the chosen medium to test body armor due to its ease of use, mechanical properties, cost effectiveness, and repeatability. Prior to this study, no correlation of human injury to the BABT standard existed. In an effort to correlate real world ballistic events with laboratory results, the United States and the United Kingdom teamed together to jointly collect incident report studies to obtain medical, ballistic, and



circumstantial data for 34 cases. When data from both the U.S. and the UK were comprised, they were able to recreate the real world scenarios in the laboratory and undergo ballistic testing using the same armor systems worn during actual events. All of the cases that were collected and used as a part of the study had mild to moderate injuries that did not result in loss of life. The data demonstrated that the current method for evaluating BABT is a reliable and appropriate method to ensure BABT does not result in severe injuries. This study was the first of its kind to take real world events and correlate them to laboratory testing procedures. The research demonstrated the validity of the current standard; however, with the advent of new body armor testing methodologies, the method used to assess BABT will have to be re-evaluated. The data generated by this study will provide a basis for future testing and developing new standards.

Whole Body Blast Biomechanics

Completed

Current military conflicts have seen an increase in exposure to blast loading both in vehicular and dismounted scenarios. In order to develop better vehicle protection capabilities, test dummies are required to provide injury probability results. The blast test and evaluation community has been using the anthropomorphic test device (ATD) – the Hybrid III – that was originally developed by the automotive community for crash testing. The problem with using the current Hybrid III ATD is the fact that the test device was developed for the automotive industry and crash testing, which experience loads and rates that are much lower than those experienced





during a blast event. By using an ATD tuned for events that occur at lower velocities, it begs the question whether the ATDs are providing accurate results. In an effort to develop an ATD that is tuned for the blast environment, Wayne State University has teamed with the United Kingdom (UK) to optimize the ATD for blast loading. The overall concept of the program is that the UK performed free field vehicle blast testing with an ATD and measured deflections during the blast event. The data collected in the UK is then provided to Wayne State University to recreate the same loading conditions in the laboratory using postmortem human samples. Based on the results of the laboratory testing, recommendations on how to modify components of the ATD have been made so that the ATD ultimately provides a biofidelic response in the blast regime. A blast optimized ATD will be an invaluable tool for the test and evaluation community as well as armor developers and manufacturers so that better protection systems can be created.

Blast Effects on People Wearing Helmets

Current

The incidence of brain injuries has increased significantly during recent conflicts. This could be due to improved body armor that enhances soldier survivability in events that would have been fatal in previous conflicts as well as the changed nature of combat and associated threats. Explosive devices can cause injuries via high-force blast waves, fragment penetration, and blunt impact/acceleration. Understandably, current combat helmets, designed to defeat ballistic threats and to attenuate low-level impacts, may not protect adequately against blast weapons. The unique pathophysiological mechanisms underlying primary blast waves may induce traumatic brain injury. The effects on the soldiers can be devastating, with survivors experiencing chronic headaches, sensitivity to light or noise, impaired memory, loss in problem-solving abilities, and other significant cognitive and behavioral changes. A better understanding of the effects of blast overpressure on the head is required to fully prevent and mitigate brain injury. While efforts are ongoing to research blast brain injury cases, this joint effort with Canada and the U.S. seeks to develop a tool to quantify blast overpressure experienced by the head. The tool being developed is a robust headform that can be used for blast testing. The headform will be biofidelic in that it will be as human-like as possible with a hard exterior shell, nasal cavities, and a gel-like substance to act as brain material. Pressure sensors will be placed inside the headform, and accelerometers will be placed on the exterior of the headform. Both sensors will provide valuable data to assess loads experienced by the head during blast events. Upon project completion, two headforms will be delivered and used for test and evaluation of head protection systems.



Mobile Security


Vehicle in Crowd

Current

A need exists for armored personnel or military vehicles to be able to quickly maneuver through crowds of unarmed but non-compliant and/or aggressive people in a way that protects both the occupants of the vehicle and the people within the crowd. Traditional methods of crowd control that make use of less-than-lethal munitions are sometimes deemed unacceptable because of the offensive perception that comes with their use. To address this requirement, Applied Research Associates, Inc. is developing the Integrated Conveyance Escort (ICE) system. The ICE system will allow small sound generators, placed inconspicuously on the host vehicle, to deliver a variable acoustic output at frequencies below the audible range and capable of maintaining a 10 meter standoff. The ICE system will also include a high frequency, modulated electrical pulse that can be used for individuals seeking to contact the vehicle despite the discomfort of the sound generators. The operators within the vehicle can choose to regulate delivered electrical pulses as well as couple them with the acoustic signals to selected zones. The ICE system will operate independent of vehicle power, install without permanent modification to the vehicle, and fit within a single 6,000 cubic inch transit case.







Physical Security

Mission

Identify and prioritize interagency physical security requirements to protect forces, vital equipment, and facilities against terrorist attacks, execute research and development projects that address those requirements, and transition successful prototypes into programs of record or into immediate field use to meet urgent operational needs.

The Physical Security (PS) Subgroup identifies the physical security requirements of federal, state, and local agencies, both within the United States and abroad, and develops technologies to protect their personnel and property from terrorist attacks. The subgroup manages projects to develop prototype hardware, software, and systems for technical and operational evaluation by user agencies.

Contact Information

pssubgroup@cttso.gov





Focus Areas

Blast Effects and Mitigation

Test and evaluate infrastructure components and systems to investigate and characterize potential damage to identify mitigation strategies to protect against current and evolving threats. Components include but are not limited to: buildings, bridges, tunnels, and structural members. Develop test protocols to ensure repeatable and consistent results where components and threats require evaluation under unique circumstances. Emphasize blast, debris, and shrapnel effects. Testing may also include gunfire, mortars, and rockets. Mitigation strategies may include hardened infrastructure, improved design standards, retrofit techniques, and new design criteria.

Emerging Explosive Threats

Develop projects to satisfy interagency and international requirements that address the adaptive threat associated with emerging explosives. Emphasize characterization of explosives and novel delivery techniques to combat their use in terrorist activities. Coordinate requirements received from the Homemade Explosives Working Group across appropriate CTTSO programs.

Vulnerability Identification

Develop predictive analysis software and decision aids to identify vulnerabilities and/or determine preventative courses of action. Emphasize pre-event planning and assessment of emerging threats.



Screening, Surveillance, and Detection

Develop technologies and techniques to survey and analyze facilities; improve situational awareness; detect, identify, and locate advancing threats; control access to critical assets; and neutralize confirmed threats. Emphasize automatic alerting, expeditionary kits, and exportable variants.

Integrated Solutions

Integrate technologies into force protection solution packages that will improve the effectiveness of electronic security systems, reduce manning requirements, and offer increased affordability and survivability of operators and responders.

Working Groups

The Physical Security Subgroup has regularly scheduled working group meetings that bring together scientists, researchers, intelligence officers, operators, and academia from the interagency and international communities to collaborate on efforts, to identify capability gaps, and to build a collective path forward. The following five areas have active working groups: subterranean operations, homemade explosives, vehicle barriers, video analytics, and waterside security.

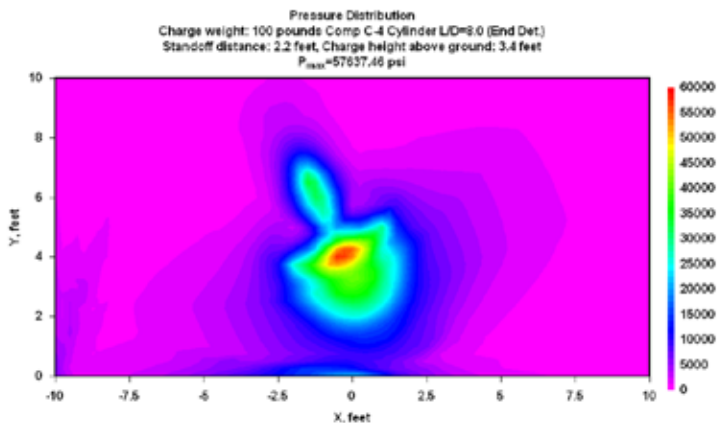


Blast Effects and Mitigation

Close-In Air Blast Software

Current

The introduction and widespread use of computer software systems in the last few decades saw the rise of various software packages such as ConWep, BlastX, and VAPO, which provide a predictive capability to engineers who design the structures and systems to resist the effects of conventional weapons. These tools have become irreplaceable and have allowed engineers to design blast resistant structures more efficiently and quickly. The main problem with these software packages is that they do not have accurate predictive capabilities for explosive charges placed very close to a structure. This inaccuracy is largely because the phenomena of close-in air blasts is not well understood and is difficult to measure since all of the instrumentation close-in to an explosion will be destroyed before an accurate measure can be recorded. Since many of the terrorist attacks throughout the world have focused on using small, strategically placed bombs, it is becoming more and more important for organizations to develop the tools for analyzing these attacks. Under this program, in coordination with Singapore, improvements have been made to the primary problem with blast load predicting software packages. A series of bombs, which were placed very close to piezoelectric pressure gages on a flat plate, have been detonated. These bombs were made of a number of common homemade explosives (HME). The measurements are being used to create equations of state for the various explosives at close range, which are then being simulated in the hydrocode SAGE. The results will be implemented in both BlastX and in a new program called Close-In Airblast Software.





Emerging Explosive Threats

Path to Safety Disruptor

Completed

A high threat to ground movement are booby traps and multiple IEDs, especially those containing low-metallic pressure plates. A standardized, low weight, hand deployed, line charge tool that could penetrate the ground and move soil to create a safer, exposed path did not exist. This project, sponsored by the Joint Improvised Explosive Device Defeat Organization (JIEDDO) and also known as "Stingray", developed two systems to expose hazards along a path in a compromised area such as choke points or courtyards. These two systems, Bandolier and Trailblazer, were selected from a proof of concept trial of multiple vendors. These systems are being deployed to theater for operational test and evaluation. The systems were designed and developed to provide safer movement during dismantled operations. They will be used to gain access to a known IED or used in an area with a high density of IEDs, disrupting or exposing other IEDs along the cleared path. The systems were designed to be less than 15 pounds to minimize weight being carried by a technician who is already carrying a full load of equipment. The systems clear a path up to 35 feet long per kit with the goal of exposing 10 inches in depth by 10 inches in width of soil to undercover buried threats without adding any additional metal fragmentation into the ground. The depth and width are variable depending on soil type and conditions. The systems can be hand or robot deployed.



Improvised Explosives and Homemade Explosives Analysis and Protocols

Completed

A common guideline was developed as part of an interagency agreement on protocols as related to measurement and testing standards for non-commercial and non-military explosives, sponsored by JIEDDO and the Department of Homeland Security Directorate for Science and Technology, and cultivated under a group of interagency subject matter experts. The interagency agreement on protocols will focus on the measurement and testing standards solely for non-commercial and non-military explosives. The overall intent is for these protocols to be common guidelines that leverage, and where possible, improve upon existing standards. As common guidelines, the protocols will allow organizations to have



the ability to document deviations but are not intended to restrict an organization's measurement and testing activities. Interagency collaboration for the protocols includes information sharing to meet the primary objective of establishing protocols, identification and cataloging of existing standards and relevant improvised explosives/homemade explosives (IE/HME) sources, and appropriate classification of protocols. The deliverables from this project are codified and appropriately classified protocols that, as common guidelines, will establish minimum and/or baseline standards to include, but not limited to: test protocols, safety protocols, signature data, verification and validation activities, lexicon, and an electronic collection of existing standards and relevant IE/HME sources for reference in the CTTSO HME Web Forum.



Ammonium Nitrate Inerting Assessment

Current

As part of an ongoing effort to quantify the threat posed by the malicious use of AN and Calcium Ammonium Nitrate fertilizer (CAN), an evaluation to determine the effectiveness of existing technologies for inerting (desensitizing) this material is being conducted with sponsorship from JIEDDO. A wide body of work has been conducted during the past 50 years on rendering AN fertilizer inert by using non-toxic additives. No effort has been made to compare, coordinate, catalogue, or analyze these previous studies, which were unable to render AN inert while maintaining its effectiveness as a fertilizer. This information will be used by U.S. Central Command, the Department of Homeland Security, the Department of Justice, and others to inform decisions on strategies to reduce the use of AN and CAN as an improvised explosive precursor. The effort will consist of a literature review of existing studies and tests that relate to the effectiveness of AN/CAN inerting technologies. The results are being compiled on the detonation characteristics of inerting techniques on AN/CAN, based on validated and appropriate data obtained





as a result of the literature search. After the literature search and review has been completed, a gap analysis will be conducted. The gap analysis shall document unresolved questions identified during the literature review and propose additional research, tests, and methodologies to bridge these gaps. Periodic in-progress reviews to a TSWG-convened panel of subject matter experts to facilitate refinement of the analytic effort, to maintain situational awareness of progress of the assessment, and to facilitate broad consensus among interested parties will be held. A final report will be developed and briefed to interested parties at the final in-progress review and to the HME Working Group.

Screening, Surveillance, and Detection

Portable and Persistent Video Surveillance System

Completed

Current remote video surveillance systems (e.g., “pole cameras”) used by field personnel require electrical and communications infrastructure support in the immediate vicinity. Other existing stand-alone systems (i.e., not connected to electrical and communications infrastructure) operate for only a limited period of time, do not provide real-time information, and require recovery of the system to play back video recordings. Additionally, existing systems frequently





preclude the ability to record and archive critical information in an easily searchable manner, such as searching for specific license plate numbers on vehicles captured in the images. Mobile “plate readers” are currently utilized by police departments in vehicle mounted applications to locate stolen vehicles, but are not being utilized in fixed and clandestine surveillance applications. The Portable and Persistent Video Surveillance System was developed to meet these needs in a single, stand-alone, small (less than 10 pounds), camouflage-able system that will integrate commercial-off-the-shelf components such as long-range vehicle sensing (pyroelectric) and lowlight imaging optics, wireless communication hardware, and solar-energy capabilities. Based on optimal integration of these components, the system offers covert, all-weather, persistent day/night surveillance with an off-angle, long-range license plate reading capability with remote control operator interface. The first prototypes have been delivered to the Drug Enforcement Administration, the Federal Bureau of Investigation, Border Patrol Tactical Unit, Customs and Border Patrol, and Army Special Forces elements.

Tactical Aerostat

Current

This effort is developing a compact, tactical aerostat surveillance system (“Light Eye”) for intelligence, surveillance, and reconnaissance applications, as well as communication between non line-of-sight forces. The system will include day and night observation payloads, a laser pointer, a dual-purpose tether for communication and energy feed from the ground to platform, and a mobile ad hoc networking system. The Light Eye observation payload is based on unique patented electro-optic and three-axis gyro stabilization concepts that enable high quality aerial imagery with 360-degree coverage and extended observation capabilities, while still maintaining small dimensions and low weight. The system is being designed for easy mobilization and rapid deployment. Light Eye will be deployable in less than 15 minutes by two soldiers, transportable by no more than two operators, and can be launched and operated from either a small vehicle or from a dismounted operator. An earlier generation of Light Eye, with only a daytime payload, is currently in use with the Israel National Police.





Integrated Solutions

Enhanced Remotely Operated Underwater Vehicle

Completed

Searching ports and harbors remains a key mission in defending against terrorist attacks. The U.S. Coast Guard (USCG) requires the capability to conduct timely and effective hull searches/inspections of vessels (commercial, Department of Defense, and Coast Guard), piers, sea floor, or anomalous events (parasitic attachments, mines; moored or drifting and improvised explosive devices). The Coast Guard currently maintains Remotely Operated Vehicles (ROV) systems devoted to the underwater port security mission. Current system performance is limited when conducting operations in low visibility and/or strong currents. This project enhanced the USCG's current ROV systems with improved thrust, an improved sonar, manipulator, image enhancement system, hull crawler, and an improved non-acoustic navigation system. These upgraded ROVs provide better search capabilities in all water clarities and in very strong currents, keeping divers out of dangerous waters while searching for hazardous devices. Systems were delivered in August 2011 to the USCG Maritime Safety and Security Teams at various ports in the U.S.

Passive Water Barrier System

Current

Type I Maritime Security Barriers such as the Port Security Barriers (PSB) in use at most Navy bases today were designed 10 years ago and are inherently unstable, prone to flipping over in rough seas,





and provide limited security. The current barriers must be deployed close to the high value asset, and due to their design, are not very effective. This results in inadequate standoff when engaging a target boat. The stopping capacity of this design is much to be desired; therefore, much interest exists in conducting testing on Type II Maritime Security Barriers. During this effort, crash tests will be conducted to demonstrate the stopping power of the Type II PSB against a water-borne threat. The functionality, life cycle support, and maintainability of the gate design, as well as its stopping power against a water-borne threat, will also be tested. During the gate tests, observations of the new barrier gate will occur to demonstrate the maintainability and ease of repeated openings and closings of the design, as well as, the overall cost savings. Crash tests and explosive tests will be conducted to determine if the gate provides the same stopping capacity as the stationary barrier.

Outpost Surveillance System

Current

Current Force Protection systems deployed overseas lack the ability to provide modular lightweight portable surveillance for both compound and dismantled perimeter security. Previous Outpost Surveillance Systems (OSS) were deployed to Afghanistan for small outpost security. Feedback on these deployed systems led to enhancements for the Portable Surveillance Platform 2 (PSP2) and the Mobile Surveillance Platform. The PSP2 was enhanced with an improved day/thermal camera mounted on an electric extendable mast that reaches 13 feet and an improved tethered handheld controller/monitor. The system contains Mesh and Wi-Fi communications as well as GPS and a digital magnetic compass. The Mobile Surveillance Platform was upgraded to a Polaris Military Version Ranger Razor with a quick and simple attachable pole-mounted day/thermal imager for both dismantled and camp security. No vehicle modifications or special tools are needed to attach this surveillance system to the Razor; thus, it is not permanent or vehicle dependent. This Rapidly Attachable Pole-mounted Tactical Observation Relay (RAPTOR) also contains Mesh and Wi-Fi communications and is controlled by a tethered handheld monitor/controller. Included in this system is the Soldier Worn Video Viewer, which is smartphone-enabled, combining soldier worn wireless communications and video display capability that will be able to view video from the RAPTOR and other OSS imaging systems. This capability integrates well with the customer's current gear and, therefore, introduces a minimal amount of additional equipment that the soldier must carry and manage.





The background of the page is a faded, high-angle view of the American flag, showing the stars and stripes in a soft, golden-brown color palette.

Surveillance, Collection, and Operations Support

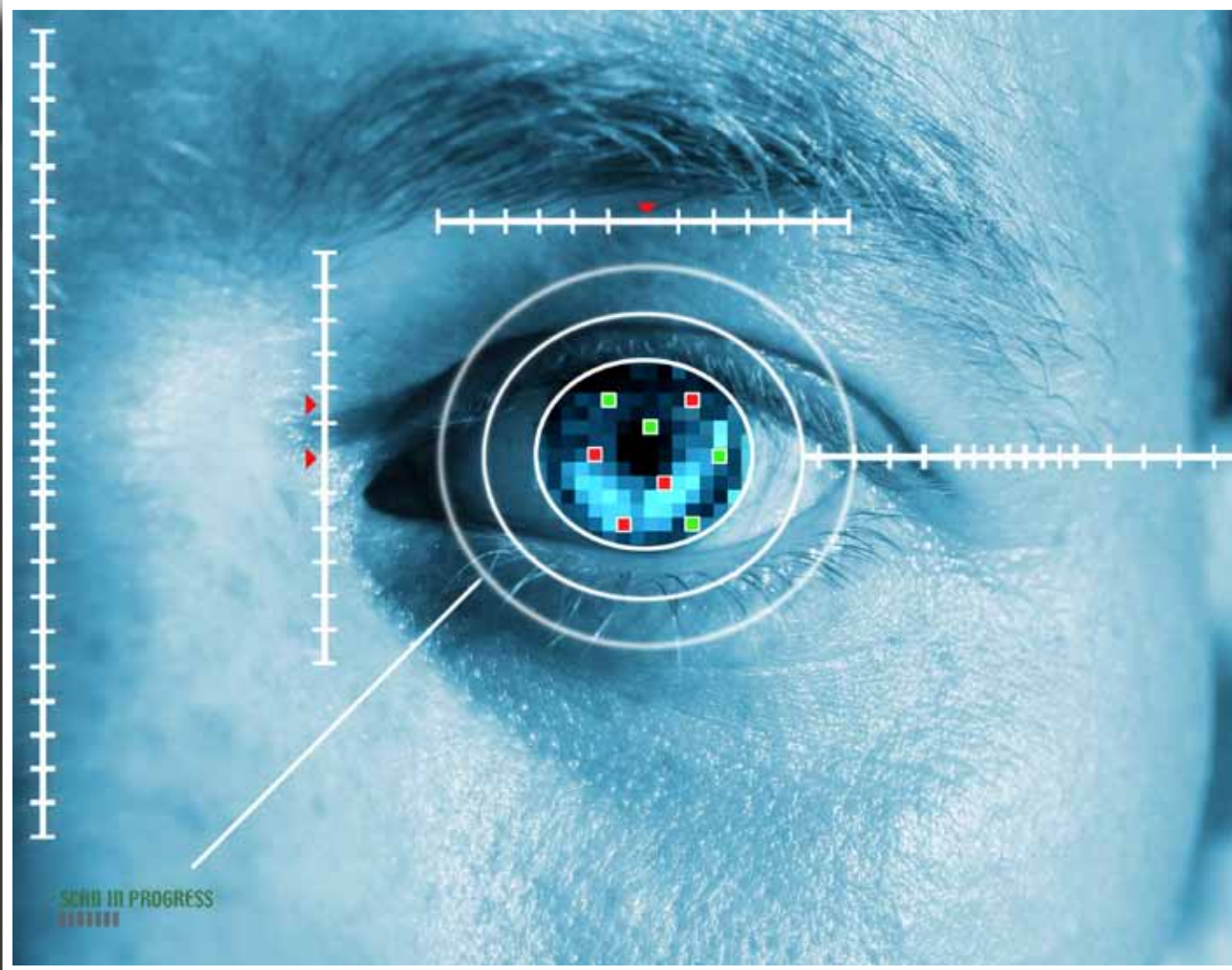
Mission

Identify, prioritize, and execute research and development projects that satisfy interagency requirements supporting intelligence collection and special operations directed against terrorist activities.

The Surveillance, Collection, and Operations Support (SCOS) Subgroup identifies high-priority requirements and special technology initiatives focused primarily on countering terrorism through offensive operations. SCOS research and development projects enhance U.S. capabilities to conduct retaliatory or preemptive operations and to reduce the capabilities and support available to terrorists.

Contact Information

scossubgroup@cttso.gov





Focus Areas

Biometrics, Recognition, Identity Protection, Tracking, and Exploitation

Improve the means to detect terrorists by developing automated tools for terrorist identification using biometrics, pattern recognition, database technologies, and exploitation methodologies.

Technical Surveillance

Develop and improve the ability to locate, identify, and track terrorists and terrorist activities. Support programs and initiatives critical to intelligence operations such as tagging, tracking, and locating; special sensors; and covert communications.

Canine Advance Technologies

Develop methodologies that enable working canine teams to operate more effectively and efficiently by enhancing canines' abilities for explosives detection, tracking, patrolling, and attacking in an operational environment.

Cyber

Develop enhanced tools including techniques and procedures that focus on finessing the cyberspace domain to improve SOF operations in fluid environments.

Counter-Surveillance Support

Develop advanced automated tools and techniques to defeat adversarial surveillance methodologies. Develop technologies to assist tactical teams with verification of assets and more effective use of interrogation data.

Human Language Technology

Develop and insert Human Language Technologies where these technologies can best assist humans – operators and analysts – to: make sense of volumes and varieties of data sources; apply timely and actionable intelligence; enhance communication skills and cultural understanding; and improve language learning.



Biometrics, Recognition, Identity Protection, Tracking, and Exploitation

Media Triage Plug-In for EnCase©

Current

Digital forensics exploitation is difficult because of the capacity and diversity of devices containing digital evidence. Media Triage Plug-in for EnCase® enhances media exploitation by adding audio, video, and imagery triage plug-ins. Key features of the plug-in include the ability to rapidly ingest large volumes of media directly from EnCase©; the ability to automatically create storyboards, large key frames, proxies, and video categories; a collection hierarchy with browsing to quickly triage content during ingest; a universal video player able to play most known video codecs; and a patent pending visual search technology to locate visually similar content.

Canine Advance Technologies

Evaluation of the SNT SKR2000 for Training Aids

Current

The sensitivity and selectivity of the canine's olfactory system provides exceptional ability to detect small quantities of material even in the presence of complex background noises. However, the complex mechanism of canine olfactory systems has yet to be fully understood and taken advantage of.

The goal of this project is to use a previously developed product built for human scent detection (SNT SKR2000) and modify it to create effective and safe training aids for explosive detection. The SNT SKR2000 will be evaluated to determine the ability to cover the spectrum of explosive materials as well as work toward a generic methodology to develop custom-made training aids suitable for ever evolving explosive recipes.





Evaluation of Pseudo Explosive Training Aids

Current



It is well known that canines are the fastest, most sensitive, and selective real-time detectors of explosives. Essential to maintaining a properly trained explosive-detecting canine, however, are uncontaminated training aids that represent the various explosive classes of interest. Such training aids have traditionally consisted of samples of authentic explosive formulations, which are particularly challenging because of storage, transportation, handling, and destruction constraints. Consequently, "pseudo-explosives", which simulate the odor of actual explosives yet contain only inert ingredients, are often used. Obvious concerns with this approach, though, are the unknown chemical composition of pseudo-training aids and whether canines that have been trained using pseudo-explosives will successfully detect actual explosives.

This project examines the chemical composition of various pseudo-explosive products currently being sold. Testing will be conducted to determine whether canines trained solely on pseudo-explosives can detect authentic explosive samples as well as whether canines trained on explosives can sustain proficiency by using pseudo-explosives for training.

Human Language Technology



Talk2Me

Current

Talk2Me is a suite of tools that allows instructors and operators to retrieve and exploit video and speech interrogation/interview content in near real time for further analysis. Talk2Me allows synchronization of all data elements, annotating of relevant segments for feedback and/or further analysis. All content can be searched, extracted, and uploaded as needed into other government databases.

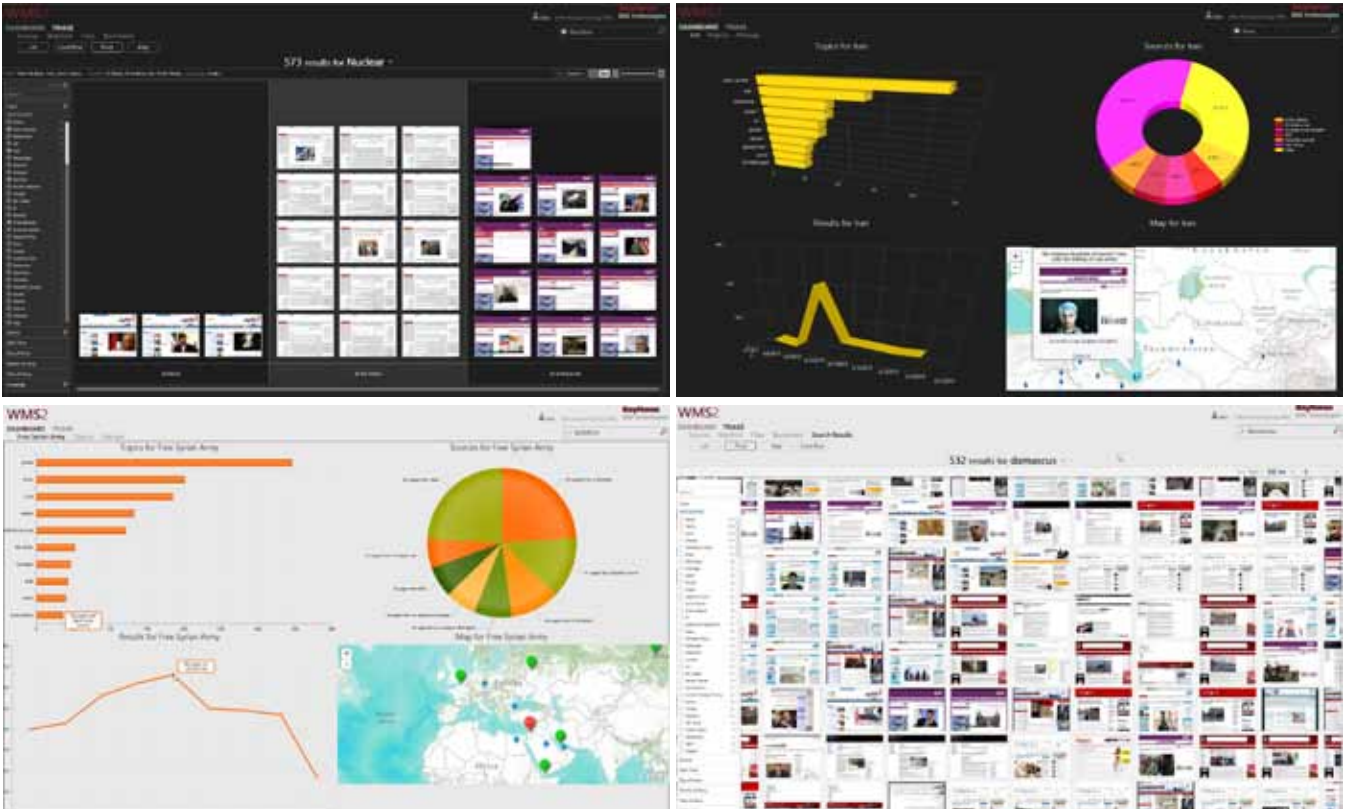


Web Monitoring for Multilingual Data Triage

Current

The Web Monitoring System is an end-to-end capability for collecting, organizing, and translating open source content from the World Wide Web. This groundbreaking system integrates and manages the media analysis process from beginning to end—from data collection and processing, to automated triage and retrieval, to machine-assisted translation and support for human translation, to export and dissemination.

The variety of visualization presentation, including charts and maps, allows for easy browsing, filtering, sorting, and grouping search results. Translation and production tools within the system focus on what matters in analysis, increasing human productivity and efficiencies in data exploitation.





Tactical Operations Support

Mission

Identify, prioritize, and execute research and development projects that enhance the capabilities of DoD and interagency special operations tactical teams engaged in finding, fixing, and finishing terrorists. This includes the development of capabilities for state and local law enforcement agencies to combat domestic terrorism.

The Tactical Operations Support (TOS) Subgroup provides technology solutions to assist “direct action” operational personnel in a variety of tactical missions and environments. Most often these solutions are in the form of rapidly prototyped and specialized equipment. Each material solution is specifically designed to provide enhanced mission effectiveness while assisting operational personnel in maintaining “situational awareness.”

Contact Information

tossubgroup@cttso.gov





Focus Areas

Communications Systems

Develop flexible and enhanced communications capabilities specifically designed for tactical forces. Emphasize reducing the size of equipment, while improving operator mobility and efficiency. Consider durability, concealment, innovative power sources, range, reception, battery life, ease of use, and low probability of detection/interception. Develop assured tactical communications connectivity in challenging environments such as buildings, caves, tunnels, below deck, or underground bunkers.

Intelligence, Surveillance, Target Acquisition, and Reconnaissance Systems

Develop technologies to assist tactical teams in conducting intelligence, surveillance, target acquisition, and reconnaissance missions. Develop systems that enhance the visual perception or other imaging capabilities of tactical operators in all conditions and environments. Develop independent, vehicular, or weapon-mounted systems for enhanced aiming, target designation, illumination, range detection, or surveillance.

Offensive Systems

Develop equipment and capabilities that enhance the effectiveness of small offensive tactical teams engaged in specialized operations. Develop specialized weapons, munitions, detonators, distraction/diversion devices, and other unique tactical equipment. Develop systems to support sniper and countersniper operations. Develop man-portable sensor systems to enhance operator security during tactical missions.



Specialized Access Systems

Develop technologies that assist tactical assault forces in gaining rapid access to objectives, improve evaluation of tactical options, and support efficiency and stealth of operations. Develop enhanced manual and dynamic breaching technologies for tactical assault teams. Develop clandestine defeat or override devices for building and vehicle entry points.

Survivability Systems

Develop clothing, individual equipment, mobility platform enhancements, and man-portable systems that provide protection from or identification of ballistic, fragmentation, explosive, and thermal threats during the conduct of tactical missions.

Unconventional Warfare, Counter-Insurgency Support

Develop innovative solutions for small specialized tactical operations teams conducting a broad spectrum of military and paramilitary operations including counter-insurgency and foreign internal defense missions through, with, or by host nation indigenous forces building partner capacity to support U.S. objectives.

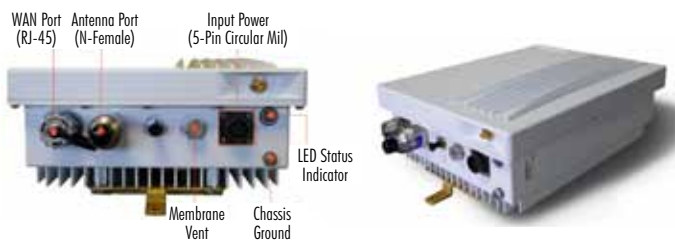
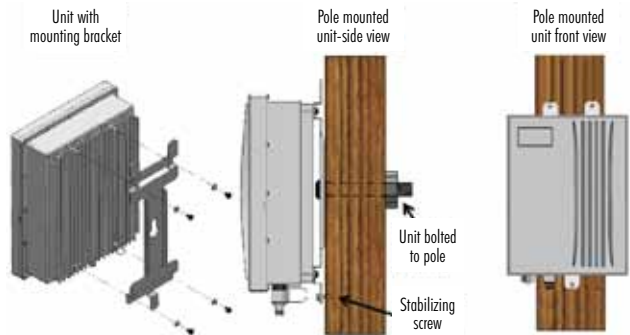
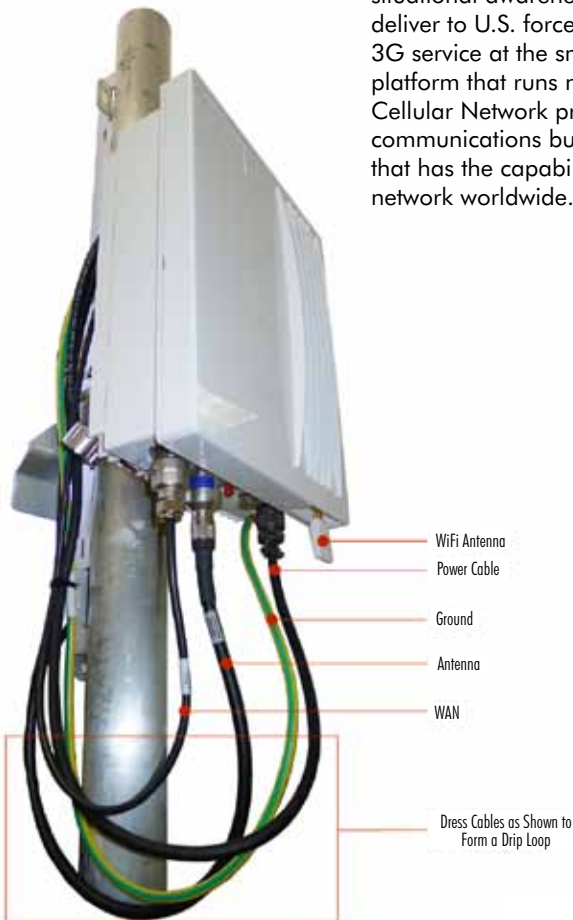


Communications Systems

Organic Cellular Network

Current

The ubiquity, capability, and accessibility of mobile devices in the United States has led to end users developing requirements for intuitive and secure mobile communications systems in order to conduct combating terrorism operations overseas. With the National Security Agency's designation of the publically available Suite B algorithms as acceptable encryption for some types of perishable data transmission and the proliferation of advanced mobile applications providing many of the key functions needed for tactical situational awareness, the Organic Cellular Network project will deliver to U.S. forces an integrated solution with commercial cellular 3G service at the small unit coupled with a secure communications platform that runs natively on Android devices. The Organic Cellular Network provides an operational end user with a secure communications bubble out to 1.5 miles beyond the base station that has the capability to reach back to any telecommunications network worldwide.





Intelligence, Surveillance, Target Acquisition, and Reconnaissance Systems

Micro Tactical Ground Robot

Current

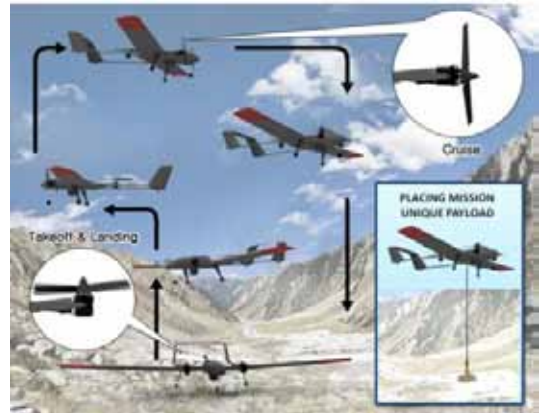
The Micro Tactical Ground Robot (MTGR) is a tactical visual (360-degree day/night camera coverage) and acoustic (internal microphone and speaker) intelligence, surveillance, and reconnaissance mission capable robot. The MTGR has high maneuverability in order to climb stairs and steep terrain, yet is light enough (e.g., less than 15 pounds) to be transported by a dismounted operator across rugged terrain over long distances. The MTGR will come with a lightweight manipulator to emplace IED counter-charges and remove debris from areas of interest and uses U.S. military standard batteries. Additionally, the MTGR will have an internal GPS receiver, digital magnetic compass, and NSA Suite B datalink encryption for robot position reporting in command and control common operating pictures for situational awareness and robot recovery.



Vertical Take Off and Land Small Unmanned Aerial System

Current

Two man-portable unmanned aerial systems (UAS) currently used by SOF to conduct intelligence, surveillance, reconnaissance (ISR) and Counter-Improvised Explosive Device (C-IED) missions do not have the ability to vertically take off and land (VTOL), transition from a VTOL configuration to fixed-wing for improved speed and endurance, and do not have the latest encryption for security via Mobile Ad Hoc Network (MANET) data-link. SOF requires the rapid development of a VTOL Small Unmanned Aerial System (SUAS) to conduct a wide range of ISR and C-IED missions. The VTOL SUAS shall be comprised of an airframe with a secure MANET data-link, ground control station, field-swappable payloads, and ancillary equipment/power supplies. The VTOL SUAS will function in a way that supports current and future SOF tactics, techniques, and procedures. The increased operating time and quicker time to deploy and secure the MANET data-link will increase SOF survivability and lethality by neutralizing IEDs.





Offensive Systems

Night VISER

Completed

Special operational forces and law enforcement require a capability to provide increased short-term site security during tactical operations in urban and suburban, rural, and wilderness environments. The Night VISER is a rugged, lightweight, man-portable, wireless infrared illuminator and motion sensing system for use by small tactical teams to enhance site security when remaining overnight at temporary hide sites, safe houses, or small base camps. Each system consists of four nodes and one remote that act as an early warning for small forces deployed forward. In Afghanistan, the system was deployed with an Army Special Forces Operational Detachment-Alpha and alerted them to the presence of hostile forces. According to the Team Sergeant, the Night VISER system 'saved' them by alerting them and allowing them to respond with the appropriate measures.





SOF Marksmanship Advancement

Current

Numerous leaps have been made in long-range shooting technologies in the past few years that can change the way U.S. Special Operations Forces (SOF) can train and fight on today's battlefield. The SOF Marksmanship Advancement program takes a holistic look at currently available technologies, developing technologies, and training methods to create a new and novel equipment and training package for SOF snipers and long-range shooters. The Tactical Operations Support Subgroup has partnered with the Joint Readiness Training Center Special Operations Training Detachment to provide these leading-edge sniper and spotter capabilities with the highest caliber training available in an effort to shape future requirements and technology development with an emphasis on evolutionary and low-cost solutions to complex long-range shooting problems.



Concealable Sniper Rifle

Current

The U.S. sniper community is currently in the process of realizing new gains from current weapon systems due to a paradigm shift in shooter technology. Current legacy sniper rifles are now able to reliably engage targets at ranges far beyond their accepted maximum effective range. As a result, TSWG has received a requirement for a Concealable Sniper Rifle that will be optimized for both subsonic and supersonic ammunition, with a maximum barrel length, exclusive of muzzle brake and suppressor, not greater than 14.5 inches. The weapon will be accurate to one minute-of-angle or better while retaining a capability of reliably engaging targets out to 800 meters.





Confined Spaces Suppressed Upper Receiver Group

Current

U.S. Special Operations Forces have a need to reduce their visual and auditory signature across the spectrum of operations. In order to address that requirement for primary weapon systems, TSWG is working to develop a Confined Spaces Suppressed Upper Receiver Group (CSSURG) that will have the same exterior and interior ballistics, same overall length, and a similar configuration as the M4A1 carbine, but with a greatly reduced sound and flash signature. The CSSURG will utilize a new two-stage, integrally suppressed system in order to maximize both signature reduction and operational endurance of the system.

Survivability Systems

Tactical Ballistic Helmet

Completed



The protection of Special Weapons and Tactics (SWAT) teams from the neck up has traditionally been provided by either a military or commercial variant of a military style Kevlar helmet. The requirements of military are somewhat relevant, but many of the operations, accessories, and threats differ from SWAT applications. SWAT operators have a higher incidence of heavier, lower velocity handgun projectiles such as the .44 Magnum and lower velocity blunt impacts. The Tactical Ballistic Helmet is an improved ballistic helmet that protects users from high caliber handgun rounds (.44 magnum), shrapnel, and blast pressures. The helmet allows users to attach a variety of external devices (e.g., night vision devices, lights, and cameras) without disturbing balance, comfort, or level of ballistic protection provided to the wearer. The helmet also features a side rail, night vision goggles shroud, drop-down ballistic eye protection, and an adjustable interior head liner.

SWEEP

Current

The importance of eye protection during combat operations is well known. Spectacles that function with interchangeable inserts to provide ballistic protection, optimize available light, and provide



a degree of laser safety currently exist on the commercial market. While operators are equipped with this eyewear system, they must still decide which particular insert to wear for each mission. In order to reduce operational load and the number of components that operators must carry into the field, the CTTSO has developed Special Warfare Electronic Eye Protection lenses that electronically change tint from near clear to Amber to blue to dark grey. The transition can occur at a touch of a button or automatically depending on the light level conditions. The glasses are corrosion resistant, meet ANSI Industrial Standards for high-mass and high-velocity impact, adhere to MIL SPEC laser safety standards, and provide 100 percent UV protection.

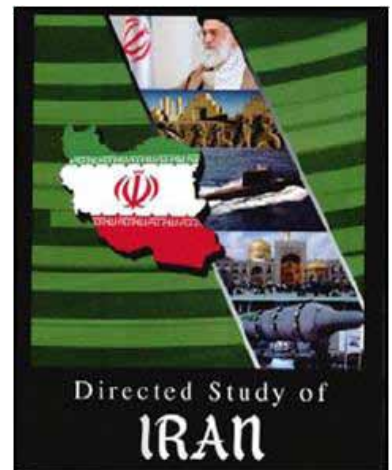


Unconventional Warfare, Counter-Insurgency Support

Directed Studies

Completed

In order to combat terrorism effectively, operators and technology developers need to be aware of any emerging threats as well as understand complex global dynamics and how they impact tactical operations. The Directed Studies program is an effort to develop and deliver in-depth analysis of the activities and motives of individual countries, organizations, or threat subjects. Subjects covered in the studies include: objectives, alliances, structure, history, and activities of the subject country, organization, or threat. The program will deliver professional bound books for easy distribution on a variety of global topics, including Foreign Freedom Fighter Phenomenon and Weapons of Mass Destruction.



Remote Access Air Mobility

Current

The Remote Access Air Mobility (RAAM) Project is a proof of concept using a low cost leased aircraft – contractor owned and government operated – to provide organic, low profile fixed wing aviation support to Special Operations Forces and the interagency in support of Unconventional Warfare Operations and Homeland Defense. Project RAAM will complement other SOF and General Purpose Force non-standard aviation by providing distributed, organic, and timely aviation support flown by military pilots and maintained by



military maintenance professionals. Project RAAM is intended to be a family of fixed wing aircraft, both dual and single engine, with the capability to support short take off and landing, lift, emergency resupply, CASEVAC, military free fall, and surveillance and reconnaissance, in a low profile (non-military aircraft) that is affordable and easily sustained when operating from remote sites to fixed base operations.





Training Technology Development

Mission

Identify, prioritize, and execute projects that satisfy interagency requirements for the development and delivery of combating terrorism related education, training, and mission performance support products and technologies.

The Training Technology Development (TTD) Subgroup delivers training and training technologies to increase mission readiness and enhance operational capabilities in the combating terrorism community. The strategy behind the mission is to analyze, design, develop, integrate, evaluate, and leverage distributed learning technologies to deliver high-quality training and education in the medium best suited to the users' needs and requirements.

Contact Information

ttdsubgroup@cttso.gov



Parachute Training Simulator being evaluated by Military Freefall personnel at USAJKFSWCS.



Focus Areas

Models, Simulations, and Games

Develop interactive models, simulations, and games (MS&G), including, but not limited to: tabletop simulations, field exercise simulations, immersive virtual-learning environments, hands-on virtual reality, simulation models, and PC-based three-dimensional and isometric simulations and games. Develop crowd models, adversarial behavior models, network-based simulations, and mini-simulations on specific combating terrorism related tasks. Incorporate beneficial game characteristics through the full range of game genres (i.e., strategy, first person tactical, massively multiplayer online game, role-playing, etc.). Develop tools, technologies, and techniques for improving MS&G design, development, and validation.

Advanced Training and Education

Develop programs of instruction, training packages, and computer- and classroom-based terrorism training courses. Develop the advanced tools, techniques, and guidelines required to analyze needs, develop solutions, and evaluate results. Analyze performance needs to identify applicable solutions. Integrate delivery technologies with combating terrorism training materials to increase the quality, effectiveness, and accessibility of training.

Training and Information Aids and Devices

Develop job aids, performance improvement solutions, and training devices to support mission performance and increase mission readiness. Support new areas in the combating terrorism domain. Provide training simulants as aids in training exercises.



Models, Simulations, and Games

Elevating Ocular Tactical Reaction System

Completed

Soldiers are required to operate in urban environments with a significant number of visual cues requiring their attention. Situational awareness, decision making, and reaction speed are critical for engaging and eliminating threats. Conflict Kinetics developed the Elevating Ocular Tactical Reaction System, which enables soldiers to process more information at a faster pace in order to keep forward momentum in assault-type missions. The laser-based performance simulation covers a 220-degree field of vision that allows trainees to visually acquire more than 1,500 targets and fire more than 500 virtual rounds in a single training session. The system consists of a five-screen, laser-based performance simulation and a computer-based eye tracking and target recognition system. The system is currently being used to train assaulters at 1st Special Warfare Training Group. During several two-week pilot courses with various end users, quantifiable increases were recorded in the speed, accuracy, and number of targets engaged.





Tactical Driving Simulation

Completed

Protective detail personnel must be prepared to effectively and efficiently respond to threats upon high-profile government officials (i.e., VIPs) when providing transportation and movement protection

within the United States and abroad. In collaboration with the Pentagon Force Protection Agency, U.S. Secret Service, and U.S. Department of State, Quantum Signal developed a PC-based Tactical Driving Simulation (TDS) to augment training and evaluation within a virtual environment for skills necessary when transporting VIPs and responding to threats. The simulation provides programmable



scenarios that require situational awareness, decision making, and action including principles of: route planning and analysis, evasive driving skills, force-on-force counter ambush tactics, vehicle dynamics during crash avoidance, and defensive driving techniques when in hostile situations. TDS also includes an after-action-review component with bookmarking and annotating features. The software is available to any U.S. military or interagency organization at no additional cost by contacting the TTD Subgroup.

Parachute Simulator

Current

Developing Special Forces (SF) skills for high altitude - low opening (HALO) or high altitude - high opening (HAHO) operations requires a significant number of training hours. Though parachute training is ideally accomplished with live jumps, a number of the emergency procedures are too risky to be trained live. To address this need, United States Special Operations Command is implementing parachute training simulators that augment the existing classroom, wind tunnel, and live jump curriculum.





The current effort involves the installation and evaluation of the Systems Technology, Inc. PARASIM® at the U.S. Army John F. Kennedy Special Warfare Center and School. This virtual reality simulator system allows SF to practice a wide range of emergency procedures in a highly realistic yet safe training environment. Systems Technology, Inc. has installed six integrated parachute jump stations to train basic through advanced techniques before conducting a HALO or HAHO live jump. The system is currently being evaluated and upgraded concurrently to maximize the operational benefits of the jump stations on mission rehearsal.

Embassy Security Simulation

Current

U.S. Embassies are a worldwide symbolic target for terrorists. Means for attack prevention and deterrence through preparation must be developed along with strong defenses during an attack. Embassy security systems are highly complex; therefore, developing an in-depth understanding of these systems among security personnel is an ongoing challenge. Security training exercises and drills are constrained to physically engage only a few systems and a subset of personnel. Quantum Signal, Inc. is developing a multi-player, PC-based, simulated environment for security-related roles in an embassy. The simulated embassy environment will integrate training modules representing the tactical and technical actions of security personnel within their various security roles in the context of scenario driven events. The Embassy Security Simulation will help train personnel and allow them to practice the full range of embassy security related tasks at the technical and tactical level in order to prevent and appropriately respond to threats.





Advanced Training and Education



Ballistics Effects Video

Completed

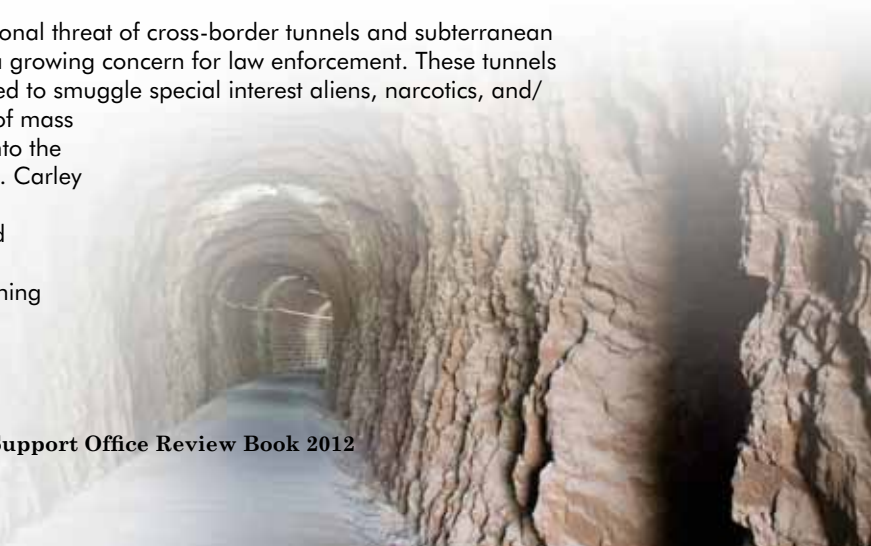
Weapon technology is continually evolving in order to combat emerging threats to civilians and the agencies responsible for protecting them. Protective forces must have advanced knowledge of ballistics and shooting skills to understand how their weapon can eliminate a threat. It is not enough to simply describe ballistics and shooting skill effects. Rather, these technical aspects must be demonstrated to the learner through tangible visual examples. The ballistics and shooting skill effects training video provides protective force personnel with

critical technical knowledge of their weapons that can ultimately save lives. The video, developed by Service Brands, LLC, features ballistics effects of the H&K MP-7, LWRC M6 Carbine, and LWRC REPR on ballistics gel, Kevlar vests, and a portable barrier. Ballistics effects were captured using a combination of high-speed cameras and high-definition broadcast cameras, resulting in exceptionally clear footage. Center mass and pelvic girdle failure drills are also demonstrated in the video through real-time, live-action scenarios integrated with 3-D animation to demonstrate bullet performance in the human body. The video has been incorporated into the Pentagon Force Protection Agency and the Washington Headquarters Service's training curriculum. The DVD is available to any federal, state, and local law enforcement agency at no additional cost by contacting the TTD Subgroup.

Counter Tunnel Investigation

Completed

The transnational threat of cross-border tunnels and subterranean passages is a growing concern for law enforcement. These tunnels are being used to smuggle special interest aliens, narcotics, and/or weapons of mass destruction into the United States. Carley Corporation designed and developed a blended learning course that





includes computer-based and instructor-led training as well as job aids concerning cross-border tunnel investigations. The course includes topics such as investigative methods, site exploitation, tunnel rescue, local tunnel perspectives, report writing, community outreach, and collaboration with partner agencies and cross-border authorities. The computer-based training is hosted on the Department of Homeland Security's Virtual University, and the instructor materials and job aids are available through the Government Printing Office.

Small Unmanned Aircraft Systems

Current

The United States Marine Corps' (USMC) Small Unmanned Aircraft System (SUAS) Training Support Package project provides a service-approved, standardized, interactive, multi-media training package based on the USMC Group 1 SUAS Training & Readiness Manual. Developed by K2 Share, the new training will include and augment current training materials for SUAS. Formal instructional systems design principles are being used to merge existing directives and SUAS training materials into a new learning system that meets the unique demands of Marine Corps SUAS operations and training. The enhanced learning system will employ the best mix of computer-based training, multimedia, modern training aids, and self-paced instruction for both classroom and field learning environments. New courseware will support instructor-led training and will also provide a resource for certified SUAS operators to review courseware or complete refresher training requirements through self-paced instruction. Additionally, the courseware will expand on the limited-scope period-of-instruction currently available, giving operators access to more detailed and comprehensive employment tactics, techniques, and procedures than are currently available in existing SUAS training materials.





Training, Information Aids, and Devices

Mobile Learning Decision Tool



Current

Instructional designers and subject matter experts across the government are implementing mobile solutions to enhance learning and provide performance support. This is predominantly being done through trial and error as well as pilot programs. To assist in making pilot efforts successful, Adayana Government Group is creating a decision tool to assist operational end users, instructional designers, and subject matter experts through the process of designing and developing mobile support. Many variables must be considered in mobile learning, and

this tool will provide the support needed to determine the approach that will yield the most benefit to the end users. The Mobile Learning Decision Tool will allow end users to provide recommendations on analysis, design, development, and transition as well as establishing evaluation criteria.



Mobile Learning Resources for Gas Chromatography - Mass Spectrometer

Current

Just in time information and performance support is often needed to facilitate the use of equipment in theater. Adayana Government Group is creating a performance support solution, particularly for end users in different locations with varying missions, accessible on a mobile device. The Gas Chromatography – Mass Spectrometer (GC-MS) is a cost effective, standardized, and portable way to provide

new and updated information to troops. The Mobile Resources for GC-MS includes the analysis, design, and development of an innovative mobile performance support solution for the GC-MS, a person-portable mass spectrometer with gas chromatograph inlet for detection, identification, and quantification of chemical warfare agents and toxic industrial chemicals.



The background of the page is a faded, high-angle view of the American flag, showing the stars and stripes in a soft, light tone.

Explosive Ordnance Disposal/ Low-Intensity Conflict

Mission

The Explosive Ordnance Disposal/Low-Intensity Conflict (EOD/LIC) Program provides Joint Service Explosive Ordnance Disposal (JSEOD) technicians and special operations forces operators with the advanced technologies and mission-focused solutions required to address current and emerging threats presented by unconventional and asymmetric warfare.

The EOD/LIC Program identifies and prioritizes JSEOD and Special Operations user requirements and competitively seeks technological solutions for combating explosive threats throughout the full spectrum of conflict. Through its participation in the JSEOD Notional Concept Working Group, and in coordination with the National Bomb Squad Commanders Advisory Board (NBSCAB) and other Department of Defense and federal law enforcement components, the EOD/LIC Program integrates technology requirements from the explosive ordnance disposal, special operations,



public safety bomb technician, and other law enforcement services communities into its process.

Contact Information

eodlic@eodlic.cttso.gov



Focus Areas

Remote Operations and Advanced Mobility

Develop capabilities to remotely approach, enter, and conduct reconnaissance operations in hazard areas and danger zones. Enhance mobility-related technologies and equipment to facilitate safely approaching, operating in, and withdrawing from hazardous environments. Develop systems and technologies to gather and store operational information for transmission to operational personnel and unit commanders. Improve technologies for the relocation of unexploded ordnance, hazardous materials, and improvised devices.

Access and Disablement

Develop tools to quickly and efficiently breach or gain access to structures, barriers, vehicles, and containers. Develop chemical, mechanical, electrical, and explosively actuated systems for the neutralization and disruption of unexploded ordnance and improvised devices. Improve technologies for rendering fuzing and firing systems inoperable.

Detection, Diagnostics, and Analysis

Develop tools to locate and verify the presence of improvised devices, unexploded ordnance, booby traps, and other threats. Develop technologies to determine the specific type, condition, and characteristics of unexploded ordnance and improvised device components and the specific hazards associated with each. Improve methods to analyze and evaluate improvised device construction.

Sustainability and Operations Management

Develop tools and equipment to enhance situational awareness and operational capability during incident response or direct action operations. Develop human performance improvement tools that foster the advancement of knowledge related to unexploded ordnance, improvised devices, and enhanced hazard environments. Develop tools and training for conducting novel and advanced missions related to improvised devices and hazardous environments.



Access and Disablement

REBUS

Completed

Radio controlled IEDs (RCIEDs) represent a significant, persistent threat to U.S. forces overseas as well as to domestic law enforcement personnel. When confronted with a suspect RCIED, law enforcement personnel have limited access to electronic countermeasures (ECM) equipment to suppress the threat. The REBUS system offers an alternative to traditional ECM systems in that it emits countermeasures signals within a tent designed to be placed over the suspect device. This configuration reduces the overall effects radius of the system, eliminates interference with nearby friendly or benign communications systems, and provides an interim capability to prevent detonation of RCIEDs. The EOD/LIC Program funded testing of the REBUS system to ensure that it performed to the manufacturer's specifications and suppressed the command signal for a variety of frequencies. Additionally, validation testing was successfully conducted to ensure the system, when powered on,





does not expose bystanders to harmful electromagnetic radiation. Acceptance by the Interdepartmental Radio Advisory Committee could lead to approval of other low power ECM-related equipment in the contiguous United States by non-federal bomb technicians and tactical teams. The REBUS system is particularly applicable for RCIED incidents at checkpoints and in mass transit scenarios (subway, airport, bus station, etc).

Electronic Warfare Grenade

Completed

Current ECM systems, or jammers, are either vehicle-mounted or man-portable backpack systems. One of their uses is to help counter the threat of RCIEDs. U.S. and Israeli military and law enforcement tactical forces have a requirement for a miniaturized, 'toss-forward,' counter-RCIED jamming device to defeat RCIEDs within close proximity during urban and indoor scenarios and Explosive Ordnance Disposal operations. The Electronic Warfare Grenade (EWG) is a portable, battery-powered active jamming device capable of defeating multiple threats within a confined space by tossing one or more of the softball-size devices into the space. It can also be hand-emplaced or robotically-emplaced proximate to a known or suspected threat. Battery replacement can be quickly and easily accomplished in the field and does not require special tools. The EWG operates on several frequency bands within a designated frequency range to jam the signals of RCIED transmitting devices such as cellular phones and ultra high frequency/very high frequency radios. Device specifications, including frequency range, power output, and battery operating time, are sensitive.

Non-lethal Small Vessel Stopping

Current

U.S. forces at sea are frequently called upon to engage vessels with potentially hostile intentions. This asymmetric threat can present a danger to both military and civilian populations. Pirates, smugglers, terrorists, or other criminal elements often disguise themselves as non-combatants to carry out their activities. Under the sponsorship of the Combating Terrorism Technical Support Office and the Coalition Warfare Program office, the Naval Research Laboratory is developing an Unmanned Surface Vessel (USV) Mounted Radio Frequency (RF) Vessel Stopper. Its objective is to use non-lethal force to stop or disable outboard marine engines on small boats. The stopper provides a middle step between shouting at and shooting a suspicious boat. Mounting the stopper on a USV enables a relatively small RF source to reach out farther than a fixed platform could while still limiting effectual hostile response. The current project will include the development of an effective RF source and its integration with a USV platform, direct measurements of system



effectiveness, and an at sea demonstration. The RF source is based around a high voltage switch that drives a charged antenna, chosen for its high peak electric field and minimal weight. This source is being refined to increase its voltage and operational longevity. A set of representative domestic and foreign outboard engines have served as targets in engine susceptibility tests to estimate system capabilities. Once complete, the RF source will be integrated with an electronically-hardened USV, as the USV controls and propulsion must be protected from the electronic emissions intended to disrupt target outboard engines. This effort will culminate with a dynamic open water demonstration and evaluation.

Detection, Diagnostics, and Analysis

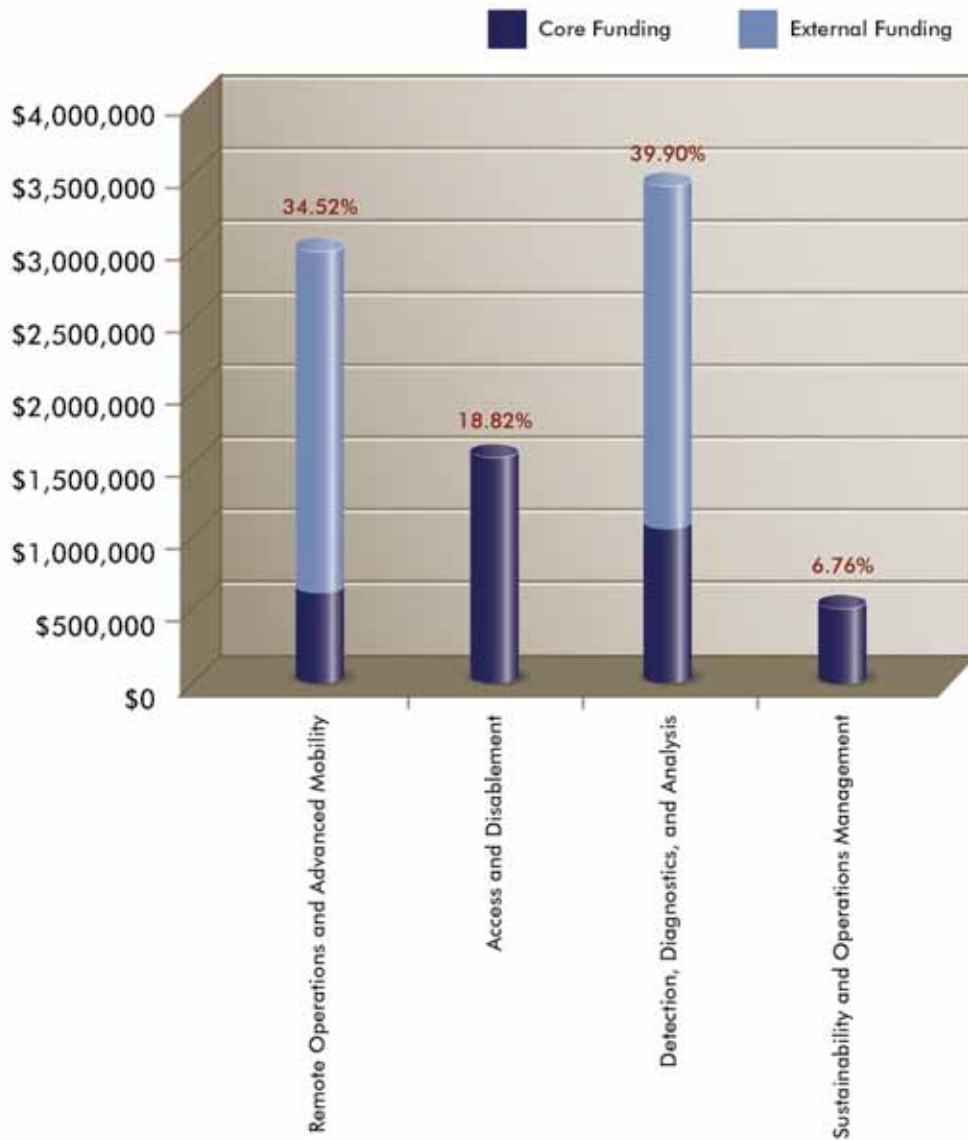
Next Generation EOD X-Ray Generator

Current

The past decade has seen the IED rise in prominence as one of the most lethal and persistent threats faced by U.S. and allied military forces. As the use of IEDs has proliferated, the creativity of the bomb maker has meant that Explosive Ordnance Disposal forces must have improved tools with which to mitigate the threat. The Next Generation X-Ray Generator project seeks to develop a system with enhanced capabilities over existing diagnostic tools. It will provide a user with selectable output with higher total energy (between 150-300 KeV) for increased penetration of dense materials and thick cased munitions. The Next Generation X-Ray Generator system will weigh less than existing systems for improved portability and will combine with the currently fielded flat panel Phosphor Storage Plate processor used in the Navy EOD Air Assault X-ray system.



EOD/LIC FY 2012 Funding by Focus Area (\$8.8 Million)





The background of the page is a faded, high-angle view of the American flag, showing the stars and stripes in a soft, light tone.

Irregular Warfare Support

Mission

Develop adaptive and agile ways and means to support irregular warfare in the current and evolving strategic environments. Support joint, interagency, and international partners who conduct irregular warfare through indirect and asymmetric approaches with solutions to erode an adversary's power, influence, and will. Identify materiel and non-materiel solutions via operational analysis, concept development, field experimentation, and spiral delivery of capabilities to defeat the motivations, sanctuaries, and enterprises of targeted state and non-state actors.

The Irregular Warfare Support Program (IWSP) builds capacity and capability for Irregular Warfare from a defense-interagency-international perspective. It develops cross-domain blended capabilities necessary to enable sustained counterterrorism and counterinsurgency operations. This program leverages ongoing research efforts of U.S. Special Operations Command, the military departments, Defense agencies, and other federal agencies to analyze, design, prototype and demonstrate enduring technical and operational capabilities. IWSP projects blend several disciplines including tactics, operations, doctrine, policy, information, training, and technology.

Contact Information

iwsp@iwsp.cttso.gov





Focus Areas

Battlespace Awareness

Conduct research, operational analysis, capability design, and implementation support to enable forces to understand dispositions and intentions as well as characteristics and conditions of the threat and operational environment that bear on national, coalition, interagency, and military decision making.

Building Partner Capacity

Conduct research, operational analysis, capability design, and implementation support in order to enable the Department of Defense to assist, train, advise, and influence foreign partners, foreign competitors, adversary leaders, military-like forces, and relevant populations by developing and presenting information and conducting shaping activities to affect their perceptions, will, behavior, and/or capabilities. This includes research and development that supports the conduct of communication, shaping missions, and activities, but does not include kinetic operations or maneuver of forces for the purpose of influence.

Indirect Communications Support

Conduct research, operational analysis, capability design, and implementation support within the scope of traditional military information operations to enhance and improve client organization efforts to erode adversaries' power, influence, and will through proactive and responsive informational, psychological, and other irregular operations. IWS seeks to increase the efficacy of military information operations while decreasing the likelihood of direct action environments.

Knowledge Management

Conduct research, operational analysis, capability design, and spiral experimentation support to increase U.S. and appropriate partners' understanding of hostile forces, current and evolving tactical and operational environments, and opportunities for successful irregular warfare operations.



Mission Rehearsal and Exercise

Conduct research, operational analysis, capability design, and implementation support to increase U.S. and coalition partners' proficiency in and capacity to wage irregular warfare on targeted state and non-state actors. IWS seeks to further the art and science of irregular warfare operations and their understanding in the appropriate agencies, forces, and bodies of government.

Operations Integration

Conduct research, operational analysis, capability design, and implementation support to synchronize interagency irregular warfare efforts. IWS refines current capabilities and develops those capabilities necessary for friendly forces to prevent and prevail in future conflicts.

Pursuit and Denial

Conduct research, operational analysis, capability design, and implementation support to enable client organizations to better apply indirect and asymmetric force to identify, disrupt, deny, exploit, manipulate, and destroy hostile organizations and their supporting enterprises.



Building Partner Capacity



LEGACY

LEGACY fulfills a U.S. Central Command joint urgent operational needs statement for building Host Nation (HN) information and intelligence capacity at the province level and below. LEGACY is an exportable, doctrinally based informant management program loosely based off of the British model successfully deployed in Malaya, Kenya, Cyprus, and Northern Ireland. LEGACY builds from a zero-baseline the necessary skills and techniques required by HN security forces to penetrate and defeat insurgent and criminal networks within the rule of law. LEGACY is designed to transition informant management capacity to the HN through interface training between the mentor/trainer and the HN student. Based off of formal classroom instruction, on-site mentoring, and “train the trainer” tutelage, LEGACY builds future HN capability. LEGACY is supported by a formal compliance framework to monitor consistent program delivery and the transition process throughout the program timeframe. LEGACY espouses the principle that actionable intelligence necessary for the defeat of insurgent and criminal networks is best gleaned locally. As such, LEGACY focuses on the mentorship of HN security forces operating within the community.

LEGACY was initially implemented and tested in Iraq first with the U.S. Marines assigned to Multi National Force-West in Al Anbar Province and then migrated to Multi National Security Transition Command-Iraq in the Multi-National Division-North sector. LEGACY initially focused on police informant management capacity building at the province level and below. With its growing successes, LEGACY expanded to include the linkage between the province and national headquarters, training of other “non-police” security forces, and formal instruction at the National Intelligence Training Centers. LEGACY is currently operating in Afghanistan, building security force intelligence capacity from the national level to the provinces and the districts. LEGACY teams are deployed in Regional Command (RC)-East, RC-South, RC-South West, Kabul, the Network Targeting Exploitation Center, the Afghan Intelligence Training Center at Sia Sang (military), and the Afghan National Intelligence Training Center in Kabul (police). The doctrinal approach of LEGACY has been adopted by both Iraq and Afghanistan as the national model for security force informant management operations.

LEGACY seeks to further develop this unique mentoring and advisory model in support of Coalition and HN partners in other regional locations to help criminalize and marginalize similar network based



threats. LEGACY is supported by the Afghan Intelligence Transition Directorate and the Combined Security Transition Command Afghanistan.

SEQUEL

SEQUEL fulfills the House Armed Service Committee (HASC) National Defense Authorization Acts (NDAA) of 2011 and 2012 directing the Department of Defense to “develop a plan to institutionalize, within the U.S. government, the capability necessary to institutionalize and train foreign forces to gather and exploit counterinsurgency intelligence at a local level within the U.S. government.”

As current U.S. informant management doctrine is not exportable, an alternative solution is necessary to meet the intent of the HASC NDAA's of 2011 and 2012. SEQUEL is a Train the Trainer (TtT) initiative that incorporates the non-U.S. exportable informant management model “LEGACY” into U.S. Security Force Assistance (SFA) capabilities. SEQUEL delivers 12 weeks’ worth of LEGACY doctrine and training courses to seasoned U.S. informant managers through a three-week TtT program. These U.S. informant managers then deliver the LEGACY model to Host Nation Security Forces (HNSFs) where informant management training is necessary to defeat network-based threats.

By delivering SEQUEL to U.S. informant managers, HNSF informant management assistance can now be provided by the U.S. where contracted support is not feasible, greatly expanding this capability at a fraction of the cost to the U.S. tax payer.

SEQUEL is currently being delivered to the U.S. Marine Corps in support of its SFA mission. Other U.S. federal organizations are reviewing the LEGACY curriculum for applicability to their SFA missions.

Mission Rehearsal and Exercise

Advanced Situational Awareness Training

Advanced Situational Awareness Training (ASAT) responds to the need for a non-materiel solution to enhance the effectiveness and survivability of soldiers engaged in asymmetrical warfare and threatened by IEDs. While materiel solution protective measures may offer improvements, they add weight to the already overburdened



Irregular Warfare Support

soldier, and quite often their solutions are fleeting. By instilling in the individual soldier a cognitive process for attacking the problem, he is armed with the capability to effectively confront an ever changing threat.

ASAT focuses on teaching the individual soldier to confront his environment using Human Behavior Pattern Recognition and Analysis (HBPR&A). HBPR&A instills in the soldier the capability to analyze the environment using the six domains (heuristics, proxemics, geographics, kinesics, atmospheric, and biometrics) of human behavior. By combining the skills of the hunter, tracker, and investigator, ASAT builds into the soldier the ability to rapidly evaluate his environment and to act prior to being acted upon, thus maintaining the initiative and achieving success on the battlefield.

ASAT delivers to the individual soldier an intensive five-day training package, which has been denoted as “a game changer” by commanders in the field. In addition to the five-day training package, a 22-day TtT package is being delivered to determine the effectiveness of transitioning the HBPR&A expertise from the contractor to the U.S. Army. If successful, the ASAT methodology can become an organic capability within the U.S. government. Currently, the Irregular Warfare Support Program’s focus on ASAT is on the individual general purpose soldier during his training at the U.S. Army Maneuver Center of Excellence. The ASAT methodology is currently under review for a Mobile Training Team capability that can be delivered to general purpose combat units preparing to deploy.





Operations Integration

Marine Expeditionary Intelligence Analysis for the 21st Century

Marine Expeditionary Intelligence Analysis for the 21st Century (MEIA-21) fulfills a requirement by the United States Marine Corps (USMC) to improve Marine Corps Expeditionary Intelligence Analysis for the current and future engagements. The Director of Marine Corps Intelligence has directed that intelligence methods used by field-based units be gathered, assessed, improved, validated, and documented, and then made available for enterprise-wide use.

A core component of MEIA-21 is the development of field-derived analytic techniques known as structured models, approaches, and techniques (SMATs). These SMATs will collectively serve as reliable analytic tradecraft across the Marine intelligence enterprise. SMATs are intended to provide easy-to-understand, practical, analytic methods to assist in diagnosing threats, conditions, and opportunities found on the modern battlefield. This approach to structuring and standardizing tactical intelligence analysis is intended to present rigorous methods and techniques as a fundamental component of expert thinking. It will help equip intelligence analysts with “enabling structured tradecraft” to empower them to conduct more effective analysis to enhance operations. By harvesting the best analytical practices and innovations from the field, the USMC can capture, validate, and reuse this knowledge. Through MEIA-21, the USMC seeks to establish a repository for SMAT development, dissemination, use, and improvement.

To aide in this effort, the IWSP has partnered with the Defense Intelligence Agency and the RAND Corporation to incorporate Department of Defense, federal agency, and industry standards into the USMC developed SMATs. RAND is currently reviewing and improving each SMAT as presented by the USMC Intelligence Community. The end result will be an enhanced expeditionary intelligence analytical capability for intelligence-led operations in current and future engagements.

Strategic Art in Irregular Warfare

This three-phase effort identified and addressed gaps in understanding of the indirect and irregular threats that confront the U.S., now and in the future. The project analyzed historical approaches and capabilities for application in contemporary and future environments, with focus on successful cases of the



strategic use of non-kinetic methods. This applied research and associated products will provide new answers and uncover previous methodologies for how to apply a whole-of-government indirect approach to irregular threats and how best to utilize SOF assets in the non-kinetic, non-traditional domain against globally dispersed unconventional adversaries such as the growing threat of transnational criminal organizations and other non-governmental adversaries.

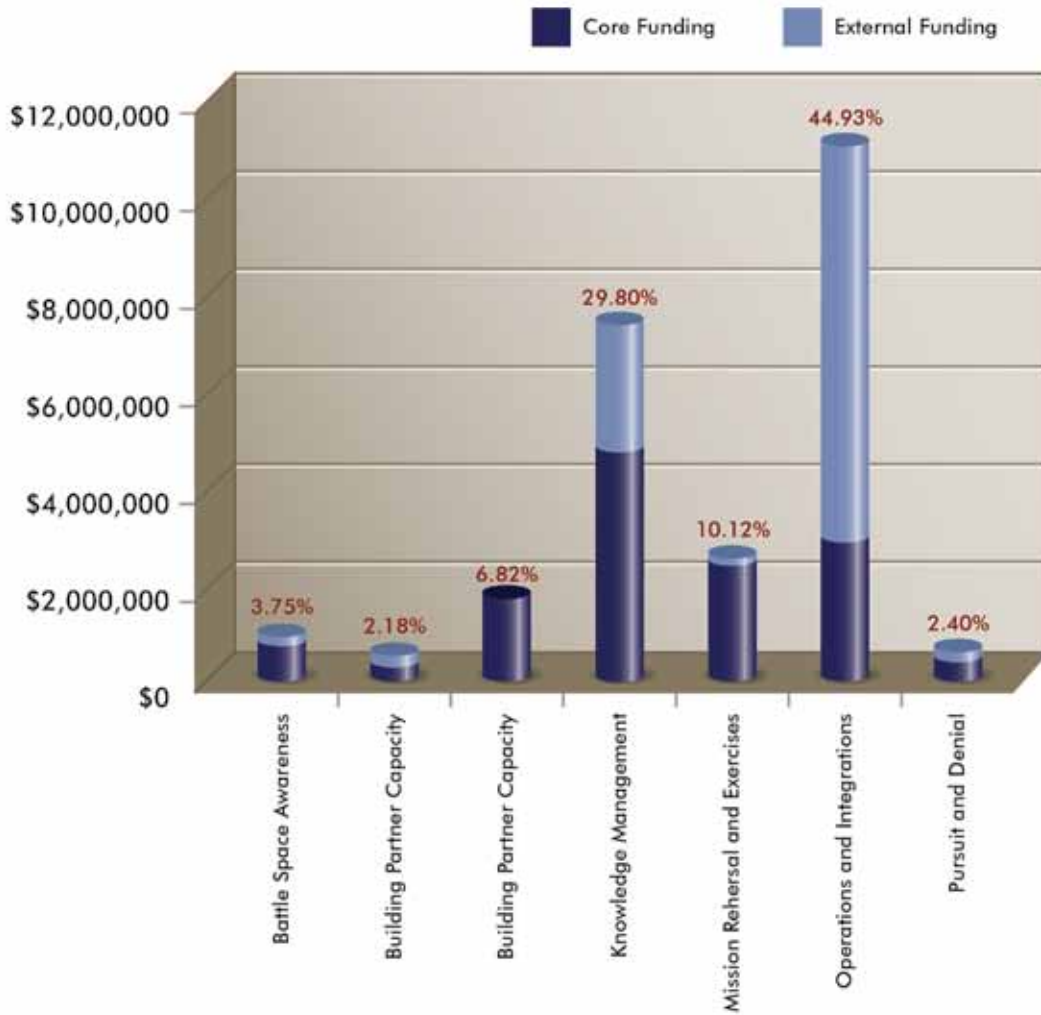
Pursuit and Denial

Digital Overwatch

The Digital Overwatch (DO) project is an effort to collect data, assess, evaluate, analyze, and determine suitability of a wide array of technologies and resources associated with cyber threats and countermeasures. The contractor conducted research, development, and test and evaluation to include training and mentoring on unique contractor products, analytical support, capability development of other products, and other cutting edge support to countering emerging and extant threats in the cyber and physical domains. During one test and evaluation, the DO team provided real-time data and analysis capability. With mentorship and training, end users are able to understand and monitor critical events in open source social media. The performer also developed training and mentoring methods for end users to apply to include analysis and training of unique software to counter illicit threats through social media analysis for high interest events.



IWS FY 2012 Funding by Focus Area (\$24.6 Million)



The background of the page is a faded, high-angle view of the American flag, showing the stars and stripes in a soft, light tone. The flag is positioned on the right side of the page, with the stars in the upper right corner and the stripes extending downwards and to the left.

Appendix





CTTSO Technology Transition Office

Technology transition is the process of taking a technology from the developmental and prototype phase to production and deployment by the end user community. Transition success is achieved when research and development products have evolved to the commercial market and/or have been inserted into government acquisition programs and can be easily and continuously obtained by the combating terrorism community. The path from the research and development phase to transition success can be challenging, and it is the mission of the Technology Transition Office at CTTSO to help overcome transition challenges to ensure success for the developers and end users. The Technology Transition Office at CTTSO works with internal Program Managers, external government agencies, end users, industry, and developers to overcome any barriers that may prohibit the successful transition of CTTSO technologies.

Planning for technology transition starts at the beginning of the CTTSO business cycle and continues throughout the life cycle of the program. In order to increase the likelihood of transition success, Technology Transition Plans are developed to provide a framework for how the technology will transition to the commercial market and/or government acquisition.





Topics discussed in the Technology Transition Plan include:

- The capability gap addressed by the development of the technology;
- Identifying customers and defining the market size;
- Understanding and managing intellectual property and data rights;
- Production strategies, including partnering, investment capital, and licensing;
- Commercialization and affordability;
- Environment, safety, and regulatory issues;
- Security and export control provisions;
- Test and evaluation planning and independent operational testing; and
- Operational suitability and operational support planning.

The keys to accelerating the complicated process of moving many prototypes to production includes having a disciplined process, available assistance, and teamwork among the project manager, technology transition manager, and developers. Additional information is available on the Technology Transition section of the CTTSO Web site at <http://www.cttso.gov>.



BAA Information Delivery System (BIDS)

The Broad Agency Announcement (BAA) Information Delivery System, better known as BIDS, works to support the CTTSO mission through the electronic publication of its annual BAAs. BAAs are the solicitation method of choice to bring the most urgent combating terrorism requirements forward for publication. CTTSO staff monitors BAA package instruction in light of submitter responses and feedback, and CTTSO implements improvements as needed each year to clarify the submission process.

To ensure the widest possible distribution to potential submitters, BAAs can be downloaded at the BIDS Web site (<http://www.bids.cttso.gov>) and are also advertised at the Federal Business Opportunities Web site (<https://www.fbo.gov>). In addition to conventional government solicitation notices, the BIDS Web site provides a BIDS Advisory and Announcement area that posts BAA news, coming events, and partnering agency solicitations. In addition to the advisory, the RSS (really simple syndication) news feed allows interested users to receive real-time broadcast information at a local computer when connected to the Internet.





BIDS is a rich source of submitter information, providing small business outreach, online help, and guidance for offerers proposing the use of human subjects in research. Overall BAA statistics are posted once the BAA closes.

BIDS not only functions as a response collection system, but also provides for submission evaluation and submitter notification. Submitter data is fully protected in a 128-bit encrypted environment. Evaluators must comply with source selection data handling requirements and accept a nondisclosure agreement to access BIDS. In addition to the nondisclosure, evaluators must also certify that there is no conflict of interest before access is granted to any submissions. The evaluation process is monitored for timely notice to submitters with the typical response via an automated e-notice complete within 90 days.

BIDS continues to serve as a leading solicitation process model for other federal programs by providing a streamlined electronic solution to receive proposals, providing access for subject matter expert evaluation, processing submissions through the approving authority, notifying the submitter of status, and maintaining a record of solicitation results.



2012 Membership

Advanced Analytic Capabilities

Intelligence Community

- Defense Intelligence Agency
- Office of the Director of National Intelligence

U.S. Department of Defense

- Joint Staff
- National Security Agency
- Naval Postgraduate School
- Office of the Secretary of Defense for Special Operations/Low-Intensity Conflict
- Office of the Secretary of Defense Rapid Fielding Office
- U.S. Army Training and Doctrine Command
- U.S. Marine Corps Intelligence Department
- U.S. Navy Naval Special Warfare Group
- U.S. Special Operations Command

U.S. Department of Homeland Security

- Immigration and Customs Enforcement

U.S. Department of State

Chemical, Biological, Radiological, Nuclear, and Explosives

Environmental Protection Agency

Federal Reserve Board

Intelligence Community

InterAgency Board

State and Local Agencies:

- Arlington County (VA) Fire Department
- Fairfax City (VA) Fire Department



- Fairfax County (VA) Fire and Rescue Department
- Fairfax County (VA) Police Department
- Fire Department, City of New York
- New York City Police Department
- NYC Office of Chief Medical Examiner
- Seattle (WA) Fire Department
- U.S. Department of Agriculture
- Animal and Plant Health Inspection Service
- Food Safety and Inspection Service

U.S. Capitol Police

U.S. Department of Commerce

- National Institute of Standards and Technology

U.S. Department of Defense

- Assistant to the Secretary of Defense for Nuclear and Chemical and Biological Defense;

Acquisition, Technology and Logistics

- Defense Advanced Research Projects Agency
- Defense Intelligence Agency
- Defense Threat Reduction Agency
- Joint Chiefs of Staff
- Joint Improvised Explosive Device Defeat Organization
- Joint Program Executive Office for Chemical and Biological Defense
- National Security Agency
- Pentagon Force Protection Agency
- Special Operations Command
- U.S. Air Force Air Combat Command
- U.S. Army 20th Support Command – Chemical, Biological, Radiological, Nuclear, and high yield Explosives (CBRNE)
- U.S. Army 22nd Chemical Battalion
- U.S. Army ARDEC Picatinny Arsenal
- U.S. Army Chemical School, Maneuver Support Center
- U.S. Army Medical Department
- U.S. Army National Ground Intelligence Center
- U.S. Army Research, Development, and Engineering Command – Edgewood Chemical Biological Center
- U.S. Marine Corps Chemical Biological Incident Response Force



- U.S. Marine Corps Explosive Ordnance Disposal
- U.S. Marine Corps Systems Command
- U.S. Navy Bureau of Medicine
- U.S. Navy Naval Air Warfare Center
- U.S. Navy Naval Explosive Ordnance Disposal Technology Division
- U.S. Navy Naval Forces Central Command
- U.S. Navy Naval Research Laboratory
- U.S. Navy Naval Surface Warfare Center

Explosive Ordnance Disposal/Low-Intensity Conflict Program

U.S. Department of Defense

- Defense Threat Reduction Agency
- Joint Improvised Explosive Device Defeat Organization
- Special Operations Command
- U.S. Air Force Air Combat Command
- U.S. Army 20th Support Command – Chemical, Biological, Radiological, Nuclear, and high yield Explosives (CBRNE)
- U.S. Army ARDEC Picatinny Arsenal
- U.S. Army Research, Development, and Engineering Command
- U.S. Army Research Laboratory
- U.S. Marine Corps Chemical Biological Incident Response Force
- U.S. Marine Corps Explosive Ordnance Disposal
- U.S. Marine Corps Special Operations Command
- U.S. Marine Corps Systems Command
- U.S. Navy Expeditionary Combat Command
- U.S. Navy Naval Explosive Ordnance Disposal Technology Division
- U.S. Navy Naval Research Laboratory
- U.S. Navy Office of Naval Research
- U.S. Navy Naval Surface Warfare Center, Panama City
- U.S. Navy Naval Surface Warfare Center, Dahlgren
- U.S. Navy Sea Systems Command

Improvised Device Defeat

U.S. Department of Defense

- Defense Threat Reduction Agency
- Joint Improvised Explosive Device Defeat Organization



- Pentagon Force Protection Agency
- Special Operations Command
- U.S. Air Force Air Combat Command
- U.S. Army 20th Support Command – Chemical, Biological, Radiological, Nuclear, and high yield Explosives (CBRNE)
- U.S. Army ARDEC Picatinny Arsenal
- U.S. Army Research, Development, and Engineering Command
- U.S. Army Research Laboratory
- U.S. Marine Corps Chemical Biological Incident Response Force
- U.S. Marine Corps Explosive Ordnance Disposal
- U.S. Marine Corps Special Operations Command
- U.S. Marine Corps Systems Command
- U.S. Navy Naval Explosive Ordnance Disposal Technology Division
- U.S. Navy Naval Research Laboratory
- U.S. Navy Naval Surface Warfare Center, Panama City
- U.S. Navy Naval Surface Warfare Center, Dahlgren

U.S. Department of Commerce

- National Institute of Standards and Technology

U.S. Department of Energy

U.S. Department of Homeland Security

- Coast Guard
- Customs and Border Protection
- Immigration and Customs Enforcement
- Science and Technology Directorate
- Secret Service
- Transportation Security Administration

U.S. Department of Justice

- Bureau of Alcohol, Tobacco, Firearms and Explosives
- Federal Bureau of Investigation
- National Institute of Justice

National Bomb Squad Commanders Advisory Board

State and Local Agencies:

- Arlington County (VA) Fire Department
- Fairfax County (VA) Police Department



- New York City Police Department
- San Diego County Sheriff's Bomb Squad
- Arizona Department Of Public Safety
- City of San Diego Bomb Squad
- El Paso (TX) Police Bomb Squad
- New Mexico State Police Bomb Squad
- Pima County (AZ) Regional Bomb Squad

U.S. Capitol Police

Investigative Support and Forensics

Environmental Protection Agency

- National Enforcement Investigations Center

Federal Reserve Board

Intelligence Community

National Transportation Safety Board

New York Police Department

U.S. Capitol Police

U.S. Department of Commerce

- National Institute of Standards and Technology – Office of Law Enforcement Standards

U.S. Department of Defense

- Defense Computer Forensics Laboratory
- Defense Criminal Investigative Service
- Defense Intelligence Agency
- Defense Threat Reduction Agency
- National Center for Credibility Assessment
- National Geospatial Intelligence Agency
- Office of the Provost Marshall General
- Pentagon Force Protection Agency
- U.S. Air Force Office of Special Investigations
- U.S. Army Criminal Investigation Command
- U.S. Navy Naval Criminal Investigative Service
- U.S. Special Operations Command

**U.S. Department of Energy**

- Office of Health, Safety, and Security

U.S. Department of Health and Human Services

- Office of Inspector General

U.S. Department of Homeland Security

- Federal Protective Service
- Forensic Document Laboratory
- Immigration and Customs Enforcement
- Secret Service
- Transportation Security Administration

U.S. Department of Justice

- Bureau of Alcohol, Tobacco, Firearms, and Explosives
- Drug Enforcement Administration
- Federal Bureau of Investigation
- Marshals Service
- National Center for Forensic Science
- National Forensic Science Technology Center
- National Institute of Justice

U.S. Department of State

- Office of the Coordinator for Counterterrorism

U.S. Department of Transportation

- Federal Aviation Administration

U.S. Department of the Treasury

- Internal Revenue Service
- Office of the Inspector General

U.S. Postal Inspection Service**U.S. Department of Veterans Affairs****Personnel Protection****Intelligence Community****Federal Bureau of Investigation****U.S. Capitol Police**



U.S. Department of Commerce

- National Institute of Standards and Technology
- Office of Law Enforcement Standards

U.S. Department of Defense

- Defense Threat Reduction Agency
- Joint Improvised Explosive Device Defeat Organization
- Joint Personnel Recovery Agency
- Pentagon Force Protection Agency
- Rapid Reaction Technology Office
- U.S. Air Force Office of Special Investigations
- U.S. Army
- U.S. Army Criminal Investigation Command
- U.S. Army Joint Trauma Analysis and Prevention of Injury in Combat
- U.S. Army Medical Research and Materiel Command
- U.S. Army Program Executive Office Soldier Protective Equipment
- U.S. Army Research, Development and Engineering Command
- U.S. Army Research Laboratory
- U.S. Army Soldier Systems Center (Natick)
- U.S. Army Special Operations Command
- U.S. Army Tank Automotive Research, Development and Engineering Center
- U.S. Navy Naval Air Systems Command
- U.S. Navy Naval Criminal Investigative Service
- U.S. Navy Program Executive Office Ships

U.S. Department of Energy

U.S. Department of Homeland Security

- Federal Air Marshal Service
- Federal Law Enforcement Training Center
- U.S. Secret Service, Special Services Division, Technical Security Division
- Bureau of Customs and Border Protection

U.S. Department of Justice

- Marshals Service
- National Institute of Justice

U.S. Department of State



Physical Security

Environmental Protection Agency

Federal Reserve Board

Intelligence Community

State and Local Agencies

- DC Metropolitan Police
- Jacksonville (FL) Port Authority
- Lynchburg (VA) Sheriff's Office
- New York Police Department
- Pinellas County (FL) Sheriff's Office
- Port Authority of New York & New Jersey
- Protective Services Police Department
- U.S. Capitol Police

U.S. Department of Agriculture

- Forest Service

U.S. Department of Commerce

- National Institute of Standards and Technology

U.S. Department of Defense

- Defense Advanced Research Projects Agency
- Defense Intelligence Agency
- Defense Threat Reduction Agency
- Explosives Safety Board
- Joint Chiefs of Staff
- Joint Improvised Explosive Device Defeat Organization
- Joint Task Force North
- Joint Warfare Analysis Center
- National Reconnaissance Office
- Offices of the Secretary of Defense
- Physical Security Equipment Action Group
- Unified Combatant Commands
- U.S. Air Force Research Laboratory
- U.S. Army Armaments Research, Development and Engineering Center
- U.S. Army Asymmetric Warfare Group



Appendix

- U.S. Army Chemical School
- U.S. Army Corps of Engineers
- U.S. Army Maneuver and Support Center
- U.S. Army Office of the Provost Marshal General
- U.S. Army Product Manager-Force Protection Systems
- U.S. Army Product Manager-Guardian
- U.S. Army Rapid Equipping Force
- U.S. Army Research, Development and Engineering Command
- U.S. Army Research Laboratory
- U.S. Army Special Forces Command
- U.S. Army Special Operations Command
- U.S. Army Training and Doctrine Command
- U.S. Marine Corps Central Command
- U.S. Marine Corps Special Operations Command
- U.S. Marine Corps Systems Command
- U.S. Marine Corps Warfighting Laboratory
- U.S. Naval Facilities Engineering Command
- U.S. Naval Facilities Engineering Service Center
- U.S. Navy Chief of Naval Operations
- U.S. Navy Commander Navy Installations Command
- U.S. Navy Criminal Investigative Service
- U.S. Navy Expeditionary Combat Command
- U.S. Navy Explosive Ordnance Disposal Technology Division
- U.S. Navy Office of Naval Research
- U.S. Navy Sea Systems Command
- U.S. Navy Strategic Systems Programs
- U.S. Navy Surface Warfare Center

U.S. Department of Energy

- Lawrence Livermore National Laboratory
- National Nuclear Security Administration
- Nuclear Regulatory Commission

U.S. Department of Homeland Security

- Coast Guard
- Customs and Border Protection
- Immigration and Customs Enforcement
- Science and Technology Directorate



- Secret Service
- Transportation Security Administration
- Transportation Security Laboratory

U.S. Department of the Interior

- Bureau of Reclamation

U.S. Department of Justice

- Bureau of Alcohol, Tobacco, Firearms and Explosives
- Drug Enforcement Administration
- Federal Bureau of Investigation
- Federal Bureau of Prisons

U.S. Department of State

Bureau of Diplomatic Security

U.S. Department of Transportation

Surveillance, Collection, and Operations Support

Intelligence Community

United States Cyber Command

United States Special Operations Command

Tactical Operations Support

National Tactical Officers Association

State and Local SWAT Teams

U.S. Department of Defense

- Defense Threat Reduction Agency
- U.S. Army
- U.S. Marine Corps
- U.S. Navy
- U.S. Special Operations Command

U.S. Department of Energy

- National Nuclear Security Administration



- Office of Health, Safety and Security

U.S. Department of Homeland Security

- Urban Search and Rescue
- U.S. Border Patrol Tactical Unit
- U.S. Coast Guard
- U.S. Immigration and Customs Enforcement
- U.S. Secret Service

U.S. Department of Justice

- Ballistic Research Facility
- Bureau of Alcohol, Tobacco, Firearms and Explosives Special Response Team
- Federal Bureau of Investigation Hostage Rescue Team
- U.S. Marshals Service

Training Technology Development

Intelligence Community

InterAgency Board

National Bomb Squad Commanders Advisory Board

National Tactical Officers Association

U.S. Department of Defense

- Defense Intelligence Agency
- Joint Improvised Explosive Device Defeat Office
- Office of the Undersecretary of Defense for Personnel and Readiness
- Pentagon Force Protection Agency
- U.S. Army Asymmetric Warfare Group
- U.S. Army John F. Kennedy Special Warfare Center and School
- U.S. Army National Guard Bureau
- U.S. Army Research Lab Simulation and Training Technology Center
- U.S. Army Special Operations Command
- U.S. Army Training and Doctrine Command
- U.S. Army War College
- U.S. Joint Forces Staff College
- U.S. Marine Corps
- U.S. Marine Training and Education Command
- U.S. Naval Special Warfare Command



- U.S. Special Operations Command

U.S. Department of Energy

U.S. Department of Homeland Security

- Customs and Border Protection
- Federal Emergency Management Agency
- Federal Law Enforcement Training Center
- Office of Bombing Prevention
- Science and Technology Directorate
- Secret Service
- Transportation Security Administration

U.S. Department of Justice

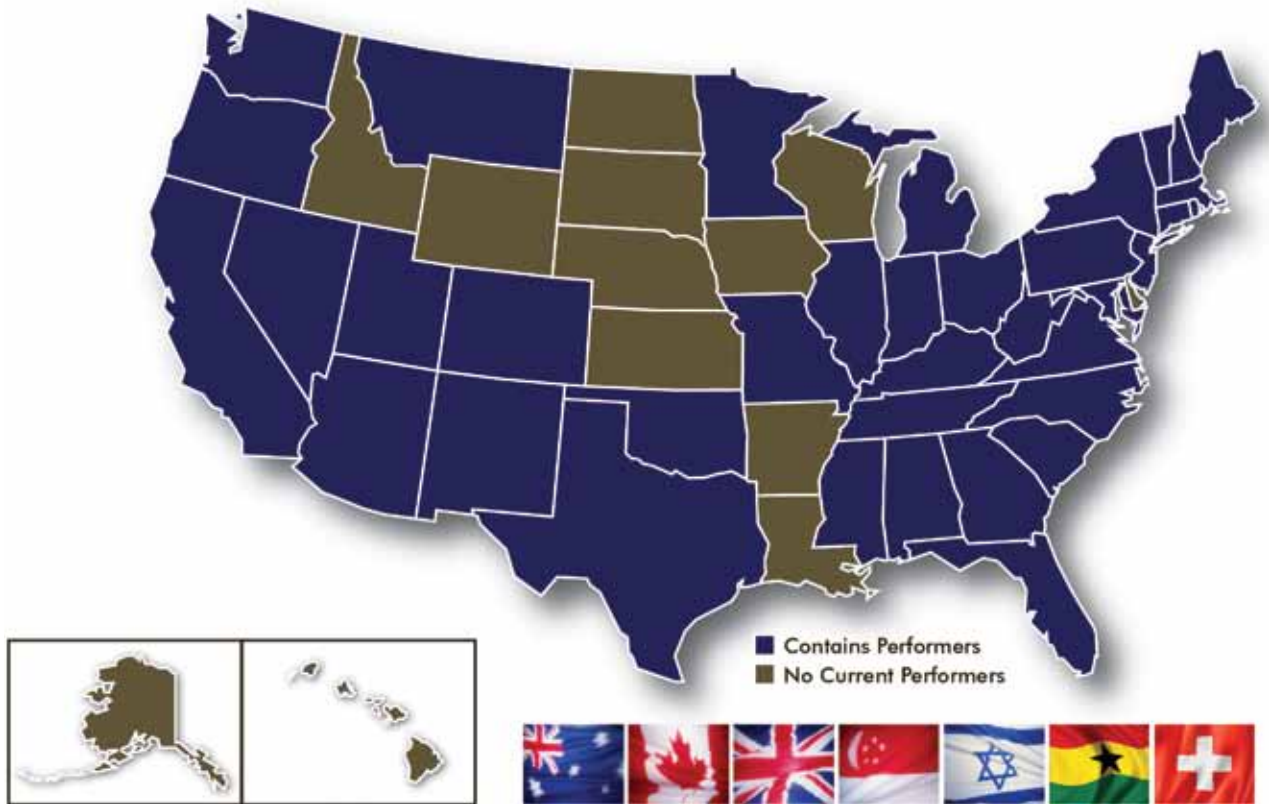
- Federal Bureau of Investigation

U.S. Department of State

- Bureau of Diplomatic Security



2012 Performers



Alabama

Army Space and Missile Defense Command, Huntsville
Auburn University, Auburn

Arizona

Armorworks Inc., Chandler
Exponent, Phoenix
Nivisys Industries, LLC, Tempe

California

Aerovironment, Inc., Simi Valley
Altobridge Corporation, San Jose
General Dynamics Ordnance and tactical Systems, Healdsburg
Jet Propulsion Laboratory, Pasadena
Language Weaver, Los Angeles
Mirage Systems, Inc., Sunnyvale
Naval Air Warfare Center, China Lake



Naval Facilities Engineering Service Center, Port Hueneme

Neptunic Technologies, Inc., San Diego

Palantir USG, Inc., Palo Alto

Precision Optics Corporation, Torrance

Quantum Magnetics, Inc., San Diego

Rapiscan Systems Neutronics and Advanced Technologies, Sunnyvale

Raymat Materials, Inc., Fremont

Safariland LLC, Ontario

Sandia National Laboratory, Livermore

Science Applications International Corporation, San Diego

Science Applications International Corporation, Vista

Smiths Detection, Pasadena

System Technology, Inc., Hawthorne

Visualize Technologies, Inc., Santa Monica

Western Psychological Services, Torrance

Colorado

Applied Research Associates, Inc., Littleton

APTEK, Colorado Springs

Ball Aerospace & Technologies Corp., Westminster

Colorado State University, Fort Collins

NEK Advanced Securities Group, Inc., Colorado Springs

RadiantBlue Technologies, Inc., Colorado Springs

Rocky Mountain Scientific Laboratories, Littleton

Sierra Nevada Corporation, Centennial

Connecticut

Ensign-Bickford Aerospace & Defense Co., Simsbury

United Technologies Research Center, Hartford

District of Columbia

Bureau of Alcohol, Tobacco, Firearms, and Explosives

Naval Research Laboratory

Florida

Air Force Research Laboratory, Tyndall Air Force Base

CAE USA Inc., Orlando

Carley Corporation, Orlando

CTC Tampa Bay, Largo

Cubic Defense Applications, Orlando

Engineering and Computer Simulations, Inc., Orlando

Dreifus Associates, Ltd., Maitland

Field Forensics, Largo

Florida International University, Miami

Naval Surface Warfare Center, Panama City

Perception IR Manufacturing, LLC, Palm Harbor

Service Brands, LLC, Sarasota

Technology Training Center (U.S. Army Research Lab), Orlando

Georgia

Georgia Tech Research Institute, Atlanta

Squires-Fulcher LLC, Locust Grove



Illinois

Argonne National Laboratory,
Champaign

Brain-Body Center, University of
Illinois at Chicago

Illinois Fire Service Institute,
Champaign

University of Illinois, Urbana-
Champaign

Indiana

Conflict Kinetics, Merrillville

Indiana University Purdue University
Indianapolis, Indianapolis

Naval Surface Warfare Center, Crane

Kentucky

Ideal Products, Inc., Lexington

L-Tech Enterprises, Inc., Eubank

Oakridge National Laboratory

Maine

Falcon Performance Footwear,
Auburn

Monroe Infrared Technology, Inc.,
Kennebunk

Maryland

Army Research Laboratory, Aberdeen
Proving Ground

Avon Protection Systems, Inc.,
Belcamp

Ballard Power Systems, College Park

Edgewood Chemical Biological
Center, Aberdeen Proving Ground

G3 Technologies, Inc., Columbia

Garrison, Adelphi Laboratory Center
IMNE-ALC-RMO, Hagerstown

HazTrain, Waldorf

Impact Computing Corporation,
Silver Spring

Mistral Security Incorporated,
Bethesda

Naval Air Systems Command,
Patuxent River

Naval Explosive Ordnance Disposal
Technology Division, Indian Head

Naval Surface Warfare Center,
Indian Head

Oceaneering International, Inc.,
Hanover

SimQuest, Silver Springs

Transformational Security, LLC,
Hanover

TRX Systems, Inc., Greenbelt

U.S. Army Research Laboratory,
Aberdeen Proving Ground

U.S. Army Test and Evaluation
Command, Aberdeen Proving
Ground

Vehicle Systems Integration, LLC,
College Park

W.L. Gore, Elkton

Massachusetts

American Science & Engineering,
Inc., Billerica

Artisent, Inc., Boston

BAE Systems, Burlington

BBN Technologies, Cambridge

C-2i, Inc., Stow

Charles River Analytics, Cambridge

ENSR International Corporation,
Westford

Excellims Corporation, Maynard

Flir Government Systems, Boston



HALO Maritime Defense Systems,
Andover

Pixel Forensics, Inc., Burlington

Reveal Imaging Technologies,
Bedford

Morpho Detection, Wilmington

Physical Sciences, Inc., Andover

QinetiQ North America, Inc.,
Waltham

Thermo Fisher Scientific, Inc.,
Wilmington

Michigan

Avon Protection Systems, Inc.,
Cadillac

Baker Enterprises, Alpena

Cybernet Systems Corporation, Ann
Arbor

General Motors LLC, Warren

Quantum Signal LLC, Ann Arbor

Quantum Signal LLC, Saline

Wayne State University, Detroit

Minnesota

Agile Defense, LLC, Minneapolis St.
Paul

University of Minnesota, Minneapolis

Mississippi

Rapiscan Security Products, Inc.,
Ocean Springs

University of Mississippi, University

U.S. Army Engineer Research and
Development Center, Vicksburg

Missouri

Clean Earth Technologies, LLC, Earth
City

Midwest Research Institute, Kansas
City

Washington University in St. Louis,
St. Louis

Montana

Veridical Research and Design,
Bozeman

Nevada

Remote Sensing Laboratory, Las
Vegas

Sierra Pacific Innovations, Las Vegas

New Hampshire

Elbit Systems of America, Merrimack

Globe Manufacturing Company,
Pittsfield

Sig Sauer, Inc., Exeter

Warwick Mills, Inc., New Ipswich

New Jersey

Armament Research, Development
and Engineering Center, Picatinny
Arsenal

Goodrich Corporation Sensors
Unlimited, Inc., Princeton

Picatinny Arsenal, Picatinny

Structured Materials Industries,
Piscataway

New Mexico

Applied Research Associations,
Albuquerque

Energetic Materials Research and
Testing Center, Socorro

Los Alamos National Laboratory, Los
Alamos



National Assessment Group,
Albuquerque

Sandia National Laboratories,
Albuquerque

New York

GE Global Research, Niskayuna

General Dynamics Information
Technology, Getzville

International Biometric Group, New
York

Kitware, Inc., Clifton Park

Persistent Systems, LLC, New York

Vuzix Corporation, Rochester

Weapon Systems Technology
Information Analysis Center, Rome

North Carolina

Archangel Armor, Fayetteville

Atlantic Aero, Greensboro

Emerging Technology Support LLC,
 Mooresville

North Carolina State University,
Textile Protection and Comfort
Center, Raleigh

Partnership for Defense Innovation,
Fayetteville

Signalscape, Inc., Cary

Vertical Innovation Associates, Inc.,
Fayetteville

XinRay Systems, Research Triangle
Park

Ohio

Battelle Memorial Institute, Columbus

Lion Apparel, Dayton

Multiple Intelligences Research and
Consulting, Inc., Kent

Plug Power, Sydney

Oklahoma

Flir Government Systems, Stillwater

Southwest Research Institute, Midwest
City

Oregon

P&R Technologies, Inc., Portland

Pennsylvania

DRS Laurel Technologies, Johnstown

Foreign Policy Research Institute,
Philadelphia

NIOSH NPPTL, Pittsburgh

Nomadio, Inc., Philadelphia

Rhode Island

Naval Undersea Warfare Center,
Newport

South Carolina

Advanced Mission Systems, Fort Mill

Time Cuffs, LLC, North Charleston

Tennessee

Northrop Grumman Remotec,
Clinton

Universal Strategy Group, Inc., Mt.
Pleasant

Texas

Accuracy 1st, Inc., Arthur City

Applied Research Associates, Inc.,
San Antonio

G2 Associates, Heath



Infrared Camera, Inc., Beaumont
 International Personnel Protection, Inc., Austin
 OSS Law Enforcement Advisors, Spring
 Protection Engineering Consultants, LLC, Austin
 Southwest Foundation for Biomedical Research, San Antonio
 Southwest Research Institute, San Antonio
 Texas A&M University, College Station

Utah

Torion Technologies, Inc., American Fork

Vermont

Plasan North America, Bennington
 Sound Innovations, Inc., White River Junction

Virginia

Axiom Corporation, Fairfax
 Adayana Government Group, Falls Church
 AGNITIO Corp., Arlington
 Analytic Services, Inc., Alexandria
 Applied Research Associates, Arlington
 Avir, LLC, Charlottesville
 Battelle Memorial Institute, Arlington
 Blackbird Technologies, Herndon
 The Bode Technology Group, Inc., Lorton
 Corporation for National Research Initiatives, Reston
 Defense Life Sciences, LLC, McLean

Deloitte Consulting, LLP, Arlington
 Federal Bureau of Investigation, Quantico
 Gatekeeper, Inc., Sterling
 Hazard Management Solutions, Inc., Arlington
 ManTech International Corporation, Chantilly
 National Crash Analysis Center of George Washington University, Ashburn
 Naval Surface Warfare Center Carderock Combatant Craft Division, Little Creek

Naval Surface Warfare Center, Dahlgren

Night Vision and Electronic Sensors Directorate, Fort Belvoir

Northrop Grumman Training Solutions Sector, Herndon

Platinum Solutions, Inc., Reston

S4 Tech, Reston

Science Applications International Corporation, McLean

Sparta, Inc., Centreville

SRA/Platinum Solutions, Inc., Reston

System of Systems Analytics, Inc., Fairfax

SyTech Corporation, Alexandria

Trident Systems, Inc., Fairfax

U.S. Army Night Vision and Electronic Sensors Directorate, Fort Belvoir

White Canvas Group, LLC, Arlington

Washington

The Boeing Company, Seattle

Cascade Designs, Inc., Seattle

Cling Cal Corp, Deming



Creative Machining Co., Sedro Woolley
NextLevel Training, LLC, Ferndale
Pacific Northwest Laboratory, Richland
Pioneer Consulting, Ferndale
Stark Aerospace, Redmond

West Virginia

Azimuth, Inc., Morgantown
STS International, Berkeley Springs

International

Australia

Australian Government Department of the Prime Minister and Cabinet
Bond University, Gold Coast, Queensland
Catapult Innovations, Scoresby
Defence Science and Technology Organisation, Edinburgh
Defence Science and Technology Organisation, Fisherman's Bend, Melbourne
Department of Prime Minister Cabinet
Emergency Management Australia, Canberra
Flinders University, Adelaide
iWebGate Pty Ltd, Perth
National Security Science and Technology Center, Canberra
Queensland Fire and Rescue Services, Brisbane
Queensland University of Technology, Brisbane
Semantic Science Pty Ltd, Stirling

University of Adelaide, Adelaide
University of Tasmania, Hobart

Canada

Ballard Power Systems, Burnaby, British Columbia
Biokinetics & Associates, Ltd., Ontario
Canadian Border Services Agency, Ottawa, Ontario
Canadian Commercial Corporation, Ottawa, Ontario
Defence Research and Development Canada, Suffield
Defence Research and Development Canada, Valcartier, Quebec
Oculus, Toronto, Ontario
Optosecurity, Inc., Quebec City, Quebec
Royal Canadian Mounted Police, Ottawa, Ontario
Transport Canada, Ottawa, Ontario

Ghana

mPedigree Network, Ltd., Accra

Israel

DEA Research and Development, Ltd., Jerusalem
Elbit Land/Platforms, Yokne'am
Electro-Optics Industries, Ltd., Rehovot
The Hebrew University of Jerusalem, Jerusalem
Israel Defense Force
Israeli Ministry of Defense, Tel Aviv
Israel National Police, Jerusalem
Israel Security Agency, Tel Aviv



National Information Security
Authority

National Nuclear Research Center,
Negev

Netline Communications
Technologies, Inc., Tel Aviv

PrevenTech, Ltd., Jerusalem

Roboteam, Tel Aviv

Soltam Systems, Ltd., Yokne'am

Thruvision Systems, Ltd., Abingdon

United Kingdom Ministry of Defence

Singapore

Defence Science and Technology
Agency

Envisage Reality

Ministry of Defense

Switzerland

Artkis Radiation Detectors, Ltd.,
Zurich

United Kingdom

Buckler Davies Consultancy Limited,
Swindon

Centre for the Protection of National
Infrastructure

Cognitive Consultants International
Ltd., Southampton

Counter Terrorism Science and
Technology Centre, Salisbury

Defence Science and Technology
Laboratory, Fort Halstead, Kent

Defence Science and Technology
Laboratories, Porton Down

Home Office Scientific Development
Branch, London

Ministry of Defence, London

Providence SA Limited, Hereford



Glossary of Acronyms

AAC	Advanced Analytic Capabilities
AN	Ammonium Nitrate
AO	Areas of Operation
ASAT	Advanced Situational Awareness Training
ASD SO/LIC	Assistant Secretary of Defense for Special Operations/ Low-Intensity Conflict
ATD	Anthropomorphic Test Device
BAA	Broad Agency Announcement
BABT	Behind Armor Blunt Trauma
BBTK	Body Bomb Tool Kit
BIDS	Broad Agency Announcement Delivery System
BTTR	Ballistic Blunt Trauma Test Rig
CAN	Calcium Ammonium Nitrate Fertilizer
CB	Chemical and Biological
CBRN	Chemical, Biological, Radiological, Nuclear
CBRNE	Chemical, Biological, Radiological, Nuclear, and Explosives
C-IED	Counter-Improvised Explosive Device
CSSURG	Confined Spaces Suppressed Upper Receiver Group
CTTSO	Combating Terrorism Technical Support Office
DIDSOH-DH	Dual-Imaging Digital Sonar-Diver Held
DO	Digital Overwatch
DOS	Department of State
ECM	Electronic Countermeasures
EOD	Explosive Ordnance Disposal



EOD/LIC	Explosive Ordnance Disposal/Low-Intensity Conflict
EWG	Electronic Warfare Grenade
FBI	Federal Bureau of Investigation
GC-MS	Gas Chromatography-Mass Spectrometer
HASC	House Armed Service Committee
HBPR&A	Human Behavior Pattern Recognition & Analysis
HME	Homemade Explosives
HN	Host Nation
HNSF	Host Nation Security Forces
HRP	High-Risk Personnel
ICE	Integrated Conveyance Escort System
IDD	Improvised Device Defeat
IED	Improvised Explosive Device
IG/T	Interdepartmental Group on Terrorism
iLIVE	inLine Instant Video Enhancement
ISF	Investigative Support and Forensics
ISR	Intelligence, Surveillance, and Reconnaissance
IWS	Irregular Warfare Support
IWSP	Irregular Warfare Support Program
JIEDDO	Joint Improvised Device Defeat Organization
JSEOD	Joint Service Explosive Ordnance Disposal
MANET	Mobile Ad Hoc Network
MEIA-21	Marine Expeditionary Intelligence for the 21st Century
MMD	Mask-Mounted Display
MPC	Model Predictive Controller
MS&G	Models, Simulations, and Games
MSP	Mobile Surveillance Platform



MTCBA	Multi-Threat Concealable Body Armor
MTGR	Micro Tactical Ground Robot
NAVEODTECHDIV	Navy Explosives Ordnance Disposal Technology Division
NBSCAB	National Bomb Squad Commanders Advisory Board
NDAA	National Defense Authorization Acts
NFPA	National Fire Protection Association
NIJ	National Institutes of Justice
NSWC PCD	Naval Surface Warfare Center Panama City Division
OE-SGT	Operational Environment Scenario Generation Tool
OSS	Outpost Surveillance System
PAPR	Powered Air Purifying Respirator
PBIED	Person-Borne Improvised Explosive Device
PCB	Printed Circuit Board
PMESII	Political, Military, Economic, Social, Information, and Infrastructure
PP	Personnel Protection
PRISM	Planning, Research, and Intelligence Scalable Modeling
PS	Physical Security
PSB	Port Security Barriers
PSB-X	Mobile Port Security Barrier System
PSP2	Portable Surveillance Platform2
RAAM	Remote Access Air Mobility
RAPTOR	Rapidly Attachable Pole-Mounted Tactical Observation Relay
RC	Regional Command
RCIED	Radio Controlled Improvised Explosive Device
RF	Radio Frequency



ROV	Remotely Operated Vehicle
SAVANT	Susceptibility and Vulnerability Analysis Tool
S-CAPS	Social Cultural Assessment from Passive Sensing
SCBA	Self-Contained Breathing Apparatus
SCOS	Surveillance, Collection, and Operations Support
SF	Special Forces
SFA	Security Force Assistance
SIDD	Scalable Improvised Device Defeat System
SMATs	Structured Models, Approaches, and Techniques
SNAP	Social Network Analysis Platform
SNM	Special Nuclear Materials
SOF	Special Operations Forces
SUAS	Small Unmanned Aerial System
SWAT	Special Weapons and Tactics
TATP	Triacetone Triperoxide
TDS	Tactical Driving Simulation
TICs	Toxic Industrial Chemicals
TOS	Tactical Operations Support
TSWG	Technical Support Working Group
TTD	Training Technology Development
TtT	Train the Trainer
UAS	Unmanned Aerial Systems
USCG	United States Coast Guard
USMC	United States Marine Corps
USV	Unmanned Surface Vessel
VBIED	Vehicle-Borne Improvised Explosive Device
VBIEDTK	Vehicle-Borne Improvised Explosive Device Tool Kit



Appendix

VTOL

Vertically Take-Off and Landing

WBIED

Water-Borne Improvised Explosive Device

