COMBATING TERRORISM TECHNICAL SUPPORT OFFICE

2017 REVIEW BOOK

The terrorism landscape continues to be an enduring and rapidly evolving problem that attacks the fundamental freedoms of democratic societies. The U.S. Government along with its allies focus a continuous stream of resources to battle this ongoing threat. The Combating Terrorism Technical Support Office (CTTSO) is working collectively with Department of Defense, interagency, and international partners to stem the rising tide of terrorism today. Focusing on near-term solutions that can bring immediate capability to the fight, CTTSO strives to rapidly prototype and deliver capability to the field. CTTSO, along with its partners, address a broad range of combating terrorism issues that include—warfighter survivability, force protection, kinetic operations, intelligence, training, and forensics.

This review book highlights some of our accomplishments in 2017 and ongoing research and development as we look to the future. During the past year, CTTSO focused on developing systems to improve the performance of explosive detection, counter unmanned aerial systems, detect tunnels, increase military operators' lethality, and use analytics for improved situational awareness in the terrains that both the military and law enforcement sectors operate.

We continue to collaborate with our research and development counterparts across the U.S. Government and with our international partners to ensure CTTSO responds quickly, efficiently, and effectively to critical capability gaps.

TABLE OF CONTENTS

COMBATING TERRORISM TECHNICAL SUPPORT OFFICE

MISSION

The mission of the Combating Terrorism Technical Support Office (CTTSO) is to identify and develop capabilities to combat terrorism and irregular adversaries and to deliver these capabilities to Department of Defense (DoD) components and interagency partners through rapid research and development, advanced studies and technical innovation, and provision of support to U.S. military operations.

History and 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 developed 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. In FY16, portions of the EOD/LIC and IWS Programs that support the CTTSO mission were transitioned to TSWG under the Improvised Device Defeat/Explosives Countermeasures and Irregular Warfare and Evolving Threats Subgroups, respectively.

CTTSO and Other Agencies

CTTSO is charged with providing a forum for interagency and international users to discuss mission requirements to combat terrorism, prioritize these requirements, fund and manage solutions, and deliver capabilities. 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.

CTTSO accomplishes its mission in three ways. First, CTTSO takes operational requirements from warfighters, incorporates policy priorities of the Department of Defense (DoD) civilian leadership[1], and rapidly identifies, develops, and delivers advanced capabilities for Special Operations Forces and General Purpose Forces to improve the capacity of the DoD to combat terrorism and irregular adversaries. Second, CTTSO collaborates with and supports related requirements of non-DoD U.S. government agencies and state/local/tribal governments to understand those users' priorities and requirements to share expertise, and to develop mutually beneficial capabilities. Third, CTTSO works with partner country ministries of defense under bilateral arrangements to conduct cooperative research and development, which allows the U.S. DoD to leverage foreign experience, expertise, and resources in the fight against terrorists and their infrastructure.

Technology Transition

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 program at CTTSO to help overcome transition challenges to ensure success for the developers and end users. The Technology Transition program 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 lifecycle 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 managers, and developers. Additional information is available at the Technology Transition section of the CTTSO website, http://www.cttso.gov.

Innovation

In the current budget environment of focusing on doing more with less, the need for innovation increases as we look for new ways to combat terrorism. Novel solutions come from individual entrepreneurs and tinkerers, and in order to leverage those solutions, CTTSO must constantly look for ways to actively engage them. The Innovation program at CTTSO has, at its core, the following objectives:

- Identify new ways to obtain success, rather than uncertain development, through prizes, challenges, and other rewards;
- Provide additional tools and resources to fulfill operational capability gaps;
- Increase the number and diversity of solution providers;
- Provide rapid and agile ways of doing business that lower both cost and risk.

[1] *Applicable policy guidance includes Presidential National Security Strategy, Defense Strategic Guidance, and any guidance or instructions issued by the ASD SO/LIC.*

Innovation is a model that enables Government research and development programs to identify the best solutions in the shortest amount of time possible at a lower cost. The following initiatives are underway at CTTSO to support the Innovation program.

- Rapid Innovation Fund: Facilitates the rapid insertion of innovative small business technologies into government systems or programs that meet critical national security needs.
- Challenge Driven Innovation: Crowdsourcing challenging problems to the world to provide ideas and solutions to fulfill important scientific and technical challenges.
- Laboratory Innovation Crowdsourcing (LINC): Conduit for field operators to submit their operational challenges to solvers in the U.S. Government.

International Partners

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.

We have decades long histories of mutual support, technical cooperation, and information sharing. The rise of international terrorism began hundreds of years ago but reached new depths in the 1960s and 70s. Its subsequent proliferation in the 21st century spurred U.S. efforts to broaden the scope of cooperative activities to combat this threat to international peace and security.

From modest beginnings in the early 1990s, CTTSO's international relationships have matured and grown into wide-ranging and multifaceted programs that address a variety of technically sophisticated threat capabilities employed by terrorist groups and their state sponsors. Tactics, techniques, procedures, countermeasures, and associated equipment identified, developed, and tested under terms our expanding cooperative arrangements found their way into the inventories of U.S. and partner operators where they enhanced our respective national capabilities and permitted all partner nations to respond more effectively to the threats.

The partnerships provide insights into regional affairs, access to a broader technology base, and allows for the use of unique facilities offered by each country. Each of the agreements are 50/50 cost shared, comprised of financial and non-financial contributions, to address joint requirements, reducing duplication of efforts and scientific trial and error. Bilateral meetings are held on a regular basis to review ongoing projects and to discuss new areas of collaboration.

In addition to CTTSO's bilateral partners, CTTSO cooperates with other countries when appropriate. 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.

Our international partnerships continue today and will for the foreseeable future as we strive to blunt the efforts of those who would seek to destroy our freedoms and compromise our way of life.

TECHNICAL SUPPORT WORKING GROUP

MISSION

The mission of the Technical Support Working Group (TSWG) is to identify, prioritize, and coordinate interagency and international research and development (R&D) requirements for combating terrorism. Through the Department of Defense's Combating Terrorism Technical Support Office and funding provided by other agencies, the TSWG rapidly develops technologies and equipment to meet the high-priority needs of the combating terrorism community, and addresses joint international operational requirements through cooperative R&D with major allies.

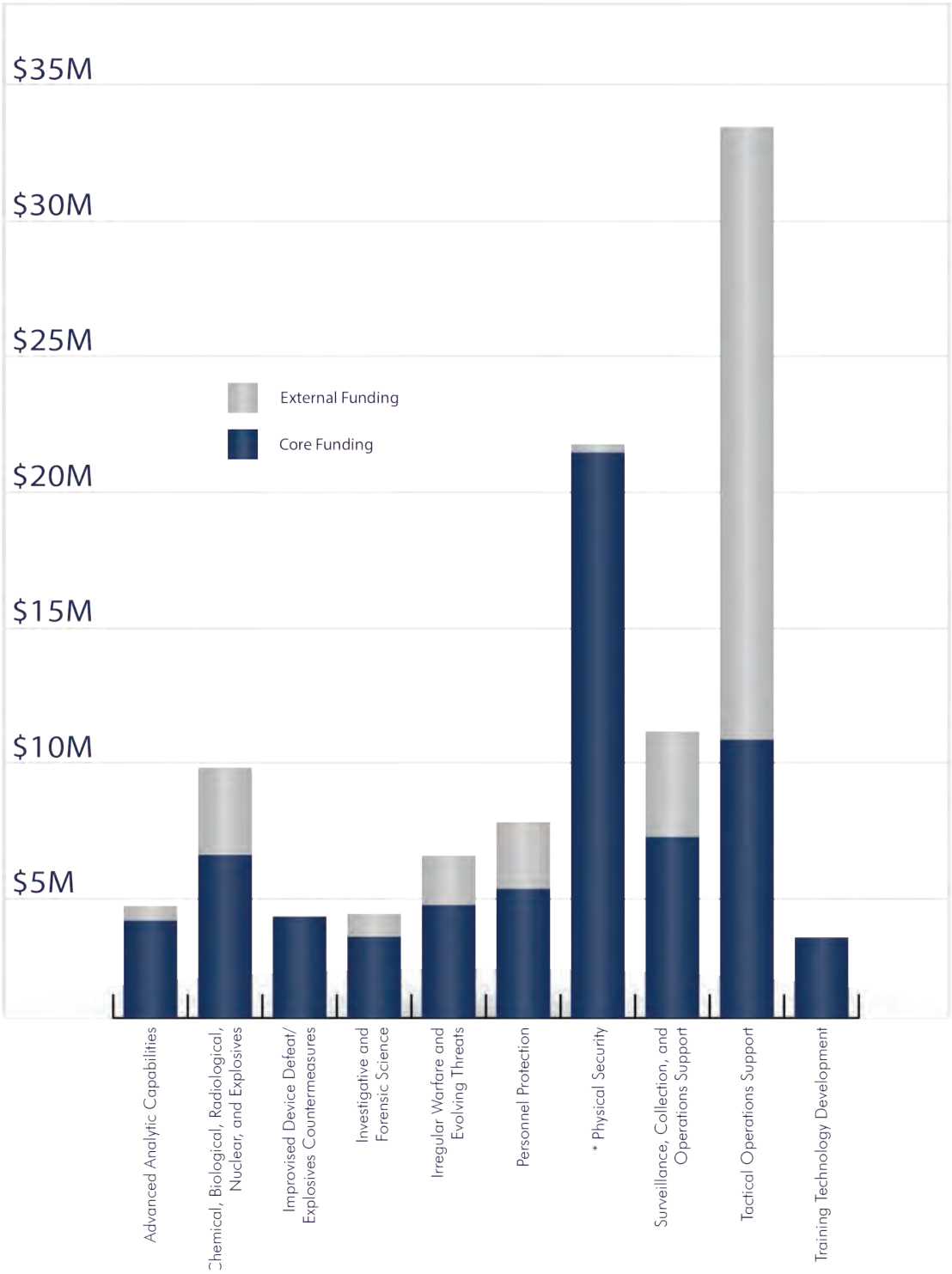
History and Organization

In April 1982, the National Security Decision Directive 30 assigned responsibility for the development of an overall United States policy on terrorism to the Interdepartmental Group on Terrorism (IG/T), chaired by the Department of State. TSWG was an original subgroup of the IG/T, which later became the Interagency Working Group on Counterterrorism (IWG/CT). 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."

TSWG operates under the management and technical oversight of the Department of Defense (DoD) Assistant Secretary of Defense for Special Operations/Low-Intensity Conflict (ASD SO/LIC) and the policy oversight of the Department of State's Bureau of Counterterrorism and Countering Violent Extremism.

TSWG's 10 subgroups are chaired by senior representatives from DoD, other federal agencies, and national organizations with special expertise in those functional areas. Chairmanship of subgroups is as indicated in the organizational chart below.

TSWG Fiscal Year 2017 Project Funding ($102M)



*$17.5M congressionally directed for cooperative anti-tunnel work with the Government of Israel.

ADVANCED ANALYTIC CAPABILITIES

aacsubgroup@cttso.gov

FOCUS AREAS

Advanced Computing

Develop, apply, and integrate advanced computing systems and methodologies to the operational environment.

Anticipatory Analytics and Foresight

Apply, develop, and integrate new anticipatory analytic tools to the full spectrum of the operational environment. Apply, develop, and integrate strategic foresight analytical methods, systems, capabilities, and tools to strategic planning.

Big Data, Algorithms, and Decisions

Integrate big data, algorithms, and decision making tools to enhance tactical-to-strategic decision making.

COMPLETED PROJECTS

Tactical Intelligence Automation

Military and law enforcement organizations can benefit from real-time intelligence automation during surveillance and detection operations at the tactical level. Operators and intelligence analysts are currently overwhelmed with sensor data and while there is no shortage of information, it is problematic to analyze and make use of this information in a timely fashion. In order to address critical gaps identified by the United States Special Operations Command (USSOCOM), Federal Bureau of Investigation (FBI), and U.S. Customs and Border Protection (CBP), Gantz-Mountain packaged multiple cameras and acoustic sensors along with micro-sized supercomputing and artificial intelligence algorithms at the tactical edge in a small low-visibility form factor. This technology allows for user-defined alert criteria and behavior analysis while conducting processing, exploitation, and dissemination of tactical level intelligence on board the sensor. The technology forms a network of electronic listening and observation posts providing tremendous force multiplication, manpower, and bandwidth savings during both surveillance and anti-terrorism force protection applications. The systems are being evaluated by USSOCOM, FBI, and U.S. CBP. This capability is available as the Mini Tactical SOF Intelligence Automation System (MT-5) through Gantz-Mountain Intelligence Automation Systems, Inc.

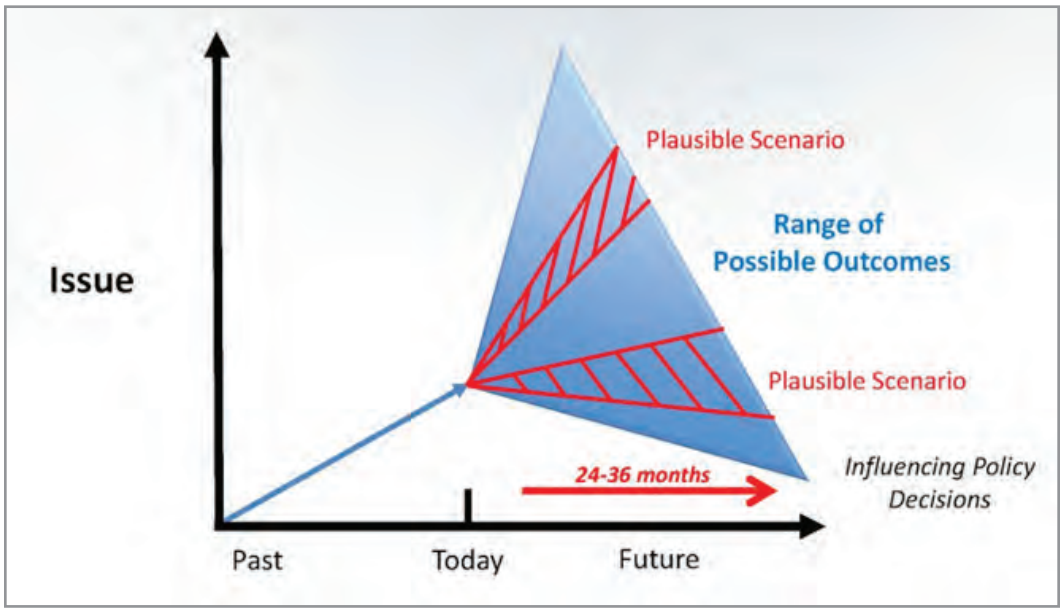
Mini Tactical SOF Intelligence Automation System

Open Source Unmanned Remote and Autonomous Vehicle Planning System

Rapid growth of the commercial unmanned aerial vehicle (UAV) marketplace created a compliance gap for state and local law enforcement and emergency management agencies to operate UAVs in an emergency/counterterrorism mission. Leaps in technical performance, user-friendly operation, and reduced costs has caused the market and skies to be flooded with UAVs. CTTSO, with the assistance of Department of Homeland Security's Science and Technology Directorate (DHS S&T), initiated the Open Source Unmanned Remote and Autonomous Vehicle Planning System project to address operational and regulatory compliance concerns, and facilitate efficient adoption of UAV technologies by law enforcement and emergency management agencies in rural state and local communities. The project engaged over 60 federal, state, and local agencies in multiple workshops that identified specific benefits and challenges for state and local government agencies using unmanned vehicle systems in rural communities. The Open Technology Center has provided information collected at these workshops to DHS S&T for planning and future development.

Analytically Driven Anticipation for Policy Transformation

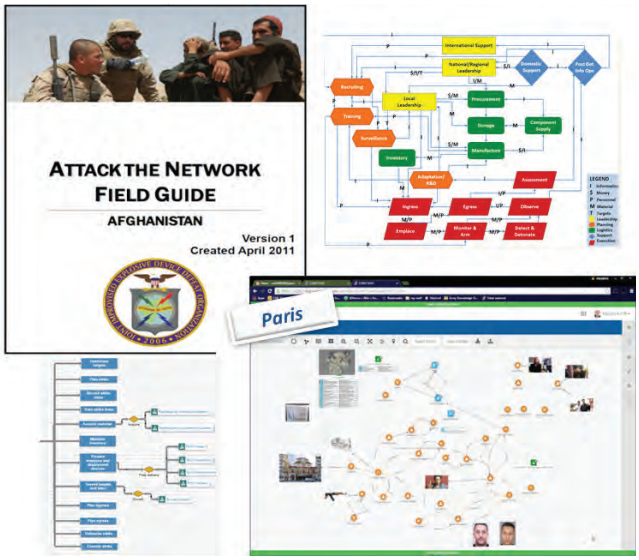
While hardly new, gray zone is that area of operations between healthy economic and political competition and open warfare. Analytically Driven Anticipation for Policy Transformation (ADAPT) demonstrated the feasibility of using different analytical approaches to conduct anticipatory and "what if" analyses for gray zone activities. The intent was to inform resource decisions for policy planning activities for the out years. Combining data driven machine learning analyses, dynamic modeling, and subject matter experts produced useful metrics for decision making. The proof of concept has successfully concluded as a final report. The concepts will be implemented in new software products under development. Access to this report is limited to U.S. Government agencies. The report can be acquired by contacting the Advanced Analytic Capabilities Subgroup, AACsubgroup@cttso.gov.



Benefits of Anticipatory Analytics Using Non-Linear Approaches

Attack-the-Network

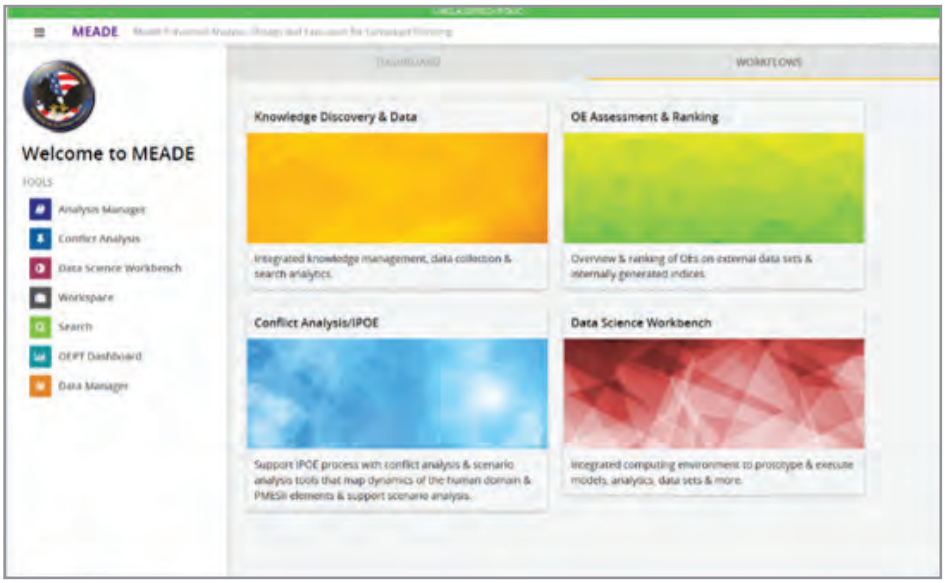
Attack-the-Network (AtN) is an expansion of an analytic platform developed by the Joint Improvised-Threat Defeat Organization and CTTSO to detect networks associated with improvised explosive device (IED) networks. AtN expands the network definition beyond IEDs to include network detection from other threats related to weapons of mass destruction. The current evolution of this technology, developed by System of Systems Analytics, Inc., provides a platform on which data, algorithms, analytics, and processes can be combined to define terrorist networks and identify key signatures and observables required for a collections program. AtN has been modified for cell phone use to support user-friendly tactical site exploitation and is being transitioned to several federal agencies for operational use.



ONGOING PROJECTS

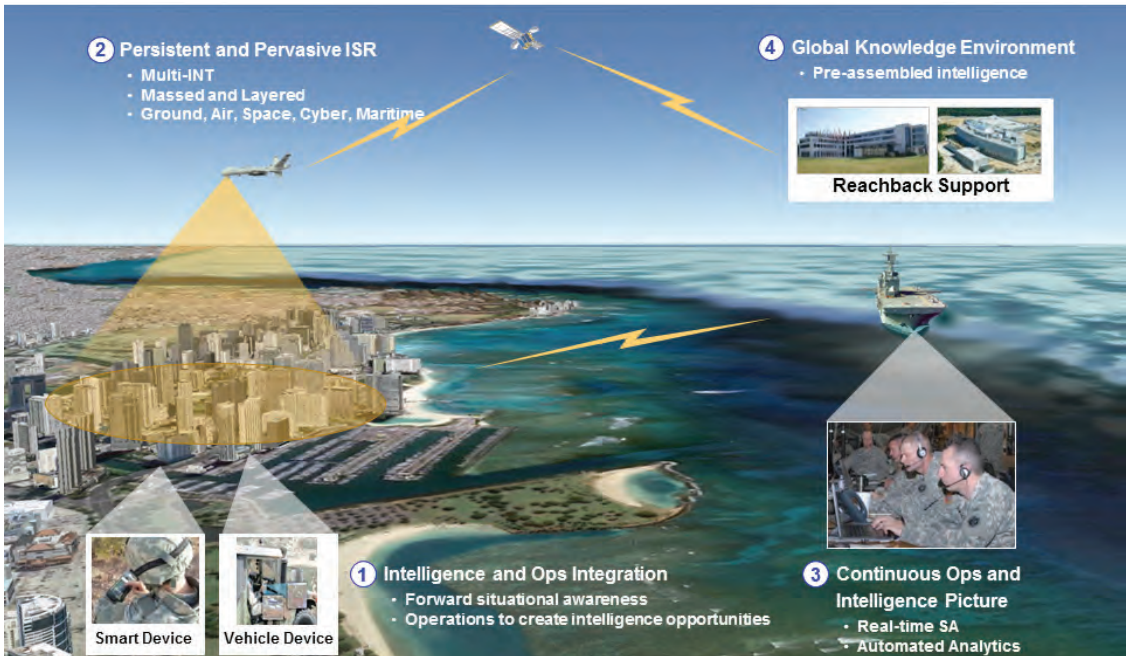
Model Enabled Analysis, Design, and Execution

Model Enabled Analysis, Design, and Execution (MEADE) expands the original platform on which Attack-the-Network is based to enable the application of dynamic modeling that can support analyses of non-kinetic effects and impacts on the human domain of various courses of action. Results of such models can help decision makers and analysts to quantify and assess higher order effects, tipping points, stability, allocation decisions, and other factors that can be evaluated using the tools, models, and methodologies incorporated into the MEADE platform. Initial applications include support of the Military Decision-Making Planning process and a tool for supporting decisions for resource allocation, Special Operating Requirements Tool-Operating Environment (SORT-OE).



Operate to Know

United States Marine Corps (USMC) warfighters are frequently required to engage in new operational environments with little preparation time. As a result, they operate with incomplete and even inaccurate analyses of the adversary and operational environment. These actions pose a risk to the operating forces, and introduces the possibility that an operation could do more harm than good. Operate to Know (OtK) is an operational concept aimed at alleviating this problem. This effort seeks significant improvement in Intelligence Preparation of the Operational Environment (IPOE) timelines and accuracy by operationalizing multiple tenets through a series of wargames and exercises. The project has aided in the design of visualization concepts, and the development of concepts of operation and anticipatory models. CTTSO hosted a seminar wargame focusing on vetting several of the tenets and the underpinning concepts. The USMC plans to further vet the concept at additional exercises, culminating in Trident Spectre 18.



OtK Operational Concept

Automated Information Discovery Environment

U.S. Marine Corps Intelligence Activity requires a man-portable, micro cloud server to bring analytics to the forward edge of the battle area. This effort applies an existing technology, the Autonomous Information Discovery Environment (AIDE), to improve current practices and significantly increase computational and storage capacities. This effort will assist in the exchange of data and analytics between intelligence personnel and warfighters, extend situational awareness to the front lines, and provide the warfighter a more seamless battle posture and increased freedom of movement on the battlefield.

MEMBERSHIP

Intelligence Community

- Office of the Director of National Intelligence

Joint Interagency Task Force South

National Reconnaissance Office

U.S. Department of Defense

- Defense Intelligence Agency
- Joint Improvised-Threat Defeat Organization
- National Geospatial-Intelligence Agency
- Naval Postgraduate School
- Office of the Secretary of Defense (Rapid Fielding Office)
- Office of the Secretary of Defense, Homeland Defense and Americas' Security Affairs
- Office of the Secretary of Defense for Special Operations and Low-Intensity Conflict
- Special Operations Command Central
- U.S. Army G-2
- U.S. Marine Corps Intelligence Department
- U.S. Special Operations Command
  - Army Special Operations Command

U.S. Department of Homeland Security

- Customs and Border Protection
  - Border Patrol
- Office of Intelligence and Analysis

U.S. Department of Justice

- Federal Bureau of Investigation

U.S. Department of State

- Bureau of Counterterrorism and Countering Violent Extremism
- Bureau of Near Eastern Affairs
- Office of Science and Technology Policy

CHEMICAL, BIOLOGICAL, RADIOLOGICAL, NUCLEAR, AND EXPLOSIVES

cbrnesubgroup@cttso.gov

FOCUS AREAS

CBRNE Characterization and Attribution

Systematically investigate and identify the unique physical and chemical characteristics of CBRNE materials; develop tools to determine the origin of CBRNE agents and materials; and evaluate clandestine methods of chemical and biological agent and homemade explosives production.

Consequence Management

Develop CBRN decontamination solutions, tools, and techniques; develop decision support tools which analyze, aggregate, and integrate multi-source data to provide enhanced on-scene situational awareness and risk assessment capabilities for CBRNE response; and develop training solutions to enhance the operational effectiveness of CBRNE operators.

Protection

Develop respiratory and dermal protective equipment to minimize exposure to CBRN materials while operationally enhancing individual performance; enhance shelter-in-place capabilities; and develop materials, tools, and techniques for hydration systems in compromised environments.

Detection and Identification

Develop equipment, tools, and techniques to sample, detect, and identify trace (gases, vapors, and non-visible amounts of solid and liquid) and bulk (microgram and higher amounts of solid and liquid) amounts of CBRNE threat materials at point, proximity (inches), and standoff (meters to kilometers) distances in both fixed and on-the-move configurations.

COMPLETED PROJECTS

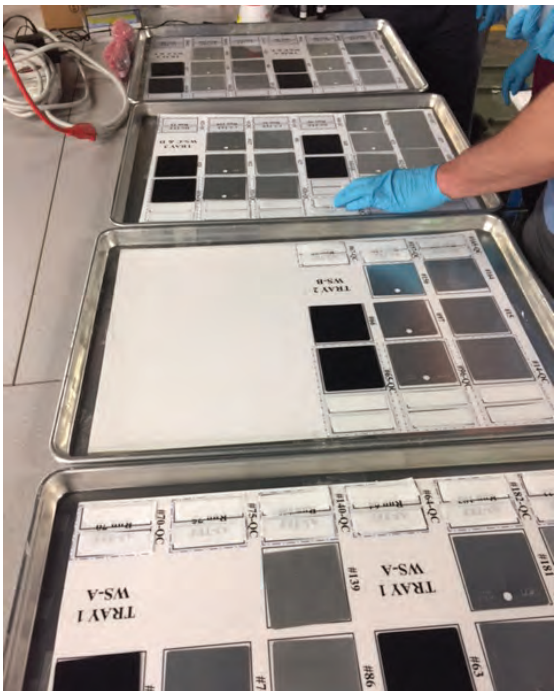
Scalable Vacuum Evidentiary Powder Collection Device

The 2001 anthrax letter attacks demonstrated the extreme hazard of collecting and handling biological agent powders and the importance of recovering as much of the agent as possible for forensic analysis. Seacoast Science, Inc. developed the SC-V10, a new hand-held, battery powered, high-efficiency powder evidence collection kit. The front-end is a self-contained, one-time use filter system that traps particles into a removable, resealable glass vial, thus providing the analytical team with easier sample handling. Different nozzle attachments allow users to collect from different surfaces. The SC-V10 collection kit contains a reusable pump handle, three pre-sealed collection nozzles, front and back nozzle end caps to protect the collected trace evidence in transport, and an extension hose with control wand for hard to reach areas. This modular design makes the collection process easy, while reducing potential cross-contamination and exposure to the user. The SC-V10 is commercially available from Seacoast Science, Inc.

Double Blind Assessment of Optical Non-Contact and/or Standoff Explosives Detection Technologies

The "Double Blind Assessment of Optical Non-Contact and/or Standoff Explosives Detection Technologies" used standard test materials developed under a previous effort to assess systems from a wide range of technology readiness levels, with standoff capabilities ranging 30 centimeters to greater than four meters. A worldwide request for information was issued to identify advancedstage prototypes for trace or near-trace detection of explosive materials at standoff or non-contact distances. Developers volunteered to participate in the assessment with systems that used technologies from multiple categories, including quantum cascade lasers, various Raman technologies such as coherent anti-Stokes Raman scattering spectroscopy, and infrared and laser-induced fluorescence.

In collaboration with the Transportation Security Laboratory, the assessment evaluated detection capabilities on 11 potential threats at various loadings, using three different deposition methods. Tests were completed for systems from Alakai, Brimrose, ChemImage Sensor Systems, Energy Research Company, Kestrel Corporation, Pendar Technologies, LLC, Physical Sciences, Princeton University, and the University of Puerto Rico. These assessments were made available to users and provided unique knowledge of where the state-of-the-art lies for using optical technologies for detection of trace explosives.



Samples used in the assessment.

Next Generation Chemical, Biological, Radiological, and Nuclear Evidence Bag

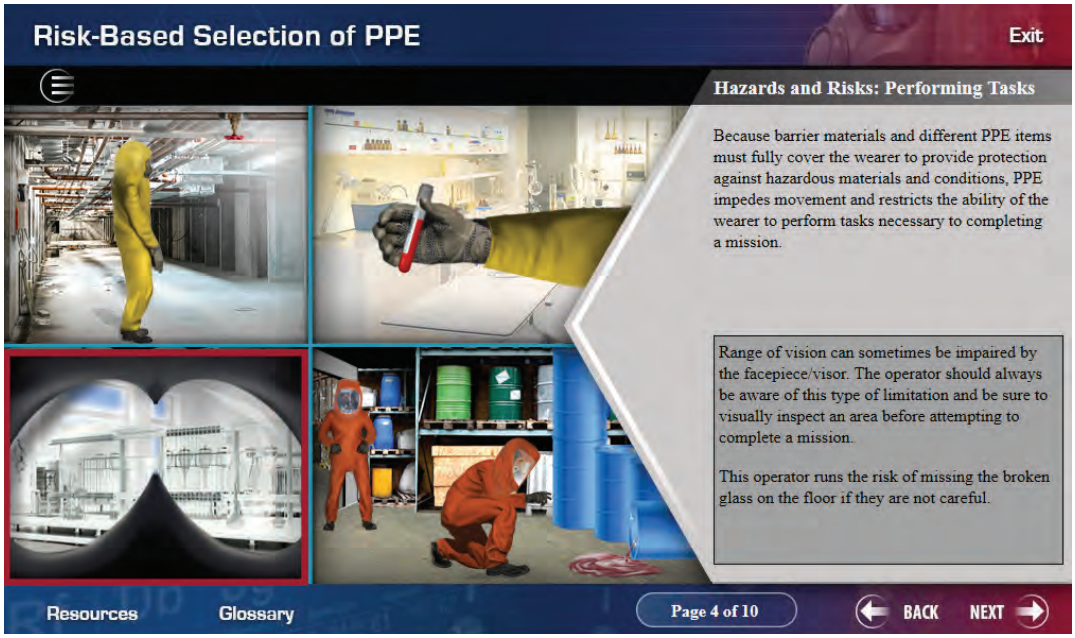
Unknown materials suspected of chemical, biological, radiological, or nuclear (CBRN) threat agents require packaging in the field prior to submission to a laboratory for further analysis. The quality and types of evidence bags used for this purpose vary based on locality and have limited or no compatibility testing with CBRN threat agents. Furthermore, no standard or recommended types of CBRN evidence bag exist on the commercial market.

In response to this gap, MRIGlobal developed a bag constructed of a transparent, flexible polymer barrier film that is resistant to permeation by several classes of toxic industrial chemicals. A patented dual-track zipper and seams have shown to be leak free in differential pressure scenarios such as those that occur during air transport. The evidence bags are available in various sizes to support collection of a range of evidence types. The product is commercially available from Loksak, Inc.

Risk-Based Selection of Personal Protective Equipment Training

When responding to the release of hazardous materials, emergency responders are required to perform technically and physically demanding tasks in an environment where chemical, biological, radiological, and/or physical hazards are present. In order to operate safely in these conditions, operators must select personal protective equipment (PPE) that meets the needs of their operations. Choosing wrong equipment can lead to the development of chronic health conditions and even loss of life.

The Risk-Based Selection of PPE developed by Battelle Memorial Institute, Resonate Learning Consultants, and International Personnel Protection, Inc. is a computer-based training course that teaches users about the strengths and limitations of various PPE and how to select appropriate equipment. The course covers the necessary background information, standards and certifications, and practical operational considerations that relate to different types of threats, modes of exposure, durability, flash-fire resistance, respiratory protection, resistance to physical hazards, operational ensemble functionality, and heat stress. The course provides users the needed knowledge to select PPE that provides the optimum level of safety.



ONGOING PROJECTS

Confined Space Self-Contained Breathing Apparatus

Current self-contained breathing apparatus (SCBA) are too large and heavy for tactical operations. The form factor of SCBAs does not permit operations in confined spaces such as tunnels. Moreover, the eight-inch minimum depth off the operator's back of traditional SCBAs is a significant snag hazard due to the profile of the cylinder. Specialized users need equipment that is lighter, smaller, and better suited for confined spaces. Avon Protection Systems, Inc. is developing a low-profile tactical SCBA that provides high-quality breathing air. The low-profile SCBA will be certified against National Institute for Occupational Safety and Health and National Fire Protection Association 1986, Technical Committee on Tactical and Technical Operations Respiratory Protection Equipment.

Next Generation Chemical Biological Glove

Previous generation butyl rubber chemical and biological (CB) gloves lack breathability and have poor heat and moisture management which causes thermal discomfort. AirBoss Defense is developing a next generation CB glove that provides

National Fire Protection Association (NFPA) 1994, Class 3 protection while providing greater tactility, durability, dexterity, breathability, and comfort over the traditional glove. The new glove will significantly reduce the thermal burden while providing extended mission percutaneous protection from exposure to the harmful effects of all traditional CB warfare agents and toxic industrial chemicals listed in NFPA 1994.

Decision Support Tool for Skin Decontamination

In the event a release of hazardous chemicals, emergency responders must quickly ensure that no victims at the scene are at risk for continued exposure from chemicals that may remain on their skin. Although many efforts have looked at the most effective method for decontamination, there is little to no information on which chemicals will interact with the skin and require decontamination. Mass decontamination is a resource intensive and time consuming process that may add trauma to civilians and take focus away from critical priorities during a hazmat response. The Decision Support Tool for Skin Decontamination contains empirical data of chemical skin interactions and allows emergency responders to input the name of the chemical that was released and receive detailed guidance and warnings that can be used to develop a strategy for effectively mitigating damage to the public.

In partnership with Australia's Department of Defence and carried out by the University of Adelaide, this effort examined the interaction of 27 chemicals by exposing human skin to a flow of the chemical agent over top of the skin. Measurements quantified the amount of chemical threat on the skin, in the skin, and the permeations through the skin over time at various operationally relevant concentrations. Additional experiments examined the effects of clothing types over the skin, lotions present on the skin, and elevated temperature and humidity. This research resulted in a number of published articles. Additional work is ongoing to research skin interactions with more chemicals. The resulting data will be added to the tool.

MEMBERSHIP

Environmental Protection Agency

Federal Reserve Board

Intelligence Community

InterAgency Board

State and Local Agencies

- Alexandria (VA) Fire Department
- Arlington County (VA) Fire Department
- Boston (MA) Fire Department
- City of Orlando (FL) Police Department
- District of Columbia Fire Department
- District of Columbia Metropolitan Police Department
- Douglas County (GA) Emergency Management Agency
- Douglas County Fire Department
- Douglas County Sheriff's Office
- Fairfax City (VA) Fire Department
- Fairfax County (VA) Fire and Rescue Department
- Fairfax County Police Department
- Los Angeles (CA) Police Department
- Metropolitan Nashville (TN) Police Department
- Nashville Fire Department
- New York City Fire Department
- New York City Office of Chief Medical Examiner
- New York City Police Department
- Northern Illinois Police Alarm System
- Raleigh (NC) Fire Department
- Seattle (WA) Fire Department
- Virginia Department of Emergency Management
- Virginia Department of Transportation

U.S. Capitol Police

U.S. Department of Agriculture

- Animal and Plant Health Inspection Service
- Food Safety and Inspection Service

U.S. Department of Commerce

- National Institute of Standards and Technology

U.S. Department of Defense

- Acquisition, Technology, and Logistics
- Defense Advanced Research Projects Agency
- Defense Intelligence Agency
- Defense Threat Reduction Agency
  - Joint Improvised-Threat Defeat Organization
- Joint Chiefs of Staff
- Joint Program Executive Office for Chemical and Biological Defense
- Office of the Assistant Secretary of Defense for Nuclear, Chemical, and Biological Defense
- Pentagon Force Protection Agency
- U.S. Air Force Air Combat Command
- U.S. Army
  - 20th Support Command, CBRNE
  - 22nd Chemical Battalion
  - Armament Research, Development, and Engineering Center
  - Chemical, Biological, Radiological, and Nuclear School
  - Medical Department
  - National Ground Intelligence Center
  - Research, Development, and Engineering Command, Edgewood Chemical Biological Center
- U.S. Marine Corps
  - Chemical Biological Incident Response Force
  - Explosive Ordnance Disposal
  - Systems Command
- U.S. Navy
  - Bureau of Medicine
  - Naval Air Warfare Center
  - Naval Explosive Ordnance Disposal Technology Division
  - Naval Forces Central Command
  - Naval Research Laboratory
  - Naval Surface Warfare Center
- U.S. Special Operations Command

U.S. Department of Energy

- National Nuclear Security Administration

U.S. Department of Health and Human Services

- Centers for Disease Control and Prevention
- Food and Drug Administration
- National Institute for Occupational Safety and Health

U.S. Department of Homeland Security

- Federal Emergency Management Agency
- National Protection and Programs Directorate
  - Federal Protective Service
- Office of Health Affairs
- Science and Technology Directorate
  - Transportation Security Laboratory
- Transportation Security Administration
- U.S. Coast Guard
- U.S. Secret Service

U.S. Department of the Interior

- National Park Service, United States Park Police

U.S. Department of Justice

- Bureau of Alcohol, Tobacco, Firearms and Explosives
- Federal Bureau of Investigation
- National Institute of Justice
- U.S. Marshals Service

U.S. Department of Labor

U.S. Department of State

- Bureau of Arms Control, Verification and Compliance
- Bureau of Counterterrorism and Countering Violent Extremism
- Bureau of Diplomatic Security
- Bureau of Overseas Buildings Operations

U.S. Department of Transportation

- Research and Innovative Technology Administration (Volpe Center)

U.S. Senate Sergeant at Arms

White House

- Homeland Security Council
- Office of Science and Technology Policy

IMPROVISED DEVICE DEFEAT/ EXPLOSIVES COUNTERMEASURES

iddsubgroup@cttso.gov

FOCUS AREAS

Improvised Device Defeat

Improve or develop operational capabilities to neutralize, render-safe, and contain blast and fragmentation during improvised terrorist device, and explosives response operations.

Device Diagnostics and Threat Characterization

Provide advanced technologies and technical solutions that improve identification, analysis, and technical characterization of explosives, improvised explosive devices (IEDs) and their components, and potential weapons of mass destruction in support of response operations.

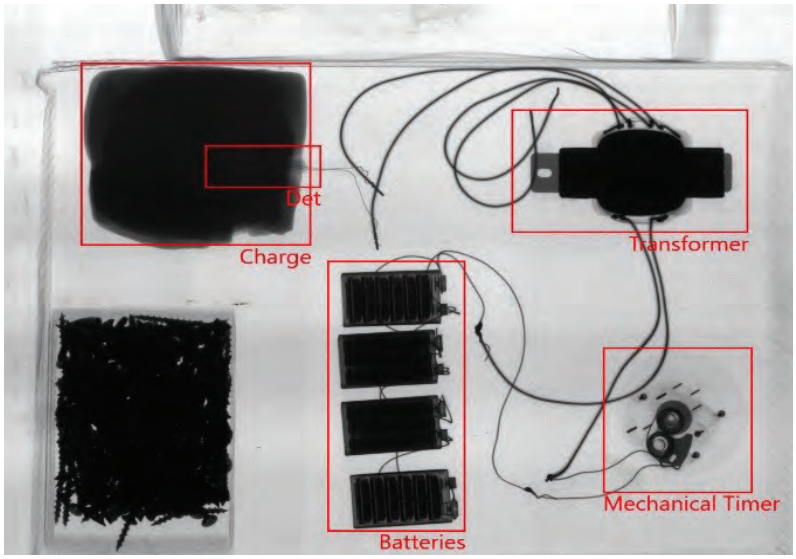
Robotics and Remote Means

Develop or enhance platforms, systems, and technologies to remotely conduct activities related to the neutralization or rendering safe of IEDs, unexploded ordnance (UXO), homemade/improvised explosives and their precursors, and enhanced hazard devices containing chemical, biological, or radiological materials.

COMPLETED PROJECTS

Automated Recognition of Bomb/Improvised Explosive Device Components

X-ray images are the primary tool used by bomb technicians to analyze internal components of a device. The technician relies on experience and multiple angles to identify key components in order formulate his course of action or render safe procedure. In order to further assist the technician with identification of key components, Sandia National Laboratories developed algorithms that automatically identify and categorize components. The Automated IED Component Recognition system works in two modes. The first mode allows the operator to select a component in the image and query the system for identification. The system returns the type of component and confidence-level. In the second mode, the system searches the entire image and attempts to recognize any components that may bepresent. The system has been integrated into the X-ray Toolkit (XTK) and was demonstrated to operators at the Western National Robot Rodeo and the International Association of Bomb Technicians and Investigators In-Service Training in the summer of 2017.

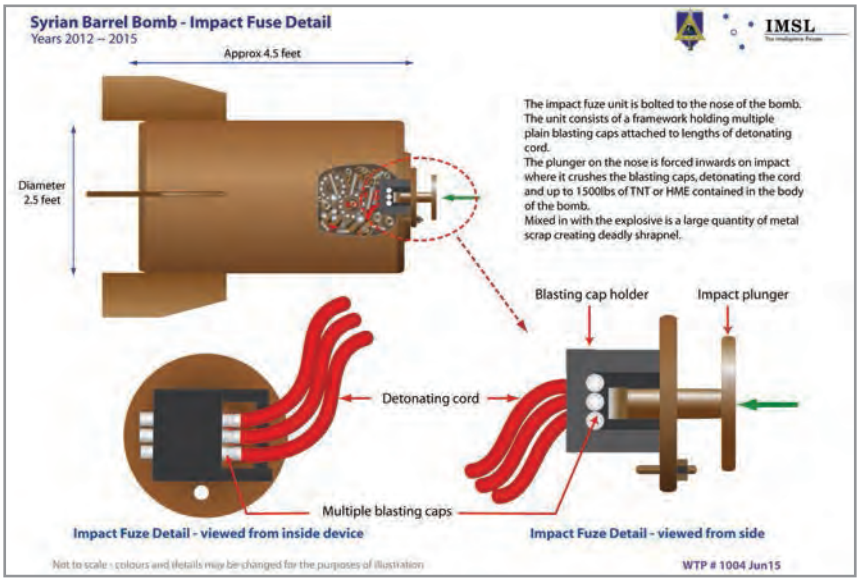


Affordable Radio Frequency Firing System

CTTSO selected PAE National Security Solutions, LLC to develop a low-cost, lightweight, battery operated firing system to reduce the cost of conducting demolition training and operations for public safety bomb technicians. The Affordable Radio Frequency (ARF) Firing System consists of a transmitter and six receivers that can operate up to 1000 meters line-of-sight and 500 meters non line-of-sight. The unit is designed to be reusable for training and normal demolition operations, but is low cost enough to be used as a disposable receiver for real-world operations. The ARF Firing System has the potential of saving bomb squads tens of thousands of dollars over its lifetime use. The ARF Firing System is commercially available from PAE.

Worldwide Improvised Explosive Device Trend Analysis

There is an information gap between improvised explosive device (IED) reports and analysis of incidents. Reporting without analysis fails to provide IED defeat personnel with the technical information necessary to inform the development of render-safe procedures should similar devices be encountered. Intelligence Management Support Services Limited (IMSL) helped to close this information gap by collecting and collating worldwide IED technical data from 2005 to 2015. IMSL gathered information on significant IED emplacement strategies, electronic circuitry, triggering mechanisms, explosive fillers, and container design. In addition to IED technical data, other relevant information was included that affects bomb disposal operations, such as diagnostics, access, and IED defeat. This information is available to the public safety bomb technician community via the Bomb Tech Wikipedia[1].



[1] *The Bomb Tech Wikipedia, developed by CTTSO, is a controlled, unclassified information repository for the public safety bomb technician community. Access to the Bomb Tech Wikipedia is limited to certified bomb technicians with access to the National Bomb Squad Commanders Advisory Board website within the Law Enforcement Enterprise Portal (LEEP). See www.nbscab.org for additional information.*

ONGOING PROJECTS

Multi-Fit Inflatable Bomb Suit Helmet Liner

The bomb suit helmet is an important piece of safety gear for bomb technicians. The fit of any helmet determines how effective it will be in terms of protecting the head and brain from damage. Med-Eng™ is developing a multi-fit inflatable liner that can be retrofitted to older bomb suit helmets to ensure proper fit and provide maximum comfort. The retrofit solution is a single bladder liner that allows adjustments to be made while worn. The bladder is inspired by technology used in sports helmets, such as football and hockey. Human factors and performance testing will ensure that helmets using the inflatable liner will retain the same levels of protection against blast, fragmentation, impact, and hazardous environments.

Bomb Suit Heads-Up Display

The bomb suit heads-up display (HUD) will enhance EOD situational awareness by providing critical visual information to technicians while conducting disposal operations. By having mission relevant data displayed within the bomb suit helmet, the HUD will eliminate the need to divert attention from other mission tasks, significantly improving safety and performance. The HUD will connect to a bomb suit wrist controller that will provide voice recognition and collect data from all subsystems, such as low-light/IR cameras, threat sensors, and suit controls. The project will integrate a HUD that is best suited for EOD applications into helmet ensembles. The HUD system will be designed to fit or retrofit to most EOD helmets used by the U.S. bomb disposal community. Additionally, the modular architecture will accommodate a wide variety of commercial-off-the-shelf peripherals, allowing data feeds from the latest technologies to integrate seamlessly with the system.

NASA Vehicle-Borne Improvised Explosive Device Robot Challenge

CTTSO and NASA are conducting a series of workshops that challenge teams made up of military and public safety bomb technicians, NASA engineers, and NASA high school interns to rapidly develop and deploy unmanned solutions for real-world bomb/IED problems. Two workshops held in 2017 required teams to access the interior of a box truck without using explosives and describe the contents in 15 minutes; first, using robotic platforms, second, using drones. Teams worked collaboratively for two and half days to design and fabricate innovative solutions to cut through the roof of a box truck. Solutions were simple and used commercial-off-the-shelf components. The workshops function as a platform for bomb technicians to learn and share knowledge about new tactics and emerging technologies. The two workshops scheduled for 2018 will be similar VBIED defeat challenges with teams competing in a timed environment against complex real-world threat scenarios.

MEMBERSHIP

Intelligence Community

International Association of Bomb Technicians and Investigators (IABTI)

Joint Program Office for Countering Improvised Explosives Devices

National Bomb Squad Commanders Advisory Board

State and Local Law Enforcement

- Arizona Department of Public Safety (Western Region)
- Delaware State Police (Eastern Region)
- Fairfax County (VA) Police Department
- Houston (TX) Police Department (Central Region)
- Maryland State Police
- Michigan State Police
- Pittsburgh (PA) Bureau of Police
- South Carolina Law Enforcement Division (Southern Region)

U.S. Capitol Police

U.S. Department of Defense

- Pentagon Force Protection Agency Bomb Squad
- U.S. Air Force
  - Air Combat Command
  - Explosive Ordnance Disposal Technical Detachment (AFCEC/CXE)
- U.S. Army
  - 52nd Ordnance Group
  - Explosive Ordnance Disposal Technical Detachment
- U.S. Marine Corps
  - Chemical Biological Incident Response Force
  - Explosive Ordnance Disposal Detachment
- U.S. Navy
  - Explosive Ordnance Disposal Fleet Liaison Office
  - Explosive Ordnance Disposal Technology Division
  - National C-IED Knowledge Network
  - Training and Evaluation Unit ONE
  - Training and Evaluation Unit TWO

U.S. Department of Homeland Security

- National Protection and Programs Directorate
  - Office for Bombing Prevention
- Science and Technology Directorate
  - Homeland Security Advanced Research Projects Agency
- Transportation Security Administration
- U.S. Coast Guard
- U.S. Secret Service

U.S. Department of Justice

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

INVESTIGATIVE AND FORENSIC SCIENCE

ifssubgroup@cttso.gov

FOCUS AREAS

Credibility Assessment (Detection of Deception and Intent)

Develop improved interviewing and interrogation equipment, methods, and techniques through behavioral/operational psychology advancements, including psycholinguistics, cognitive methods, and motivational techniques.

Crime Scene Response

Improve the quality of recognition, collection, documentation, analysis, and preservation of evidence and actionable information from incident scenes for future prosecution and targeting. Create standardized field tests, collection sets, kits, and other crime scene equipment. Develop capabilities to rapidly and visually document a scene in any environment. Increase the safety and security of law enforcement first responders at a terrorism scene.

Criminalistics

Create advanced capabilities in the traditional forensic science disciplines to identify individuals and improve the recovery, identification, evaluation, and analysis of material and traces. Develop benchtop and handheld instrumentation that decreases throughput time and automates interpretation.

Digital and Multimedia Forensics

Develop computer forensic hardware, software, decryption tools, and digital methods to investigate terrorism. Develop advanced methods to extract, decrypt, analyze, and enhance audio recordings, video images, and other forensic information from analog and digital sources.

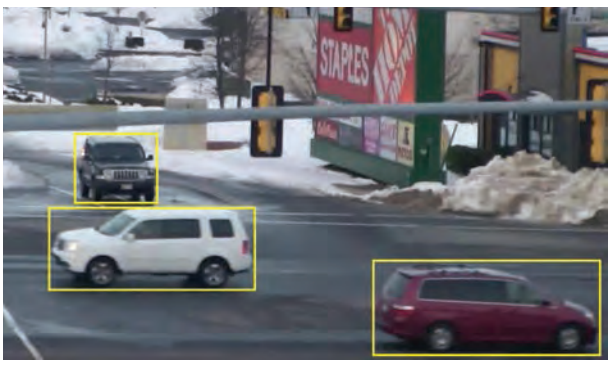
Forensic Exploitation

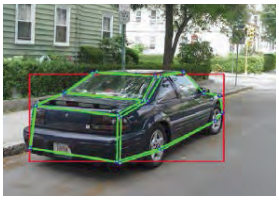
Develop a lexicon, common operating procedures, and advanced techniques for material and personnel exploitation of sensitive sites, caches, targeted objectives, and incident scenes. Advance the portable and packable expeditionary and "reach back" exploitation analysis capabilities for level I, II, and III forensic analysis. Improve law enforcement-related technical surveillance methods.

COMPLETED PROJECTS

Vehicle Image Search Tool

Forensic video and image analysis plays a key role in many combating terrorism operations. It can provide significant intelligence value, particularly through the comparison and identification of vehicles. Searching through vast amounts of video files to find and identify vehicles is difficult and extremely labor intensive. SRI International of Princeton, New Jersey, developed an automated system that can rapidly search a wide range of multimedia video files to locate vehicles. The tool provides post-event forensic analysis of video and digital image depictions and files.





The system automatically extracts vehicle images from a range of multimedia digital image files in real time. It has the ability to identify a vehicle's make and model and match individual vehicles to those stored in its image database. The system also allows users to highlight or delineate key features to improve searching and matching performance. The tool is compatible with commonly used computer hardware. The tool is commercially available from the vendor. For further information, contact the Investigative and Forensic Science Subgroup, IFSsubgroup@cttso.gov.

Heroin Origin by High Resolution Inductively Coupled Mass Spectrometry

Terrorist organizations and criminal enterprises use the production and sale of heroin and related opium products to obtain huge amounts of revenue to fund their illegal and violent activities. When law enforcement or intelligence agencies collect or seize heroin or opium, it is far from the site where it was cultivated or processed. Determining its location of origin provides valuable intelligence for law enforcement and the intelligence community. Florida International University (FIU) in Miami, Florida, has developed forensically validated procedures to measure trace elements and isotope ratios of samples of heroin and its related products to determine the geolocation of their origin. They have used the most accurately known and readily available method to measure isotope ratios which is high resolution inductively coupled plasma mass spectrometry (ICP-MS). Once the trace elements and their isotope ratios are measured, they can be compared to reference samples to accurately determine where the opium poppies were grown. FIU has also established an accompanying reference database that can be used to determine the origin of heroin as being from Mexico, South America, Southwest Asia, or Southeast Asia. The procedures developed have the ability to analyze street heroin and opium samples as small as 400 milligrams with up to 93 percent accuracy. For further information, contact the Investigative and Forensic Science Subgroup, IFSsubgroup@cttso.gov.

Head Mounted Credibility Assessment System

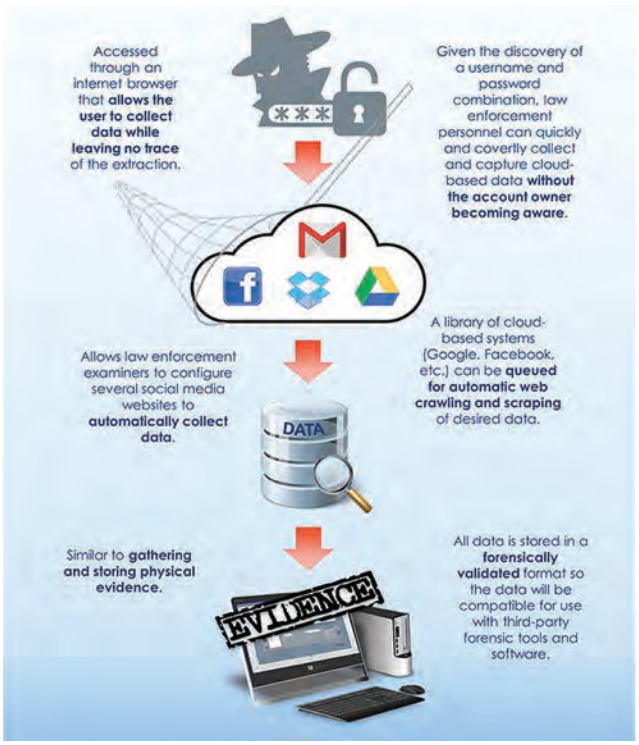
Operators in the U.S. military, law enforcement, and intelligence communities have a constant need to assess the credibility of persons and the information they provide. The processes and systems used need to be accurate, efficient, and have low inconclusive rates. They need to be quick to employ and require minimal training time to operate. Azimuth Incorporated of Morgantown, West Virginia developed the Head Mounted Credibility Assessment Screening System (HMCASS) to provide U.S. forces with these capabilities. The system is worn on the head by the interviewee and has sensors that unobtrusively measure pupillary response and collect two other traditional polygraph signals. An attached computer tablet with specialized algorithms processes the signals and provides the operator a color-coded indicator and numeric values in real time to determine the credibility of the interviewee. The system can function for several hours on rechargeable batteries and is lightweight, rugged, and highly portable. The system is commercially available for purchase through the vendor.

Anomalous Workplace Behavior Intervention

Abnormal conduct, irregular actions, or unusual behavior patterns by persons in the workplace may be indicators of an insider threat. These actions can be a forewarning of a person committing acts of sabotage, espionage, sensitive information theft, or other malevolent insider activities. Employees frequently observe behavioral indicators, but rarely report them to the authorities or others within their organization. The reasons vary, but include reluctance to cause trouble for another worker, lack of knowledge of insider threat indicators, or not knowing how to report their observations to someone who will take action. In this project, the Centre for the Protection of the National Infrastructure in the United Kingdom developed techniques and procedures that encourage and motivate employees to report observations that may indicate insider threat inclinations in the workplace. The focus is on establishing an understanding of employee perceptions of anomalous workplace behavior and ways employees might choose to intervene. This effort has the ability to identify the barriers to employees reporting those behaviors and develop prototype staff awareness campaigns. The techniques can emphasize reporting and intervention methods that are unobtrusive and anonymous for the employees. The project has led to the development of procedures for management to take quick and decisive action without bringing any attention to the reporting person. Additionally, separate training programs for the workplace have been created to educate both employees and management. One DoD agency and one federal agency have adopted the training as part of their security programs.

ONGOING PROJECTS

Next Generation Vampire (Collaborative Forensic Exploitation Platform)



The U.S. military, law enforcement, and the intelligence community have a critical requirement for fast, efficient, and accurate collection and analysis of information, evidence, and biometrics from sensitive sites and crime scenes. Military and law enforcement personnel need equipment that is not redundant, supports multiple capabilities, and requires minimal training time to employ. Booz Allen Hamilton of McLean, Virginia, is developing a rugged device weighing less than 2.5 pounds that will meet this requirement. Specific features include a 12-megapixel camera that captures images of latent prints and full crime scene photos. It will illuminate the scene with white light and two ultraviolet wavelengths, and have a laser-based image rescaling system. The device will also capture live fingerprints from persons of interest. The units will include customized software that performs fingerprint analysis and will be able to connect to databases including the FBI Next Generation Identification System. It will have the capability to form an ad hoc mobile network and share data with other Vampire units. Some facial recognition and document exploitation capabilities will also be available.

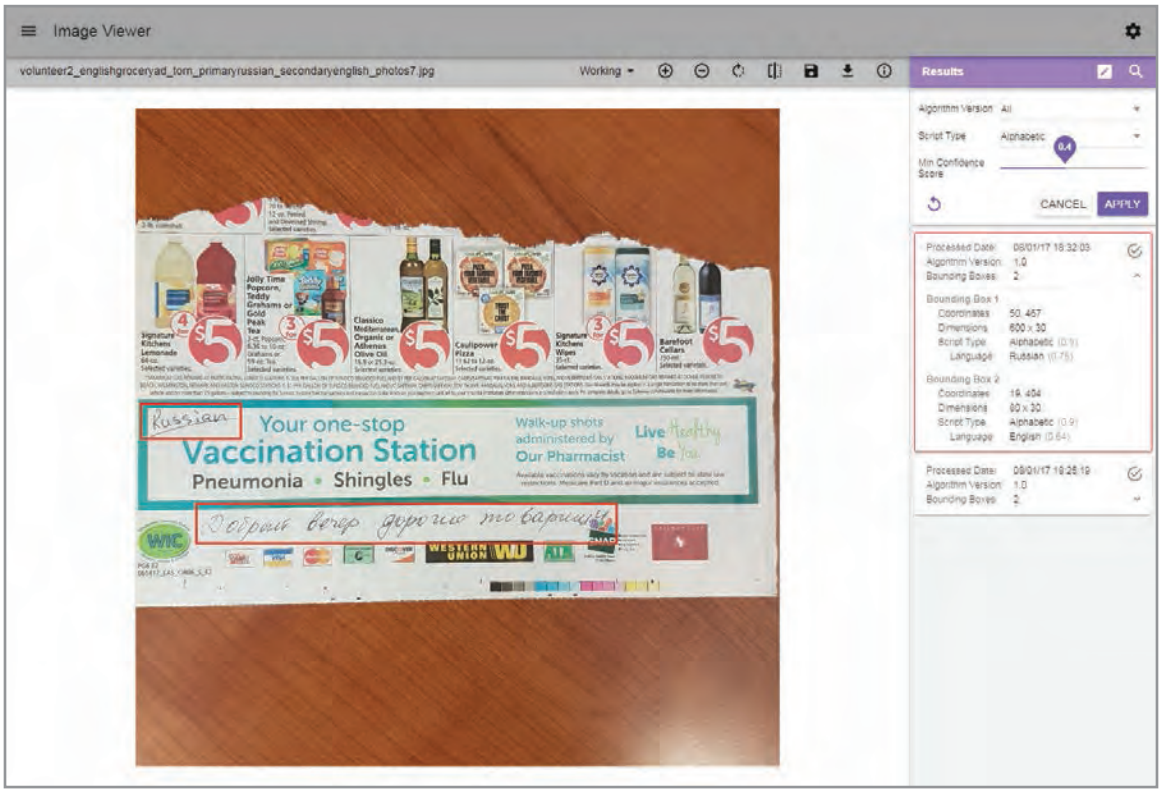
Forensic Acquisition Tool for Cloud-Based Data

Digital technology allows for large volumes of data to be stored in some type of cloud-based environment. Law enforcement and the intelligence community often need to collect data from this environment. Applied Research Associates, Inc. in Albuquerque, New Mexico is developing a forensically validated software tool that will allow

users to collect digital evidence from cloud-based storage containers in a fashion similar to how digital evidence is collected from physical storage media. They will also develop related procedures on the collection and storage of digital data, information, and evidence in cloud-based containers and services. The files collected as evidence can be logical or physical acquisitions, depending on level of access to the cloud-based service. The collected information will be stored in a format compatible with existing digital forensics image formats and contain the metadata consistent with digital forensics case documentation best practices. The tools will also be compatible with commonly used computer hardware.

Automated Handwriting Detection and Extraction from Digitized Documents

Law enforcement and intelligence personnel often encounter various printed digitized documents with handwriting of various languages and styles. Handwriting provides valuable intelligence and evidence; however, these documents must be individually examined and stored. An automated system to analyze digitized documents for handwriting and procedure to extract the writing and store it is needed. Blackbird Technologies, Inc. of Herndon, Virginia is developing an automated system that will scan documents, and quickly identify, extract, and store handwriting. This will allow investigators to conduct further analysis and cataloging that will provide significant amounts of evidence and intelligence. This tool will be able to identify and extract handwriting of various sizes, including those of various types of scripts such as alphabetic, logographic, syllabic, abjad, and abugida scripts. It will also be able to detect handwriting on various source documents and writing which is other than horizontal. The tool will process and analyze popular image formats and Adobe PDF documents. It will store the handwriting and the related metadata and create a reference database. This tool will also operate on commonly used computer platforms and on mid-range commercially available computers. The tool will allow users to operate through a graphic user interface. This new technology will be incorporated into forensic document and media exploitation (DOMEX) standards.



MEMBERSHIP

Environmental Protection Agency

- National Enforcement Investigations Center

Intelligence Community

National Forensic Science Technology Center

National Transportation Safety Board

Office of the Director of National Intelligence

U.S. Department of Commerce

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

U.S. Department of Defense

- Component Commands
- Defense Advanced Research Projects Agency
- Defense Computer Forensics Laboratory
- Defense Criminal Investigative Service
- Defense Cyber Crime Institute
- Defense Forensic Enterprise, Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics
- Defense Forensic Science Center
- Defense Forensics and Biometrics Agency
- Defense Intelligence Agency
- Defense Threat Reduction Agency
  - Joint Improvised-Threat Defeat Organization
- Headquarters, U.S. Marine Corps
- Intelligence Systems Support Office
- National Center for Credibility Assessment
- National Geospatial Intelligence Agency
- National Media Exploitation Center
- Naval Research Laboratory
- Office of the Provost Marshal General
- Pentagon Force Protection Agency
- Rapid Reaction Technology Office
- 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 Security Technology and Assistance

U.S. Department of Homeland Security

- Customs and Border Protection
  - Border Patrol
- Federal Emergency Management Agency
- Immigration and Customs Enforcement
  - Homeland Security Investigations Forensic Laboratory
- National Protection and Programs Directorate
  - Federal Protective Service
- Science and Technology Directorate
  - Transportation Security Laboratory
- Transportation Security Administration
- U.S. Secret Service

U.S. Department of Justice

- Bureau of Alcohol, Tobacco, Firearms and Explosives
- Drug Enforcement Administration
- Federal Bureau of Investigation
- National Institute of Justice
- U.S. Marshals Service

U.S. Department of State

- Bureau of Counterterrorism and Countering Violent Extremism

U.S. Department of Transportation

- Federal Aviation Administration

U.S. Postal Inspection Service

IRREGULAR WARFARE AND EVOLVING THREATS

iwetsubgroup@cttso.gov

FOCUS AREAS

Advanced Influence and Information Capabilities

Conduct research, operational analysis, capability design, and implementation support to develop new tools, techniques, and activities that enable our forces to influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries within the physical, information, or cognitive domains of the information environment.

Counter-Network Concepts and Capabilities

Conduct research, analysis, and development of new concepts and capabilities that integrate unique skill sets of combined, multi-agency and multi-national domains to identify and interdict threat networks and enterprises.

Partnership Capacity Development

Conduct research, operational analysis, capability design, and implementation support in order to more effectively assist, train, advise, and influence foreign partners, foreign competitors, adversary leaders, and relevant populations in support of expeditionary, low-cost, small-footprint operations in the air, land, maritime, and cyber domains.

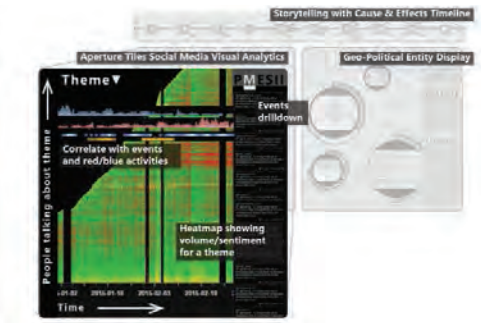
COMPLETED PROJECTS

All Source Exportable Intelligence Model

U.S. forces supporting host nation security forces (HNSF) needed a capability that rapidly enables foreign police/military to collect, manage, and act on fine-grain information harvested at the local level in order to conduct intelligence operations. The All Source Exportable Intelligence Model (ASEIM) provided the necessary ingredients and expertise—through a mix of doctrine-based training, TTPs, and mentoring—to create an enduring platform for information sharing while operating within the rule of law to help criminalize subversive elements. ASEIM has also assisted U.S. Special Operations Forces by delivering training to partner nations. This has provided key HNSFs the necessary capabilities needed to disrupt network-based threats by fully conducting the Find, Fix, Finish, Exploit, Assess and Disseminate (F3EAD) targeting cycle, thereby reducing reliance on U.S. assistance. The U.S. Government has unlimited rights to the curriculum developed under this initiative. Copies can be obtained by contacting CTTSO.

Social Network Terrain Analysis

Social Network Terrain Analysis (SNTA) is a web-based software application framework that monitors online networks, providing visual results using graphics analogous to those used for traditional military operations. SNTA ingests social media data as well as structured and unstructured content to visualize network engagement areas and other areas of operational interest. SNTA helps set the foundation for military planners and senior leaders to understand the cognitive domain of online communication and social networks. The prototype tool is hosted on SUNet's testing and development zone and CTTSO is working with the Military Information Support Operations (MISO) community to vet it.



Information Environment Common Operating Picture (ICOP) Environment

ONGOING PROJECTS

Fixed Focus

With the pervasive use of information-related capabilities, an unprecedented amount of digital data continues to be generated by our allies and adversaries. Digital communication enables adversaries to quickly communicate with and disseminate information to sympathizers and new recruits. Fixed Focus is a controlled-access internet-hosting platform that not only stores various types of digital data, but also conducts limited facial, object, and ISIL brand recognition. This project enhances the efficiency of information operations communicators to search, retrieve, share, analyze, and exploit photo, audio, and video files.

Foreign Criminal Law Analytic Capability

Due to the irregular nature of threats facing the U.S., diverse and non-traditional approaches are required to defeat adversaries. To this end, the Foreign Criminal Law Analytic Capability (FCLaw) seeks to operationalize law through and with partner nations in order to take action against identified threat networks. FCLaw will enable U.S. Government agencies to leverage foreign criminal laws, which provides an alternative avenue to counter violent extremism. This tool also provides a platform from which U.S. Government agencies can collaborate with foreign partners to achieve non-kinetic objectives. While initially focusing on violent extremist organizations, FCLaw provides the groundwork for application across a range of international threats, such as proliferation networks and transnational criminal organizations.

Information Environment Common Operating Picture

The digitization of communication has created an environment saturated with instantaneous engagement, real-time decision making, and an exponential production of new data. The Information Environment Common Operating Picture (ICOP) seeks to bring together multiple streams of digital data and provide analytic insight to an often complex and rapidly evolving domain. This capability will support mission management of the information environment (IE) and provide greater insight into adversaries, near-peer competitors, and violent extremist organizations by succinctly presenting key information gleaned from the IE.

Remote, Advise, and Assist Full Spectrum Virtual Accompany Kit

Virtual Accompany Kits (VAKs) paved the way for making advise and assist operations more efficient; however, they are currently limited in scope. Specifically, first-generation VAKs do not support the full range of special operations and general-purpose activities required to aid security cooperation and partner capacity building missions. The Remote, Advise, and Assist Full Spectrum VAK project will fill this gap by developing a comprehensive, wide-range capability to assist partner capacity missions where direct contact is currently limited. Once complete, this tool will provide a capability to holistically advise foreign partners remotely, enabling them to rapidly learn and retain necessary skills in support of their counterterrorism and irregular warfare missions.

Behavioral Responses to Cyber Disruption and Deception

The Behavioral Responses to Cyber Disruption and Deception (BRCDD) project is an effort undertaken by Sandia National Laboratories through a joint endeavor between CTTSO and the United Kingdom Ministry of Defence – Defence Science and Technology Laboratory. This project will develop a tool that provides analysis on how people will respond to different types of cyber interventions and effects. As such, BRCDD seeks to fill current gaps in how operational planners and decision makers understand the way people react to an array of cyber engagements in order to better protect their networks.

MEMBERSHIP

Intelligence Community

National Defense University

United Kingdom

- Strategic Analysis Group – Policy and Capability Studies
- Defence Science and Technology Laboratory

U.S. Agency for International Development

U.S. Department of Defense

- Acquisition, Technology, and Logistics
- Coalition Joint Forces Land Component Command
- Combined Joint Task Force – Operation Inherent Resolve
- Defense Institute of Security Assistance Management
- Defense Threat Reduction Agency
- Peacekeeping and Stability Operations Institute
- Strategic Capabilities Office
- U.S. Africa Command
- U.S. Army
  - War College
- U.S. Central Command
- U.S. European Command
- U.S. Marine Corps
- U.S. Pacific Command
- U.S. Southern Command
- U.S. Special Operations Command

U.S. Department of Homeland Security

- Immigration and Customs Enforcement
- Office of Community Partnership
- Office of International Affairs

U.S. Department of Justice

- International Criminal Investigation Training Assistance Program
- Federal Bureau of Investigation
  - Global Training Unit
  - Instructional Systems
  - Terrorist Explosive Device Analytic Center
- Office of Overseas Prosecutorial Development Assistance and Training

U.S. Department of State

- Bureau of African Affairs, Office of Regional Security Affairs
- Bureau of Counterterrorism and Countering Violent Extremism
- Bureau of Educational and Cultural Affairs
- Bureau of Political-Military Affairs
- Global Engagement Center

U.S. Department of the Treasury

- Office of Terrorism and Financial Intelligence

U.S. Patent and Trademark Office

Wilson Center

- Africa Program

PERSONNEL PROTECTION

ppsubgroup@cttso.gov

FOCUS AREAS

Communications and Situational Awareness

Develop situational awareness and communication capabilities that aid in identifying threat indicators, conducting risk assessments and providing early warning to personnel providing protective services for VIPs. Develop tools to facilitate situational awareness, reporting, and communications for incident response personnel.

Individual Protection and Survivability

Develop advanced personnel protection systems that mitigate ballistic, blast, and emerging operational threats. Personal protective equipment focuses on novel materials and designs to provide maximum protection.

Personnel Tracking and Recovery

Develop inconspicuous systems to geolocate and track high risk personnel, signal situations of duress, and facilitate recovery of missing or captured personnel.

Ballistic and Blast Threat Assessment

Research ballistic and blast effects on the human body and develop guidelines, tools, and techniques to mitigate the effects.

COMPLETED PROJECTS

Enhanced Vehicle Tracker

Global Positioning System (GPS) deprived or denied environments are prevalent in high risk areas in which vehicles travel and lose reception to location servers. Raytheon Blackbird Technologies, Inc. of Herndon, Virginia, developed the Enhanced Vehicle Tracker (EVT), a vehicle embedded device, which employs a means to track the location of a vehicle within 15 meters for a minimum of 30 minutes when the GPS is lost. The EVT employs Raytheon Blackbird's SmartCore™ for tracking and communications. The EVT uses both absolute position references and position estimating techniques to maintain accurate vehicle positions. Absolute position references are obtained using radio frequency (RF) signal trilateration from cell towers and Wi-Fi emitters. Position estimates are obtained by using the device's inertial measurements and information about vehicle motion from the Onboard Diagnostics (OBD2) port. The data collected is transmitted to a remote Fusion server established specifically for this device and is processed, analyzed, and prioritized to assess errors and correlate information to provide an accurate location of the vehicle. The system is designed to operate effectively under challenging operational scenarios where tracking capabilities are interfered with, or jammed, through RF interference or physical obstructions. The EVT provides location data within four minutes of the vehicle's engine start and if the GPS is lost, the EVT enables command center personnel to maintain the vehicle's location for enhanced situational awareness and incident response capabilities. Twelve Enhanced Vehicle Tracker prototypes were issued to the Department of State—Diplomatic Security for operational evaluation in dense urban environments. The Enhanced Vehicle Tracker is available as a commercial product from Raytheon Blackbird Technologies.

Event Pin Identification

Federal agents are assigned a set of event pins to designate their participation in major interagency events. Command post officers perform a visual pin inspection to identify approved personnel. This raises security concerns if a pin is lost, stolen, or duplicated with high fidelity. Impact Research and Technology, LLC of Phoenix, Arizona developed the Event Pin Identification (ID) system to mitigate this security concern and assist in agent recognition. The Event Pin ID system integrates long-range passive radio frequency identification (RFID) technology, secure network server, and custom database software to discretely detect event pins. An event pin containing a unique RFID tag will be assigned to each protective service agent. Upon entry to a venue, the system will provide the command post officer with the agent's name, photograph, physical description (i.e., height, weight, eye color, etc.), and pin status for visual comparison. Invalid tags and unauthorized agents trigger visual and audible alarms to alert command post officers of a potential security breach. Additionally, the system is capable of distinguishing between an agent entering and exiting a post. The system has a minimum detection range of 30 feet. Agent identifying information contained within the database and communicated across servers is secured by the Advanced Encryption Standard (AES)-256. The Event Pin ID facilitates improved security over visual pin inspection to identify approved and unapproved personnel during large interagency events. Four Event Pin ID prototypes were issued to the Department of State – Diplomatic Security for operational evaluation. The Event Pin ID system is available for purchase and customization from Impact Research and Technology, LLC.

Used Armor Response Corridors

Law enforcement, military personnel, and protective details perform their tasks in many environmental conditions and climatic regions. Each region has a unique climate that contributes to the lifecycle of body armor. Extreme heat, moisture, and frigid temperatures could affect the longevity of personal armor. Each duty performed by personnel, storage conditions, laundering schedule, and general care can all have cumulative effects on the lifecycle of body armor. Armor manufacturers recommend a service life of five years based on a generalized, average lifecycle. This project sought to validate the recommended service life across the various environments and duty uses seen by law enforcement personnel. HP White Laboratory, Inc. of Street, Maryland collected hundreds of armor samples from federal, state, and local law enforcement through voluntary donation of out of service armor. Each piece of armor was evaluated on its condition, use history, model number, protection level, duty use, and other variables. The armor was tested to determine the ballistic limit of the armor in the used condition. HP White Laboratory, Inc. compiled the test and historical data of the armors to determine what lifecycle conditions contributed to demonstrated performance degradation. The results of this study will be used to craft recommendations for storage and care protocols and inform procurement cycles for law enforcement agencies.

Wireless Tactical Headset

The United States Army Special Forces (SF) face unique challenges that require a balance between operational effectiveness and personnel safety. Communication is a key factor in operational effectiveness, and SF operators must monitor the operational environment for acoustic cues and communicate with their team. Currently, SF operators are issued a fully wired tactical communications headset. These wired systems can tangle with clothing and equipment, can be costly to replace damaged wired components, and are slow to put on and take off. In the past, many operators sacrificed their hearing protection in order to better monitor communications systems and ambient sounds. Without hearing protection, temporary or permanent hearing loss due to rounds fired or blast events can render an operator unable to detect ambient noises such as cracking twigs or rounds being chambered. Gentex Corporation developed an innovative wireless tactical communications headset suite with hearing protection/amplification to replace wired headsets. The system includes a wireless push-to-talk capability that is immune to jamming. Standard battery

power provides over 100 hours of operating time. The system will survive in harsh environments, is immersible, and provides backwards compatibility with current solution set components. Ten prototypes were issued to the United States Army 1st Special Forces Command (Airborne) for further operational evaluation. The Wireless Tactical Headset is being evaluated by Program Manager SOF Survival, Support, and Equipment Systems for program of record requirement compliance analysis.

ONGOING PROJECTS

Counter Unmanned Aerial Vehicle


zapp2photo/Adobe Stock

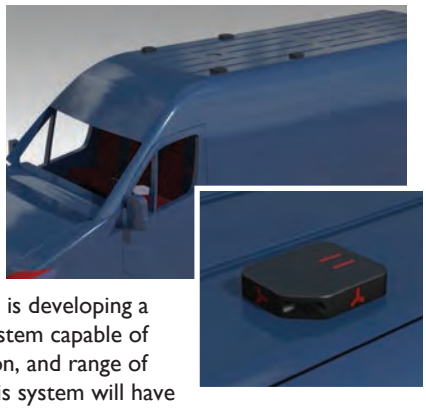
Unmanned aerial vehicles (UAVs) or drones have entered the commercial market space and are readily available for purchase. Their ease of use and accessibility has drawn increasing attention to the potentially harmful uses of UAVs. Overseas enemy threat groups are using UAVs to attack friendly civilian and military targets. Homeland attacks have been attempted; however, no documented events have been successful. Additionally, UAVs have been found operating in restricted airspace, creating potentially dangerous situations. In many cases, the UAV operators are not operating with malice, but UAVs flying in unauthorized spaces cause concern for the safety of personnel and aircraft operating in the area. In order to protect U.S. personnel and facilities, CTTSO is managing several projects that identify and characterize problems posed by UAVs. CTTSO is investing in technologies that detect and mitigate UAV threats. The goal is to develop an interoperable suite of technologies where the modality of the system can be tailored to the operating environment. The project portfolio is considering both kinetic and non-kinetic solutions as well as a range of mitigation techniques.

Helmet for 7.62 × 39 mm Mild Steel Core Protection

U.S. Special Operations Forces encounter high power rifle threats in areas of operation worldwide. Special Operations Forces require scalable personal protection equipment that offers increased coverage and threat protection, allowing them to select appropriate protection for each mission. Increased head protection against prevalent threats could exponentially increase the survivability of operators during missions. XTEK, LTD in Symonston, ACT, Australia is developing a lightweight ballistic helmet, to include mandible protection, capable of defeating 7.62 × 39 mm mild steel core (MSC) projectile threats. The helmet will limit backface deformation to 25.4 mm and provide impact attenuation in accordance with the U.S. Department of Transportation Federal Motor Vehicle Safety Standard 218. XTEK, LTD will use advanced ballistic fibers and matrix materials combined with a proprietary isostatic pressing process to achieve optimum consolidation and mechanical properties of ballistic composites in order to meet the aggressive requirements of this effort.


U.S. Army

Mobile Gunshot Detection



Security forces transporting high risk personnel (HRP) or executing on-the-move vehicle operations in high risk environments are targets for small arms fire. If subjected to incoming small arms fire, security forces gain an advantage when provided timely information regarding the firing source. These advantages lead to improved tactics for returning fire, apprehending the shooter(s), and avoiding future fire. Current military mast-mounted acoustic gunshot detection systems (GDS) are not practical for law enforcement/civilian vehicle operations due to the system size and construction. Hyperion Technology Group of Tupelo, Mississippi is developing a mobile gunshot detection system capable of determining bearing, elevation, and range of incoming small arms fire. This system will have a low false alarm rate with no more than one false alarm over a 150-hour period. The system will be low profile and discreet, work in challenging environments, and perform well at a speed of no less than 40 miles per hour. The system will report on supersonic rounds that pass within at least 25 meters with a minimum probability of detection of 90 percent. The system will also report on subsonic rounds when only muzzle blast is detected.

U.S. Army photo by Capt. Daniel Bustamante

Special Operations Tactical Stand Alone Plate

U.S. Special Operations Forces (SOF) require lightweight, tactical, stand-alone ballistic plates capable of providing elevated threat protection without degrading mobility or further encumbering the operator. The goal is to develop a hard armor solution that will meet SOF requirements and defeat a single shot of 7.62 × 51 mm M993, a single shot of 7.62 × 54R armor piercing incendiary (API) B32, or two shots 7.62 × 39 mm API BZ, each at their respective muzzle velocity. The plate will limit backface deformation to 44 mm for all three listed threats and possess an areal density of no more than 5.9 pounds per square foot. Two parallel efforts are under way to address this challenging requirement. One approach by Southwest Research Institute of San Antonio, Texas uses advanced ceramic materials enhanced by thick surface coatings of nanocomposite materials applied to the ceramic strike face through plasma enhanced magnetron sputter deposition. The nanocomposite layers increase the hardness and toughness of the ceramic substrate, thus enhancing its overall ballistic performance. The coated ceramic strike face and a ballistic composite backing layer will comprise a system optimized for weight, thickness, and ballistic performance. A parallel effort to address the same requirement is being performed by Karagozian & Case of Glendale, California. They are developing ceramic matrix composite (CMC) materials to impart increased crack resistance to traditional ceramics. CMC's achieve higher tensile strength, ductility, and toughness than conventional ceramics by embedding ceramic fibers such as carbon or oxide into a ceramic matrix material. Karagozian & Case is combining CMC layers and fiber reinforced polymer layers to create an optimized metamaterial band gap design that will disrupt the projectile induced tensile wave that defeats most conventional ceramics.

U.S. Marine Corps photo by Lance Cpl. Erik Villagran

MEMBERSHIP

Intelligence Community

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 Personnel Recovery Agency
- Pentagon Force Protection Agency
- Rapid Reaction Technology Office
- U.S. Air Force
  - Office of Special Investigations
- U.S. Army
  - Criminal Investigation Command
  - Joint Trauma Analysis and Prevention of Injury in Combat
  - Medical Research and Material Command
  - Natick Soldier Systems Center
  - Program Executive Office Soldier
    - Soldier Protection and Individual Equipment
  - Research, Development, and Engineering Command
  - Research Laboratory
  - Tank Automotive Research, Development, and Engineering Center
- U.S. Navy
  - Naval Air Systems Command
  - Naval Criminal Investigative Service
  - Office of Naval Research
  - Program Executive Office, Ships
- U.S. Special Operations Command
  - Army Special Operations Command
  - Marine Corps Forces Special Operations Command
  - Naval Special Warfare Command

U.S. Department of Energy

U.S. Department of Homeland Security

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

U.S. Department of Justice

- Federal Bureau of Investigation
- National Institute of Justice

U.S. Department of State

PHYSICAL SECURITY

pssubgroup@cttso.gov

FOCUS AREAS

Blast Effects and Mitigation

Evaluate blast threats and develop anomaly detection and mitigation approaches to protect groups of personnel, facilities, installations, and venues. Develop decision support tools and technical solutions related to blast effects.

Screening, Observation, Detection, and Protection

Develop technologies and techniques to protect personnel in facilities, and infrastructure, by improving situational awareness; detecting, identifying, and locating threats; and, controlling access to critical assets. Emphasize automatic threat detection/alerting.

Maritime Security

Develop technologies to protect ships, ports, shore and offshore facilities. Develop sensors and devices for detection and tracking; physical barriers; and stopping devices.

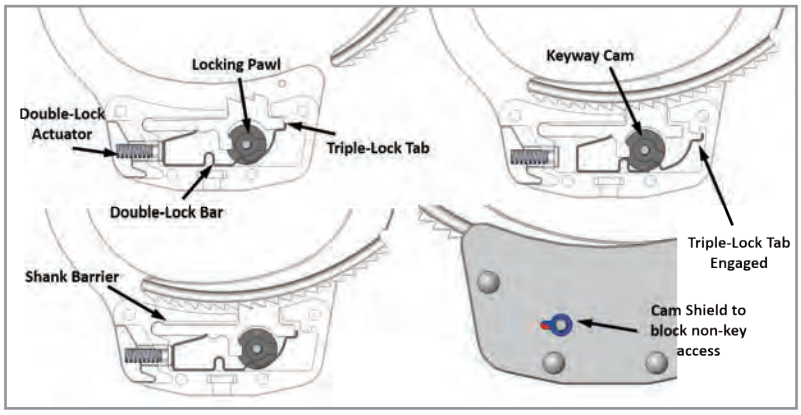
Subterranean Activities

Develop capabilities to detect, locate, map, monitor, survey, and disrupt subterranean infrastructure and activities in permissive and non-permissive environments.

COMPLETED PROJECTS

Improved Handcuffs

Handcuffs that are used by the U.S. military and law enforcement agencies have not significantly changed since their initial design in 1914 despite well-documented flaws. These design vulnerabilities have allowed some detainees to defeat their restraints. This effort modified the handcuff design by creating a new key actuator and a double locking mechanism, as well as additional barriers for shims and shanks that are commonly used to defeat handcuffs. The design improvements did not add size or significant weight to the handcuff. The improved handcuff is a safer and more effective personnel restraint mechanism for military and law enforcement use, and represents a considerable stride forward from the current handcuff design. The improved handcuff is transitioning to a commercially available product.

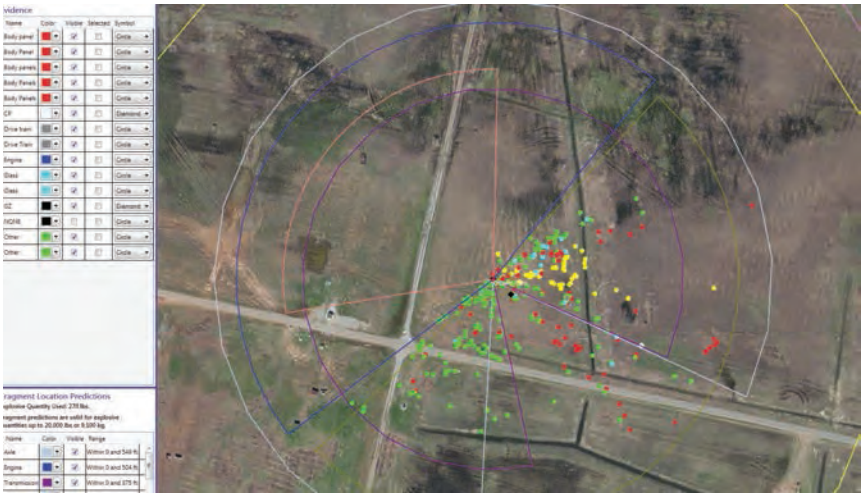


Enhanced Vehicle Explosion Analysis Software

CTTSO and the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) developed the Vehicle Explosion Analysis Software (VExAS) to assist investigators responding to a vehicle-borne improvised explosive device (VBIED) or pipe bomb attack. The software enables users to focus their search for evidence in the most likely locations, document the evidence once found, and create a virtual layout of the post-blast scene.

Subsequently, CTTSO and ATF initiated a bilateral effort with the Future Systems and Technology Directorate, Singapore Ministry of Defence, to update and upgrade the desktop software and added a VExAS mobile application. This effort provided first responders and investigators the capability to more effectively and efficiently process a post-blast scene. The Enhanced VExAS app helps users to determine the amount of explosive used and the size of the debris field, and allows the user to collect and tag evidence via pictures.

The Enhanced VExAS app is hosted on CTTSO's app store and is available for download by authorized users in the U.S. and Singapore. For more information, please contact PSsubgroup@cttso.gov.



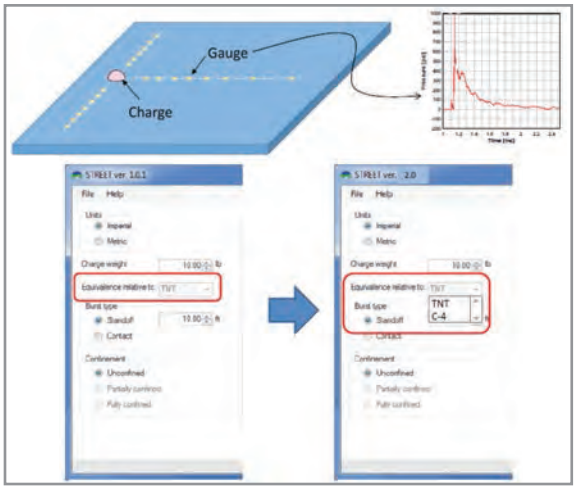
ONGOING PROJECTS

Forced Entry Resistant Roller Door

Personnel entry and exit ways for embassies and secure facilities are protected by side-hinged forced entry and ballistic resistant doors that are designed to delay an attacker for up to 60 minutes and adhere to Department of State (DOS) Standard SD-STD-01.01. Logistics entry points (cargo bays, loading docks, and vehicle garages) for these facilities use roller doors that open and close vertically on a track. Currently, there are no roller doors that qualify under SD-STD-01.01 for any period of time, leaving them susceptible to forced entry attacks. To remedy this vulnerability, CTTSO and DOS have teamed up to create a roller door that meets the DOS standard for a 15-minute forced entry resistant door. The end result will provide a more secure and durable door for use in U.S. Government facilities and commercial facilities.

U.S. Department of State-Diplomatic Security

C-4 Scenario- and Target-Relevant Explosive Equivalence Tool



In 2015, CTTSO created the Scenario- and Target-Relevant Explosive Equivalency Tool (STREET), a comprehensive software tool which equates the pressure, impulse, and brisance of an explosive into trinitrotoluene (TNT) equivalence. A wide variety of end users have found STREET to be extremely useful in their modeling and design, and there is a requirement for a new C-4 equivalence feature. Current building and retrofit materials are being tested with C-4 in addition to the older method of testing with TNT. A new C-4 and TNT equivalence algorithm is being developed that will relate pressure and impulse equivalence versus standoff to any explosive in the STREET library. This software tool, C-4 STREET, will benefit engineers and architects by determining the appropriate loads being exerted on targets as a result of an explosive event using range-dependent equivalency values.

Enhanced Security Observation Set (eSOS)

U.S. Special Operations Forces (SOF) have an ongoing operational need to enhance their situational awareness and to scan for potential threats at outposts in remote and potentially vulnerable locations. The U.S. Secret Service (USSS) requires a small, modular, portable security system for protecting government officials, dignitaries, and VIPs. The eSOS effort will update the technology and enhance the capabilities of the previously developed Security Observation Set (SOS) force protection kit to meet current SOF and USSS requirements. The eSOS kit will extend the range of the current Sensor Alarm System (SAS) to greater than 50 yards in a non-line-of-sight indoor environment for VIP and soldier protection during short-duration stays. It will also incorporate internet protocol (IP) and megapixel video capabilities to provide wider coverage and high-resolution assessment. Other eSOS improvements include an integrated power management system and a wireless mesh communications infrastructure that will allow rapid set up and provide automated detection capabilities over a larger area. The eSOS will be available for procurement on the GSA schedule.

Tunnel Collapse Response Guide

Underground operations can place personnel in difficult environments—little or no ambient light, claustrophobic spaces, restricted movement, poor communications, and limited tracking capabilities. Operations are made all the more challenging by potential environmental risks such as flooding, cave-ins, suffocation, and harmful air quality

resulting from smoke, airborne debris, or hazardous gases. The Tunnel Collapse Response Guide effort is two-fold—conduct a comprehensive study delineating measures for rescuing victims inside collapsed tunnels and produce an in-depth guide of best practices for subterranean scenarios typically encountered by operators, primarily U.S. Customs and Border Protection and rescue personnel. The study will take into account the varying size, depth, configuration, and geologies of earthen tunnels and underground municipal infrastructure encountered along the U.S. southwest border. The Tunnel Collapse Response Guide will list existing technologies that support tactics, techniques, and procedures for rescue personnel responding to a subterranean structure collapse. It will also describe the advantages and disadvantages of technologies and identify capability gaps. Finally, the guide will provide a menu of specialized equipment and training recommended for post-collapse personnel recovery and operationally achievable recommendations to aid in enhancing safety while executing a counter tunnel mission or rescue operation.

Portable Advanced Imaging Technology

Aviation screening checkpoints use full-body scanner systems known as Advanced Imaging Technology (AIT) to detect metallic and non-metallic threats. However, these are rarely used outside of airports because they are not portable or designed for outdoor use.

CTTSO in partnership with the Government of Israel is developing a portable backscatter X-ray AIT. Tek84 Engineering Group is modifying a full-body scanner, known as the AIT84, into a smaller, portable, and ruggedized system while maintaining the same level of detection. Similar to aviation checkpoint AITs, the portable AIT is a low dose X-ray system that will be used to screen people for concealed threats. A trained operator reviews the X-ray image to detect concealed items, such as guns or explosives, and detected anomalies will undergo additional screening. The portable AIT will be a rugged system used for security screening at outdoor events, as well as government buildings or embassies located in areas with reduced infrastructure. It is stored in three rolling modules and can be assembled by two people in less than two hours. The United States and Israel will test the system to ensure the detection capability and personnel throughput meet operational requirements.

Technology Development for Subterranean Operations

Terrorist and criminal organizations are using underground tunnels to launch rockets, cache weapons, smuggle goods and personnel, and conduct other illicit and hostile activities that threaten our borders and security forces operating overseas. Israel has significant experience with tunnel detection and remediation due to the enduring tunneling activities along their borders. During the conflict with Hamas in the summer of 2014, the Israel Defense Forces discovered and destroyed 32 tunnels, and Hamas has spent considerable resources since then to rebuild its tunnel network.

The 2016 United States National Defense Authorization Act directed the United States to carry out research, development, testing, and evaluation of anti-tunnel technologies with Israel. The development of effective capabilities in support of subterranean operations will help protect both Israel and the United States from potential threats due to illicit tunnel activity.

MEMBERSHIP

American Society for Testing and Materials

Environmental Protection Agency

Federal Reserve Board

General Services Administration

Intelligence Community

National Reconnaissance Office

State and Local Agencies

- DC Metropolitan Police Department
- DC Protective Services Police Department
- New York City Police Department
- Port Authority of New York and New Jersey
- Virginia Department of Transportation

U.S. Capitol Police

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
  - Joint Improvised-Threat Defeat Organization
- Explosives Safety Board
- Joint Chiefs of Staff
- Joint Non-Lethal Weapons Directorate
- Joint Task Force North (NORTHCOM)
- Joint Warfare Analysis Center (JFCOM)
- National Ground Intelligence Center
- Office of the Secretary of Defense
- Physical Security Enterprise and Analysis Group
- Unified Combatant Commands
- U.S. Air Force
  - Research Laboratory
- U.S. Army
  - Armament Research, Development, and Engineering Center
  - Army Research Laboratory
  - Asymmetric Warfare Group
  - Communications-Electronics Research, Development and Engineering Center
  - Corps of Engineers
  - Engineer Research and Development Center
  - Office of the Provost Marshal General
  - Night Vision and Electronic Sensors Directorate
  - Rapid Equipping Force
  - Research, Development, and Engineering Command
  - Training and Doctrine Command
- U.S. Marine Corps
  - Central Command
  - Systems Command
  - Warfighting Laboratory
- U.S. Navy
  - Chief of Naval Operations
  - Commander Navy Installations Command
  - Expeditionary Combat Command
  - Naval Criminal Investigative Service
  - Naval Explosive Ordnance Disposal Technology Division
  - Naval Facilities Engineering Command
  - Naval Facilities Engineering Service Center
  - Naval Sea Systems Command
  - Naval Undersea Warfare Center
  - Office of Naval Research
  - Strategic Systems Programs
- U.S. Special Operations Command
  - Army Special Operations Command
    - Army Special Forces Command (Airborne)
  - Joint Special Operations Command
  - Marine Corps Forces Special Operations Command
  - Naval Special Warfare Command
    - Naval Special Warfare Development Group

U.S. Department of Energy

- Federal Energy Regulatory Commission
- National Nuclear Security Administration
- Nuclear Regulatory Commission

U.S. Department of Homeland Security

- Customs and Border Protection
- Immigration and Customs Enforcement
- National Protection and Programs Directorate
  - Federal Protective Services
- Science and Technology Directorate
  - Transportation Security Laboratory
- Transportation Security Administration
- U.S. Coast Guard
- U.S. Secret Service

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. Marshals Service

U.S. Department of State

- Bureau of Diplomatic Security

U.S. Department of Transportation

- Volpe National Transportation Systems Center

SURVEILLANCE, COLLECTION, AND OPERATIONS SUPPORT

scossubgroup@cttso.gov

FOCUS AREAS

Biometrics, Recognition, Identity Intelligence, Tracking, and Exploitation (BRITE)

Improve technologies to identify and/or mask entities of interest using or countering biometrics, pattern recognition, database technologies, and exploitation methodologies.

Cyber and Convergence Technologies

Support or improve technologies for cyber and signals collection as these technologies increasingly converge with other systems and technologies to include, but not limited to the "Internet of Things."

Human Language Technology (HLT) and Media Exploitation

Develop and employ HLT where these technologies can best assist humans – operators and analysts – to make sense of volume and the variety of media sources; apply timely and actionable information in theater; and enhance communication skills and cultural understanding.

Surveillance/Counter-Surveillance

Develop audio, video, and advanced surveillance technologies, as well as automated tools and techniques to defeat adversarial tactics, techniques, and procedures, and methodologies.

Technical Collection/Special Communications

Improve ISR by developing and enhancing multi-INT sensors, SIGINT collection, and tagging tracking, locating technologies for intelligence operations. Develop and enhance special communications and canine advanced technologies in support of Special Operations and intelligence collection activities.

COMPLETED PROJECTS

Social Media Identity Location and Extraction System (SMILES)

Currently, biometric information is captured and processed through direct human interaction. This process is time consuming and may not result in a positive identification. This delay may permit the person of interest to slip away before the identity can be determined. In such cases, even if identity can be established, it will not have value until the individual is encountered again. There was a clear and pressing need to identify people of interest at or before the initial encounter. Biometrics extracted from social media is an effective way to establish identity and tag a person of interest without physically encountering the individual. SMILES is an automated software-based tool that extracts face and hand related data from video streams and fuses the results to present the strongest possible measure of identity from available data. This provides a functional platform that could be expanded to include other biometric factors found in video such as voice, gait, movements, and gestures. The SMILES software application was delivered to the National Media Exploitation Center (NMEC) and other intelligence community partners for final operational test and evaluation. NMEC will be the approving authority for distribution of the software to other users.

Multimedia Processing and Analysis (MPA)

Both the United States and the United Kingdom have been working on numerous efforts to develop better Human Language Technologies (HLT). This effort combined the expertise from both countries to develop an enhanced HLT processing and exploitation capability. The MPA effort tested a mix of HLT tools to process and analyze audio, video,

text, and image content and explored capabilities to evaluate performance readiness and utility for operational use. The HLT tools were tested using the U.S. Air Force Research Lab's baseline Multi-Media Information Extraction Retrieval (MMIER) architecture and the CTTSO-developed Multimedia Multilingual Monitoring System.

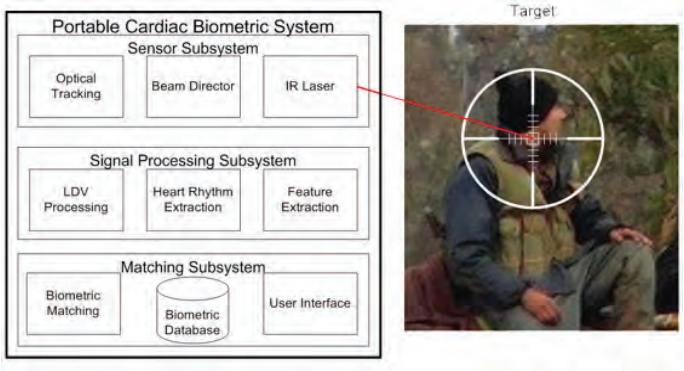
ONGOING PROJECTS

Beetlejuice

The government requires the ability to develop and deliver novel and high-performance speech-based noise reduction and speaker tagging, tracking, and locating to support and enhance Department of Defense capabilities. The technologies being developed under this project will provide near real-time situational awareness of incoming signals, filtering speakers, messages, languages, and location. The capabilities will be integrated into a lightweight platform in support of operators on the move and handle a variety of noisy audio media. Applications Technology, LLC, is developing a capability that uses a beamforming microphone array in combination with deep neural networks. This unique combination will improve performance in both noise reduction, source location, and human language technologies. The final solution will be integrated with Intelligence, Surveillance, and Reconnaissance (ISR) tactical sensors.

Jetson

Existing long range biometric methods that rely on facial recognition suffer from acquiring enough pixels at a distance to use the face matching algorithms and require high performance optics to acquire visual signatures at significant distances. Additionally, movement, environmental conditions, changes in facial appearance such as beards, sunglasses, and headwear can obfuscate the face and result in significant inaccuracies. Being able to measure unique cardiac signatures obtained from an individual at a distance provides additional biometric identification when environmental conditions and changes in facial appearance hinder use of a facial recognition system. The Jetson effort being developed by Ideal Innovations, Inc. is a ruggedized biometric system that will capture cardiac signatures to aid in the positive identification of an individual at a distance up to 200 meters and within five seconds.



MEMBERSHIP

Intelligence Community

Special Operations Forces

TACTICAL OPERATIONS SUPPORT

tossubgroup@cttso.gov

FOCUS AREAS

Offensive Systems

Develop advanced equipment and capabilities that enhance the effectiveness of small tactical units engaged in direct action operations. Develop specialized weapons, munitions, detonators, distraction/ diversion devices, and other unique tactical equipment.

Unconventional Warfare and Counter-Insurgency Support

Develop advanced tools and equipment specifically for small tactical units conducting a broad spectrum of military, paramilitary, special warfare, and digital operations focused on force protection, assisted and unassisted recovery, and operational preparation of the environment.

Tactical Communications

Develop flexible, enhanced, full spectrum communications capabilities specifically designed for tactical forces, with emphasis on reducing operational load while improving operator mobility and efficiency. Develop assured tactical communications connectivity in challenging environments such as complex urban, subterranean, and maritime.

Tactical Reconnaissance, Surveillance, and Target Acquisition Systems

Develop technologies to assist small tactical teams in conducting organic reconnaissance, surveillance, and target acquisition missions. Develop systems that enhance the visual perception or other imaging capabilities of tactical operators in all conditions and environments.

Specialized Infiltration, Access, and Exfiltration Systems

Develop technologies that assist tactical assault forces in gaining rapid insertion, access and egress to and from objectives. Improve evaluation of tactical options, and support efficiency and stealth, including remote operations. Develop enhanced target analysis, manual and dynamic breaching technologies for small tactical assault teams.

Survivability Systems

Develop man portable tools and equipment to enhance operator survivability during the conduct of tactical missions.

COMPLETED PROJECTS

Cyber Operator Greyhat

We continue to encounter an increasing cyber threat where a "Digital Divide" exists between Governments and our cyber opponents. Larger government and military organizations are standing up capacities and capabilities to address this threat at the strategic level. At the request of Special Operations Forces (SOF), CTTSO took on the initiative to complement this larger build by training operators at the tactical level from the United States, Australia, Canada, Israel, and the United Kingdom. Cyber Operator Greyhat (COG) was an open source digital operations course tailored to train tactical operators to understand the cyber domain and to identify and mitigate cyber threats. The five-week intensive course provided foundations in computer science, information security, social media, social

engineering, and advanced computer networking. The classroom instruction was validated in over twenty practical field training events and one comprehensive full mission profile three-day culmination exercise. At the completion of a COG course, tactical operators returned to their units as trainers in cyber tactics, techniques, and procedures. In addition, digital operators from the course now have the capacity to inform and advise Commanders on concept of operations and rules of engagement within the digital domain. This course enabled tactical operators to counter cyber opponents and set success criteria to hold the high ground within the digital domain in future battlefields. COG contributed to the development of SOF tactical capabilities build for 21st century Special Warfare cyber enabled operations. Industry partners Advanced Mission Systems and SensePost trained over 200 SOF, DoD, interagency, and select international partner operators from FY15 to FY17. Since the successful completion of COG, the course transitioned to a United States SOF funded program of record while also influencing international partner digital force protection capabilities.

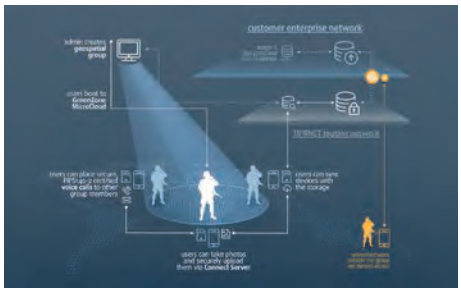
Cyber Open Source Methods and Operations

Protection against current and increasing digital threats require special skills in order to understand and operate in the digital battle space. The 21st century social media medium is being leveraged and exploited by state and non-state actors to recruit, command, control, and conduct illegal and terrorist activities against U.S. and allied interests. Cyber Open Source Methods and Operations (COSMO) was a three-week intensive, tactical level training course that teaches operationally relevant capabilities to execute 21st century Special Warfare mission sets. COSMO focused on the operator, refining methodologies based on best practices, tactics, techniques, and procedures. The course introduced state-of-the-art social media tools against operationally relevant themes, exploiting publicly available social media information. The training program was designed to enhance a unit's digital force protection, digital identity management, and digital operational preparation of the environment for tactical operators all while being conducted with managed attribution in a global environment. By design, COSMO was a unique, combined, joint, interagency digital task force training capabilities exercise that trained over 210 Special Operations Forces (SOF), DoD, interagency, and select international partner operators from FY15 to FY17 by industry partner White Canvas Group. Since the successful completion of COSMO, the course transitioned to a United States SOF funded program of record while also influencing international partner digital capabilities.

Maritime Canister-Launched Small Unmanned Aerial System (MCLSUAS)

Special Operations Forces (SOF) operating in maritime environments lack an organic Small Unmanned Aerial System (sUAS) capable of launch, operation, and recovery while being subsurface to support surface surveillance and reconnaissance missions. The Maritime Canister-Launched Small Unmanned Aerial System (MCLSUAS) gives SOF maritime forces the capability to launch, operate, and recover a collapsible-wing sUAS while remaining underwater in Sea State Three (3) conditions. The MCLSUAS is inclusive of a Vector Hawk sUAS, Canister Launch Unit, and a Maritime Ground Control Station. The MCLSUAS, developed by Lockheed Martin, has a minimum operating time of 40 minutes with a dash speed of 50 knots, and will stay afloat for a minimum of 30 minutes for recovery and reuse after a water landing.

GreenZone Tactical Communications



Tactical operators require secure and discrete communications for operations. GreenZone Tactical Communications (GZTC), by SAIFE, meets the priority communications needs of tactical operators by creating a secure ecosystem based on a holistic communications approach of combining cutting-edge software, hardware, and telecommunications technologies. This capability features a public key infrastructure (PKI) software suite for versatility on common operating systems, a virtual machine based routing system for infrastructure connectivity for data in transit (DIT) security, and the first complete computer on a chip via a micro SD for data at rest (DAR) security. GZTC brings government communications into the 21st century by allowing the use of smartphone devices and off the Department of Defense Information Network (DoDIN) technologies through an approved for use (Risk Management Framework/Authority To Operate) solution architecture that allows for plug-n-play flexibility with third party applications and hardware.

Augmented Reality System-Navigation (ARES-N)

Currently, tactical operators conduct route planning and navigation during missions using applications such as Android Tactical Assault Kit (ATAK), which allows the end user to simultaneously view navigation directions, data, and friendly and/or foe positions. There is no safe way to drive and navigate a vehicle while in a combat or hazardous area without one team member looking down at a mobile device running these current capabilities. The Augmented Reality System-Navigation (ARES-N) project, developed by industry partner PAR Government, allows the driver and all team members to keep their heads up to improve situational awareness and force protection during mobile operations through a dashboard-mounted tablet or phone and software based solution. ARES-N features an augmented reality system that overlays live camera footage from a tablet, navigation instructions, and targeting information for enhanced situational awareness while navigating on the move.

HERO-30SF Lethal Miniature Aerial Munition System (HERO-30SF LMAMS)

Special Operations Forces (SOF) are required to perform high-risk missions regardless of the availability of close air support, artillery, or mortar indirect fire support. On today's asymmetric battlefield, each location or country SOF operates in may have different rules of engagement, different authorities or permissions granted by the host country in regards to the type of fire support permitted in each situation. However, SOF should always have the ability to provide surgical fire support for force protection, and when authorized offensive lethal application. The HERO-30SF provides a surgical strike capability organic to small tactical teams operating in denied areas when fire support assets are limited or not available, and the Lethal Miniature Aerial Munition System (LMAMS) provides improved lethality, deeper attack angles, and a higher percentage of first-round hit capability in both urban environments and difficult terrain. The HERO-30SF can launch from a portable canister and strike the intended target, or conduct intelligence, surveillance, and reconnaissance (ISR) until the operator confirms the target allowing the operator to find, fix, and finish threat targets. The capability allows engagement of enemy combatants without exposing the SOF operator to direct enemy fires, allowing time sensitive targeting of line-of-sight or beyond line-of-sight stationary or moving targets. U.S. Army Aviation and Missile Research, Development, and Engineering Center, as part of their investment in Small Organic Precision Munition Program to support the LMAMS requirement, developed the HERO-30SF warhead and fuse design. The HERO-30SF with warhead and fuse was developed by an industry team made up of Dynetics, Mistral Inc., NTS, PER, SPECTRA, UVision

and in partnership with the U.S. Army Dugway Proving Ground. In May 2017, a successful test of the HERO-30SF was conducted and DoD tactical operators received complete kits in FY17 for further operational test and evaluation or combat evaluation. This system is a candidate for multiple DoD requirements in FY17 and FY18, stimulating competition in the LMAMS space for the U.S. Government.

ONGOING PROJECTS

Ammunition Initiatives Meeting IX (AIM IX)

The individual tactical operator armed with small arms and ammunition is the most employed weapon system in the fight against terrorism in U.S. and allied arsenals. In response to user community requests to bring together both government and select industry representatives, CTTSO Tactical Operations Support Subgroup conducts a three-day DoD, interagency, and select international partner subject matter expert workshop called Ammunition Initiatives Meeting (AIM). AIM discusses new and promising initiatives related to small caliber ammunition and related weapon and accessory development. This workshop meets annually with several primary focus areas:

- Threat Weapon and Ammunition Developments
- Joint U.S. and International Lessons Learned/Capability Gap Session
- U.S. DoD and NATO Ammunition and Small Arms Systems Initiatives
- Select Industry Ammunition and Small Arms Initiatives
- Exterior and Wound Ballistics Overview and Testing
- Lightweight Ammunition Technology
- Projectile Aerodynamic Design, Interior Ballistics, Exterior Ballistics, and Terminal Effects
- Modern Ammunition Production and Testing
- Leap-Ahead Ammunition, Projectile, Propellant and Case Technology
- Intermediate Caliber Cartridge Developments
- The Law Enforcement Perspective
- Geopolitical Influences on Small Arms Ammunition Development and Employment
- Fire Control Systems

In its ninth year, the AIM workshop has been the incubator for rapid interagency development of various novel and advanced ammunition technologies including: lightweight polymer combat ammunition with enhanced terminal performance; intermediate caliber rifle and machine gun cartridges to improve standoff range for allied tactical personnel; advanced next generation sighting devices; signature suppression; as well as an assortment of new combating terrorism-related technologies. The AIM government-only sessions are held at the SECRET level. The AIM is the only classified meeting of its type dedicated to this focus area, and attracts more than 60 agencies and over 100 government personnel from four countries to include Australia, Canada, the United Kingdom, and the United States. AIM also includes a live-fire demonstration of advanced technologies from both government and industry developers. AIM X will be held April 17–19, 2018 in the Washington, D.C. National Capitol Region.

Micro Weather Sensor-Air to Surface Employment Kit (MWS-A2SEEK)

Currently fielded Micro Weather Sensor (MWS) prototypes are critical to collecting meteorological data that provide commanders, mission planners, SOF operators, and weather support elements/personnel with the necessary environmental fidelity to plan and execute missions. In order to gather weather data, small tactical units hand deliver, the MWS in hostile environments that can lead to potential losses in personnel. To reduce the risk to personnel, SOF requires a method to deliver the MWS by air via fixed or rotary wing aircraft.

To meet this requirement, STARA Technologies Corporation is developing an Air to Surface Employment Kit (A2SEEK) for the MWS. The MWS-A2SEEK will be hand launched from military aircraft, descend, and land to a predetermined location, automatically attain a stable position, and begin autonomous weather reporting operations for up to 150 days.

Silicone Membrane Amplified Lightweight Speaker (SMALS)

Currently fielded military communication device speakers are antiquated, large, and conspicuous. The Silicone Membrane Amplified Lightweight Speaker (SMALS) project is developing a state-of-the-art amplified speaker-transceiver unit to work with a number of military and commercial radio devices. SMALS, developed by industry partner GromaTech, leverages commercial off-the-shelf technologies to provide an advanced system that enhances current communication packages. This state-of-the-art silicone membrane speaker-transceiver technology has extended frequency response and improved audio output in comparison to the performance of legacy sub-miniature cone type speakers. Ongoing development has coupled high performance audio drivers with a specially tuned acoustic chamber that provides superior performance at one-fifth the weight and less than half the size of the currently fielded radio speaker.

.338 Norma Magnum Lightweight Medium Machine Gun and Polymer Ammunition

United States and United Kingdom tactical operators currently have a choice between 7.62 mm or .50 caliber machine guns for long-range combat engagements. The 7.62 mm M240 machine gun variants provide dismounted troops with maneuverability, but limited range. Current inventory .50 caliber machine guns are too heavy and cumbersome for dismounted use, and are almost exclusively used at fixed sites and on mounted patrols due to this limitation. The 23-pound .338 Norma Magnum Lightweight Medium Machine Gun made by General Dynamics Ordnance and Tactical Systems, and polymer ammunition made by MAC Ammo fills the gap between the light, but limited range 7.62 mm weapons, and the longer range, but cumbersome .50 caliber weapon systems. With an effective range out to 2,000 meters and linked ammunition that is 15 percent lighter than conventional .338 Norma Magnum linked ammunition and nearly 65 percent lighter than .50 caliber linked ammunition, the .338 Norma Magnum Lightweight Medium Machine Gun and its polymer ammunition provides an optimal capability for long distance direct fire combat engagement.

Enhanced Mortar Targeting System-Mobile 120 mm (EMTAS-120M)

Current deployments for SOF require agility and mobility for all combat resources due to the constantly changing battlespaces. The Enhanced Mortar Targeting System 120 mm-Mobile (EMTAS-120M) provides SOF with an organic, precision 120 mm mortar capability that can be used on mounted patrols or for protection of mobile operating bases. The EMTAS-120M uses common Army 120 mm mortar and mortar rounds coupled with precise laying accuracy provided by EMTAS' 360-degree electrically driven targeting system out to 7.2 kilometers with only a two-man crew delivering 10 rounds from a short halt. The system, designed by Elbit Systems of America, is a roll-on-roll-off design for use with common Army M1083 Family of Medium Tactical Vehicles (FMTVs) and can be used in a mounted or dismounted configuration depending on end user requirements.

7.62 × 51 mm NATO Subsonic Ammunition Optimization – Position Insensitive Subsonic Round

United States and United Kingdom tactical operators require the development of an advanced round for precision subsonic 7.62 × 51 mm NATO ammunition due to inconsistencies in the performance of current subsonic cartridges. This 7.62 × 51 mm NATO subsonic round will negate powder position sensitivity issues and increase maximum effective range of the subsonic projectile. This performance increase will be accomplished through a new and advanced case design that compacts the powder load and ensures consistent ignition and burn characteristics while firing. The result will be an optimized subsonic round that has greater range and accuracy allowing end users to more effectively engage targets in situations where a subsonic projectile is required.

Multi-Ability Reconfigurable SUAS (MARSUAS)

Special Operations Forces tactical teams are currently constrained to singular design sUAS that are not able to adapt to multiple mission roles and rapid changes to situations on the ground. SOF currently relies on single form factor Group 1 and 2 fixed and vertical lift sUAS to perform current mission tasks. Units are challenged with maintaining training currency and standardization, interoperability between platforms, sustainment of the systems, and an increase in operational load when deploying these different sUAS.

The MARSUAS by UAV Solutions will provide SOF a single sUAS platform that can be configured in the field to support missions requiring a quad rotor sUAS, tilt rotor/vertical take off and lift sUAS, and fixed wing long endurance sUAS with one common tablet controller. When fielded, SOF will have a rapidly reconfigurable sUAS that has the potential to replace all existing Group 1 sUAS. MARSUAS is under development in partnership with UAV Solutions with four systems scheduled for final testing and delivery in first quarter of FY18.

MEMBERSHIP

American Society for Testing and Materials

National Tactical Officers Association

State and Local Agencies

- Alexandria (VA) Police Department
- Austin (TX) Fire Department
- Boston (MA) Fire Department
- Boston Special Weapons and Tactics
- Charleston (SC) Special Weapons and Tactics
- Colorado Springs (CO) Police Department
- Denver (CO) Special Weapons and Tactics
- Indianapolis (IN) State Police Bomb Squad
- Los Angeles (CA) Police Department
- Los Angeles Sheriff's Department
- Maryland State Police Special Weapons and Tactics
- Massachusetts State Police Bomb Squad
- New Jersey State Police
- New York City Police Department and Fire Department
- Pasco County (FL) Sheriff's Office
- San Diego (CA) Fire Department and Bomb Squad
- San Diego Sheriff's Department
- Savannah (GA) Special Weapons and Tactics
- South Carolina State Police Bomb Squad
- South Carolina State Police Special Weapons and Tactics
- Virginia State Police

U.S. Department of Defense

- Cyber Command
- Defense Advanced Research Projects Agency
- Defense Innovation Unit Experimental
- Defense Intelligence Agency
- Joint Improvised-Threat Defeat Organization
- Joint Personnel Recovery Agency
- National Guard Bureau
- National Security Agency
- U.S. Air Force
  - Counter-UAS Force Protection
  - Explosive Ordnance Disposal
  - Global Strike Command
- U.S. Army
  - 20th Support Command, CBRNE
  - Armament Research, Development, and Engineering Center
- Asymmetric Warfare Group
- Maneuver Center of Excellence
- Night Vision and Electronic Sensors Directorate
- Office of the Army G-3/5/7 (Operations/Plans)
- Office of the Army G-8 (Financial Management)
- Program Executive Office Soldier
- Program Manager Unmanned Aircraft Systems (PMUAS)
- Rapid Equipping Force
- Soldier Systems Center
- U.S. Marine Corps
  - Explosive Ordnance Disposal
  - 2nd Marine Aircraft
  - Marine Corps Forces Cyber Command
- U.S. Navy
  - Naval Academy
  - Naval Air Weapons Station, China Lake
  - Naval Postgraduate School
  - Naval Surface Warfare Center, Carderock Division
  - Naval Surface Warfare Center, Crane Division
  - Naval Surface Warfare Center, Dahlgren Division
  - Navy Explosive Ordnance Disposal Group 2
- U.S. Special Operations Command
  - Air Force Special Operations Command
  - Army Special Operations Command
    - 1st Special Forces Command (Airborne)
    - 75th Ranger Regiment
    - Army Special Operations Aviation Command
    - Civil Affairs
    - Military Information Support Operations Command
    - U.S. Army John F. Kennedy Special Warfare Center and School
  - Joint Special Operations Command
  - Marine Corps Forces Special Operations Command
  - Naval Special Warfare Command
    - Naval Special Warfare Groups
    - Special Boat Teams
  - Theater Special Operations Commands

U.S. Department of Energy

- National Nuclear Security Administration

U.S. Department of Homeland Security

- Customs and Border Protection
  - Border Patrol Tactical Unit
  - Border Search, Trauma, and Rescue
  - Rio Grande Valley Sector
  - Special Operations Group
  - Tucson Sector
  - Yuma Sector
- Federal Air Marshal Service
- Immigration and Customs Enforcement
  - Homeland Security Investigations
- Office for Bombing Prevention
- Transportation Security Laboratory
- U.S. Coast Guard
  - Maritime Security Response Team
  - Maritime Safety and Security Team
- U.S. Secret Service

U.S. Department of Justice

- Bureau of Alcohol, Tobacco, Firearms and Explosives
  - Special Response Teams
- Drug Enforcement Administration
  - Special Operations Division
- Federal Bureau of Investigation
  - Ballistic Research Facility
  - Critical Incident Response Group
  - Hostage Rescue Team
  - Joint Terrorism Task Force – National
  - Joint Terrorism Task Force – Local
  - Washington Field Office
- U.S. Marshals Service

U.S. Department of State

- Bureau of Diplomatic Security

TRAINING TECHNOLOGY DEVELOPMENT

ttdsubgroup@cttso.gov

FOCUS AREAS

Innovative Training and Educational Concepts

Research, develop, and evaluate training and educational programs that employ novel instructional design and/or delivery methods for accelerating and enhancing the acquisition of advanced knowledge and skills.

Human Performance Technology

Analyze the full range of performance gaps and select interventions to improve and sustain human performance. Develop, test, and evaluate performance improvement technologies and programs based on cognitive and physiological principles to optimize operator training and ultimately mission performance.

Mobile Learning

Design and develop intuitive, interactive learning solutions for anywhere, anytime access from mobile devices. Develop mobile applications and technology that supports learning through ubiquitous and just-in-time access to educational resources, collaborative learning environments, and user-generated content.

Immersive Learning Technology

Research and develop technology that allows a learner to seamlessly interact with, and become immersed in, a learning environment. Develop tools, technologies, and techniques for improving the design, development, and validation of interactive and immersive learning technology.

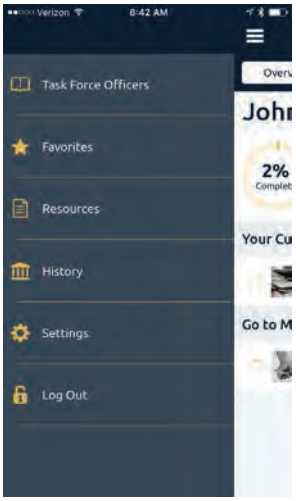
COMPLETED PROJECTS

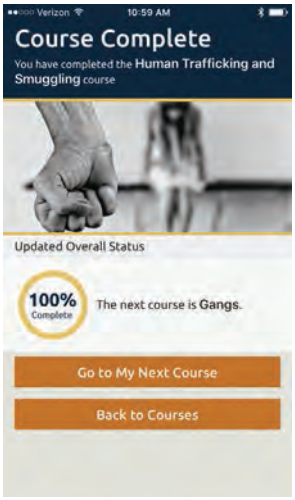
Robotic Human Type Targets T30

Live fire on a realistic moving target is often experienced for the first time during combat instead of training exercises. The Robotic Human Type Target (RHTT) T30 capability, developed by Marathon Targets, addressed this training challenge by providing reality-based training with unpredictable scenarios and a variety of dynamic tactical maneuvers. The RHTT T30 was built to move autonomously on a live-fire range, withstand a large volume of fire, and operate in rugged terrain. The RHTT T30 provides instant feedback by slowing down when it senses a non vital shot and coming to a complete stop with a vital shot. The T30 Target's unique features improve operational effectiveness and human performance in preparation for encountering threats in a combat environment. Four T30 targets were delivered to the United States Marine Corps and additional targets, as well as other versions, are available through purchase and lease options.

Task Force Officer Mobile Learning and Performance Support

Task Force Officers (TFOs) have increasingly complicated jobs and ever-increasing bodies of knowledge they must reference in order to execute their work effectively. As demand increases, the rules, regulations, and role-specific considerations are becoming more difficult to navigate. In addition, TFOs are often away from a computer or traditional training venue due to this significant demand. Mobile devices allow for the delivery of training content and just-in-time information anytime, anywhere, thereby overcoming geographical and time constraints. The TFO Mobile Learning and Performance Support application, developed by Float, LLC, provides TFO training content on smartphones and tablets to augment existing training. The on-demand training and performance support material covers topics such as human trafficking, financial crimes, and smuggling to optimally prepare TFOs to perform their duties alongside federal law enforcement partners. For more information about accessing the app, please contact the Training Technology Development Subgroup.

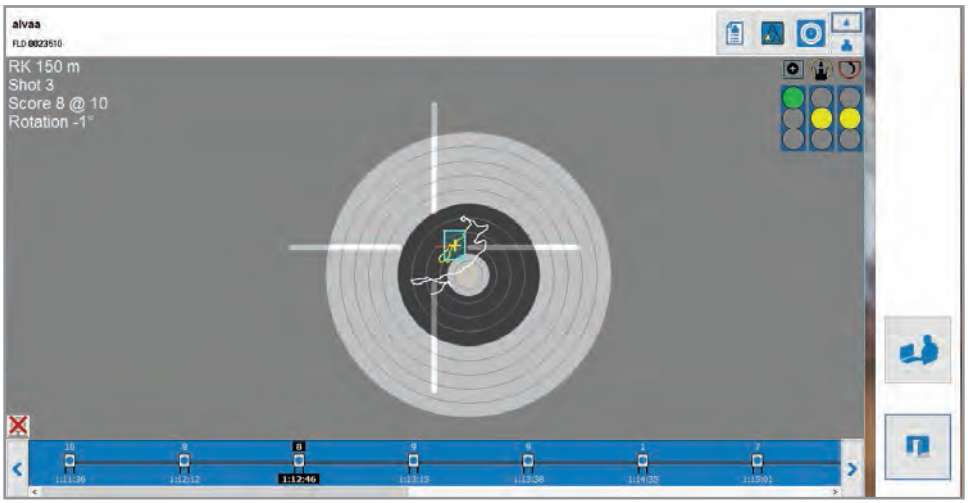




ONGOING PROJECTS

Automated Diagnostic Capability: Marksmanship Training

Proficient marksmanship is critical for military and law enforcement personnel. Even the most experienced instructors find proficient marksmanship training a challenge to teach due to the fine motor skills it requires. The Automated Diagnostic Capability: Marksmanship Training (ADCMT), developed by Quantum Improvements Consulting, will automatically diagnose shooter problems, enhancing an instructor's ability to rapidly identify root causes and provide accurate tailored feedback to advance shooter performance. The ADCMT's precision will increase marksmanship training efficiency and effectiveness by improving marksmanship skills and reducing ammunition requirements, range requirements, and overall instructor workload.



Force Assessment Simulation Tool (FAST)

There is a direct relationship between the amount of past relevant experience and the probability of success of officers when dealing with non-compliant subjects. Without past experience, an officer's decision-making and reaction time increases, often leading to adverse consequences for both officers and subjects. While there is no substitute for experience achieved through real-life encounters over years of field work, the Force Assessment Simulation Tool (FAST) seeks to expand and accelerate officer's knowledge through scenario-based interactive training. FAST, being developed by Carley Corporation, will use gaming technology to provide law enforcement officers with simulated scenarios in which they must interact with individuals and environmental conditions to determine appropriate responses. FAST aims to improve retention of lessons learned, reduce decisional stress, decrease potentially dangerous lags in decision-making time, and minimize unfavorable outcomes between officers and subjects. Within each scenario, officers will be given opportunities to discern potential threat indicators; make real-time decisions on the use of force; gain a practical understanding of laws, policies, attitudes, and biases; and gain insight into their own propensity to make choices that escalate or de-escalate tensions. Each scenario will include post-scenario assessments, customized feedback, and instructor reports on student performance.

Virtual Reality Part Task Trainer

The Air Force Special Operations Command (AFSOC) is leveraging advanced technology for warfighting readiness application. Special operations aircraft are in high demand in multiple theaters, limiting the availability of training aircraft at home station. Additionally, many training readiness capabilities and methodologies were developed over 40 years ago and are limited in their ability to provide immersive environment mission fidelity, streamlined and rapid response modification, and affordability. The AC-130 Virtual Reality Part Task Trainer (vrPTT) project aims to overcome these limitations through an interactive 3D high-definition virtual reality training environment integrated with an automated intelligent virtual instructional tutor. The vrPTT will consist of an untethered, wearable, and lightweight visual display linked to a high capacity computer. AFSOC personnel will be able to view, manipulate, and operate 3D high-definition virtual images of aircraft mission systems and components through "bare-handed" interactive functions to provide real-time feedback (i.e., touch, move, operate, and access selectable exploded views of components). The automated and interactive intelligent tutoring program will adjust in complexity based on graduated skill development, and will include task performance evaluation and remediation. The recently tested alpha version of the vrPTT has received positive feedback from AFSOC and USSOCOM. Two fully functional vrPTT systems will be delivered to AFSOC, which is planning to develop the system further to include all AC-130J crew positions.

Tools and Techniques to Optimize Human Cognitive Performance

Maksim Kabakou/Adobe Stock

There are a number of commercially available applications and tools used by the United States and United Kingdom Special Operations Forces to optimize cognitive performance. Because there is mixed evidence to support industry claims that these applications and tools optimize cognitive performance in the real world, this effort aims to provide unbiased scientific evidence regarding their actual utility. A literature review was conducted to identify commercial products, followed by a review of the underpinning scientific evidence. Based on these reviews, the Neurotracker training program was selected for further research, development, test, and evaluation. Empirical studies are being conducted to determine whether Neurotracker could have real-world benefit to operators. Studies will initially take place with a student population to explore performance gains and determine the most efficient way (frequency/length) to use the training program. Additionally, collaborative relationships have been established with other research groups investigating the utility of the Neurotracker training program for military tasks. Research findings will be made available to the United States and United Kingdom defense and interagency organizations.

City Life: Illusion of Life in a City Environment

The objective of City Life is to improve the quality of simulation-based training by providing a more realistic virtual reality (VR) environment that simulates life typical of a real city. The VR environment will immerse students into representative scenarios for training skill sets such as surveillance, security, and personnel protection. City Life will feature realistic indoor and outdoor structures and spaces (i.e., residential and commercial) for one generic North American city and one generic foreign city. Unique, non player characters (NPC) in quantities approaching 10,000 will move and interact inside and outside the structures exhibiting realistic human behaviors over a 24-hour cycle. The student-controlled avatars will be able to observe the NPC behaviors and, in certain cases, engage in purposeful interaction. City Life is a significant improvement upon existing immersive training simulation in terms of realistic patterns of life within a virtual city space thereby increasing the capabilities of United States and Canadian military and interagency personnel.

MEMBERSHIP

Intelligence Community

InterAgency Board

National Bomb Squad Commanders Advisory Board

National Tactical Officers Association

U.S. Department of Defense

- Advanced Distributed Learning Initiative
- Defense Intelligence Agency
- Joint Improvised-Threat Defeat Organization
- Office of the Under Secretary of Defense for Personnel and Readiness
- Pentagon Force Protection Agency
- U.S. Army Asymmetric Warfare Group
- U.S. Marine Corps
  - U.S. Marine Training and Education Command
  - Weapons Training Battalion
- U.S. Special Operations Command
  - Joint Special Operations Command
  - Air Force Special Operations Command
  - Army Special Operations Command
    - 75th Ranger Regiment
    - U.S. Army John F. Kennedy Special Warfare Center and School
  - Naval Special Warfare Command

U.S. Department of Homeland Security

- Customs and Border Protection
- Federal Law Enforcement Training Center
- Immigration and Customs Enforcement
  - Homeland Security Investigations
- Protection and Programs Directorate
  - Office for Bombing Prevention
- Science and Technology Directorate
- Transportation Security Administration
- U.S. Coast Guard
- U.S. Secret Service

U.S. Department of Justice

- Bureau of Alcohol, Tobacco, Firearms and Explosives
- Federal Bureau of Investigation
- Office of the Attorney General
- U.S. Marshals Service

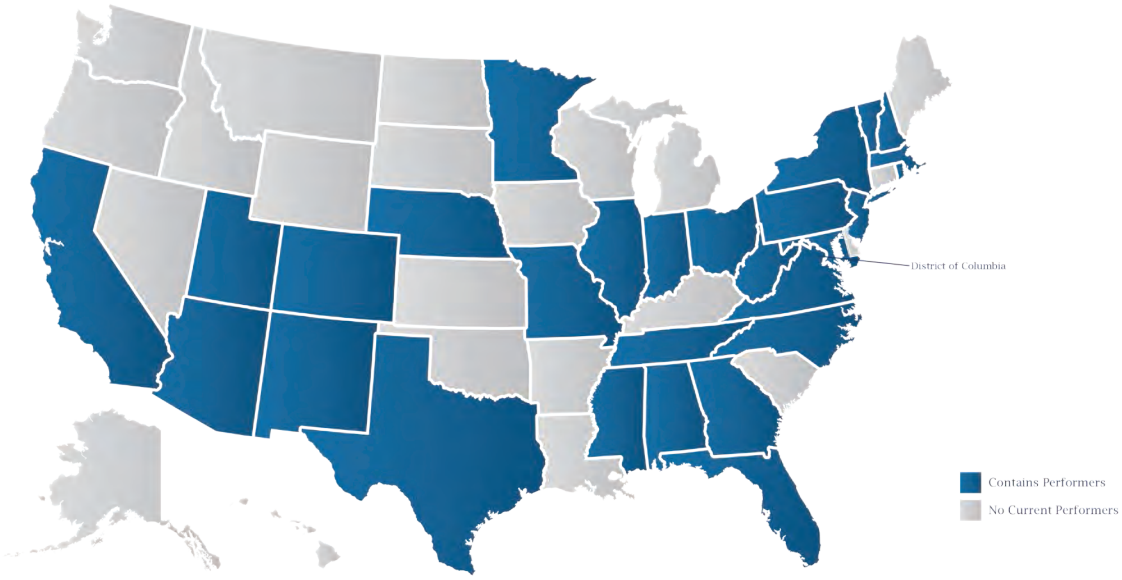
U.S. Department of State

- Bureau of Counterterrorism and Countering Violent Extremism
- Bureau of Diplomatic Security

U.S. Department of the Treasury

- Financial Crimes Enforcement Network

2017 PERFORMERS



International Performers

Alabama

Army Aviation and Missile Research, Development, and Engineering Center (AMRDEC), Redstone Arsenal

Kailos Genetics, Inc., Huntsville

Arizona

Impact Research and Technology, LLC, Phoenix

Metris, LLC, Mesa

SAIFE, Inc., Tempe

STARA Technologies Corporation, Gilbert

University of Arizona, Tucson

California

AeroVironment, Inc., Simi Valley

Baker Engineering and Risk Consultants, Inc., El Segundo

Decision Sciences International Corporation, Poway

Gantz-Mountain Intelligence Automation Systems, Inc., Carmel Valley

Karagozian & Case, Inc., Glendale

Lawrence Livermore National Laboratory, Livermore

Naval Health Research Center, San Diego

Naval Postgraduate School, Monterey

Seacoast Science, Inc., Carlsbad

Spectral Labs, Inc., San Diego

SRI International, Menlo Park

Tek84 Engineering Group, San Diego

Colorado

Applied Research Associates, Inc., Littleton

NEK Advanced Securities Group, Inc., Colorado Springs

RadiantBlue Technologies, Inc., Colorado Springs

District of Columbia

Department of Homeland Security Science and Technology Directorate

Naval Research Laboratory

Florida

Carley Corporation, Orlando

Florida International University, Miami

Naval Surface Warfare Center, Panama City

Navy Experimental Diving Unit, Panama City

Ocean Optics, Inc., Dunedin

Quantum Improvements Consulting, Orlando

WinTec Arrowmaker, Inc., Tampa

Georgia

Georgia Tech Research Institute, Atlanta

Illinois

Float, LLC, Morton

Motorola Solutions, Inc., Schaumburg

Vertex Solutions Group, Urbana

Indiana

Naval Surface Warfare Center, Crane

Maryland

Army Communications-Electronics Research, Development and Engineering Center (CERDEC) Intelligence and Information Warfare Directorate (I2WD), Aberdeen Proving Ground

Army Research Laboratory, Aberdeen Proving Ground

Army Test and Evaluation Command, Aberdeen Proving Ground

Avon Protection Systems, Inc., Belcamp

Edgewood Chemical Biological Center, Aberdeen Proving Ground

Efficio, Inc., Laurel

ELTA North America, Fulton

GromaTech, LLC, Laurel

Intelligent Automation, Inc., Rockville

Johns Hopkins University Applied Physics Laboratory, Laurel

Mistral, Inc., Bethesda

National Biodefense Analysis and Countermeasures Center, Frederick

Naval Surface Warfare Center, Explosive Ordnance Disposal Technology Division, Indian Head

W.L. Gore & Associates, Inc., Elkton

Massachusetts

908 Devices, Inc., Boston

Blauer Manufacturing Company, Boston

Crimson Hexagon, Boston

Infoscitex Corporation, Littleton

Navy Clothing and Textile Research Facility, Natick

Raytheon BBN Technologies, Cambridge

Systems & Technology Research, Woburn

Minnesota

GreenZone Systems, Inc., Minneapolis

Mississippi

Applied Research Associates, Inc., Vicksburg

Army Engineer Research and Development Center, Vicksburg

Hyperion Technology Group, Inc., Tupelo

Kopis Mobile, LLC, Flowood

MAC, LLC, Bay Saint Louis

Open Technology Center, Camp Shelby

Missouri

MRIGlobal, Kansas City

Nebraska

National Strategic Research Institute, Omaha

New Hampshire

Gentex Corporation, Manchester

Kollsman, Inc. / Elbit Systems of America, Merrimack

L-3 Communications Corporation – Warrior Systems Sector, Londonderry

New Jersey

Signature Science, LLC, Egg Harbor

SRI International, Princeton

Transportation Security Laboratory, Egg Harbor

New Mexico

Energetic Materials Research and Testing Center, Socorro

Sandia National Laboratories, Albuquerque

New York

EJ2 Communications, New York

Intertek, Cortland

Lockheed Martin Mission Systems and Training, Owego

Mastodon Design, LLC, Rochester

Med-Eng, LLC, Ogdensburg

PAR Government Systems Corporation, Rome

North Carolina

Advanced Mission Systems, Charlotte

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

Ohio

Air Force Research Lab, Dayton

Battelle Memorial Institute, Columbus

Lion Apparel, Inc., Dayton

Pennsylvania

Gentex Corporation, Simpson

Rhode Island

Naval Undersea Warfare Center, Newport

Tennessee

Digital Reasoning Systems, Inc., Franklin

Texas

Baker Engineering and Risk Consultants, Inc., San Antonio

International Personnel Protection, Inc., Austin

Laser Shot, Inc., Stafford

National Aeronautical Space Administration (NASA), Houston

Protection Engineering Consultants, LLC, Austin

Southwest Research Institute, San Antonio

Stratfor Enterprises, LLC, Austin

Utah

Dugway Proving Ground, Dugway

Vermont

Deep Analytics, LLC, Montpelier

General Dynamics Ordnance and Tactical Systems, Williston

Virginia

Applications Technology (AppTek), LLC, McLean

ATA, LLC, Vienna

Babel Street, Reston

Battelle Memorial Institute, Arlington

BCF Solutions, Sterling

Booz Allen Hamilton, Inc., McLean

CACI International, Inc., Sterling

CONTROP USA, Inc., Manassas

D A LABS, Arlington

ECS Federal, LLC, Fairfax

Ideal Innovations, Inc., Arlington

In-Q-Tel, Arlington

Information Systems Worldwide, Arlington

IST Research, Fredericksburg

L-3 Technologies, Leesburg

ManTech International Corporation, Chantilly

Millennium Engineering and Integration Company, Arlington

MITRE Corporation, McLean

NAL Research Corporation, Manassas

National Ground Intelligence Center, Charlottesville

Naval Special Warfare Development Group, Virginia Beach

Naval Surface Warfare Center, Carderock

Naval Surface Warfare Center, Dahlgren

NexGen Communications, LLC, Dulles

Night Vision and Electronic Sensors Directorate, Ft. Belvoir

Novetta, Inc., McLean

Novetta, Inc., Reston

Oceans Edge, Inc., Reston

PAE National Security Solutions, LLC, Fredericksburg

Planet Risk, McLean

Progeny Systems Corporation, Manassas

Raytheon Blackbird Technologies, Inc., Herndon

Research Innovations, Inc., Alexandria

Resonate Learning Consultants, LLC, Reston

Roka Security, Herndon

Sphere of Influence, Inc., McLean

Stone Smart Solutions, LLC, Arlington

System of Systems Analytics, Inc., Fairfax

Technical Intelligence Solutions, LLC, Herndon

White Canvas Group, LLC, Alexandria

West Virginia

Azimuth, Inc., Morgantown

Australia

Defence Science and Technology Group, Canberra, Australian Capital Territory

Defence Science and Technology Group, Edinburgh, South Australia

Defence Science and Technology Group, Fisherman's Bend, Melbourne, Victoria

Flinders University, Adelaide, South Australia

Marathon Targets, Sydney, New South Wales

Queensland University of Technology, Brisbane, Queensland

University of Adelaide, Adelaide, South Australia

University of Technology, Sydney, New South Wales

XTEC Limited, Symonston, Australian Capital Territory

Canada

AirBoss Defense, Acton Vale, Quebec

Defence Research and Development Canada, Medicine Hat, British Columbia

PyroGenesis Canada Inc., Montreal, Quebec

Royal Canadian Mounted Police, Regina, Saskatchewan

Uncharted Software, Inc., Toronto, Ontario

Ireland

D4H Technologies, Dublin

Israel

Ben Gurion University, Beer-Sheva

CS3 Composite Solutions, Inc., Holon

Elbit Systems, Ltd., Yokneam

IAI ELTA Systems, Ltd., Tel Aviv

Israel Defense Forces

Israel Ministry of Defense, Tel Aviv

Israel Security Agency, Tel Aviv

Pearls of Wisdom Advanced Technologies, Ltd., Kefar Netter

Prime Minister's Office

Rafael Advanced Defense Systems, Ltd., Haifa

Shilat Optronics Ltd., Rehovot

StemRad, Ltd., Tel Aviv

Tamar Explosives, Ltd., Tel Aviv

Technion – Israel Institute of Technology, Tel Aviv

University of Tel Aviv, Tel Aviv

Netherlands

Netherlands Organisation for Applied Scientific Research

Spain

SEDET, Valladolid

Singapore

Defence Science and Technology Agency

Sweden

Saab, Linköping

United Kingdom

Centre for the Protection of National Infrastructure

Defence Science and Technology Laboratory, Fort Halstead

Defence Science and Technology Laboratory, Porton Down

Landguard Systems, Ltd., Fareham

Ministry of Defence, London

WWW.CTTSO.GOV