WEAPONS TECHNICAL INTELLIGENCE HANDBOOK

VERSION 2.0
MARCH 2014

The WTI Handbook cover photograph depicts two Free Syrian Army fighters displaying an improvised mortar tube, mortar, and fuse, all of which were machined using equipment located in abandoned factories in rebel controlled Syria. *(Photo Credit: Reuters/Hamed Khatib)*

Comments or requests for copies of the most current edition of the WTI Handbook can be submitted to Joint IED Defeat Organization (JIEDDO) at jieddowti@jieddo.mil.

DISTRIBUTION STATEMENT X. Distribution authorized to U.S. Government Agencies, their contractors (Deputy Secretary of Defense Memorandum dated April 2006, Policy on Discussion of IEDs and IED-Defeat Efforts in Open Sources, 20120907; FOIA Exemption 2 applies), state and local law enforcement, and partner nations (disclosure and release of this document is authorized to Five Eyes [FVEY] and North Atlantic Treaty Organization [NATO] members). Department of Defense Controlling Office is JIEDDO J5 Division. Provision of this information does not imply a commitment on the part of the United States government to furnish, transfer, or export information or equipment referred to herein.

Preface

The Weapons Technical Intelligence (WTI) Handbook is a guide to help commanders, staff, and service members understand and apply WTI concepts, capabilities, and processes.

Through WTI's technical and forensic collection, exploitation, and analysis of terrorist and insurgent weapons, the US and partner nations are able to learn who the enemy is and how it operates. WTI provides the capability to identify individual insurgents and terrorists and link them to places, devices, and events, as well as their enabling network, leading eventually to their isolation, targeting and prosecution. The WTI Handbook is a single-source reference that:

- Prescribes the WTI framework
- Explains the WTI enterprise
- Informs intergovernmental agency and joint Services processes
- Influences future joint Services doctrine development

WTI is the enabling process that provides network attributions to Attack the Network (AtN), tactical and technical characterization to Defeat the Device (DtD) and tactical characterization of tactics, techniques, and procedures (TTP) that enable Train the Force (TtF). The Defense Intelligence Agency (DIA) and the Joint IED Defeat Organization (JIEDDO) are the proponents for WTI in accordance with Department of Defense (DoD) Directives 2000.19E and 5205.15E. Subject matter experts (SMEs) from DoD and the Department of Justice (DoJ) contributed to the developed of this publication. This Handbook complements established doctrine and serves as a single-source reference to prescribe the WTI framework by which WTI enabling capabilities and processes may be employed now and in the near future. This Handbook serves to inform various joint, service, and intergovernmental processes and may be used to influence future joint and service doctrine development.

Even as our presence in Afghanistan draws down, U.S. forces and our partner nations will continue to confront the dangers and challenges posed by improvised weapon systems and the networks that employ them globally. During the past thirteen years, we have met the challenge head-on, learning many lessons at great cost. It is the responsibility of the U.S. Department of Defense to capture, preserve and institutionalize these lessons and the knowledge, experiences and capabilities to address this growing worldwide threat both now and in the future.

Weapons Technical Intelligence (WTI) is one such capability. Developed in 2005, WTI is the organizing framework that synchronizes the disparate capabilities and processes conducting the technical and forensic exploitation of information and material associated with the improvised weapon threat and the asymmetric battlefield. This critical framework removes the veil of anonymity our adversary enjoys and enables the U.S. and partner nations to identify and target them.

Countering the improvised weapon threat requires a whole-of-government approach that synchronizes the efforts of our joint, interagency, intergovernmental and multinational partners, with the U.S. Department of Defense playing a crucial enabling role – both at home and abroad. The WTI Handbook Version 2.0 catalogues the important capabilities and processes that have contributed to this whole-of-government approach and provides commanders, their staffs and our interagency and intergovernmental partners a comprehensive guidebook to understand and apply WTI concepts, capabilities and processes.

Developed in conjunction with joint and interagency WTI subject-matter experts, this handbook reflects the WTI community’s most current judgments, conclusions, and lessons learned. The WTI Handbook Edition 2.0 does not replace or supersede established doctrine but rather compliments those texts and serves as a single-source reference for the WTI framework.

With this handbook, and close interagency cooperation, we can make sure we bring all of the U.S. government’s resources to bear against the dangers of improvised weapons systems and we are prepared for the challenges that lie ahead.

Michael T. Flynn

Michael T. Flynn
Lieutenant General, U.S. Army
Director, Defense Intelligence Agency

John D. Johnson
Lieutenant General, U.S. Army
Director, Joint IED Defeat Organization

APPENDIX

Executive WTI Review and Future Intent

By

Mr. Russell L. McIntyre

Chief, Office of Collection & Exploitation

Directorate for Science and Technology

Defense Intelligence Agency

Mr. McIntyre is a career intelligence officer who has served more than 40 years in intelligence billets from the tactical to strategic level. Mr. McIntyre has been instrumental in the establishment of and advancements to Weapons Technical Intelligence (WTI) and remains one of its most influential proponents.

Mr. McIntyre entered the Army in 1968 and retired from active duty in 1994. Career military highlights include: Leader of a Combined Tactical HUMINT Team assigned to the 173rd Airborne Brigade in the Republic of Vietnam; Strategic Debriefer, 18th Military Intelligence Battalion, Munich, Germany; Chief Targeting Officer, 75th Ranger Regiment; and in Joint Intelligence (J2) Operations, Special Operations Command Europe (SOCEUR). In addition, he helped to establish the Army's Survival, Evasion, Escape, and Resistance to Interrogation (SERE) course at Fort Bragg, NC.

Following his retirement from the U.S. Army, Mr. McIntyre returned to government service where he worked on issues involving transnational terrorism, counter proliferation, and foreign material acquisition for the Secretary of Defense. In 2003 Mr. McIntyre joined the Defense Intelligence Agency (DIA), Directorate for Measures and Signals Intelligence (MASINT) and Technical Collection where he helped to establish the Special Collections Coordination Center. Additionally, Mr. McIntyre served in Iraq at the Joint Operations (J3), Counter Improvised Explosive Device (IED) Cell, Multi-National Coalition-Iraq (MNC-I). Following his return from Iraq, he was named Chief for DIA's Irregular Warfare Branch, followed by his selection for the Defense Intelligence Senior Executive Service as the Chief, Forensic Intelligence Office. Mr. McIntyre currently serves as the Chief, Office of Collection and Exploitation, Directorate for Science and Technology at DIA.

Figure 1. The Long Walk. *An EOD Technician from the 717th OD CO (Explosive Ordnance Disposal [EOD]), approaches a suspected IED on Haifa Street, Baghdad as security elements provide overwatch on a hot day in August 2005.* (Photo Credit: USA)

Background

"IEDs will remain a threat in full spectrum operations. IEDs are not synonymous with or specific to the counterinsurgency environment. IEDs have a broader application to any adaptive networked threat that may challenge US forces engaged across the continuum of operations, from peacetime military engagement through major combat operations."[1]

Operating in a battlefield where IEDs were present (**Figure 1**) and posed a potent casualty-producing threat is not new to US forces. By 1967, IEDs produced battlefield casualties in South Vietnam, prompting a concerted Department of Defense (DoD) effort to develop countermeasures. Unfortunately, their impact and shaping effect in the battlespace were a distant memory when they reappeared in Iraq and Afghanistan. The dramatic impact IEDs can have on operations is illustrated as follows: "Previously collected data indicated that in Vietnam, during 1967, one-third of the casualties sustained in the units interviewed were from contact with mines and booby traps. Since mines and booby traps are likely to be used on future battlefields at least as much during the Vietnam conflict, a need clearly exists to improve the soldiers' ability to deal with these devices."[2]

To respond to the booby trap threat, the US Army Vietnam established the Mine Warfare Center, which directed operational field research to study the problem at the unit level, published training circulars, and harnessed the Combined Intelligence Center Vietnam to produce studies on enemy tactics, techniques, and procedures (TTP) based on enemy prisoner of war interrogations and technical evaluations of captured devices.

[1] COL Gerhald Muhl, Jr. USA, "Defeating Improvised Explosive Devices (IED) Asymmetric Threats and Capability Gaps," (U.S. Army War College, Carlisle Barracks, PA, 2011), pg. 22.

[2] Jeffery L. Maxey and George J. Magner *A Study of Factors Affecting Mine and Boobytrap Detection: Subject Variables and Operational Consideration, (*Alexandria, VA: Human Resources Research Organization, 1973), pg. 3.

In the Continental United States (CONUS), the US Army Material and Combat Development Command developed service and national level solutions to the booby trap threat. For example, "Kits were developed for armored personnel carriers to provide supplemental armor for the hull bottom and to relocate and strengthen the fuel line."[3] Other initiatives that the US Army Material and Combat Development Command investigated ranged from energy absorbing systems to reduce the shock of a mine explosion, observation towers, expendable mine rollers, and the inducement of electrical current in the mine's initiation system using radio frequencies to remotely disable the device. An elegant technological solution was not found before the termination of US ground combat operations in Vietnam, and the Service's efforts to mitigate or neutralize the booby trap threat ended as well.

Unfortunately, the persistent threat of booby traps was effective in negatively impacting the behavior of friendly forces in the field. "Just the knowledge that a mine or booby trap could be placed anywhere slowed combat operations and forced allied troops to clear almost the entire Vietnam road network every day."[4] By the end of US military operations in South Vietnam, the mine and booby trap threat accounted for 70 percent of all vehicle losses and 20 percent of personnel casualties.

After the Vietnam War, the Services refocused their institutional energies on rebuilding and modernizing their forces to fight the main enemies, the Soviet Union and the Warsaw Pact. LTC Phillip W. Carroll (USA) voiced the concern that the IED, improvised weapon, mine and/or booby trap threat would remain, ready to populate a future battlefield. In 1988 he wrote "Understand the threat in the low intensity conflict will use mine/booby trap operations much like those currently experienced in Malaysia and Thailand and like our Viet Nam [sic] experiences of 20 years ago. The enemy force's doctrine for employment will change very little from our past experiences because it is simple, resource feasible, trainable and easily exportable, and historically it works." [5] Unfortunately, the message that IEDs posed a future threat was not significant enough to gain senior-level decision makers' attention. The threat was noted but did not in a way that garnered support for a dedicated collection, exploitation, and analytic program to monitor its evolution and distribution throughout the Combatant Commands.

At that time, analysis and collection efforts were directed at assessing an evolving Soviet threat that, since the beginning of the Vietnam War, was significantly upgrading its conventional and strategic force capabilities. While Soviet capabilities were evolving, insurgents and terrorists were busy developing and innovating IED design and employment concepts outside of the realm of immediate US global security interests to negatively shape the battlespace. Improvised weapons and IEDs were used by the Provisional Irish Republican Army (PIRA) against British forces in Northern Ireland, by Euskadi Ta Askatasuna (ETA) in their campaign for the succession of the Basque region from Spain, by the Revolutionary Armed Forces of Colombia (FARC) in Colombia (with technical assistance provided by PIRA), and by Hezbollah in Southern Lebanon against the

[3] LTG John Hay, USA, *Vietnam Studies: Tactical and Material Innovations*, Publication 90-21. (Washington, DC: Department of the Army, Center for Military History. 1974), pg. 131.

[4] LTG Julian J. Ewell, USA and MG Ira A. Hunt, Jr., USA, "Vietnam Studies: Sharpening the Combat Edge The Use of Analysis to Reinforce Military Judgment, Department of the Army, Washington, D.C. 1974, pg. 147.

[5] LTC Philip W. Carroll III USA, *Mine and Booby Trap Warfare: Lessons Forgotten*, US Army War College, Carlisle Barracks, PA, February, 1988, pgs. 14-15.

Israeli Defense Forces (IDF) and Lebanese Army. In all of these instances, the IED was effective, requiring significant military and scientific resources to suppress and mitigate it. [6]

An Army Center for Military History Study on the Vietnam War published in 1974 highlighted the error. "There was one area where American ingenuity failed: countermine warfare. Considering the magnitude of the enemy's effort in mines and booby-traps , US experts failed to find the answer to the problem of how to counter them."[7] Unfortunately, the threat remained – and evolved.

Figure 2. Clearing a Route. *Bravo Company soldier from the 1st Battalion, 6th Infantry Regiment, assigned to Task Force 1-35 Armor, 2nd Brigade Combat Team, 1st Armored Division, patrols the road as a canal burns in Tahwilla, Iraq on July 30, 2008. Extremists used the cover that the intricate canal system provides to emplace IEDs at night. (Photo Credit: USA)*

Iraq: The IED Cauldron

"The IED problem is getting out of control … We have to stop the bleeding.."[8]

"Beginning in June 2003, IED incidents targeting coalition forces began to escalate from 22 per month to over 600 per month by 2004."[9]

[6] NOTE: There was a robust exchange of information between the EOD Technicians in the countries mentioned and Defense Intelligence; however, the fruits of that analysis fell within the purview of the CT analytic community then regarded as a niche threat area for investment of time and resources.

[7] Hay, *Vietnam Studies: Tactical and Material Innovations*, pg. 181.

[8] NOTE: Comments made by then Army Deputy Chief of Staff for Operations LTG Richard A. Cody cited by Rick Atkinson, in his seminal series of articles on the Counter-IED effort published by the Washington Post from September 30, 2007 to October 02, 2007. Rick Atkinson's complete set of The *Washington Post* articles on the IED threat can be found at the online Small Wars Journal's September 30, 2007 post "Weapon of Choice." It contains hyperlinks to the series: http://smallwarsjournal.com/blog/weapon-of-choice-updated

[9] Government Accounting Office, *Actions Needed to Improve Visibility and Coordination of Counter-IED Efforts*, GAO Report 10-95, October 2009, pg. 9.

Figure 3. The IED: Weapon and Propaganda Tool. *The pictured US Army HMMWV is about to be engaged by an insurgent IED in 2005. (Photo Credit: Task Force Troy)*

Prior to the coalition's invasion in March 2003, the primary technical intelligence (TECHINT) collection and exploitation task for Central Command (CENTCOM) was Iraqi Weapons of Mass Destruction (WMD). As the invasion proceeded, the suspected locations of WMD munitions and production activity were either empty or damaged beyond reconstitution by CENTCOM's previous air and cruise missile campaign. The threat that emerged was not a chemical, biological, or nuclear weapon, but rather one of a battlefield's most basic weapon, the IED (**Figure 2 and Figure 3**). "When Operation Iraqi Freedom (OIF) commenced in March 2003, the IED was not a threat to US ground forces. However, by the summer of 2004 the IED threat in Iraq was credible, prevalent, and lethal. Five years later in 2008, the IED became part of the US military vernacular."[10]

The emphasis for the TECHINT community in Iraq, and to a lesser degree in Afghanistan, was the discovery of state and terrorist group produced weapons of mass destruction and other conventional weapons systems for later exploitation. Per Joint Doctrine, CENTCOM requested a Joint Captured Material Exploitation Center (JCMEC) be deployed to support its TECHINT requirements. The JCMEC, anchored by the 203rd Military Intelligence (MI) Battalion (Bn) and augmented by the joint TECHINT community and by contributions from Coalition partners. During pre-Iraqi invasion planning, CENTCOM did not anticipate a need for this capability to remain in theater beyond one calendar year. It was not for a lack of will or desire to support the warfighter that the 203rd MI Bn returned to CONUS; it was a force structure problem. The 203rd was the Services' Technical Intelligence unit, designed for a short war and comprised of Active Duty Army and Reservist personnel.[11] The 203rd MI Bn provided Weapons Intelligence Teams

[10] CPT Joseph M. Garaux, USMC, "The IED Fight: Technical Shortcomings and the Value of Strategy," *Marine Corps Gazette*, January 2010, pg. 8.

[11] 2LT Daniel R. Arnold, U.S. Army Reserve, "The 203rd MI Battalion (Technical Intelligence) in Operation IRAQI FREEDOM," *Military Intelligence Professional Bulletin*, 31, no.1, January-March 2005:, pgs 41-46, cont pg 55. NOTE: The author deployed with the battalion to Iraq and this article provides an excellent overview of the unit's activities and accomplishments performing its Technical Intelligence mission. The battalion ran over 400 collection missions that resulted in the largest U.S. TECHINT effort since World War II.

(WITs) to assist in IED site exploitation in Iraq beginning in 2005. However, the personnel with the experience to manage a theater-wide exploitation effort departed theater with the Bn headquarters and staff. In Iraq, the C-IED Task Force (Task Force Troy) and its equivalent in Afghanistan (Task Force Paladin) were established to synchronize the C-IED effort and manage IED event material collection, exploitation, and analysis. Troy and Paladin helped mitigate the gap caused by the absence of a theater JCMEC structure.

Coalition forces were suffering casualties from IEDs with little opportunity to kill or capture the enemy. The emplacer disappeared into an urban maze or hid in plain sight in the inevitable crowd of onlookers after an attack. The Brigade Combat Teams (BCT) lacked intelligence assets, including tools, training, reach back support, and an analyst staff to respond effectively. As a result, they could not begin the process of defining networks, characterizing their activity, and developing targeting strategies to eliminate them. The enemy was fluid and adaptive, evidencing the characteristics of a complex adaptive system. A complex adaptive system is "… a dynamic network of agents that act in parallel, constantly framing and reframing in reaction to the external environment. Its control is highly dispersed and decentralized. Its behavior arises from competition and cooperation. There is little to no control — the collective action of the complex adaptive system is a result of a near infinite number of decisions made concurrently by the constituent agents from which it is comprised." [12]

The IED was an unexpected and highly disruptive threat imbedded in a burgeoning and rapidly evolving insurgency. In the early stages of OIF there was no concerted intelligence-led response to understand and suppress the IED threat. It was not until November 2004 that the Multi-National Corps Iraq (MNC-I) made collection on IED bomb makers and their associated networks a priority intelligence requirement (PIR).

To counter the IED threat, the Commander and his staff needed a constant flow of information to fuse analysis so that they could adapt, adjust, and tailor their targeting approach and force protection measures for their respective operational area. The Commander's need for a steady flow of intelligence reporting, beginning with tactical assessments at the scene of the IED event or find, was a key driver in developing the WTI process. The WTI approach focused on horizontal integration and analysis of raw, incoming intelligence data obtained from collection and exploitation occurring in the battlespace. Subsequent levels of exploitation and analysis provide finished intelligence products that result from the more traditional, vertically integrated approach, with value added as the report moves up echelon. "Because the integration process is operating at the data level of the intelligence cycle, temporal, spatial, and logical merging of these multiple sources or information

[12] LTC Ian Langford, "Understanding and Defeating a Complex Adaptive System," *Australian Army Journal*, Volume IX, no. 3, (Summer 2012); pg. 108.

can take place in nearly real time."[13] The horizontal integration and analysis of intelligence data was enabled and refined by the introduction of the Army's Company Intelligence Support Team (COIST) and the Marine Corps' Company-Level Intelligence Cell (CLIC).

The COIST or CLICs gave tactical Commanders an intelligence-driven picture of their immediate operational area, feeding data latterly and up to the Bn S2. They served as a conduit for the provision of higher level analysis down to the tactical edge. "A Company's fusion cell combined battalion intelligence with company intelligence, generated from knowledge of the population, to facilitate better planning and execution of lethal targeting. This allowed our company to correctly discriminate threats from the general population and execute raids to neutralize these threats." [14]

Enabling optimum situational awareness required systematic and thorough post-event evaluation, collection, and exploitation processes. These processes had to be sufficient in scope and fidelity to detect early changes in enemy tactical and technical approaches, characterize their effectiveness, and then communicate findings efficiently and accurately. Commanders did not have the tools, training, equipment, staff, or special troop support to respond with precision and effectiveness. They needed continuous reporting to address a range of outcomes (e.g., targeting, force protection, and component material sourcing) that the TECHINT community was not designed, manned, or equipped to provide.

With the JCMEC's departure, the collection and threat assessment of this new pervasive insurgent threat fell to Service EOD units and their intelligence officers. On the fly, EOD units began piecing together a framework of collection and exploitation capabilities to understand and help counter the IED threat. The initial response was led by then LTC Dick A. Larry, USA, Commander of the 63rd EOD Bn, who established the first Combined Explosive Exploitation Cell (CEXC) to provide detailed exploitation of IEDs and their components. These early, nondoctrinal responses included:

- The Navy's very successful and innovative Combined Explosive Exploitation Cell (CEXC) built on LTC Larry's early initiative, and which later evolved into a Joint and combined entity with participation by the, allied nations, DIA, FBI Services, and the Bureau of Alcohol, Tobacco and Firearms (ATF)
- WITs to assist in IED incident reporting and trend analysis
- Counter IED Targeting Program (CITP) analytic effort by the National Ground Intelligence Center (NGIC)

[13] Brian A. Jackson, et al., "What Do We Need to Know and How Do We Learn It?" Project Memorandum 1929-OSD, RAND Corporation, Arlington, VA, October 2005. pg. 51. (NOTE: This publication was part of a series of field surveys based operational assessments of existing MNF-I counter-IED capability directed by the Joint IED Defeat Organization, funded by the Under Secretary of Defense for Acquisition, Technology & Logistics and supported by Mr. Ben Riley of Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics. The goal of the effort was to insert RAND staff with field operating elements to provide observations and recommendations to the then Director of JIEDDO, BG Joe Votel, USA, on the efficiency of fielded support by JIEDDO and identify opportunities that would assist in the C-IED fight. Interestingly, this report, published in October 2005, identified the benefit of the horizontal processing of intelligence data at the lower tactical levels to enable units attacking local insurgent networks and affiliated networks. Later, both the Army and Marine Corps introduced company level intelligence support teams with great success.)

[14] 1LT David Liebmann, et al., "COIN and Company Fusion Cell Operations", *Infantry Magazine*, January-April 2010, pg. 30.

- Incorporation of latent finger prints recovered from IED components by NGIC at the CEXC located in Camp Victory
- Fielding of vehicular mounted electronic countermeasures by US Navy Electronic Warfare Officers to provide technical field support to tactical formations

Much of the aforementioned effort was funded by the US Army Counter IED Task Force that transitioned in 2006 to the Joint Improvised Explosive Device Defeat Organization (JIEDDO). In 2004, the first phase of the focused, departmental response to the IED threat began. Service EOD Technicians' onsite collection and exploitation activities were instrumental to effective threat response and allowed the coalition to begin characterizing the nature of the threat they faced. The CEXC led the way by combining technical, biometric, and forensic exploitation tools and processes to maximize the benefit from recovered material.

The WTI process was established to provide an organizing framework to support the expanded scope of collection and exploitation capabilities that began in theater in 2004. The process began with the definition of five specific outcomes that include:

- Force protection
- Attack the network
- Component and material sourcing
- Prosecution of captured insurgents
- Signature development for IED emplacements and fabrication processes and material usage

These processes expanded traditional TECHINT outcomes with a greater emphasis on achieving a broad collection and exploitation effort designed to support tactical Commanders operating in a high-threat IED environment. The payoff for Commanders begins with initial analysis of the IED event or find. Each stage of the exploitation and analytic process adds value as material moves up through the theater and national level laboratory systems. Providing constant feedback on enemy IED technical and tactical emplacement evolutions was the principle driver in shaping and designing of the WTI process.

Tools for Adaptation: Building the Foundation

"The rise of the improvised explosive device (IED) as the insurgent weapon of choice combined with the loosely coupled decentralized command and control structure demanded developing new intelligence methods and strategies."[15]

The rapid introduction of new collection and exploitation capabilities and processes into the Iraq theater increased Service EOD capability and included fielding specialized intelligence, surveillance, and reconnaissance (ISR) platforms to detect IED emplacements and processing results of newly introduced wide area surveillance systems. At the same time, it created new challenges. The key challenge was in managing information while simultaneously making it discoverable across the battlespace. The theater's early C-IED effort lacked the following:

[15] Richard Crawford and LtCol Adam Tharp, USMC, "Role of Law Enforcement Professionals in Attack the Network Strategy," *Air Land Sea Bulletin, 2012-3 (September 2012:*, pg. 27.

- A common lexicon to provide a coherent conceptual framework and operational vocabulary to address the IED threat
- IED symbols that portray previous enemy activity for use in automated battle command systems (explosions, caches, finds, false alarms, hoaxes)
- An IED event, exploitation, analysis, and reporting schematic, consisting of, three, and later five "herring bone" diagrams that graphically portray all steps in the WTI process, based on the Ishikawa or Fishbone Diagram. These diagrams are designed to illustrate complex processes and the interrelationships of all actors that contribute to the process incorporating material exploitation and information flow mapping
- Defined levels of exploitation with associated responsibilities and scope of associated activity, including process outputs with timelines for process completion

To address the four basic needs iterated above, DIA, in collaboration with JIEDDO, developed WTI in 2005. WTI was established to provide the organizing framework, processes, and procedures required to synchronize and structure existing ad hoc capabilities and responses in theater. New partners were introduced, including the FBI's newly established Terrorist Explosive Device Analysis Center (TEDAC); the ATF, which provided field post-event analysis training; and the Services' contributions, including the Army's Intelligence and Information Warfare Division (I2WD), US Army National Ground Intelligence Center (NGIC), and US Navy Indian Head Explosive Ordinance Disposal Technical Division (IHEODTD), formally known as NAVEODTECHDIV. The Service's EOD Technicians and units are important contributors to the WTI process but were not previously considered to be battlefield collection and site/event exploiters. "Before 9/11 few Commanders would have considered EOD units as members of the Combined Arms Team. After 9/11 with the reemergence of the improvised explosive device (IED) as a weapon of war, the paradigm changed."[16] That paradigm shifted because, "EOD forces are unique because of their mission to 'render safe' explosive ordnance. This has made EOD a much sought after and necessary combat enabler (**Figure 4**). EOD forces also provide explosive ordnance exploitation which includes assisting in the collection and safe handling of explosive components of IEDs; plus their fuzing and firing systems, without destroying these critical bomb making components."[17] That capability was critical to identifying bomb makers and their networks.

[16] COL Dick A. Larry, USA, "Evolution of EOD in the Combined Arms Fight," *Air Land Sea Bulletin, 2009-2, (*May 2009): pgs. 21-22.

[17] COL Larry, USA, "Evolution of EOD", pg. 21.

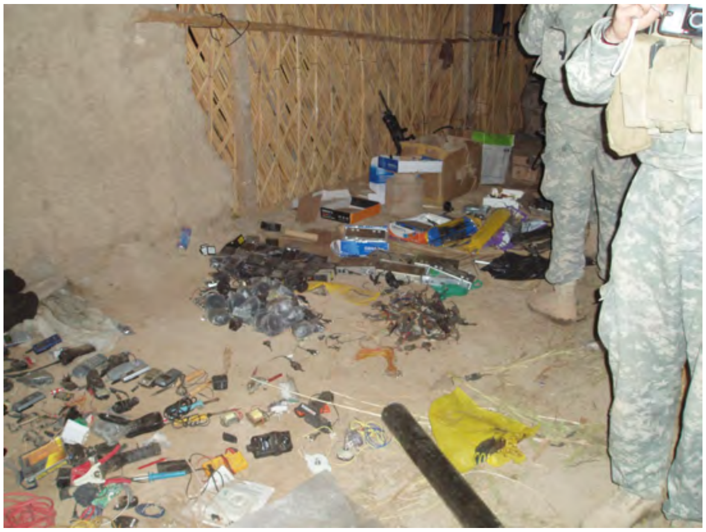


Figure 4. EOD Team Records IED Materials Cache. *An EOD team from the 717th OD CO (EOD) captures images of IED components and bomb making materials seized during a raid conducted by the 502nd BCT, 101st Airborne Division (Air Assault) near Baghdad in Dec 2005. (Photo Credit: SFC Herndon, 717th OD CO [EOD])*

Exploitation and WTI

"The ability to provide time-sensitive, actionable intelligence to the Combatant Commander is the purpose of IED exploitation. The intelligence derived from forensic analysis is fused with existing intelligence regarding the insurgent or event. The result is fully integrated into existing military intelligence systems and processes and transmitted to the battle space owner in a timely fashion so the Commander can maximize the use of the information."[18]

WTI began as a cross functional capability led by EOD Technicians and tactical, on-scene Commanders starting at the point of contact with the enemy and device, feeding and analyzing data, and adding value at each level of exploitation, analysis, and data fusion (**Figure 5**). "The mission of completing a post-blast investigation had grown for EOD forces based on the operational requirements of the battlefield. Post-blast investigation is an important bottom-up intelligence activity that supports defeating the IED network." [19] [20]

[18] COL Gerhald Muhl, "Defeating Improvised Explosive Devices (IED) Gaps," pg. 10.

[19] Combined Arms Center, Center for Army Lessons Learned, *Commander's Guide to EOD Operations: Observations, Insights, and Lessons,* Handbook No. 10-20, Fort Leavenworth, KS, January 2010: pg. 3.

[20] NOTE: To compliment site exploitation of IED events the US Army Intelligence Center and School established a Weapons Intelligence Team training program. The WTIs have evolved to provide an EOD lead and intelligence driven site exploitation capability for a range of events and finds addressing the Commanders' Priority Intelligence Requirements. A description of WIT training and its background can be found in the following article; Chris Britt, MAJ, USA, "WIT – The Battlefield Commander's Force Multiplier in the CIED Fight," *Military Intelligence Professional Bulletin,* 35, no 2, (April-June 2009): pgs. 51-55.

Figure 5. CEXC Field Lab. *A Navy EOD Technician examines IED components at one of the Navy's innovative forward deployed CEXCs. (Photo Credit: USN)*

Because the IED was the primary and most effective weapon of the insurgent, improving WTI collection and exploitation capabilities became the priority of the steadily expanding network of specialist troops (e.g., EOD units, Explosive Detection Dogs, and WITs) in theater and field deployed laboratories. These expeditionary exploitation laboratories were backstopped at the national level by Service exploitation centers and TEDAC. After an IED incident, it was rare for the attacked unit to find and discover the device emplacer. But the IED incident was the one time that the enemy showed his head above the parapet, not exposing so much his person, but rather his operative persona — how he thought, where he procured device materials, and who his associates were, all of which could yield information that links device to parent networks.

"The detonation of an IED on the battlefield is the culmination of a series of enemy actions. The IED cycle is part of a system relying on experts in supply, explosives, personnel, terrain, and tactics. While much has been written on systems both in military and civilian literature, IEDs represent a complex enemy weapon "system" made up of several parts – to include insurgent networks – bringing a level of complexity to what is seemingly a simple "device."[21]

IED design, fabrication, emplacement, and use employs a complex process that requires an open, adaptive system to exploit it to support multiple end users with a range of needs to support varied activities. The need for a capability to maximize the yield from an IED event or cache discovery drove the development of the WTI collection, exploitation, and intelligence fusion process. To meet customer needs, the WTI process had to provide a range of outcomes that addressed the following:

- Event characterization
- Force protection
- Support to targeting

[21] MAJ Rick Black and MAJ Rob Kelly, "3rd Infantry Division Improvised Explosive Device Defeat Cell Operations in Operation Iraqi Freedom V," *3ID Battle Command Tactics Techniques, and Procedures*, Center for Army Lessons Learned Newsletter 08-41, Fort Leavenworth, KS, September 2008, pg. 12.

- Support to component and material sourcing and tracking
- Support to prosecution
- Signature characterization

Event characterization includes the technical assessment of the type of device, its main charge, and tactical evaluation that answers the following questions:

- Why this location?
- Why this time?
- Why against this target?
- Why this type of IED?

This outcome supports all the other outcomes listed below and is dependent on the availability of EOD personnel familiar with the area of operations to exploit the site. The EOD operator, over a period of time working the same area of operations, begins to identify fabricators and emplacer's habits, preferences, choice of terrain, and target patterns. These patterns allow distinctions to be made between insurgent cells, networks, and bomb makers working within the operator's sector. The key role the Service EOD Operator plays in IED site exploitation is highlighted in the Army's recently released Army Training Publication (ATP) for Technical Intelligence: "EOD personnel serve as the primary technical analysts, technical experts, and collectors on all foreign ordnance and IEDs." [22] WIT photography, site sketches, and interviews of eye witnesses compliment EOD Technicians' assessments in recording the incident, equipment/material damage, and enemy's use of terrain, as well as other signatures associated with the devices placement.

Data regarding US and partner nation behaviors that affect enemy response, or that the enemy exploits to their advantage, must be collected and evaluated. "There are four important research questions, all dealing with the interaction between friendly and enemy forces in an insurgency.

1. What operational patterns are friendly forces exhibiting?
2. How is the behavior being exploited by the enemy?
3. How can the friendly force alter its behavior to make its patterns more difficult to discern?
4. If its patterns *are* discerned, how can the friendly force make them more difficult for the enemy to exploit?"[23]

The questions listed above form the basis for an "honesty trace." The British Army in Northern Ireland developed the honesty trace technique to discern if patrolling activities were setting a pattern that could be exploited by PIRA to their advantage. The cause, possibly friendly forces behaviors and the post event, effect was recorded by the unit's after action reporting and site

[22] Headquarters Department of The Army, *"Technical Intelligence ATP 2-22.4,"* Washington, DC, November 2013, pgs. 2-7.

[23] Walter L. Perry and John Gordon IV, "Analytic Support to Intelligence in Counterinsurgencies," Santa Monica, CA, RAND Corporation, 2008, pg. 39.

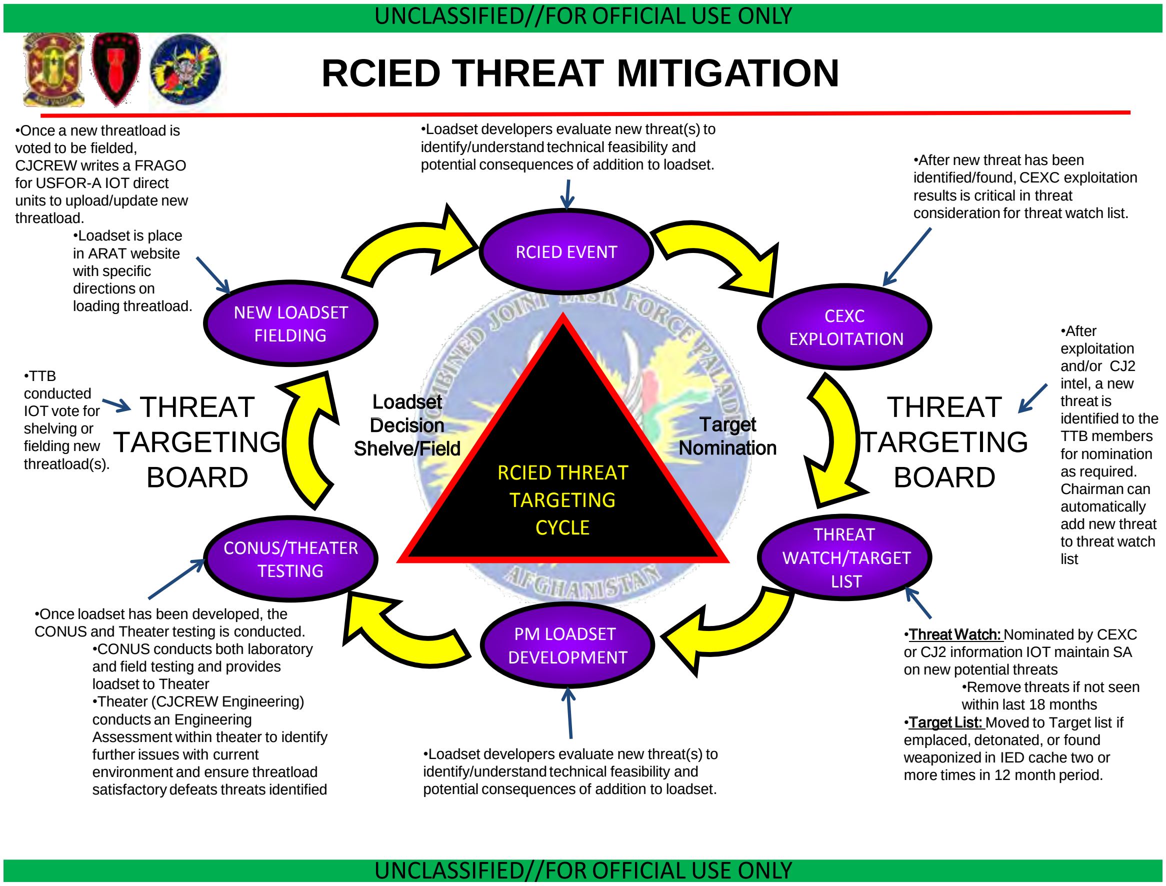
exploitation activities.[24] [25] The Marine Corps' innovative CLIC was based on their examination of the British Army's honesty trace of patrol activities and the value of intelligence led activities at the tactical edge of the battlespace.

Force Protection (FP) is significantly enhanced through timely identification of new enemy TTP and IED designs that defeat friendly countermeasures, including electronic jamming devices and armor. Maintaining current radio frequency (RF) loads for jamming systems to defeat enemy radio-controlled IEDs (RCIED) is critically important and requires the recovery of enemy RF initiation devices from event site when practical (**Figure 6**). This is to ensure the database of frequencies used by the enemy is current. The onsite exploitation, when it includes an EOD operator, identifies the type of device used, its explosive filler, and the post-blast effects on targeted vehicles. The tactical and technical procedures to counter the IED threat often have a short shelf life because insurgents rapidly develop countermeasures based on observations of an event, its effects, and post incident EOD response procedures. As an EOD Company Commander noted, "… the bad guys would sit back and watch your [TTP]; they'd watch what you would do. If you just ran up there with a robot and snatched det cord out of the nose of fuse, well, then they'll cement it in next time. If you go out there and cut it, they'll do something else to it. They just kept improving. As they improved their TTP, we improve ours."[26]

[24] NOTE: Refer to John R. Jackson's article, "Fool the Enemy by Using Honesty Traces," found in Counter-IED Bulletin X, Center for Army Lessons Learned, Fort Leavenworth, KS, March 2012, pgs. 41-45.

[25] NOTE: MAJ Gettig's article identified bomb type, trigger type, observer/triggerman and target and bomb location as the five factors critical to a successful IED attack that, once assessed post an attack, can assist with predictive analysis and developing a profile of the enemy employing it. MAJ Gettig, Major, USA, "Five Factors of an IED Attack," *Military Intelligence Professional Bulletin,* 37, no 3, (July-September, 2011) pgs. 26-28.

[26] "Operational Leadership Experiences, Interview with MAJ Percy Rhone," Ms Jenna Fike, Combat Studies Institute, Fort Leavenworth, KS, December 01, 2010, pg. 6. NOTE: MAJ Rohne served as commander of the 710th Explosive Ordnance Disposal (EOD) Company in *Tikrit*, Iraq 2003-2004 in support of Operation Iraqi Freedom.



UNCLASSIFIED//FOR OFFICIAL USE ONLY

RCIED THREAT MITIGATION

•Once a new threatload is voted to be fielded, CJCREW writes a FRAGO for USFOR-A IOT direct units to upload/update new threatload.

•Loadset is place in ARAT website with specific directions on loading threatload.

•Loadset developers evaluate new threat(s) to identify/understand technical feasibility and potential consequences of addition to loadset.

•After new threat has been identified/found, CEXC exploitation results is critical in threat consideration for threat watch list.

•TTB conducted IOT vote for shelving or fielding new threatload(s).

•After exploitation and/or CJ2 intel, a new threat is identified to the TTB members for nomination as required. Chairman can automatically add new threat to threat watch list

•Once loadset has been developed, the CONUS and Theater testing is conducted.

•CONUS conducts both laboratory and field testing and provides loadset to Theater

•Theater (CJCREW Engineering) conducts an Engineering Assessment within theater to identify further issues with current environment and ensure threatload satisfactory defeats threats identified

•Loadset developers evaluate new threat(s) to identify/understand technical feasibility and potential consequences of addition to loadset.

•**Threat Watch:** Nominated by CEXC or CJ2 information IOT maintain SA on new potential threats

•Remove threats if not seen within last 18 months

•**Target List:** Moved to Target list if emplaced, detonated, or found weaponized in IED cache two or more times in 12 month period.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Figure 6 (U//FOUO). Radio-Controlled IED Threat Cycle. *(Slide excerpted from Commander, Combined Joint Task Force PALADIN After Action Review presented by COL Leo Bradley, USA, Commander, from July 2011 – June 2012.)*

Because the insurgent can rapidly adapt IEDs to exploit vulnerabilities in a vehicle's design or post event responses by specialist troops, changes in enemy device capability and employment TTP need to be reported by friendly forces as soon as possible. The EOD operator plays a key role in identifying adaptations and changes in IED effects. "Because of his day-to-day missions rendering IEDs harmless, the noncommissioned or junior officer EOD team leader is best suited to recognize similarities and trends in IED attacks in his area of operations."[27] The enemy's threat evolutions must be communicated throughout the force and flagged for evaluation by program managers and research and development centers to begin countermeasures development or adaptations to existing programs or those in development. The speed that the enemy can adjust to friendly force countermeasures has forced JIEDDO and affiliated and supporting C-IED force protection programs into trying to be a "fast second" in responding to shifts in enemy behaviors and IED design. Evolutions include changes in enemy IED emplacement TTP designed to kill EOD Technicians, who are the first responders to IED events.

[27] John Moulton, USN, "Rethinking IED Strategies: From Iraq to Afghanistan," *Military Review*, (July-August 2009): pg. 31.

What has continually challenged the counter-IED effort is the ability to process and validate requirements, field test new procedures and equipment, and provide maintenance and training for new capabilities before they are introduced into the theater. A process to integrate new capabilities into the operational system was lacking. New capabilities were received in theater, typically at the tactical level, without documentation or training. For example, in November 2004, MNC-I had a science advisor responsible for reviewing more than 100 capability proposals. As OIF progressed, forward Commanders insisted on more stringent testing protocols and validation exercises of new technologies, software, ISR systems, etc. However, unit after action reports revealed that they were field testing new systems in theater without being trained on them prior to deployment. "Units are still being exposed to C-IED equipment and capabilities after they arrive in country that have not yet been fielded back in the United States. Not having this equipment available during the pre-deployment training program (PTP) forces units into discovery learning once in country and in-extremis classes during reception, staging, onward movement and integration (RSO&I)."[28]

Being able to quickly recognize evolutions in an enemy's capability, assess their impact, identify capability gaps, and report that information to the owner of that problem outside of theater requires a finely tuned system with robust feedback loops for relevancy and currency. Improvements to the requirements process, supported by WTI collection and exploitation efforts, will decrease response time to evolving threat environments.

Support to targeting occurs as a result of forensic and biometric exploitation of recovered information and material that can link recovered fingerprints and DNA to an event and later be used to identify participants in the activity. Technical analysis of the device can link a recovered device to a particular bomb maker or insurgent cell through assembler patterns and components used. Proper on-scene collection and processing by EOD and other specialist troops, including WITs, complement the forensic and technical exploitation of the device and its components. Data derived from WTI becomes part of an all-source analytic process that helps associate the IED emplacer with insurgent networks and their members for targeting.

A USMC Regimental Combat Team Commander commented on the value of the Marine's Joint Prosecution and Exploitation Center (JPEC) operations in Iraq where fusion was incorporated into their center's processing of captured material. "When was the last time our snipers took out an IED cell? It hasn't in over a year. How many IED cells have the JPEC helped us take out? Numerous, and six, eight, ten, at a time, and it is not all just 'Bang', he's dead. It's we capture them, exploit his stuff, and then we continue to roll up others."[29] The close relationship that developed between the Services' exploitation centers in support of detainee processing and interrogation was an important factor in developing information about insurgent networks, their activities, and the identities of network members.

Supports component and material sourcing and tracking and supply chain interdiction by exploiting IED components to identify trends and possible links to the supporting logistic network and local supply sources, or to identify a state or non-state sponsor collaboration on the basis of system type (e.g., the explosively formed projectile [EFP] and Iranian support to Iraqi insurgents or materials critical to bomb making, such as the plastic explosive, SEMTEX, which Libya provide to PIRA

[28] United States Marine Corps, Regimental Combat Team 7, II Marine Expeditionary Force (Forward), *After Action Report for Operation Enduring Freedom (OEF) 12.2-13.2*, August 20, 2013, pg. 6.

[29] Marine Corps Center for Lessons Learned, *Joint Prosecution and Exploitation Center (JPEC) Operations and the Use of Forensics in Iraq (Revision 1),* (Quantico, VA, February 04, 2009), pg. 9.

in Northern Ireland). Identification of unique IED components or materials supports theater and national level efforts to interdict or preclude their introduction into the battlespace. The theater J2 directs systematic collection of components and materials used in IED fabrication to enable precise identification. His staff is responsible for identifying, characterizing, and reporting captured enemy material and equipment. For example, the work accomplished by JIEDDO's Homemade Explosives Task Force, supported by a whole-of-government approach and by the Government of Pakistan and others, reduced the threat posed by ammonium nitrate fertilizer illegally imported into Afghanistan in defiance of Kabul's prohibition on its use. JIEDDO's Homemade Explosives (HME) Task Force has been instrumental in supporting the US government's engagement with the Pakistani government to curb the export of ammonium nitrate fertilizer to Afghanistan. This type of effort is dependent on battlefield recovery of IED component materials and the documentation of its frequency in theater to provide the proof necessary to associate a manufacturer, importer of materials, group, or government.

Support to prosecution is accomplished when materials are handled in a forensically sound manner with a chain of custody that tracks materials' progress through the exploitation process. Site exploitation and subsequent laboratory findings provide evidentiary-level "facts" that can be used to support detainment and prosecution of captured insurgents or to associate suspected perpetrators who are connected later with a hostile act. "Evidence collection must be weighed against the tactics of the enemy and the risk of the Marine involved. No amount of evidence is worth the legs or life of one of our Marines. Encourage the "On Scene Commander" and EOD Team Leader to collect as much evidence as they are comfortable with and then dispose of what they are not comfortable with."[30]

Signature characterization derives from enemy IED fabrication and emplacement methods that can aid in cuing ISR platforms and ground reconnaissance. Signatures also refer to characteristics relating to the manufacture of the device. Signature characterizations allowed Multi-National Forces-Iraq (MNF-I) C2 Major General Rick Zahner to link captured EFPs to an Iranian source (**Figure 7**). In September 27, 2007 press conference, Zahner noted: "When you talk about devices such as EFPs, that is almost uniquely Iranian: in fact, the fingerprint of the copper plate [liner] being formed in a machine shop. I mean, the pattern so identical that, you know, we can easily identify right there."[31]

[30] (FOUO) GySgt Jason R. Hart, USMC, *Weapons Intelligence Team After Action Report for Counter IED Operations in Support of Regimental Combat Teams 2 and 8 from December 2010 to May 2011*, Combined Joint Task Force Paladin SOUTHWEST, July 10 2011.

[31] Michael Knights, "Deadly Developments: Explosively Formed Projectiles in Iraq," *Jane's Intelligence Review*, March 2007, pg. 8.

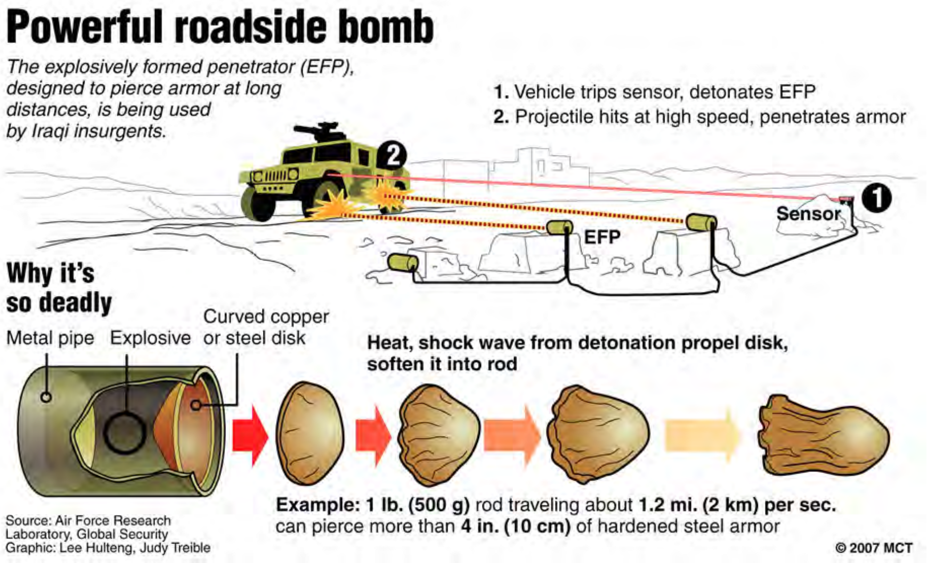

Powerful roadside bomb
The explosively formed penetrator (EFP), designed to pierce armor at long distances, is being used by Iraqi insurgents.
1. Vehicle trips sensor, detonates EFP
2. Projectile hits at high speed, penetrates armor
2
Sensor
1
EFP
Why it's so deadly
Metal pipe
Explosive
Curved copper or steel disk
Heat, shock wave from detonation propel disk, soften it into rod
Example: 1 lb. (500 g) rod traveling about 1.2 mi. (2 km) per sec. can pierce more than 4 in. (10 cm) of hardened steel armor
Source: Air Force Research Laboratory, Global Security
Graphic: Lee Hulteng, Judy Treible
© 2007 MCT

Figure 7. EFP Diagram and Employment. (*The EFP's effectiveness against recently up-armored HUMVEEs helped spur the next evolution of vehicular armored protection for US forces, the MRAP, and yet another evolution of countermeasures. (Photo Credit: USAF Research Laboratory)*

In that same September 2007 press conference, LTG Zahner states that "… the military grade C-4 explosives used in explosively formed projectiles were marked with the same batch number as explosives seized on the *Abu Hassan*, an Egyptian-owned, Lebanese-flagged fishing boat captured by Israeli naval forces off Haifa in 2003. The intercepted shipment, believed to belong to Hezbollah captured on the *Abu Hassan* appears to have been critical in making the case for Hezbollah involvement in Iraq."[32] Signatures relate to patterns of activity associated with emplacing an IED, also the manufacturing process.[33]

Weapons of Concern

In 2005, NGIC and Multi-National Corps-Iraq (MNC-I) J2 established an innovative and necessary category of weapons and weapon systems, which they named a "weapon of concern." A weapon of concern is one whose discovery on the battlefield has reporting and recovery priority for further exploitation. A weapon of concern's capability appears rapidly and unexpectedly on the battlefield, and avoids or overmatches friendly force protection measures, requiring a rapid response to negate its temporary advantage. In 2007, the RAND Corporation, in a study titled "Stealing the Sword: Limiting Terrorist Use of Advanced Conventional Weapons," expanded on the weapon of concern category and identified "… five types of advanced conventional weapons that could, in the absence of mitigating measures, provide terrorists with a qualitatively new and different capability. Each of these weapon types threatens to change the nature of terrorist attacks:

[32] Ibid.

[33] NOTE: For further information on EFP use in Iraq and its link to Iranian assistance, refer to Michael R. Gordon and GEN Bernard E. Trainer, USMC (RET), Chapter 17, "League of the Righteous," *"The Endgame: The Inside Story of the Struggle for Iraq, From George W. Bush to Barack Obama,"* (New York: Pantheon Books, 2012), pgs 312-328. Also see, Kimberly Kagan, "Iran's Proxy War against the United States and the Iraqi Government," Iraq Report, Institute for the Study of War. Washington, DC, May 2006-August 20 2007. http://www.understandingwar.org/sites/default/files/reports/IraqReport06.pdf.

- Sniper rifles and associated instrumentation
- Improved squad-level weapons of several types
- Long-range antitank missiles
- Large limpet mines
- Precision indirect fire systems."[34]

(An example of commercially available instrumentation to improve performance of snipers includes laser range finders and ballistics calculators to determine environmental conditions that would impact the flight of the round and its accuracy.)

A weapon of concern does not need to be a technically advanced system but can be an existing munitions' design that is well suited to exploit a target's vulnerability. This could be in terms of terrain or in other advantageous operational circumstances that have not been previously encountered on the battlefield.

An example of a weapon of concern from OEF was the insurgent use of the Soviet RKG-3 (*Ruchnaya Kumulyatiynana Granata)* high-explosive antitank (HEAT) handheld shaped-charge grenade **Figure 8**). This weapon is more than 60 years old, but when Iraqi insurgents used it in a crowded urban battlespace, it proved to be a threat to coalition force patrols. It was, for a period, "… the most lethal and prolific weapons system in the Sunni rejectionists' arsenal and its employment is on the rise throughout Iraq." [35]

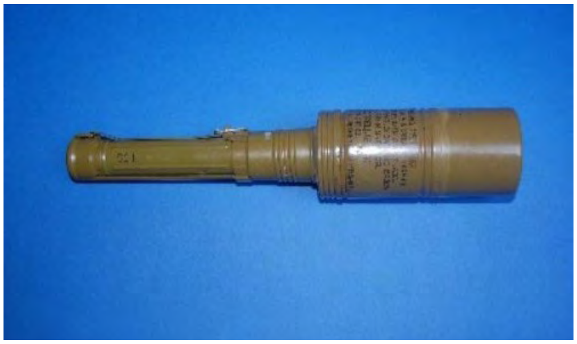


Figure 8. Soviet RKG-3 (Ruchnaya Kumulyatiynana Granata). *This is an example of a high-explosive antitank (HEAT) handheld shaped-charge grenade. (Photo Credit: DIA)*

To respond to the increase in effective RKG-3 attacks in Baghdad, the 5-4 Cavalry adapted their existing processes designed to counter IED activity. "Following a number of enemy RKG-3 ambushes against coalition forces throughout northwest Baghdad, 5-4 Cavalry established an

[34] James Bonnomo, et al., *Stealing the Sword: Limiting Terrorist Use of Advanced Conventional Weapons,* (Santa Monica, CA: RAND Corporation, 2007, pg. XVI. NOTE: Brian Jackson of RAND Corporation, a member of the authorship team that wrote *Stealing the Sword,* contributed to a two-volume study, also published by RAND, titled *Aptitude for Destruction, Volume 1: Organizational Learning in Terrorist Groups and Its Implications for Combating Terrorism,* and Volume 2: *Case Studies of Organization Learning in Five Terrorist Groups.*

[35] LTC John B. Richardson IV, USA "Be the Hunter, Not the Hunted Defeating the RKG-3 Ambush," *Armor,* May-June, 2009.pg. 5.

RKG-3 defeat working group modeled after the successes of JIEDDO, to study enemy TTP, develop countermeasures, and then adapt new friendly TTP and modify equipment to defeat this emerging threat."[36] Like the IED Defeat Working Groups established in Iraq and Afghanistan, the RKG-3 Working Group focused the unit's and staff's efforts to accurately report on previous incidents involving this weapon system by analyzing enemy and friendly actions relative to the attack, exploring and developing TTP to counter the thrower of the weapon, identifying FP best practices, adapting training and equipment, and making material modifications. The 5-4 Cavalry was able to collapse the enemy's adaptive cycle by countering the earlier effectiveness of the Soviet RKG-3 by using the working group to evaluate progress in countering the threat, making adjustments based on lessons learned, and monitoring enemy responses to coalition increased effectiveness.

From Vietnam to Today: IED Big Data Processing and Its Dissemination

"*In no other war have we been deluged by so many tidbits of information for we have been accustomed to an orderliness associated with established battle lines."*[37]

During the Vietnam War, MG Hollis, the Commander of the 25th Infantry Division, observed that the volume of reporting from counterinsurgency operations makes meaningful analysis of resultant data a challenge. To address the volume of information that resulted from reporting from multiple sources, the Army deployed its most capable computer system — the UNIVAC 1005 (**Figure 9**). One of its tasks was to record mine and booby trap incidents in the divisional area of responsibility to support pattern and predictive analysis of device placement by North Vietnamese Army and Viet Cong units.

Figure 9. A UNIVAC AC 1005 Computer Suite. *(This is the first computer system deployed to support logistic, personnel, and combat related databases and analysis in Vietnam. (Photo Credit: Wikipedia)*

Major General Hollis's challenge was to report, record, and analyze hundreds of disparate activities occurring in counterinsurgency operations, establish understandable patterns, and use historical data to improve operational efficiencies and integrate disparate ISR system feeds and results. The volume of information operational units were capable of providing and the need for nearly continuous situation awareness in the battlespace expanded exponentially post-Vietnam.

[36] LTC John B. Richardson IV, "Be the Hunter", pg. 5.

[37] Hay, Vietnam Studies, "Tactical and Material Innovations," pg. 157.

But a theater reporting system was initially not available. Like many adaptations in Iraq and later in Afghanistan, it was built on the fly. It was known as the Combined Information Data Network Exchange (CIDNE) and the data it stored was critical to improving a commander's battlespace awareness

As coalition forces conducted their internal security operations in Iraq, they started to accumulate large amounts of data on insurgent activities in their area, the nature of local infrastructure, economy, ethnographic profile, local leader biographies, and information on the evolving nature of IED activity. Additional ISR capabilities expanded this base of knowledge along with the associated challenges of monitoring, fusing, archiving, and recalling that data. The increase in data brought with it the challenge for tactical formations to mine it for information and to fuse the information in a timely fashion. A RAND study that used experienced analysts conducting field research on potential coalition ISR requirements anticipated this challenge and recommended a center based in CONUS to process this information as a solution.

"Remote location would make it possible to take advantage of unique capabilities in CONUS designed to assist analysts in dealing with the mass of low-quality data that could be obtained from a combination of broad and narrow collection activities, as well as from theater specific sources. The importance of the cell from a strategic standpoint is that it taps into one of the main advantages of a nation state relative to a terrorist organization, the ability to sift [sic] through vast amounts of data in all forms to take advantage of operational lapses on the part of its opponents."[38]

In response to this flood of data, JIEDDO, in collaboration with DIA, established the Combined Counter-IED Operations/Intelligence Center (COIC). JIEDDO's COIC was initially established to support a training function, a battle lab that would allow BCT Commanders and their staffs to become familiar with and to apply emerging ISR capabilities in Iraq-centric simulations prior to their deployment. The above RAND analyst's observation was reinforced by one of the conclusions drawn from the report: "The inference of actionable information from enormous quantities of highly diverse information poses huge technical challenges. Automated technology-based methods offer the potential to sift through such quantities of data that would be impractical for human analysis, but methods that can draw subtle inferences from uncertain data are needed so that actionable knowledge can be obtained. Decision makers also need to be able to probe the raw data to allow the application of temporal and judgmental factors."[39] COIC later developed a substantial analytic role to support these functions. Examples of reports and analysis prepared by the COIC include the Ground Moving Target Indicator (GMTI) analysis, Pattern of Life Analysis, Compounds of Interest, and significant activities (SIGACT) deep dives for a particular geographic area for a specified period of time.[40]

[38] Brian A. Jackson, et al., "Intelligence Support to Counter-IED Operations: Sustaining Intelligence Directed Attrition Efforts, RAND, National Security Research Division, Washington, D.C., PM-1929-OSD, October 2005.

[39] National Research Council of the National Academies :*Countering the Threat of Improvised Explosive Devices: Basic Research Opportunities*, (Washington, DC, National Academies Press, 2007) pgs. 3-24.

[40] Combined Joint Task Force Paladin, *Counter-IED FAT (Fusion, Analysis, Training Report), Attack the Network Part II*, Combined Joint Task Force Paladin, Volume 1, Issue 5, March, 01 2011, Bagram Air Base, AF, pg. 5. NOTE: The FAT Report was one of the newsletters that were developed to share changes in enemy IED TTP and Coalition Forces lessons learned to aid attack networks, protect the force and introduce new capabilities in theater in a timely fashion. Please note that Maneuver Center of Excellence (MCoE) *IED Defeat Newsletter*, Fort Benning, GA provides threat, training and C-IED equipment updates.

The rotation of units in Iraq and Afghanistan posed challenges for the maintenance and transference of the previous unit's accumulated knowledge of that operational area. The information for a particular operational area of responsibility had to be passed on in an orderly manner to the next owner of that battlespace. Over the course of OEF, this amounted to several years of SIGACT reports, Intelligence Summaries, and special analytic products. The COIC played a key role in this handover, because they had the analytic staff and computing power to retain and rapidly retrieve a previous occupant's accumulated knowledge of that battlespace. Success in support of Commanders in the execution of their counter-IED and counterinsurgent operations necessitated the maintenance of an area's trends and activities in level of detail that was unique to the warfighters' recent experience. To process and evaluate the burgeoning amount of data, the Army had to rebalance their BCT staff manning. "Today's BCT has three times the original analytic capability and twice the human intelligence capability of a 2003 legacy BCT."[41] That expansion naturally increased the amount information that was processed, allowing more value added to the reporting, with a corresponding requirement to improve analyst tools to find and recover stored data. In fact, analysts were forced to deal with a myriad of software tools to process reports, and at the same time monitor and assess multiple near- and real-time ISR feeds. This task complexity made standardization of terms relating to IED incident reports and their technical characterization imperative, as described in the section below.

[41] LTG Raymond T. Odierno, USA, LTC Nichoel E. Brooks, USA, and LTC Francesco Pg. Mastracchio, USA, "ISR Evolution in the Iraqi Theater," Joint Forces Quarterly, no. 50, (July-September 2008) pg. 54.

Weapons Technical Intelligence (WTI)
Improvised Explosive Device (IED) Lexicon 4th Edition

Figure 10. Cover of the 4th Edition of the WTI Lexicon. *(Photo Credit: DIA/JIEDDO)*

IED Terminology and Lexicon Development

"Standardization of terms is critical to the automation of reporting, storage, processing, and visualizing information."[42]

When the counter-IED fight began in earnest it quickly became apparent that there were multiple terms with different meanings for device components and variations in the description of exploitation and what was meant by enhancements. There was not an agreed upon way to structure the data to support the development of an IED-specific ontology. Without a common language to describe the threat it was difficult to search for information required or gain an accurate interpretation of data that originated from multiple sources without the explicit definition of terms and relationships. "In addition to US Army doctrine, SOPs are used extensively to describe and report IEDs. SOP report procedure and formats may or may not support the automation of IED information management and feed mission command systems with necessary details to seamlessly reveal actionable intelligence. As stated previously, intelligence personnel at all levels rely heavily on the interpretation of the free-text portion of IED reports. The free-text portion can be misread or misunderstood by analysts."[43] The lexicon (**Figure 10 and Figure 11**) was designed to help prevent misinterpretation. Terms describing the IED and the event have elements common to the EOD operator and are used uniformly throughout the collection, exploitation and analysis cycle, which involves a multiplicity of DoD agencies and federal and international entities such as the FBI and NATO.

[42] Creg Good, *IED Reporting with the Weapons Technical Intelligence Lexicon*, Counter-IED Bulletin X, Center for Army Lessons Learned, Fort Leavenworth, KS, March 2012, pg. 37.

[43] Good, *IED Reporting*, pg. 37.

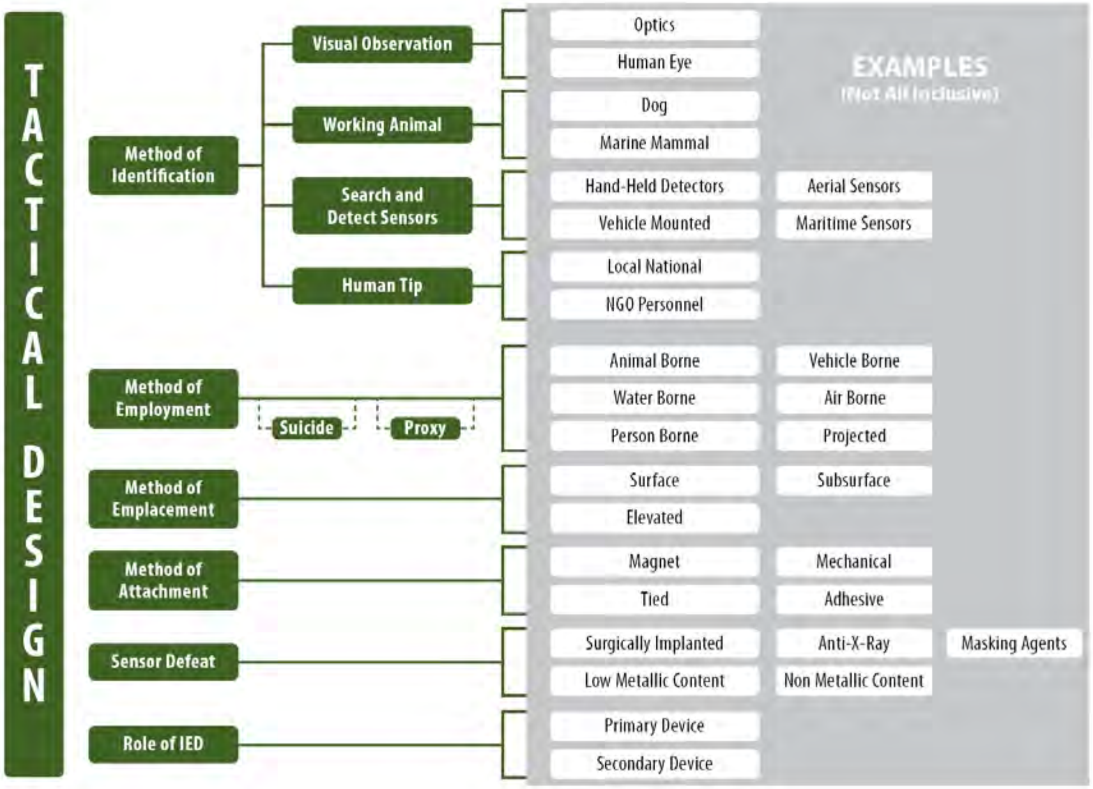


Figure 11. Tactical Design. *This figure from Lexicon Version 4 is an example of some of the elements or ontology, that constitute the tactical design of an IED incident (e.g., Method of Employment, Method of Attachment, Method of Identification) and what comprise these elements. (Figure Credit: DIA/JIEDDO)*

A threat-specific lexicon was a new initiative necessitated by the massive amounts of big data in databases and analysts' need to precisely frame the key word and phrase search fields to find the information they needed. Establishing this standard language was a very important step forward. "The WTI IED lexicon is authored by technical experts from key organizations and agencies engaged in assessing the IED threat and devising operational IED countermeasures. It is a 'living' document that is reviewed periodically to ensure its accuracy, relevance, and currency against the constant changing IED threat."[44] Contributors to the lexicon included multiple Service members from DoD and interagency and allied representatives, such as from the FBI and DHS. This participation dates from the first edition released in 2006. The lexicon was organizationally agnostic in its design, with multiple Service, departmental, and interagency and allied contributors allowing its use by state, local, federal and tribal law enforcement entities to describe an IED event and mine and interpret data provided by DoD from the battlefield that may be of value. The lexicon is designed to prevent misinterpretation because the terms describing the IED and event will have elements common to the EOD operator, the analysts, and scientific staff who contribute to all levels of the WTI process. "Although sensors are used extensively in the C-IED fight, most of the analytic applications in C-IED are built upon the application of *information fusion* – merging already known geographic or intelligence information with new information collected constantly from sensors (SIGACTs, reports, observations from unmanned aerial vehicle infrared sensors,

[44] Good, *IED Reporting*, pg. 40.

human reports)." [45] Use of a common lexicon to describe IED activity and their construction enables the discovery of data across multiple data bases because terms are used uniformly for the same purpose greatly facilitating information or data fusion. Analysts time is not wasted trying to reconcile the meanings associated with different terms for the same event or IED component. Lack of discipline in reporting also makes the task of Operational Research to develop meaning for the Commander out of a large number of reports much more difficult and less reliable in their conclusions.

Changes in Operational Environment

The training and equipment or the nature of any threat faced will be sufficiently different to drive changes in how the WTI process functions and supports the Commanders' C-IED fight as evidenced in Iraq and Afghanistan. These differences are briefly summarized here, with an examination of what differences could be and how current capabilities would fare in these different circumstances.

The IED threats faced in Iraq and Afghanistan exhibited differences in device type employment methods. In Afghanistan, IEDs were integrated by the Taliban as part of a broader tactical scheme or complex ambush on and off lines of communication (LOC). In Afghanistan, jamming systems carried by the Soldiers and Marines on dismounted patrol were an integral part of force protection measures. Unit deployments in Afghanistan were distributed in company and platoon bases where resupply was generally by fixed and rotary wing aircraft. Unit activities included dismounted patrols, ambushes, and clearing sectors of Taliban presence. These sites were often too remote to supply by convoy. In Iraq, the IED tended to be more effectively employed as a weapon to interdict and harass coalition use of LOCs. As opposed to Afghanistan, in Iraq the battlespace was more contiguous, allowing easier definition of unit boundaries. In Iraq the terrain and weather could impede operations but not to the extent that mountains and winter could in Afghanistan. In Iraq, complex urban terrain that favored the insurgents and channelized movement, challenged coalition forces.

The Taliban in Afghanistan demonstrated great skill in integrating the IED as part of their overall tactical design for engaging coalition forces. "They upped their complexity in tactic by reducing the complexity of the device that they employ… People say it's not very sophisticated over here, but in terms of the tactics and methods of employment, it's incredibly sophisticated. It reminds me of the more capable PIRA scenarios where you weren't impressed by the bomb but by how the ambush was set up and the thought that was put into it."[46] The skill exhibited by the Taliban in their incorporation of the IED into a broader tactical design was a trait that required coalition forces to adapt to across Afghanistan. The Taliban understood its value to shape the battlespace to their advantage, using it to harass, channelize, and delay the movement of coalition maneuver units.

[45] Samuel H. Huddleston et al., *The Warfighter's Guide to Counter-IED Analysis,* Joint Improvised Explosive Device Defeat Organization, pgs 77-78.

[46] Toby Harnden, *Dead Men Risen: The Welsh Guards and the Real Story of Britain's War in Afghanistan* (London: Quercus, 2011), pg. 212. Please refer to Toby Harnden's book *Bandit Country: The IRA & South Armagh,* published by Hodder & Stoughton in 2000. It is a balanced and insightful analysis of the conflict in Northern Ireland prior to the Peace Agreement with excellent insights on IRA use of IEDs, sniper teams and British Army countermeasures and challenges posed by the culture of the residents of South Armagh.

These differences required adaptation in the collection and exploitation of suspected insurgents, caches, and IED components and materials. Availability and capacity of supporting airlift and weather was always a factor in Afghanistan, with distinct fighting seasons that were less prevalent in Iraq. The impact of mountainous terrain, poorly maintained lines of communication, a sparse road network, and a dispersed, noncontiguous battlespace made moving enemy material and personnel a challenge. Collection and exploitation capability was dispersed to the Regional Commands by specialist troops (e.g., EOD Technicians and WIT) deployed as far forward as practical in any sector to mitigate the challenges of Afghanistan's terrain and weather.

Environmental and threat characteristics also drove the use of IEDs. FARC in Colombia was the most proficient and prolific user of IEDs in our hemisphere, using them to accomplish the following three general objectives:[47]

- As an obstacle or area denial weapon to protect their base areas from Colombian Army operations
- In areas under government control, particularly large metropolitan areas, as a weapon of terror by targeting key infrastructure
- As indirect fire weapon to attack isolated government outposts

FARC's use of improvised and conventional explosive devices such as VBIEDs, mailed IEDs and propane tanks filled with black powder created a challenge for the Colombian Army and national security forces in terms of training and equipping its forces to meet a broad range of threats. **Figure 12** illustrates two representative IEDs used by FARC that the Colombian Army recovered.

Colombia's challenge with FARC's use of IEDs and conventional mines was made more dangerous when PIRA began selling technical support and lessons learned to the FARC. Niall Connolly (at the time of his arrest resided in Colombia and claimed be the IRA Representative to the Cuban Government), James Monaghan (also known as 'Mortar' for his skill in fabricating homemade mortars; arrested twice on terrorism related charges), Martin McCauley (charged with weapons possession in Northern Ireland), all members of the IRA, were detained by Colombian authorities when they attempted to leave the country. Colombian authorities had been alerted to their identities and presence by a foreign intelligence service. "Although the "Colombia Three" claimed initially that they were "ecotourists" and later that they were liaising with FARC to understand their peace process, Colombian authorities—in addition to questioning the inconsistency in their explanations—noticed an almost instantaneous improvement in FARC's ability to conduct more sophisticated and lethal operations in Colombia. Beginning in early 2001, FARC began intensifying its operations, killing more than 400 members of the Colombian armed forces in 18 months, using car bombs, "secondary devices," and homemade mortars. In addition, the group expanded its campaign to Colombian cities, conducting large-scale urban operations, including the February 2003 bombing of the El Nogal country club in Bogotá that killed 36 people. The FARC also displayed an ability to use radio-controlled improvised mortars, a technological capability that only PIRA and ETA

[47] NOTE: For an excellent summary of IED threat in Colombia please refer to the *IED Watch: Summary of 2010 Strategic Environment*, Volume 3, Issue 6, Naval Post Graduate School Program for Culture & Conflict, October 2010, pgs. 22-32.

had previously demonstrated. Members of the Colombian armed forces subsequently recovered captured barracks-busting mortars."[48]

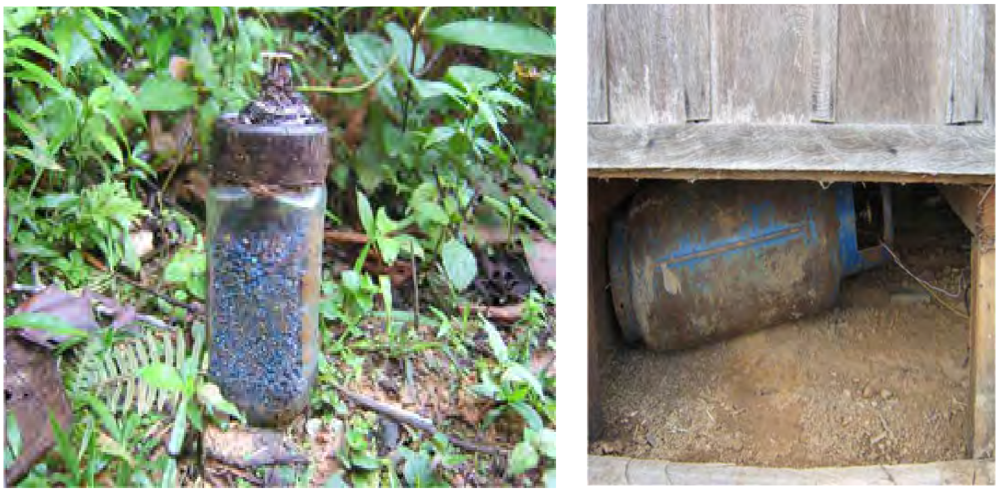


Figure 12. Improvised Landmine and Gas Cylinder Filled with Explosives *(Photo Credit: Ejército de Colombia — Escuala de Ingenieros Militares.)* [49]

Not only are the IEDs employed by FARC prevalent and sophisticated, the terrain of Colombia poses unique mobility challenges to current ISR systems. Heavily canopied jungle and thick undergrowth inhibit technical collection platforms and make visual detection of the threat more difficult. Movement is channelized by jungle growth, poor road infrastructure, and numerous major rivers and swamps. In fact, the FARC used IEDs in boats along waterways to attack Colombian Marine (COLMAR) outposts (**Figure 13**).

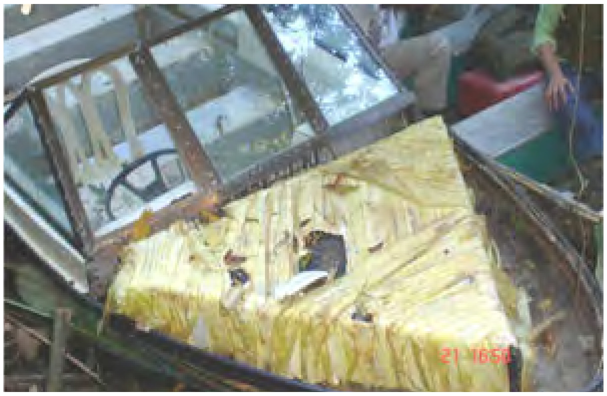


Figure: 13 FARC Waterborne IED. *This waterborne IED was found on a boat that was planned to be used in a river attack. (Photo Credit: Ejército de Colombia — Escuela de Ingenieros Militares)* [50]

[48] Adam Ward and James Hackett, eds., "The IRA's Foreign Links: Externalizing Its Expertise?" *IISS Strategic Comments*, 9, no. 5, (July 2003), quoted in Kim Cragin, et al., *Sharing the Dragon's Teeth: Terrorist Groups and the Exchange of New Technologies,* Santa Monica, CA: RAND Corporation, 2007, pg. 72.

[49] Pablo Esteban Parra Gallego, "IEDs: A Major Threat for a Struggling Society," *The Journal of ERW and Mine Action*, Winter 2009 no 13.3.

[50] Ibid

FARCs use of IEDs, and challenges experienced by its military provide a useful prism from which to evaluate US doctrine, its capabilities in an environment other than that experienced in another operational environment. The Colombian EOD capability received training and material support from DoD and advice on biometric and forensic exploitation and databasing. They've received EOD support since the late 1990s. Interestingly, the Colombian Army did not have an EOD capability, but instead relied on the National Police for that support. The Colombian Army Engineers treated the IED as an obstacle to be neutralized or removed, but they did not exploit the device for forensic or material data. An assessment of the impacts resulting from not having a military EOD capability, or fusing analysis that describes the totality of the threat capability and the development or lack thereof of COLMAR countermeasures; a process or system that can produce the five outcomes expected of the WTI process. The WTI process will help to mitigate the challenges seen in Colombia that are reflective of a larger global post Afghanistan threat.

The Way Ahead

"Let's not lose sight of our most recent experiences because the hot spots in the world today are finding the same kind of mine and boobytrap warfare encountered 20 years ago."[51]

Figure 14. Lance Cpl. Jason M. McCormick USMC Leads from the Front. *USMC Cpl using a compact metal detector to clear a path for his fellow Marines while conducting security patrols near their fire base, Headquarters Battery, 2nd Battalion, 11th Marine Regiment. (Photo Credit: Sgt. Earnest J. Barnes)*

Success in suppressing the IED threat is dependent on collaborative and systematic efforts from a range of disciplines, which are continually adjusted to meet the needs of the Commander (**Figure 14**). No single line of operation will succeed against a skilled and determined enemy employing these devices. "The United States must focus on strategic solutions to defeating IEDs because technical solutions to defeating IEDs will not achieve defeat. Units that rely on superior technology

[51] LTC Philip W. Carroll III, USA, "Mine and Boobytrap Warfare: Lessons Forgotten." Individual Study Project, U.S. Army War College, Carlisle Barracks, PA, 1988., pg. 10.

and armor protection to mitigate the effectiveness of IEDs will find themselves playing an infinite and costly number of cat and mouse games. Changing these conditions will not be done through vehicle armor, jamming devices, or route clearing equipment. The units that attack networks, target civilian populations, and foster an environment of IED intolerance will achieve victory over the IED."[52]

Eliminating the IED threat from the battlespace begins with the efforts of the individual Marine or Soldier, moving forward to engage the enemy – a systems of systems approach. They must have the training and equipment necessary to detect and defeat the device and the intelligence needed to drive operations against the networks that employ IEDs. The WTI process was designed to provide the range of outcomes to meet those needs. Its contribution to the targeting process is succinctly and aptly described in the October 2011US Marine Air Ground Task Force (MAGTF) Counter-Improvised Explosive Device Operations: "Stemming from technical intelligence concepts, WTI is a process to systematically collect and exploit information and material to produce analytical inputs for the targeting process. It can be obtained not only from an IED attack site, but also from other locations/events, such as caches and IED supply chain interdiction."[53] Targeting insurgent networks that employ IEDs and eliminating the bomb maker reduces activity in the area they operate in. For example, operational analysis conducted by Combined Joint Task Force Paladin from 2011 through 2012 showed that the removal of a bomb maker in Afghanistan suppressed IED activity by 18 percent for 6 weeks following the bomb maker's removal from the battlespace.[54]

The current trend is site exploitation to collect forensic materials and expeditionary laboratories to support the establishment of the rule of law to assist in nation building. These are worthy goals; however, there is more to site exploitation and processing of captured materials then producing evidence for a subsequent prosecution. If the enemy is emplacing or has fielded IEDs that are defeating existing force protection measures, that circumstance requires a more robust exploitation effort then does the recovery of forensic information from recovered materials. It requires the skills of EOD Technicians to assess the device, conduct field trials to test comparable devices against current force protection measures, and scientists or electrical engineers to assess devices and to make recommendations to the Commander forward and program managers in the rear. The WTI process must be a balanced application of a range of disciplines that have not traditionally functioned in a collaborative system in the battlespace. For example, EOD Technicians have emerged as a critical source of intelligence on enemy IED TTP, in addition to playing a key role in building profiles of insurgent networks based on the results of site exploitation. EOD units would benefit from infusion of intelligence personnel in the headquarters and field operating units to provide operators current intelligence on worldwide IED trends and intelligence support once deployed. In 2004, the exact opposite occurred when the US Army EOD Battalion's had their S2 staff reduced.

[52] CPT Joseph M. Garaux, USMC, "The IED Fight: Technical Shortcomings and the Value of Strategy," *Marine Corps Gazette,* January 2010, pg. 11.

[53] US Department of Navy, Headquarters United States Marine Corps, *MAGTF Counter-Improvised Explosive Device Operations,* 2011 Washington, DC, 2011, pgs. 3-8.

[54] NOTE: Data provided by COL Leo Bradley, USA, Combined Joint Task Force Paladin Commander from June 2011–2012. He employed operational research to monitor battlefield trends and effects the task force targeting and impact of the introduction of new counter-IED systems and TTP.

In 2003, the doctrine for TECHINT was not suited for the scale and sophistication of the IED threat as it evolved in Iraq and Afghanistan. The time it took to establish a WTI capability that provided value within the battlespace cost lives. The Services were forced to dynamically adapt while engaging a threat they were just beginning to understand. In the space of a decade, we acquired the knowledge and experience to make the appropriate doctrinal, material, and training adaptations to better counter and defeat future IED threats. One key adjustment is making clear that the Commanders forward own the capability, and the intelligence staff directorates at each level of command are responsible for directing process activities to support operations. When serving as the ISAF J2 in Afghanistan, LTG Flynn, USA, established the J2E, in which "E" stands for exploitation. He did this to synchronize and direct the theater's collection and exploitation of captured enemy material and equipment. The gap that he identified needs to be addressed by Joint and Service doctrine.

The Intelligence Community (IC) erred in examining IEDs as an analytic element that fell within the counterterrorism responsibility for technical analysis and its employment. To be sure, terrorists incorporated IEDs in their attacks. However, Hezbollah, in their campaign against the Israeli Defense Forces (IDF) in Southern Lebanon, perfected their use of EFPs whose effectiveness was known. Another insurgency, known collegially as "The Troubles," engaged British Ammunition Technical Officers (ATOs) against highly skilled PIRA bomb making networks in Northern Ireland. There the British learned that electronic jamming capability was vital to soldiers on patrol and a necessary piece of equipment in vehicles. The British also learned to integrate forensic collection into exploitation of incident sites and recovery of materials. This helped to form WITs with ATOs, military police, and intelligence specialists to extrapolate as much data as possible out of recovered IEDs to feed a range of needs. EOD Technicians, who learned from allied partner nations operating in these environments, were responsible for US IC knowledge about the IED threat impact pre-9/11. US experience with mines and booby traps in Vietnam laid a foundation of understanding. That threat shaped the battlespace negatively by absorbing resources, hindering movement, and making the conduct of resupply convoy operations a daily life or death struggle. Engineer route clearance teams, dog teams, EOD Technicians, and riflemen walked their sectors of the road each morning to clear enemy mines and IEDs. In hindsight, we realize this hard-earned knowledge did not receive the attention it deserved.

The timely identification, reporting, and response to enemy IED adaptations and emplacements require continual analysis and process improvement. In his testimony to the Oversight and Investigations Subcommittee of the House Armed Services Subcommittee on Defeating the IED, JIEDDO Director, LTG Thomas F. Metz, USA stated that:

"Since our last meeting in September (2009), there have been over 10,000 IED incidents in Iraq. These incidents are diverse, and the devices that were used reflect the wide range of arming and firing switches, ranging from relatively simple command wire to sophisticated radio-controlled and passive infrared switches. Yet in spite of the large volume and the diversity of the IED attacks, the numbers that are effective against our forces continue to decline for the second straight year."[55]

[55] Oversight and Investigations Sub-Committee of the House Armed Services Sub-Committee on Defeating the IED and Other Asymmetric Threats: Reviewing the Performance Oversight of the Joint IED Defeat Organization, Congressional hearing, chaired by Representative Vic Snyder (D-AR), Capital Building, Washington, DC, October 29, 2009.

LTG Metz's comments suggest progress in reducing friendly force casualties from IEDs. That progress reflected the efforts of the Services and JIEDDO in suppressing this threat. What is of concern is the continuing high volume of IED emplacement activity — more than 10,000 incidents in Iraq in 2008. If the enemy can make a broad shift in technical capability or innovative tactical emplacement across the battlespace, with such a large number of emplacements, the effect will be widespread and lethal. To detect early shifts in enemy employment requires that the theater of operations have a systematic and timely event exploitation effort complimented by a SIGACTS reporting system.

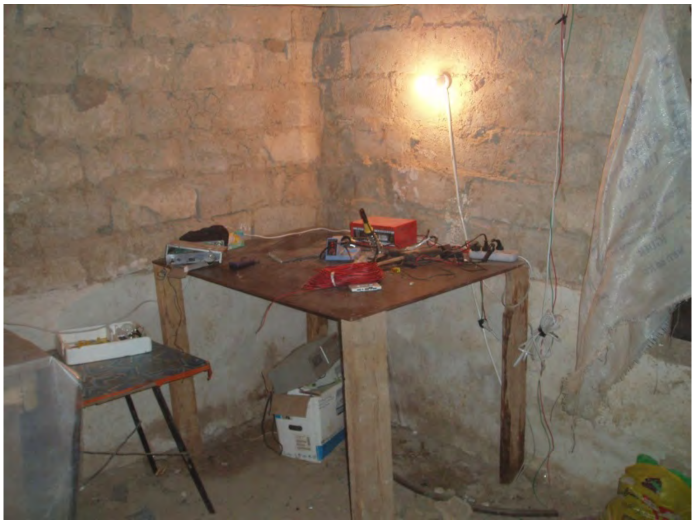


Figure 15. Iraqi IED Facilitator and Bomb Maker Work Area – It Can Be This Simple. *An operation conducted by the 502nd Brigade Combat Team, 1 01st Airborne Division near Baghdad, led to the capture of a suspected IED facilitator, IED components, and other bomb making materials in November 2005. Pictured is the work station used to construct IEDs. (Photo Credit: CPT Gregory Hirschey)*

The success achieved by insurgents in Iraq and the Taliban in Afghanistan exposed our vulnerabilities to this asymmetric threat. It was the principle cause of friendly force casualties. It took a national level effort directed by JIEDDO and the extraordinary hard work and innovative talents of the Services to suppress and mitigate its battlefield impact. The threat posed by IEDs endures (**Figure 15**). It will take a sustained effort to monitor its worldwide evolution and make the organizational, doctrinal, and material adaptations necessary to be ready for the next round. Areas that require special attention post operations in Afghanistan include:

- Identifying and confirming insurgent and terrorist threat evolutions rapidly to be a "fast second" in developing countermeasures to defeat new enemy technical and tactical initiatives

- Red Teaming future enemy IED developments and their anticipated response to friendly force protection countermeasures

- Matching current WTI and counter-IED doctrine, training, and material capabilities against operational environments outside of those recently experienced in Iraq and Afghanistan to identify potential capability gaps (e.g., persistent surveillance and its current capability to over watch terrain populated with triple canopy jungle

This shift in the operational environment may find field operators relying more on their own field craft, IED sign recognition skills, and combat hunter-instilled instincts to detect and respond to threat activities.

Response to this class of threat requires a systems level approach that synchronizes the capabilities of different Service branches (e.g., Engineer, Ordnance Corps, Joint EOD community, Defense IC, and laboratory capabilities from the tactical to strategic levels). The system must provide a range of outcomes that support:

1) Force protection material and training development
2) The find, fix, finish, exploit, analyze, and disseminate (F3EAd) cycle
3) Component and material sourcing and supply chain interdiction
4) Interrogation and prosecution of detainees
5) Identification of signatures associated with IED related activities.

Making this adaptation will take a sustained effort and senior leadership involvement and direction to critically examine our recent IED experience and make the necessary doctrinal, material, organizational, and training adjustments to engage and defeat the IED threat when, inevitably, we face it again.

POC: Russell L. McIntyre, NIPR Russell.McIntyre@dia.mil.

CHAPTER 1
Introduction

1.1 General Description of Problem

"The use of IEDs [improvised explosive devices] has become so widespread that they have become a global and enduring threat … C-IED [counter-IED] treats the IED as a systemic problem and aims to defeat the IED system. Therefore much of the C-IED approach could, potentially, be adapted to counter other adversary weapon systems."[56]

Adversarial use of improvised weapons, including IEDs, and conventional weapons, such as rocket propelled grenades and sniper rifles, have become signature weapons in 21st century asymmetric warfare. They are relatively cheap, easy to construct, lethal, accurate, and have proven successful when engaging a more technologically advanced and better equipped enemy. Little wonder then, that in recent conflicts the IED has been chosen as the weapon of choice. This is an enduring trend and likely to challenge the United States and its allies at home and abroad for the foreseeable future.[57]

"The use of improvised explosive devices (IEDs) threatens these [US] interests by killing, injuring, and intimidating citizens and political leaders around the world, inflicting damage on U.S. forces on the battlefield, and disrupting transportation and the flow of commerce. The terrorists and criminals responsible for these attacks are resilient, technologically adept, and adaptable. They employ the most recent and successful tactics, techniques, and procedures gained from experience in Iraq, Afghanistan, and around the world. The use of IEDs worldwide has increased in recent years…."[58]

For the past decade, combat operations in Afghanistan and Iraq have been plagued by IEDs and other improvised weapons. There, we saw rapid adaptation and counter-adaptation between the US-led coalition forces and asymmetric adversaries. As quickly as US and coalition forces developed countermeasures, terrorists and insurgents in Iraq and Afghanistan adapted their tactics to counter these countermeasures.[59] Improvised weapons, emplacement tactics, arming and firing switches, explosive types and quantities, metallic signature, and many other characteristics changed over

[56] North Atlantic Treaty Organization, Allied Joint Doctrine for Countering, *Improvised Explosive Devices*, AJP-3.15 (A), March 16, 2011, pg. 1-1. An IED is defined as "a weapon that is fabricated or emplaced in an unconventional manner incorporating destructive, lethal, noxious, pyrotechnic, or incendiary chemicals designed to kill, destroy, incapacitate, harass, deny mobility, or distract." From U.S. Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication 1-02, Washington, DC: November 8, 2010, as amended through April 15, 2012, pg. 150. The September 2012 *Weapons Technical Intelligence (WTI) Improvised Explosive Device (IED) Lexicon* alternatively defines an IED as "a device placed or fabricated in an improvised manner incorporating destructive, lethal, noxious, pyrotechnic or incendiary chemicals and designed to destroy, incapacitate, harass or distract. It may incorporate military stores, but is normally devised from nonmilitary components. Refers to a type of IED incident that involves a complete functioning device" (pg. 5).

[57] LTG Michael Barbero, *JIEDDO's Statement to the House of Representatives Committee on Appropriations Subcommittee on Defense*, JIEDDO, September 20, 2012.

[58] Introduction by President Barack Obama, *Countering Improvised Explosive Devices*, The White House, February 26, 2013

[59] National Academy of Science, *Countering the Threat of Improvised Explosive Devices*: Basic Research Opportunities, Abbreviated Version, http://www.nap.edu/catalog/11953.htm, Preface ix

periods of only days. Over time, adversaries' technological sophistication increased, allowing them to penetrate vehicles previously invulnerable, circumvent electronic countermeasures, and overcome coalition tactics, techniques, and procedures (TTP).

"Insurgents use IEDs as weapons against coalition forces and will probably continue to do so in the future. Enemy observations and understanding of coalition tactics, techniques, and procedures (TTP) and rapid IED networking knowledge enable them to change their TTP quickly as coalition forces counter or disrupt their operations. Their targeting, decision, and execution cycle becomes increasingly shorter. The ease of obtaining IED building materials and the ability to rapidly exchange technical information make the IED a logical insurgent tool that places great burdens against conventional military sources."[60]

This trend will continue as asymmetric groups openly transfer knowledge and advances through exchanges of personnel, materials, and information.[61] The ease with which this knowledge transfer occurs was evidenced in Boston by the Tsarnaev brothers learning to make pressure cooker and pipe bombs from Inspire magazine, an open source Al-Qaida publication.[62] Use of simple IEDs, like those used at the Boston Marathon, have proved effective and will continue. However, as terrorists and insurgents evolve, they will employ new and more advanced weapons that take advantage of friendly force vulnerabilities. Adaptations include shifts in targeting priorities, as was the case in Iraq and Afghanistan when military forces became too difficult to attack without excessive risk, while civilian targets posed less risk. Adversaries' advantages include ability to stand off from the attack, perceived anonymity, and the ability to freely transit between neighboring countries that lack US presence and influence. Seeking to disrupt these advantages and other innovations ensures the adaption and counter adaption competition will continue.

"The crucial issue will not be whether the United States possesses such technologies, but how affordably, how quickly, and how effectively joint forces can incorporate those technologies not only into their concepts, doctrine, and approach to war, but actually into the units and commands that will have to use those technologies on future battlefields."[63]

Mitigating the impact posed by these weapons requires a robust and comprehensive whole-of-government approach that leverages all levels of the joint, interagency, intergovernmental, and multinational (JIIM) community. Only by effectively coordinating US government efforts across departments and agencies, as well as with international partners, can the government increase its

[60] Mark O. Baker and James R. McAfee, *Using Trends to Conduct Effective Counter Improvised Explosive Device Training,* C-IED Bulletin 11 no. 10-50, July 2010, Center for Army Lessons Learned. NOTE: Although this quote focuses on US and other coalition security forces, it must be understood that IEDs are an equal threat to indigenous Security Forces.

[61] U.S. National Intelligence Council, *Global Trends 2025: A Transformed World* (Washington DC: Director of National Intelligence, November 2008) pg. 68.

[62] Pressure cooker bombs like those used in the Boston Marathon have been used around the world for decades. They are routinely used in Iraq and Afghanistan but have been used by insurgents and terrorists around the world, including in the United States in a bombing attempt in Times Square on May 1, 2010, and by Army PV2 Naser Jason Adbo who planned to blow up Fort Hood, TX soldiers. "*Pressure cooker bombs used around the world for years*." Tacey Connor, Staff Writer, NBC News, April, 16, 2013

[63] U.S. Joint Forces Command, the Joint Operating Environment 2008: *Challenges and Implications to the Future Joint Force,* Suffolk, VA: U.S. Joint Forces Command. pg. 50.

effectiveness against this threat while making the best use of existing capabilities and resources.[64] To succeed, the government must continue to foster interagency cooperation and close relations with international partners to synchronize C-IED capabilities. To facilitate that cooperation, we must establish procedures to ensure effective and timely information and intelligence exchanges.

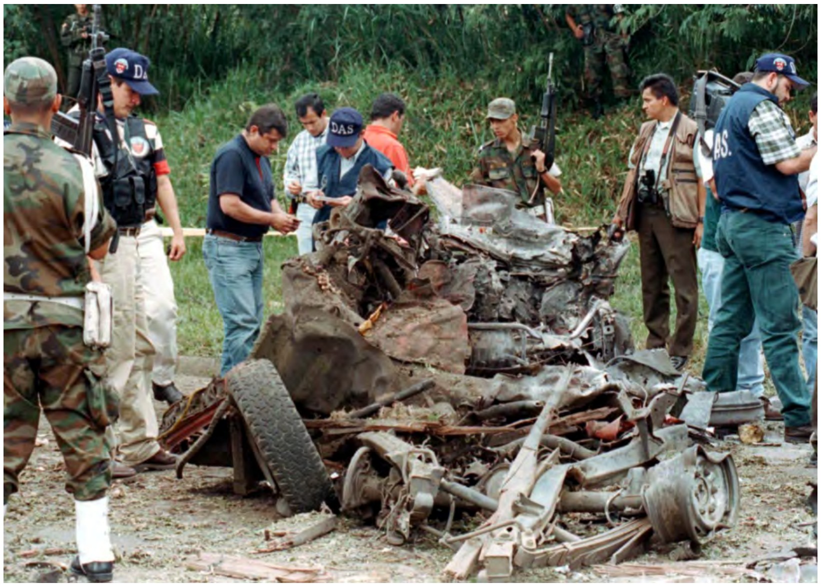


Figure 1-1. Car Bomb Investigation. *Colombian investigators examine remains of a car after it was detonated by the Revolutionary Armed Forces of Colombia (FARC). (Photo Credit: Reuters)*

As illustrated in **Figure 1-1,** improvised weapons are not exclusive to Iraq and Afghanistan or other Central Command (CENTCOM) regions. As US and coalition forces transition out of combat operations in Afghanistan, IEDs and improvised weapons will increasingly become a global threat.

"Since 2007, IED incidents outside of Iraq and Afghanistan have increased to more than 500 events per month. Since January 2011, there have been more than 10,000 global IED (reported) events occurring in 112 countries executed by more than 40 regional and transnational threat networks."[65]

1.2 Definition and Evolution of WT I

Weapons Technical Intelligence: A category of intelligence and processes derived from the technical and forensic collection and exploitation of improvised explosive devices, associated components, improvised weapons, and other weapon systems. [66]

WTI is a capability comprised of an organized framework of technical and forensic modalities and processes that systematically collect, exploit, analyze, and disseminate weapons-related information and material typically associated with an adversary. It melds site exploitation, materials handling,

[64] Obama, *Countering Improvised Explosive Devices.*

[65] LTG Michael Barbero, *JIEDDO statement to the House of Representatives Committee on Appropriations Subcommittee on Defense,* September 20, 2012

[66] U.S. Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms,* Joint Publication 1-02, Washington DC, November 8 2010 (as amended through March 15, 2013), pg. 313.

chain of custody maintenance, tactical characterization, technical categorization, latent biometrics collection and analysis, electronic engineering, application of forensic science, and other essential functions in service of the five WTI outcomes: force protection (FP), component material sourcing, targeting, support to prosecution, and signature characterization. WTI links technical and forensic information and material recovered from an incident site with existing intelligence about a threat organization or from an incident to more fully understand the adversary and better direct friendly force operations.

WTI evolved from traditional technical intelligence (TECHINT) to address the tactical commanders requirement to confront the growing IED threat in Iraq. WTI differs from traditional TECHINT; WTI capabilities help to confront the challenges of conducting exploitation in an asymmetric threat environment by supporting commanders' immediate intelligence needs, whereas TECHINT capabilities are more suited to exploiting a conventional threat **(Figure 1-2)**. WTI supports warfighters throughout the range of military operations (ROMO), but is most applicable in counterinsurgency/asymmetric environments. WTI provides input to and supports analysis conducted by multiple intelligence disciplines such as:

- TECHINT
- Signals intelligence (SIGINT)
- Measurement and signature intelligence (MASINT)
- Human intelligence (HUMINT)
- Open source intelligence (OSINT)

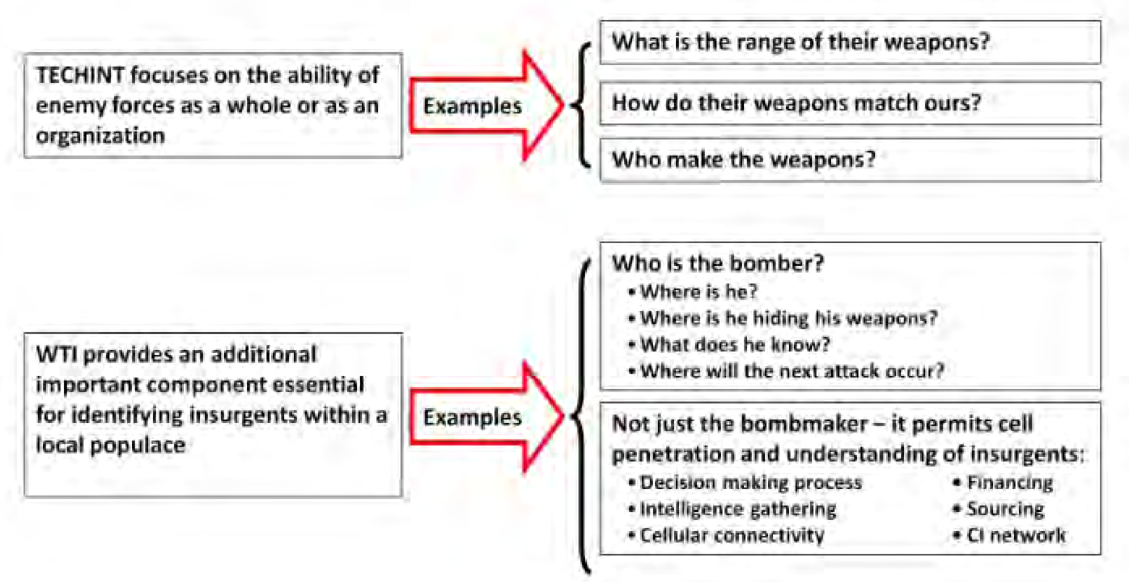

TECHINT focuses on the ability of enemy forces as a whole or as an organization
Examples
What is the range of their weapons?
How do their weapons match ours?
Who make the weapons?
WTI provides an additional important component essential for identifying insurgents within a local populace
Examples
Who is the bomber?
• Where is he?
• Where is he hiding his weapons?
• What does he know?
• Where will the next attack occur?
Not just the bombmaker – it permits cell penetration and understanding of insurgents:
• Decision making process
• Intelligence gathering
• Cellular connectivity
• Financing
• Sourcing
• CI network

Figure 1-2. The Differences Between TECHINT and WTI (Figure Credit: Joint Improvised Explosive Device Defeat Organization [JIEDDO])

WTI influences informational products within and outside of the intelligence community (IC). WTI supports the collection, exploitation, analysis, and dissemination of weapons threat material and information by providing a framework for consolidating data from disparate events across an array of domestic and international organizations.[67]

1.3 Shifting to Counter the Global IED Threat

As US and partner nation forces withdraw from Afghanistan, they must redirect focus on domestic and global IED threats. Organizations that contribute to WTI, including the DoD, must adapt to the worldwide threat (**Figure 1-3**). This shift in geographic focus will require WTI support organizations and Combatant Commanders (CCDRs) to increase emphasis on building partnerships with intelligence, interagency, and international partners to promote intelligence and information sharing, build capacity, and develop complementary capabilities.[68] A comprehensive whole-of-government approach must occur at the federal and national level, as well as at regional, state, and local levels.

Figure 1-3. Evidence Collection. *Colombian police officer collects evidence from an IED planted by the FARC.* (Photo Credit: Reuters)

As force reductions continue in Afghanistan, access to information, materials, and components related to IEDs and improvised weapons will diminish. This will limit ability to exploit information and material used to target critical adversarial vulnerabilities. Therefore, a broader set of organic capabilities must be considered to support WTI efforts. Within the DoD, these capabilities reside in Special Operations Forces (SOF), maritime interception forces, and other organizations that routinely interact with our global allies. Collection efforts that provide information and material for inclusion in the WTI process must be prioritized across the DoD.

"Small-footprint special operations missions will likely run a wide gamut in the future. Due to the end of the U.S. combat role in Afghanistan and the weakening of the core al-Qaeda organization, unilateral counterterrorism missions may evolve from high-tempo missions in a few countries to

[67] Defense Intelligence Agency/Joint IED Defeat Organization, *Weapons Technical Intelligence (WTI) Improvised Explosive Device (IED) Lexicon*, October 2012, pg. 5

NOTE: The WTI IED Lexicon provides a coherent conceptual framework and an operational vocabulary to address the IED threat worldwide. It encompasses the broad spectrum of IED Tactical Characteristics (employment scenarios), the variety of IED Technical Categorization (devices), and their critical components.

[68] Obama, *Countering Improvised Explosive Devices.*

far fewer but more geographically diffuse operations conducted against those who represent dire and imminent threats to U.S. interests."[69]

As combat operations in Afghanistan decline, WTI information gained from technical and forensic exploitation of improvised weapons will continue to support the identification, capture, and removal of global adversary networks. To support each contingency, a unique, flexible, modular/scalable WTI capability is required. WTI capabilities can be customized to counter the local threat and meet the commander's requirement to process and exploit materials and information collected. WTI exploitation capabilities range from small deployable exploitation teams with basic exploitation and analysis capabilities to an expeditionary laboratory with robust and advanced exploitation and analysis competencies. Analysis can impact immediate to long-term objectives that result in the targeting and dismantling of networks as information comes to light. Supporting organizations include local law enforcement (LE)/first responders and strategic level intelligence assets, depending on the level of threat and need. The advantage of WTI is its simplicity and scalability — few other processes have a stake in all levels of warfare. The use of IEDs, currently the preferred asymmetric weapon, requires that WTI endure.

1.4 A Whole-of-Government and Multinational Approach

"The threat from IED use is likely to remain high in the coming decade and will continue to evolve in response to our abilities to counter them. A whole-of government approach that integrates federal, state, local, tribal, territorial, private sector, and global participation in counter-IED activities will best position the United States to discover plots to use IEDs in the United States, or against U.S. persons abroad, before those threats become imminent."[70]

DIA, JIEDDO, military services, US interagency organizations, and our multinational partners have developed effective capabilities and processes to conduct timely and relevant collection, technical and forensic exploitation, and analysis of IEDs and other weapons employed in an asymmetric threat environment.

To date, WTI has been a predominantly DoD-centric function, with varying levels of support from the intelligence and interagency communities and international partners. A comprehensive whole-of-government approach to WTI is needed in a world where adversaries have proven to be resilient, interconnected, and able to freely exchange information, technologies, training, and funding.

"Similarly, other events have caused terrorist groups that are not linked ideologically to form mutually beneficial partnerships. These partnerships have provided otherwise less capable terrorist groups with the opportunity to improve their skill and their reach. In each circumstance, emerging alliances could increase the threat that terrorism will pose to the United States …"[71]

Activities conducted between the Provincial Irish Republican Army (PIRA) FARC in 1998 serve as one example of this type of exchange of information and training.

[69] Linda Robinson, *The Future of U.S. Special Operations Forces*, Council on Foreign Relations Report No. 66 April 2013.

[70] Obama, *Countering Improvised Explosive Devices.*

[71] Kim Cragin, et.al., *Sharing the Dragon's Teeth, Terrorist Groups and the Exchange of New Technologies*, RAND Corporation, 2007, Summary xiii.

"PIRA purportedly initiated contact with FARC in 1997 through the ETA [Euskadi Ta Askatasuna], with which PIRA has a long-standing relationship and has exchanged knowledge and technical know-how, particularly in bomb making. According to an April 2002 U.S. Department of State report, one of the three PIRA men, Connolly, Sinn Fein's representative in Cuba, initiated the contact with FARC in 1997; and, from 1998 to 2001, at least 15 PIRA militants have traveled to Colombia, along with Iranian, Cuban, and Basque terrorists, to train FARC."[72]

To keep pace with threat networks' information exchanges and capabilities, WTI needs to effectively exploit worldwide events that involve the employment of improvised weapons by adversaries. Failure to integrate all components of the WTI process and organizations that support the process with a whole-of-government approach puts the United States and partner nations at risk of being unprepared for future attacks.

The broader the "WTI coalition," the more fully prepared and proactive it will be. Cooperation resulting from a whole-of-government, multinational, and comprehensive DoD approach increases the likelihood that new enemy weapons/TTP will be more quickly detected and exploited. The more robust the WTI partnerships are, the faster, more expansive, and more effective information and knowledge sharing will be.

Participation by a more inclusive group brings challenges for contributing organizations. Traditional response to adversaries often entailed expert Explosive Ordnance Disposal (EOD) or Weapons Intelligence Team (WIT) tactical assessments and reporting through standardized databases to inform the WTI cycle. The wider approach will likely involve collection of materials and information by nontraditional WTI support organizations through nonstandard reporting means. Traditional WTI support organizations must develop standardized reporting mechanisms and expand training to account for an evolving approach to information collection and dissemination.

[72] Kim Cragin, et.al., *Sharing the Dragon's Teeth*,, pg. 71

CHAPTER 2
The Weapons Threat in the Operational Environment (OE)

2.1 General Description

Adversaries continue to use terrorist, guerrilla, and insurgent tactics that incorporate the use of improvised and conventional weapons in an asymmetric environment against stronger enemies. Terrorism and irregular warfare (IrW) continue to be significant threats because adversaries continue to gain the material resources, technology, and skills necessary to create and use them. When opportunity, intent, and capability to develop a particular weapon or strategy combine, those technologies and methods become a threat.

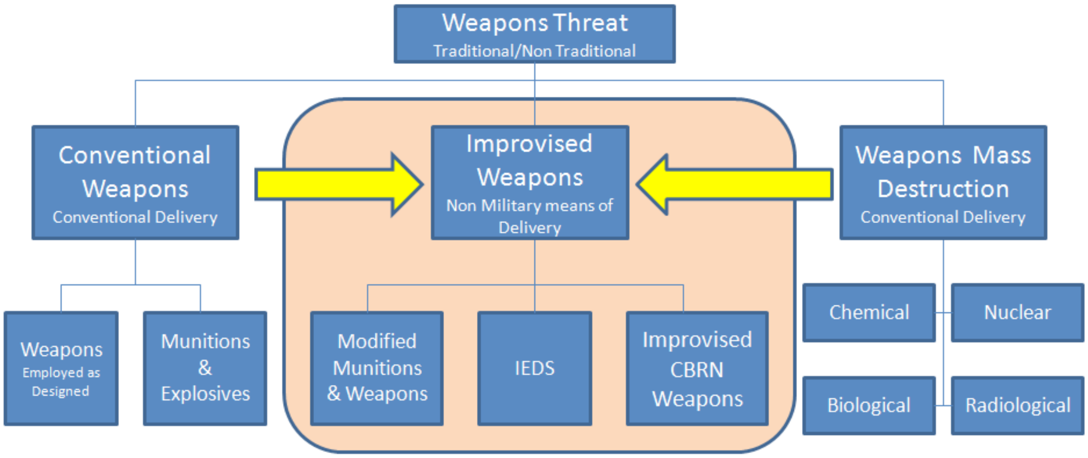


Figure 2-1. Traditional and Nontraditional Weapons Threat *(Figure Credit: DIA)*

As illustrated in **Figure 2-1**, improvised weapons are a subcategory of weapons threat that includes modified munitions and weapons; IEDs; and improvised chemical, biological, radiological, and nuclear (CBRN) weapons. Improvised weapons are effective in impacting ability to conduct operations, and are relatively inexpensive, simple to construct and emplace, and capable of achieving a tactical impact while producing a strategic effect.73

Improvised weapons are a function of enemies' intent to create instability through the use of criminal, insurgent, and terrorist activities. Terrorists and insurgents will continue to resort to the use of improvised weapons and asymmetric warfare in future conflicts because of the strength and superiority of US and partner nations' military capability and capacity. To counter this threat, WTI employs the capabilities and processes inherent in technical and forensic exploitation, and fuses its results with the products of other intelligence disciplines to better understand and mitigate the threat. WTI seeks to disrupt enemies' operational cycle and to defeat the networks that employ them. To succeed, WTI provides a framework of integrated enablers and capabilities that focus on neutralizing insurgent cells and networks.[74]

[73] National Academy of Science, *Countering the Threat*, http://www.nap.edu/catalog/11953.html, 2007, pg. 1

[74] Combined Joint Task Force Paladin, *FAT Report, Attack the Network*, Volume 1, Issue 3, October 6, 2011

2.2 Evolving Threat Capabilities

In terms of specific capabilities, future adversaries could possess highly adaptive combinations of weapon systems in all OEs, including land, maritime, space, and cyberspace. These could involve the use of highly adaptive combinations of anti-access and area-denial capabilities that challenge entry operations to a much greater degree than in the past and could potentially involve the use of weapons of mass destruction (WMD). These weapon capabilities comprise specific systems that can counter joint force entry operations. In an asymmetric threat environment, non-state actors (terrorists, insurgents, and criminals) use conventional and improvised weapons that are rapidly adaptable, easy to manufacture, and lethal.

The current and future strategic environment is and will likely continue to be characterized by multiple actors, adaptive threats, rapid change, chaotic conditions, and advanced technology-enabled threat groups seeking to dominate the battlefield and information environment. These threat groups are able to rapidly respond to changing OEs by employing new technologies, altering TTP, and changing organizational structures. They do so to gain strategic advantages in a world undergoing rapidly changing economic conditions, shifting political alliances, new informational environments, and changing ideological and cultural sensitivities. The adversary's objective extends beyond causing casualties and seeks to affect the psychology of the population by creating fear, instability, and discomfort.[75] The DoD and its interagency and international partners must therefore be operationally adaptive to identify, understand, and mitigate these complex challenges within these changing environments.

To better understand exploited information and material, it is necessary to understand the development and asymmetric use of emerging military and commercial technologies. As military and commercial technologies evolve, our adversaries will exploit them to develop new weapons and TTP to continue to influence the current and future OE. To combat this threat, commanders must understand how terrorist/insurgent organizations learn to adapt their weapons to be effective in each situation and how they overcome countermeasures intended to defeat their efforts.[76]

2.3 Employment of Threat Systems

Asymmetric threats are unlikely to stop anytime soon because our adversaries continue to gain material resources, technology, and skills to create and use improvised weapons. In Afghanistan, prior to 2001, despite over 30 years of continual warfare, there was not one documented suicide bombing. However, during the first decade of this century, the region experienced a significant cultural/ideological shift toward violent extremism. In 2002, as this ideological shift spread, suicide attacks began in Afghanistan. In 2005, the Taliban re-emerged as a serious threat to peace and security in Afghanistan, and spread an ideology that sanctions suicide attacks and exalts martyrs. This ideological shift resulted in 17 suicide attacks in 2005, and increased to 139 by 2006.

Future threats will likely expand the use of improvised chemical and biological weapons and advance anti-armor weapons. Development of sophisticated sensors, robotics, and encrypted communications technologies will enhance the capabilities and global reach of terrorist organizations. These technologies will be useful to threat groups around the world as they gain

[75] National Academy of Science, *Countering the Threat* http://www.nap.edu/catalog/11953.html, 2007, pg. 2

[76] Brian A. Jackson, *Aptitude for Destruction: Organizational Learning in Terrorist Groups and its Implications for Combating Terrorism*, RAND Corporation, 2005

financial, material, manpower, logistical, intellectual capabilities, and cultural/ideological resolve.[77] Additionally, US Army National Ground Intelligence Center (NGIC) assessed that "improvised weapons will become less [‘improvised’] as industrial bases in some countries manufacture devices that are more easily transported and emplaced by regular and irregular combatants – much like the booby traps and fuzes manufactured in former Yugoslavia."[78]

2.4 Conventional Weapons

Conventional weapons consist of state-manufactured ammunition and components produced for use by its armed forces in support of its national defense and security and do not contain chemical, biological, radiological or nuclear materials. Insurgent and terrorist groups employ conventional weapons in one of two ways. They either employ them as designed (e.g., sniper rifles and rocket propelled grenades [RPGs]), or by incorporating them into IEDs and other improvised weapon systems. Although "sophisticated explosive-based conventional weapons" (e.g., RPGs, mortars, and rockets) are commonly used by terrorists and insurgents, the use of explosives followed by firearms is most prevalent.[79]

High-explosives produced by nation states are also incorporated in improvised weapons. The proliferation of C-4 (i.e., military plastic explosives), trinitrotoluene (TNT), SEMTEX (a commercially available plastic explosive), and components for building IEDs is widespread in nations sponsoring terrorism and insurgent organizations. Conventional weapons and unexploded ordnance are commonly found on the battlefield, in locations of previous conflicts (i.e., in the Pacific region from WWII), and in failing/failed states, and are used as main charges in IEDs and improvised weapons by insurgents and terrorists, as illustrated in **Figure 2-2**.[80] At other times, conventional weapons escape state control during periods of instability within a nation or during wars and conflicts, as occurred during the Arab Spring.[81]

[77] UN's Assistance Mission in Afghanistan, *Suicide Attacks in Afghanistan(2001-2007),* September 9, 2007, pg. 38

[78] DIA, *Threat Trends Affecting U.S. Major Defense Acquisition Programs,* 2013-2033, May 2013, pg 76.

[79] Brian A. Jackson and David R. Frelinger, *Stealing the Sword, Rifling Through the Terrorist's Arsenal*, Working Paper, Rand Corporation, October 2007, pg. 8.

[80] NOTE: The Iraqi military had vast stockpiles of conventional military ordnance that remained unguarded after the collapse of the regime. Compounding that problem was a similar situation pertaining to the commercial explosives used in mining and construction. Unsecured military and commercial explosives (e.g., time fuse and blasting caps) provided Iraqi insurgents ready access to key IED components. Knowledge of both military ordnance and explosives that are used in the area of operations supports component sourcing and assists in determining evolutions of the insurgent threat.

[81] C.J. Chivers, "Counting Qaddafi's Heat-Seeking Missiles, and Tracking Them Back to Their Sources, At War, Notes From the Front Lines," *The New York Times,* July 26, 2011

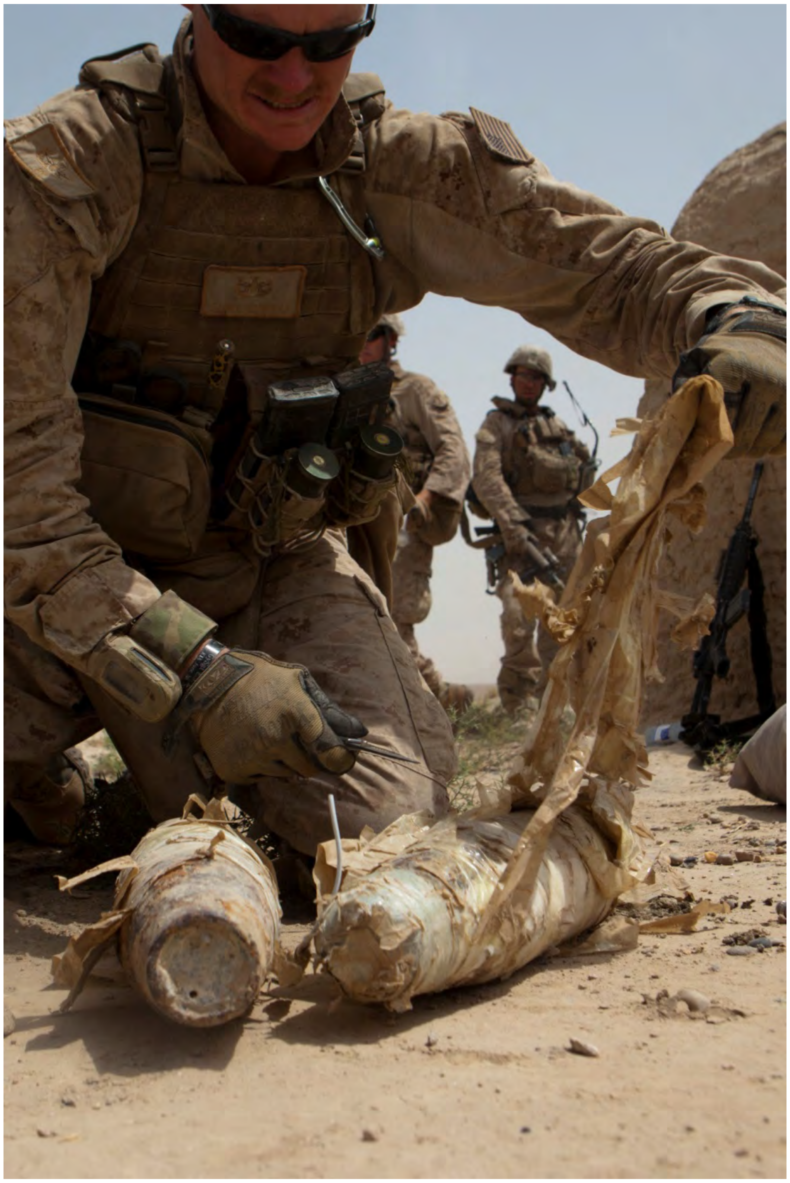


Figure 2-2. Conventional Ordnance Used in an IED. *An EOD Technician examines conventional ordnance repurposed as the main charge of an IED. (Photo Credit: DoD)*

Identification of conventional weapons is instrumental in determining how adversaries source materials. WTI technical and forensic capabilities play an important role in determining the source of conventional weapons and their supply networks. By identifying the nomenclature of a weapon or weapon system, analysts can potentially identify the country of manufacture and how the threat organization procured the weapon. Often, conventional weapons can be directly linked to the same transnational networks supplying IED components to terrorists and insurgents or used for drug trafficking, as demonstrated in Afghanistan. For example, exploitation conducted on ordnance recovered in Iraq determined that much of it originated in Iran, demonstrating how weapons can be identified and linked back to their source. In Iraq, the following conventional weapons were identified and traced back to their source: 81mm mortars, 82 mm mortars, 107 mm rockets, and RPG-7.[82]

Military munitions are often used as main charges in IEDs and can be provided by nation states sympathetic to an insurgent or terrorist cause. In many cases, the same network used to source IED materials is involved in acquiring and shipping foreign ordnance and other illegal contraband to insurgent and terrorist organizations. Gaining an understanding of the local OE can expose connections between IED supply networks, conventional ordnance supply networks, and improvised weapon fabrication and assembly networks.

Commercial explosives such as blasting caps, detonation cord, and liquid and bulk explosives typically used for construction, road building, quarrying, like those illustrated in **Figure 2-3,** are also sourced by insurgents and terrorists. Insurgent and terrorist access to commercial explosives via the black market or theft is common. Recent events in Nigeria and Mali highlight how easily commercial explosives are to obtain.

"It appears Boko Haram has access to large quantities of commercial explosives, rather than being forced to rely on less reliable and less stable improvised explosive mixtures. A good deal of mining occurs in central Nigeria, and it seems that the group is either stealing commercial explosives from mining companies, extorting mining companies for explosives using a front company or companies."[83]

"Last week soldiers combing abandoned jihadist hideouts also found a stash of NITRAM 5 explosives hidden inside rice bags that were left in a communal trash area. The explosives are manufactured for use in mining, but can cause considerable damage when used as bombs."[84]

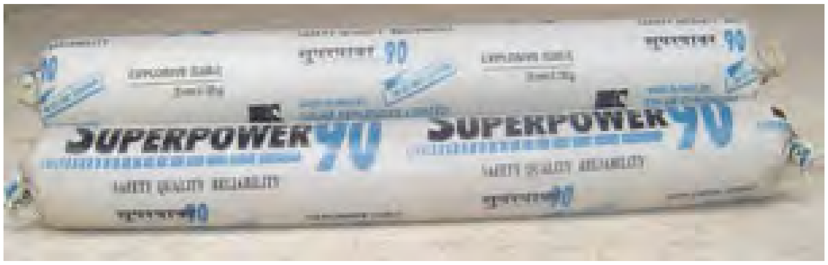


Figure 2-3. Superpower 90. *This is an example of a commercially available explosive specially designed for tunnel blasting and all kinds of underground and aboveground blasting operations. (Photo Credit: Wikipedia)*

[82] Kimberly Kagan, Iraq Report, *Iran's Proxy War against the United States and the Iraqi Government*. The Institute for the Study of War, May 2006-August 20, 2007, pg. 17

[83] STRATFOR Global Intelligence, "Nigeria's Broko Haram Militants Remain a Regional Threat," January 26, 2012.

[84] Krista Larson Associated Press, "French Mali Troops Recover Explosives in Gao." *USA Today,* February 13, 2013

2.5 Improvised Weapons

Improvised weapons include modified weapons and munitions, IEDs, and improvised CBRN weapons similar to those in **Figure 2-4**. Improvised weapons include conventional weapons (e.g., air-to-air rocket fired from an improvised ground launcher) that can be employed in an improvised manner (i.e., not as intended). These weapons incorporate destructive payloads and fillers designed to kill, destroy, incapacitate, harass, or distract.[85] Improvised weapons can incorporate military ordnance, but are normally made from a combination of military ordnance and nonmilitary components. For the purpose of this handbook, improvised weapons include:

- Modified weapons and munitions
- IEDs
- Improvised CBRN weapons

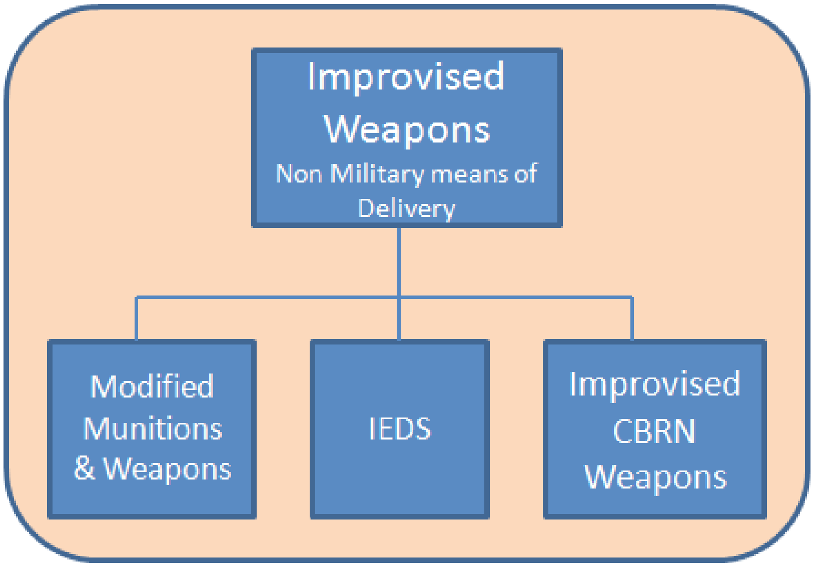


Figure 2-4. Categories of Improvised Weapons *(Figure Credit: DIA)*

2.5.1 Modified Weapons and Munitions

Modified weapons and munitions are fabricated from military and nonmilitary hardware and can have design and functional characteristics similar to conventional weapons. Terrorists and insurgents develop modified weapons by altering the use ordnance manufactured for a specific outcome (e.g., air-to-ground rocket) to achieve a different outcome (e.g., ground-to-ground rocket). As illustrated in **Figure 2-5** and **Figure 2-6,** a modified weapon system can incorporate multiple weapons, associated support equipment and delivery means, and can closely resemble conventional weapons. Conventional weapon systems can also be repurposed by adversaries to achieve an outcome other than the one for which the system was originally designed. One such example is the improvised rocket-assisted munitions (IRAM), which was constructed and employed in Iraq and Afghanistan and by the Palestinians against the Israelis, by the Syrian Rebels, and by both sides

[85] Defense Intelligence Agency/Joint IED Defeat Organization, *WTI IED Lexicon*, pg. 68.

in the Libyan conflict.[86] The IRAM uses a conventional rocket motor to extend the range of an attached improvised warhead and fusing system. The IRAM typically incorporates an improvised launch platform to provide a means of delivery.[87] This system combines conventional ordnance and design with improvised devices and design. These weapon systems are often fabricated from common materials available in hardware and electronics stores.

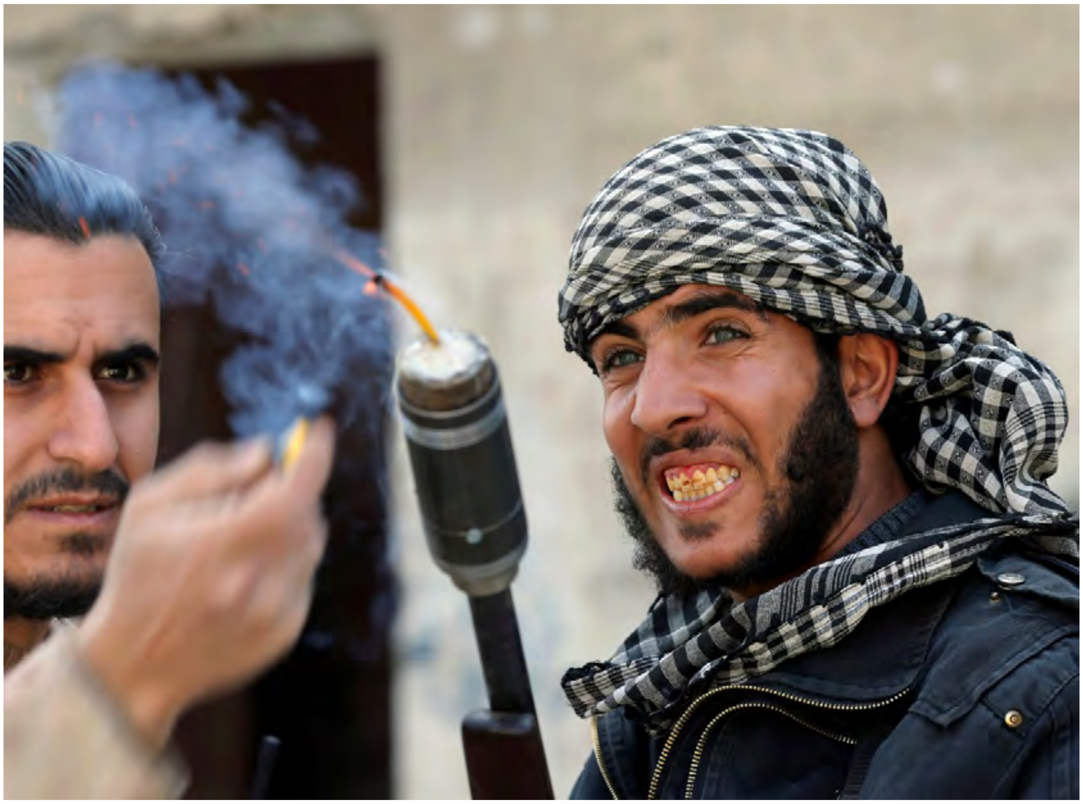


Figure 2-5. Modified Conventional Weapon. *Free Syrian Army forces use a modified shotgun to fire an improvised grenade at Syrian Army soldiers in Damascus, February 9, 2013. (Photo Credit; Reuters/ Goran Tomasevic)*

[86] C.J. Chivers, At War, Notes From the Front Lines, Mao's Rockets and Modern War, Part III, *The New York Times*, December 19, 2011.

[87] NOTE: IRAM launch platforms were often mounted in vehicles such as trucks and vans to allow expedient mobility.

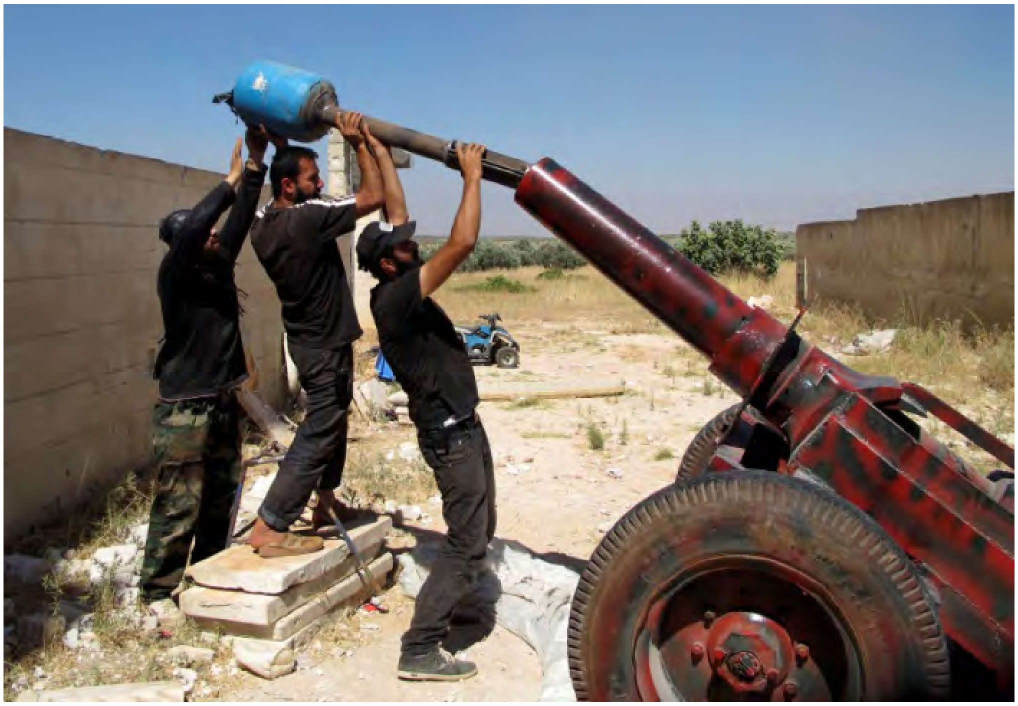


Figure 2-6. Repurposed Conventional Artillery. *Free Syrian Fighters Loading Locally Made Improvised Projectile into a conventional piece of artillery, July 17, 2013. (Photo Credit: Reuters/Hamid Khatib)*

The PIRA developed a range of improvised mortars, using locally procured and manufactured components whose progression and capability reached such a level of sophistication that it required a type and modification model number naming convention. This skill was later passed by PIRA to the FARC in Colombia.[88]

Analyzing insurgent manufacturing processes and geographical areas that favor weapon production helps tactical units focus search efforts and makes the enemy supply chain vulnerable to detection and interdiction. Disrupting the sourcing of a weapon employed in an asymmetric environment is an intended outcome of WTI. In an example of supply chain vulnerability, Intelligence Analysts discovered that PIRA was using light engineering factories to fabricate advanced improvised weapons after comparison of welds, metallurgy, circuit wiring, main charge, and flight stability design were conducted during technical exploitation and analysis. [89] More recently, Free Syrian Army fighters have established similar light engineering facilities to manufacture various weapons such as those illustrated in **Figures 2-7** and **Figure 2-8**.

[88] Cragin, et al., *Sharing the Dragon's Teeth,* pg. 84.

[89] A.R. Oppenheimer, *IRA, The Bombs and the Bullets* (Dublin: Ireland, 2009), pg. 231.

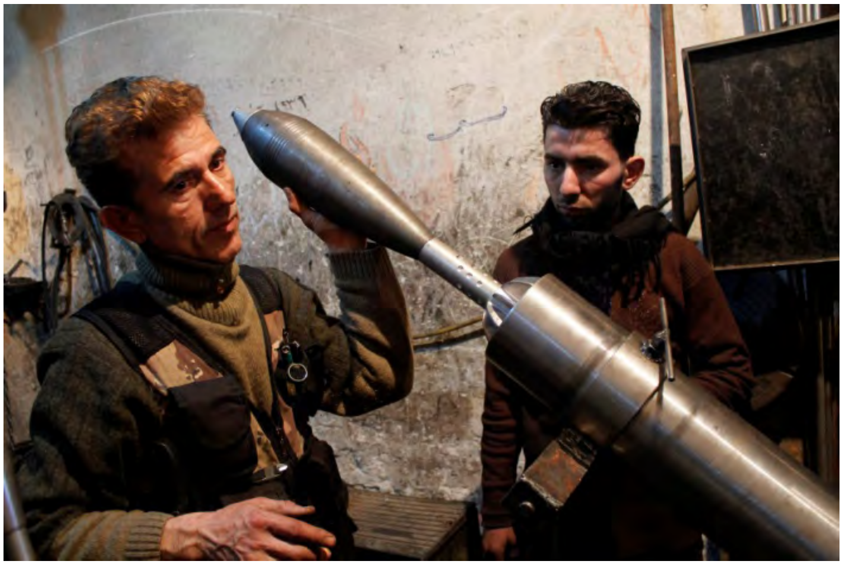


Figure 2-7. Light Engineering Facilities. *Free Syrian Army fighters manufacture homemade mortar tube, mortar, and fuze in Damascus, February 18, 2013. (Photo Credit: Reuters/Hamid Khatib)*

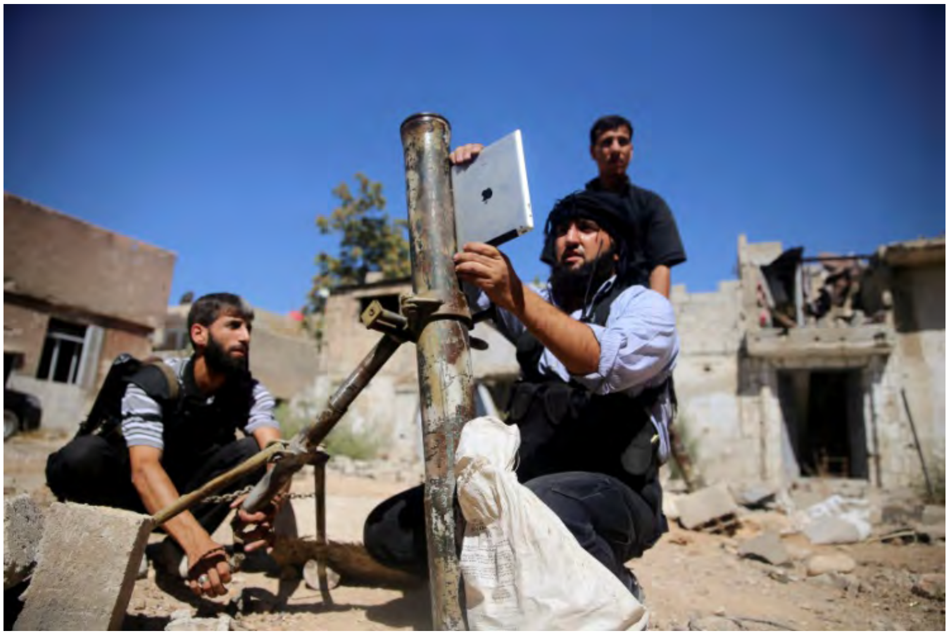


Figure 2-8. Homemade Weapons. *Free Syrian Army fighters use an iPad to aim a homemade mortar in Damascus, September 15, 2013. (Photo Credit: Reuters/Mohamed Abdullah)*

2.5.2 Improvised Explosive Devices (IEDs)

An IED is a weapon fabricated or emplaced in an unconventional manner that incorporates destructive, lethal, noxious, pyrotechnic, or incendiary chemicals, and is designed to kill, destroy, incapacitate, harass, deny mobility, or distract.[90] It can incorporate military munitions and hardware, but is generally constructed from components that are nonmilitary in nature.[91] IEDs can have enhancements (e.g., propane, scrap metals, chemicals, biological materials, nails) to achieve a secondary effect. However, the primary tactical outcome of the IED is its explosive effect.[92]

IEDs have five principle components: switch, initiator, main charge, power source, and container (**Figure 2-9**). The acquisition and use of components frequently requires a supporting network — an infrastructure of suppliers, financiers, manufacturers, tacticians, and operators, and, in the case of a large IED operation, trainers. Cells often include trainers when IEDs are constructed from a combination of military and nonmilitary components, or when IEDs incorporate more sophisticated technologies, such as cell phones or satellite phones as either arming or firing switches. If the IED operation is large enough and sufficiently active, each level of the organization leaves several "footprints" — indicators of their activities (observables[93] and signatures) — in the OE, which can be exploited to identify and interdict the cell's operations.

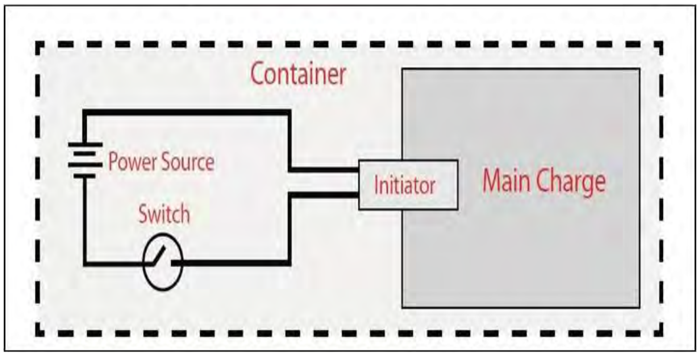


Figure 2-9. Principle IED Components Diagram *(Figure Credit: JIEDDO)*

For example, in Iraq, during the summer of 2006, insurgents routinely placed explosively formed projectiles (EFPs) in arrays to penetrate heavily armored coalition vehicles, and kill many US and coalition forces. Shortly thereafter, EFPs and components used to construct them were recovered along Iraq's southeastern border. Exploitation of the recovered explosives (C-4) used in the EFPs revealed that they chemically matched a specific lot of explosives sold by Iran's Defense Industries Organization.[94] Additional exploitation and intelligence revealed that "Iran originally manufactured EFPs for Lebanese Hezbollah and that copper EFPs require a great deal of metallurgical and

[90] U.S. Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms,* Joint Publication 1-02, Washington, DC, November 8 2010, as amended July 15, 2012, pg. 135.

[91] U.S. Joint Chiefs of Staff, *Counter-Improvised Explosive Device Operations*, Joint Publication 3-15.1, Washington, D.C., January 9, 2012, pg. vii.

[92] Defense Intelligence Agency/Joint IED Defeat Organization, *WTI IED Lexicon*, pg. 58

[93] NOTE: An observable is a unique descriptive feature associated with the visible description of the target, whether it is specific units, equipment, or facilities. *Joint and National Intelligence Support to Military Operations,* Joint Publication 2-01, Washington, D.C., Joint Chiefs of Staff, January 5, 2012, pg. III-21

[94] Rick Atkinson, "There was a two-year learning curve…and al lot of people died in those two years.", *The Washington Post,* October 1, 2007.

technological precision to manufacture. Consequently, they could not be made without specific machinery, access to which the Iranians have controlled."[95]

When properly constructed and employed, IEDs have a direct correlation to intended outcome and tactical design of an attack.[96] Terrorists/insurgents target a specific type of vehicle, discern its material vulnerability, and employ a device to cause a specific tactical outcome. For example, to effectively attack the light-skinned, flat underbelly of a high-mobility multipurpose wheeled vehicle (HMMWV), insurgents may choose to employ a buried IED, incorporating a large enough main charge so it functions as an anti-vehicle IED. **Figures 2-10, 2-11,** and **2-12** illustrate various types of IEDs and the damage they can cause.

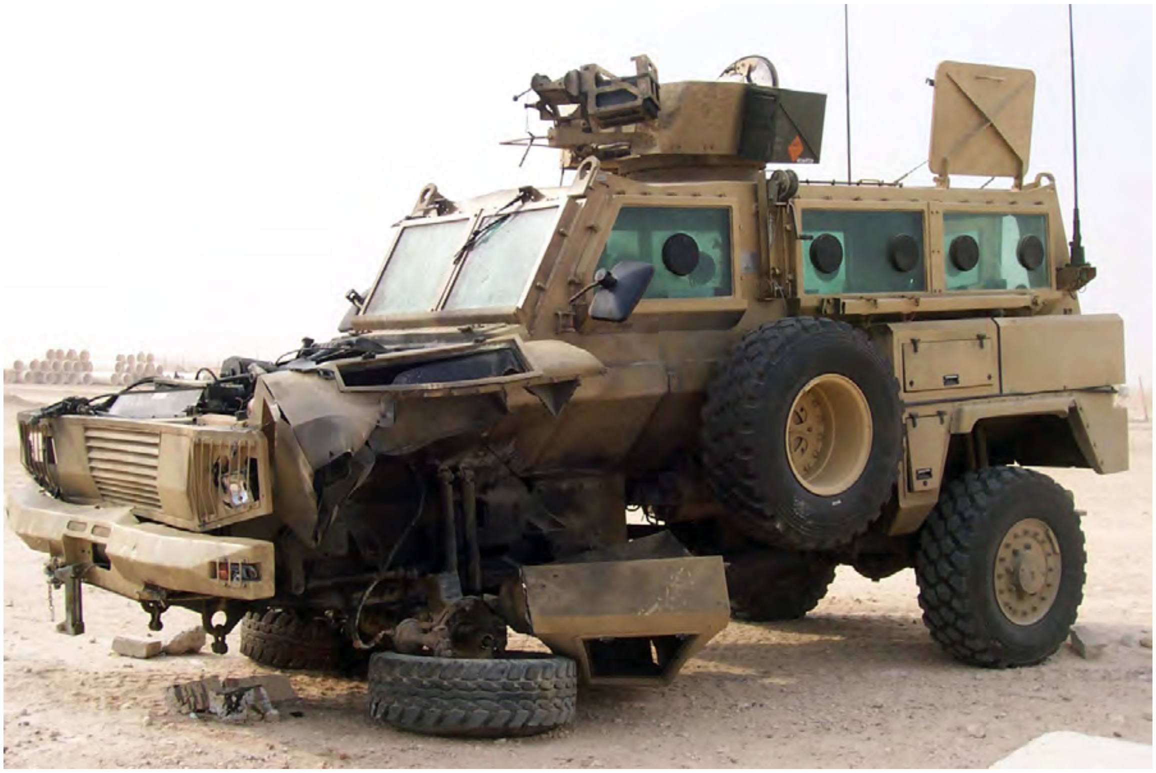


Figure 2-10. Underbelly Attack Results. *This shows the outcome of an underbelly attack using an IED buried in the road or in a culvert. (Photo Credit: JIEDDO)*

[95] Kagan, "Iraq Report, Iran's Proxy War," pg 17

[96] Defense Intelligence Agency/Joint IED Defeat Organization, *WTI IED Lexicon*, October 2012, pg. 11.

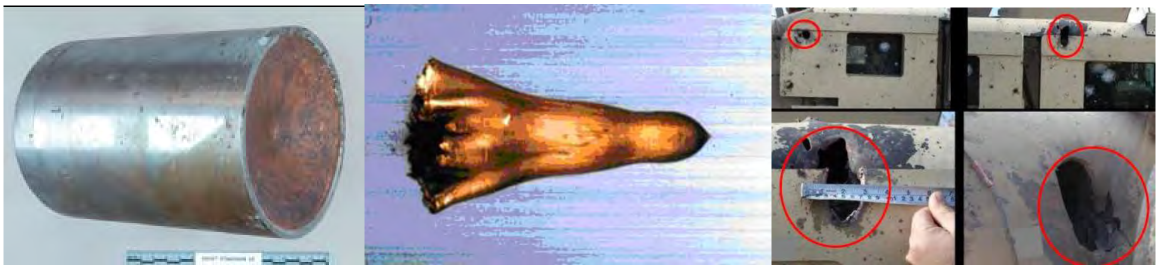


Figure 2-11. (From left to right) EFP, Its Slug, and Damage Caused by an EFP to a HMMWV *(Photo Credit: CJTF Troy)*

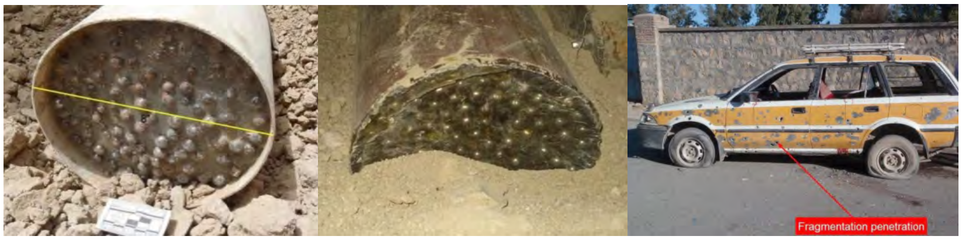


Figure 2-12. Pictures of Directional Fragmentation Charge, Directional Focused Fragmentation Charge, and Damage Caused *(Photo Credit: CJTF Paladin)*

IEDs are a proven weapon to use against a stronger and more sophisticated military because of the following reasons:

- Degree of surprise and standoff
- Cost effectiveness — they often made from unexploded ordnance; lost, stolen, or discarded military munitions; or commercial explosives. If military/commercial explosives are not available, homemade explosives (HME) can be used
- Difficult to detect and easy to adapt to multiple types of terrain
- Efficient psychological warfare weapon that creates fear ,intimidation, and desired publicity
- Perceived by the adversary to pose minimal risk from the tactical perspective. Once emplaced, the device is either fired from an isolated area or is victim operated
- Target rich environment created by vulnerable targets such as lines of communication (LOC), ports **(Figure 2-13),** airports, staging areas, and critical infrastructure.[97]

[97] U.S. Joint Chiefs of Staff, *Joint Operations Across the Range of Military Operations*, Joint Publication 3-0, Washington, DC, August 11, 2011, pg I-4.

NOTE: http://en.wikipedia.org/wiki/Line_of_communication, LOC is the doctrinal term that describes the route that connects an operating military unit with its supply base for all environments such as Sea Line of Communication (SLOC), Air Line of Communication (ALOC)

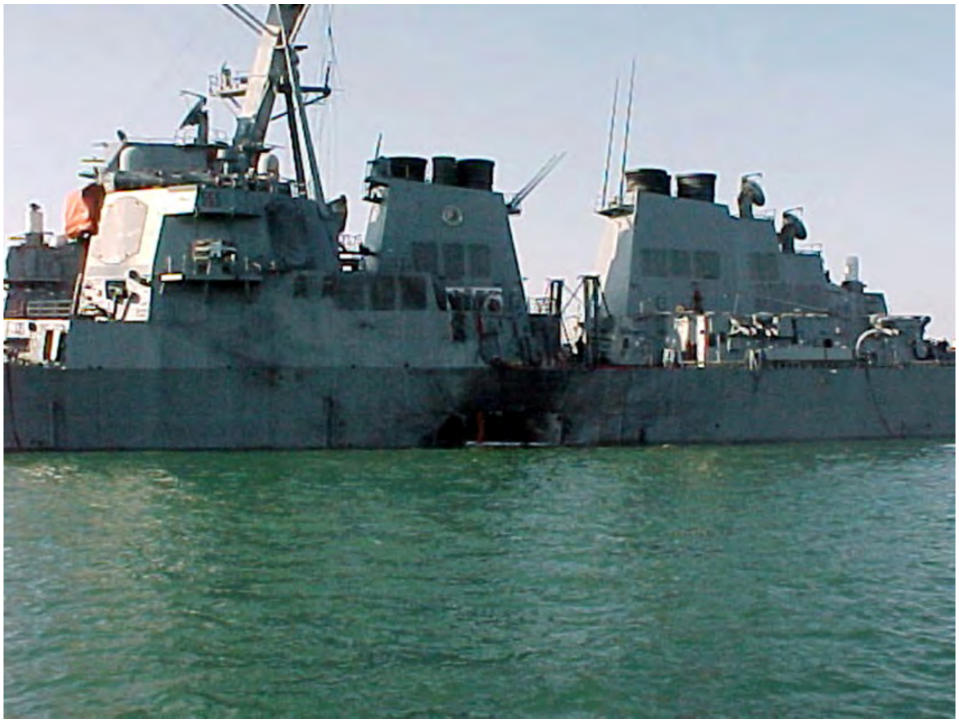


Figure 2-13. Vulnerable Target. *The USS Cole (DDG-67) was damaged by a water borne IED while refueling in the Port of Aden, Yemen, October 12, 2000. (Photo Credit: USN)*

The transfer of technology over time, relationships between various threat groups, and their efforts to improve improvised weapon effectiveness exist at all levels of operation. **Figure 2-14** illustrates the evolution of IEDs to enhanced IEDs to improvised CBRN weapons. The "PIRA and FARC case[s] also [demonstrate] that technology exchanges can increase terrorist groups' operational range and effectiveness. This success was the result of trust built between PIRA and FARC."[98]

2.5.3 Improvised CBRN Weapons

The combining of CBRN material into improvised weapons, with and without explosives (dispersal), is ongoing, as demonstrated by the explosives recovered in Moscow park from a radiological dispersal device (RDD) in 1995; the 1999 use of Sarin in the Tokyo subway; the 2001 US anthrax letters; the 2004 failed attack in Jordan (five trucks with toxic material with explosives); and the February 2007 through April 2007 attacks in Iraq (chlorine gas and explosive or nitric acid with larger caliber ammunition).[99]

[98] Cragin, et al., *Sharing the Dragon's Teeth*, pg 90.

[99] TRADOC G2 Handbook no. 1.04, *Terrorism and WMD in the Contemporary Operational Environment*, August 20 2007, pgs. II-9, II-21 and II-29.

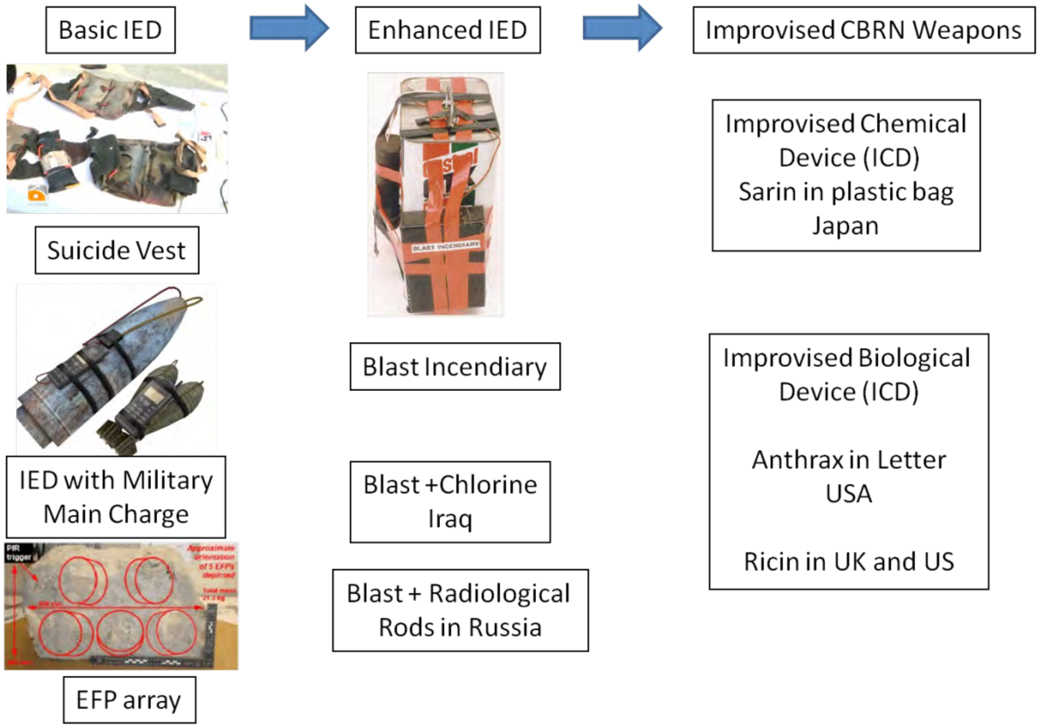

Basic IED
Enhanced IED
Improvised CBRN Weapons
Suicide Vest
Improvised Chemical Device (ICD) Sarin in plastic bag Japan
IED with Military Main Charge
Blast Incendiary
Improvised Biological Device (ICD)
Anthrax in Letter USA
Ricin in UK and US
Blast +Chlorine Iraq
Blast + Radiological Rods in Russia
EFP array

Figure 2-14. Evolution of Improvised Weapons *(Figure Credit: TRADOC G2)*

Although few instances of improvised CBRN incidents have occurred over the past decade, the CBRN threat is one of the most extreme of all terrorist tactics. Hostile state and non-state actors seeking to acquire WMD materials pose a threat to the US and its allies. The string of terrorist improvised chemical weapons terrorist attacks in Japan in 1995 made a formerly theoretical scenario a reality. Years of discussions, debates, and contrasting assessments on the possibility of terrorist organizations' use of improvised (nonconventional) weapons for mass murder came to an end when Sarin, a toxic gas, was released in the tunnels of Tokyo's subway system by the Japanese apocalyptic cult, Aum Shinrikyo, killing 13 people and prompting 6,000 others to seek hospital treatment.[100] The evolution of improvised weapons, including improvised CBRN weapons, presents a unique challenge that the WTI process is ideally suited to tackling because of its broad range of contributors, and collection, transportation, and exploitation assets. The proliferation of CBRN-related materials, technology, and expertise make the potential use of these types of weapons against the United States and its allies more likely — as evidenced in 2002, when 13 people died after being infected with anthrax, and in April 2013, after several letters containing ricin were interdicted en route to the President of the United States and a Congressman.

"The use of chemical and biological weapons by terrorist groups remains a potent risk to the United States and countries around the world."[101]

[100] Richard Danzig et al., "Aum Shinrikyo, Insights into How Terrorists Develop Biological and Chemical Weapons, Second Edition," Center for a New American Security, December 2012, pg. 5.

[101] Ibid.

2.5.3.1 Improvised Chemical Device

Improvised chemical weapons are relatively inexpensive and do not require extensive facilities or resources to manufacture; even poorer organizations can easily obtain, create, or employ improvised chemical weapons. Chemical hazards associated with improvised chemical devices include chemicals that cause death or harm through their toxic properties. Chemical hazards employed in an improvised weapon can originate from chemical weapons, chemical agents, and toxic industrial chemicals, and are relatively easy to transport. An improvised nuclear weapon is larger than an improvised chemical device, and more cumbersome to handle, requiring special vehicles and security to transport it. Conversely, a jar containing several hundred grams of a chemical substance can cause mass mortality and be transported easily without special preparation, vehicles, or security. Examples of improvised chemical weapons include hydrogen cyanide (Zkklon B) used by Aum Shinrikyo in a Tokyo shopping center restroom on April 30, 1995 and in the Tokyo subway on May 5, 1995,[102] and the use of chlorine bombs by Al-Qaida in Iraq in 2007.[103] **Figure 2-15** highlights the ease with which a chemical dispersal device can be fabricated using simple and easily obtainable commercial off-the-shelf (COTS) components. The following methods may be used to disperse improvised chemical weapons:

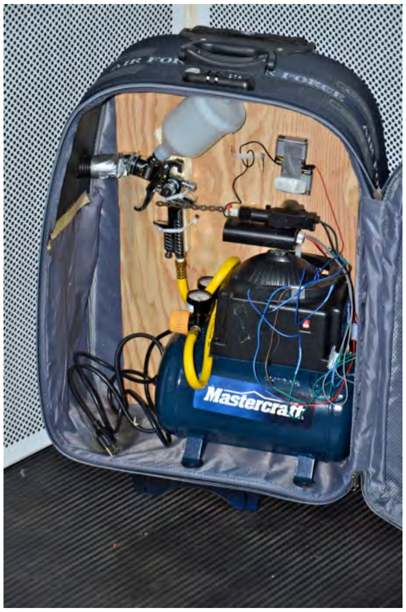


Figure 2-15. Chemical Dispersal Device. *Pictured is a Colombian military recreation of a recovered FARC chemical dispersal device. (Photo Credit: JIEDDO)*

- Release from container
- Spray/aerosol from agricultural machinery (ground or air)
- Small explosive charge to rupture major chemical container
- Improvised dissemination device that provides selective timing and standoff

Terrorists/insurgents can use improvised chemical devices to:

- Attack congested population centers, bodies of water, and unventilated areas that cause mass casualties
- Terrorize, blackmail, or cause economic damage, (e.g., contaminating a food with a toxic chemical)

2.5.3.2 Improvised Biological Device

The two most probable sources of biological improvised weapons are home manufacture or purchase from sovereign states. The most obvious toxins are botulinium, anthrax, and ricin. Each has advantages and disadvantages for users.

[102] Danzig, "Aum Shinrikyo, "Insights into How Terrorists Develop Biological and Chemical Weapons," pg. 21.

[103] Peter Bergen, "Reevaluating Al-Qa'ida's Weapons of Mass Destruction Capabilities," USMA, CTC Sentinel, 3, no. 9, (2010): pg. 2.

Improvised biological weapons can be made by those with limited capabilities, but normally require the use of sophisticated biological laboratories and resources, which are typically not available to terrorist organizations. However, various countries (particularly those that are unable to obtain nuclear weapons) have stockpiles of biological and chemical weapons (such as Syria as of December 1, 2013). These countries could provide biological weapons to terrorists they support to intimidate and panic a population.

Anthrax spores can be lethal if inhaled, and the source of the illness is not quickly diagnosed and treated. Since 2009, there have been reports of Al-Qaida currently having intent and capacity to develop an anthrax program, which has raised concern about the possibility of their anthrax program being reinitiated.[104] **Figure 2-16** shows an anthrax spore and a letter containing anthrax.

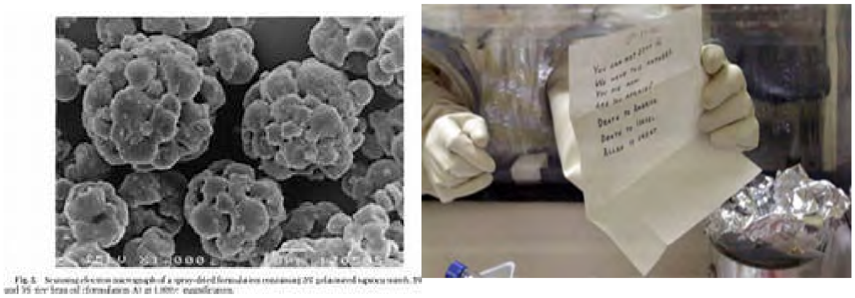


Figure 2-16. (left) Anthrax Spores and Letter with Spores. *Anthrax spores(left) were collected from letters (right) mailed to Senator Patrick Leahy in 2001.* [105] [106] *(Photo Credit: Sandia National Laboratories)(Photo Credit: FBI)*

As illustrated in **Figure 2-17,** ricin comes from the castor bean plant (*Ricinus communis*). On a small scale, it can be easily manufactured from castor beans in a14-step process, which makes it widely available; however, because of its lethality this toxin must be extremely carefully handled. It can be delivered as a powder, mist, or pill. LE officials intercepted letters containing ricin powder that were mailed to the US Congress and the President of the United States in April 2013.

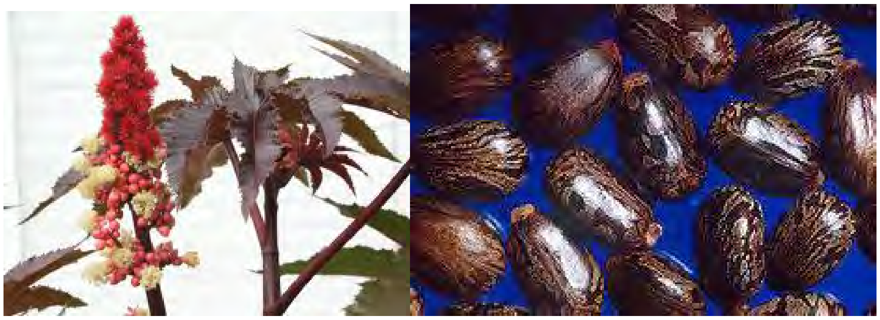


Figure 2-17. Ricin Plant and Castor Beans *(Photo Credit: Wikipedia)*

[104] Rene Pita and Rohan Gunaratna, "Revisiting Al-Qaida's Anthrax Program," USMA CTC Sentinel, 3, no. 5 (2009): pg. 1.

[105] Sandia National Laboratories, *FBI unveils science of anthrax investigation,* Sandia's work demonstrated anthrax letters contained non-weaponized form, https://share.sandia.gov/news/resources/releases/2008/anthrax.html.

[106] UCLA EDU, *Exposure Letters,* www.ph.ucla.edu/epi/bioter/detect/anteled_letter.a.hmtl

2.5.3.3 Radiological Dispersal Device (RDD)

An RDD is defined as improvised assembly or process, other than a nuclear explosive device, designed to disseminate radioactive material to cause destruction, damage, or injury.[107]

A "dirty bomb" is a type of RDD that uses conventional explosives or HME to disperse radioactive material, such as cesium 137 taken from radiotherapy machines (**Figure 2-18**). However, using explosives to disperse the radiological material is not the most effective method of dispersal because the heat of the explosion can consume or diminish the radiological materials effectiveness. Therefore, this method of dispersal results in more of a psychological affect than physiological effect, instilling fear, mass panic, and terror.

"Saddam Hussein reportedly tested such a weapon in 1987, but abandoned the effort when he saw how poorly it (RDDs) worked. In 1995, Chechen rebels buried dynamite and a small amount of the radioactive isotope cesium-137 in Moscow's Ismailovsky Park. They then told a TV station where to dig it up. Perhaps they recognized the truth: that the bomb's news value could be greater if it were discovered before it went off. For such weapons, the psychological impact can be greater than the limited harm they are likely to cause."[108]

Mixing radioactive material in food and water is a more effective dispersal method. The murder of Alexander Litvinenko, a former officer of the Russian Federal Security Service and KGB, by poisoning from the ingestion of polonium-210 on November 23, 2006, is an example of the effects of radiological poisoning by caesium-137 contamination.[109]

Figure 2-18. Cesium-137 Powder and Cesium Crystals *(Photo Credit: Wikipedia)*

[107] U.S. Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms,* Joint Publication 1-02, pg. 302.

[108] Richard A. Muller, "The Dirty Bomb Distraction, The biggest danger from radiological weapons is the misplaced panic that they would cause." *MIT Technology Review*, June 23, 2004 http://www.technologyreview.com//contributor/richard-a-muller/

[109] Ester Addley, "Alexander Litvinenko Murder," *The Guardian*, December 13, 2012.

2.5.3.4 Improvised Nuclear Device (IND)

A terrorist organization may attempt to obtain fissionable material or nuclear weapons in one of the following ways:

- Purchase fissionable material from such places as the Eastern European black market
- Purchase or obtain radioactive materials from other countries, particularly those that support terrorism. It is commonly known that "revolutionary" states like Iran actively and regularly assist various terrorist organizations
- Use its own scientists or hire scientists on the black market (many unemployed nuclear scientists are available on the world market and are willing to sell their professional expertise and experience to the highest bidder) to construct a simple radioactive device; it is unlikely that a terrorist organization could construct a nuclear bomb, which requires special resources and training that terrorist organization members do not currently possess
- Seize a nuclear stockpile, or one of many stockpiles of various nuclear devices and other hazardous substances around the world

These organizations have a different moral compass and do not fear a nuclear response or damage to their international interests as a result of using nuclear weapons. This fear deters sovereign states from using nuclear weapons. These factors make terrorist organizations more dangerous in terms of nuclear threats than sovereign states.

The simplest IND to construct is a gun-type nuclear weapon, illustrated in **Figure 2-19.**

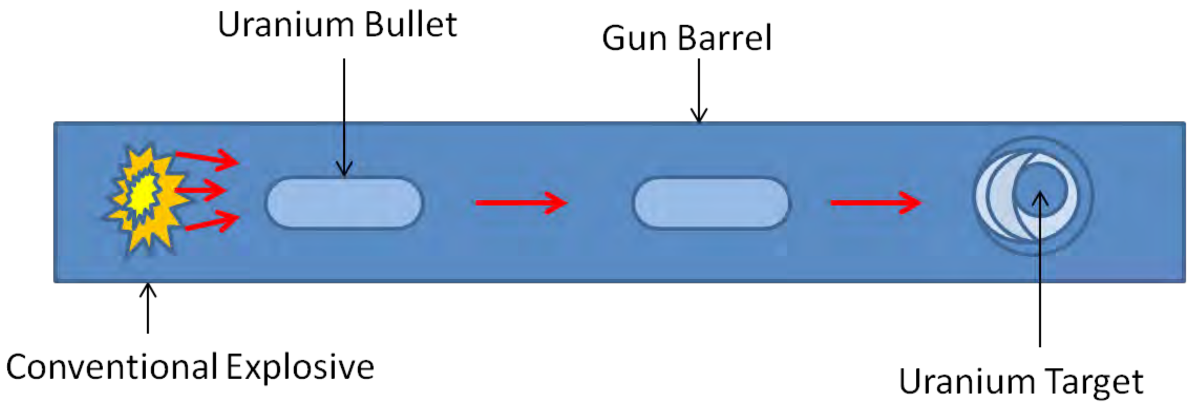


Figure 2-19. Gun-Type Nuclear Weapon *(Figure Credit: TRADOC G2)*

2.5.4 Weapons of Mass Destruction (WMD)

WMD are not the focus of this handbook, but an understanding of the difference between improvised CBRN weapons and state-produced WMD is useful. The DoD defines a WMD as "chemical, biological, radiological, or nuclear weapons capable of a high order of destruction or causing mass casualties and exclude[s] the means of transporting or propelling the weapon where such means is a separable and divisible part from the weapon."[110]

- **Chemical Weapons.** The following are considered chemical weapons:
  - Toxic chemical and its precursors, except when intended for a purpose not prohibited under the Chemical Weapons Convention
  - Munition or device, specifically designed to cause death or other harm through toxic properties of chemicals it could release
  - Equipment specifically designed for use directly in connection with the employment of munitions or devices [111]
- **Biological Weapon.** An item or material which projects, disperses, or disseminates a biological agent including arthropod vectors[112]
- **RDD**. An improvised assembly or process, other than a nuclear explosive device, designed to disseminate radioactive material to cause destruction, damage, or injury[113]
- **Nuclear Weapon**. A complete assembly (i.e., implosion, gun, or thermonuclear type) in its intended ultimate configuration, which upon completion of the prescribed arming, fusing, and firing sequence, is capable of producing the intended nuclear reaction and release of energy[114]

2.6 Weapons of Concern

Weapons of concern are defined as new or advanced conventional or improvised weapons that are significant enough to illicit a WTI-level response. NGIC coined this term to address situations that support the requirement to assess a military weapons capability, identify items for directed technical collection, support FP, support science and technology (S&T) activity, and create a professional posture.

Weapons of concern are capable of inflicting a considerable numbers of casualties, and can penetrate or defeat current countermeasures, resulting in an operational commander altering his operations and FP measures to mitigate their effects. Employment of weapons of concern illicit a dramatic response by the S&T community to rapidly understand and develop countermeasures to address existing capability gaps.

Weapons of concern are typically dynamic systems that reflect new enemy acquisitions, modifications of older weapons, or innovative uses of existing weapons and associated paraphernalia. They can include technology advancements in night vision devices and laser target designators. Often

[110] U.S. Joint Chiefs of Staff, *Combating Weapons of Mass Destruction*, Joint Publication 3-40, Washington, DC, June 10, 2009, pg. I-I.

[111] U.S. Joint Chiefs of Staff, *Operations in Chemical, Biological, Radiological and Nuclear (CBRN) Environments*, Joint Publication 3-11, Washington, DC, August 26, 2008, pg. GL-7.

[112] U.S. Joint Chiefs of Staff, *CBRN Environments*, Joint Publication 3-11, pg. GL-5

[113] U.S. Joint Chiefs of Staff, *CBRN Environments*, Joint Publication 3-11, pg. GL-6

[114] U.S. Joint Chiefs of Staff, *CBRN Environments*, Joint Publication 3-11, pg. I-8.

weapons of concern are channeled through criminal groups responsible for enabling activities, such as smuggling and laundering of illicit weapons-trade revenues.

New weapons capable of penetrating defenses of the US and its allies will likely proliferate in the future OE. Weapons of concern may include state manufactured and/or improvised weapons, including chemical, biological, and radiological weapons and weapon enhancements. Development and deployment of chemical, biological and radiological weapons leave signatures (i.e. logistical and financial, material, and SIGINT) that are accessible to investigation across the intelligence spectrum. Competent WTI analysis can trace the physical material and financial, communications (SIGINT), and demographic/sociological information, to develop a fuller intelligence picture of the networks, groups, and individuals who develop and employ these weapons of concern.

2.6.1 Improvised Weapon of Concern

EFPs used by insurgents in Iraq to effectively defeat US and coalition armored vehicles are an example of an improvised weapon of concern.

“EFPs varied in size, most were about the size of a small oil drum or a five-gallon paint bucket, but they could be even smaller [sic]. *Insurgents positioned them a few feet above the ground and aimed them to shoot laterally into the roadway. Once triggered, often by hidden infrared sensors, an explosive charge on the back of the drum forced a concave metal cone to be reshaped into a dart like stream in the direction of the target. The dense molten stream, often the size of a bowling pin and traveling at twice the speed of a bullet* [sic], *punctured inches of metal plating like water through snow. Inside the vehicle, the molten slug cut through legs and torsos, and its heat often lit the cab and the men inside on fire. Our heaviest armored vehicles were vulnerable and despite extensive countermeasures, in large number they were a potential game changer.”*[115]

2.6.2 Conventional Weapons of Concern

The most common weapons of concern today are sniper rifles, thermobaric weapons, anti-tank guided missiles, mortar and rocket warheads containing sub-munitions, improved rocket propelled grenades and anti-tank grenades, large limpet mines, precision indirect fire systems (i.e., advanced mortars), and Man Portable Air Defense Systems (MANPADS). Terrorists used Russian built MANPADS in Mombasa, Kenya, to attack an Israeli airliner in November 2002. In response, the United States negotiated multinational agreements to impose export controls on MANPADs, and S&T research to develop a countermeasure to protect commercial airliners.[116]

Likewise, the Barrett .50 caliber sniper rifle used by the PIRA against British forces in Northern Ireland is a good example of a conventional weapon of concern. The .50 caliber sniper rifle significantly changed tactical operations and caused a dramatic shift in research and development (R&D) priorities necessary to develop materiel solutions.

“*By 1997, troops were being issued with body armor containing a ceramic plate made from boron carbide, which could protect the trunk from a .50 caliber round; Kevlar flak jackets had proved*

[115] GEN (RET) Stanley McCrystal, *My Share of the Task*, (London: Portfolio Publishing, 2013), pgs. 426-427. NOTE: [sic] has been added to this quote to indicate that it was transcribed verbatim from General McCrystal’s book to convey the significant threat posed by EFPs. While generally correct, subject matter experts will note that the EFP description is not technically accurate.

[116] James Bonnomo, et al, *Stealing the Sword,* pgs. xv-xvi..

useless against such a bullet. But a set of boron carbide body armor not only cost $4000 but weighed 32 lbs. making it too heavy to be worn on patrol.”[117]

The introduction of the Barrett sniper system was complimented by a psychological warfare campaign against British and local security forces by declaring areas subject to fire by posting “Sniper at Work” road signs. In response to the sniper threat, intelligence collection resources supported by Special Air Service directed surveillance and direct action capability to identify the PIRA cells using the weapons and suppress their activity, which they successfully did; however, important and unique assets were tied up in this effort. In addition, network attack techniques were used to identify and backtrack to the origin of purchase and identify the supply routes of this conventional weapon. **Figure 2-20** illustrates a PIRA sniper rifle and used in their psychological warfare campaign propaganda.

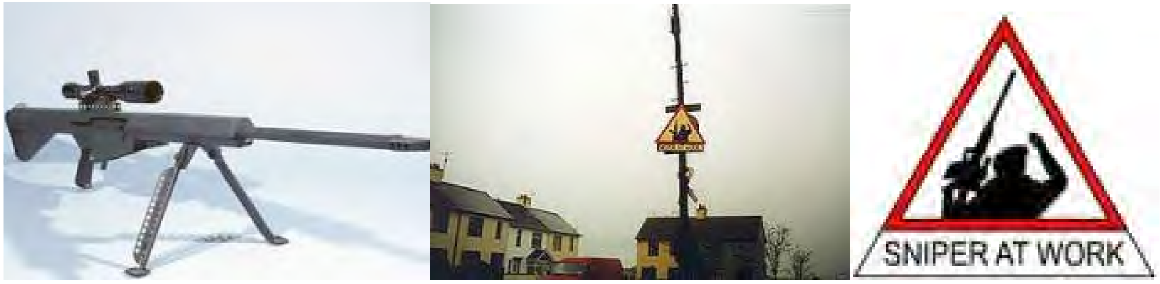


Figure 2-20. A Sniper Rifle and Propaganda *(Photo Credit: Wikipedia)*

2.7 Conclusion

As the US and its allies develop new technologies and equipment to counter the weapons threat, it will spur terrorists or insurgents’ improvised weapon innovation cycle to develop weapon systems that counter new countermeasures. Therefore, the US needs to reduce the surprise on the battlefield through the application of technical and forensic applications. The future OE’s complexity and unpredictability mandates a proactive approach to understanding weapons used by our adversaries. While a forensic component of WTI is a necessary and valuable contribution to responding to emerging weapons threats, it concedes the initiative to the adversary. A continual examination of weapons R&D, investments, enabling capabilities (e.g., night vision devices), and manufacture can contribute to a holistic view of an OE. Analysis of the characteristics of an OE and continual observation of events can help to anticipate conflict. Understanding the human dimension of the OE can help anticipate the way weapons, weapons technology, and tactical design might be employed against a joint force. Historically, the United States has been vulnerable to surprise at all levels — tactical, operational, and strategic. A new weapon or a new application of an old weapon drives effects up to the strategic level. A proactive approach to WTI and integration of worldwide developments in weapons research and production into the overall analysis of the OE will help the United States develop and adapt technical and materiel countermeasures and adopt mitigating tactical and operational procedures.

[117] Toby Harden, *Bandit Country: The IRA & South Armagh* (London: Hodder and Stoughton, 1999), pg. 405. NOTE: Toby Harnden’s book devotes an entire chapter to this particular threat, from its introduction into Northern Ireland to the SAS’s raid that lead to the seizure of one of two of the Barretts, with the second still not turned over as part of the Good Friday agreement.

CHAPTER 3
WTI Operating Concept

3.1 The WTI Operating Concept

Technical Intelligence (TECHINT): Intelligence derived from the collection, processing, analysis, and exploitation of data and information pertaining to foreign equipment and materiel for the purposes of preventing technological surprise, assessing foreign scientific and technical capabilities, and developing countermeasures designed to neutralize an adversary's technological advantages (JP 2-0)

Weapons Technical Intelligence (WTI): A category of intelligence and processes derived from the technical and forensic collection and exploitation of improvised explosive devices, associated components, improvised weapons, and other weapon systems (JP 3-15.1)

The WTI process begins with the identification of an incident (i.e., use of an improvised weapon, IED explosion, the interdiction of weapon shipments, find/cache, hoax, false, or turn-in) and continues throughout the tactical, operational, and strategic levels of exploitation and analysis with continuous feedback loops. During this process, information is extracted and actionable intelligence is produced to generate a greater understanding of the threat in the OE.

WTI evolved from traditional TECHINT to address the challenges of an asymmetric environment. WTI leverages an enterprise architecture that spans tactical collection through strategic forensic/technical exploitation and intelligence analysis and focuses on improvised weapon systems, associated components, and other weapons systems.[118] WTI enabling capabilities, processes, and functions combine elements from military services, intelligence agencies, federal LE agencies, national laboratories, and partner nations to produce actionable intelligence. WTI employs capabilities and processes, such as site exploitation, forensic material handling and chain of custody, technical categorization of a weapon, tactical characterization of an event, latent biometrics collection and analysis, electronic engineering, explosive chemistry, and the application of forensic science and analysis. WTI also provides data to and leverages the capabilities and processes of biometric enabled intelligence (BEI)/forensic enabled intelligence (FEI), document and media exploitation **(**DOMEX) enabled intelligence, indicators, observables, and signatures to support five critical outcomes: FP, targeting, component and material sourcing, support to prosecution, and signature characterization. **Figure 3-1** describes five of the critical outcomes of WTI.

Traditional TECHINT of state-sponsored, conventional weapon systems involves a deliberate development and acquisition process wherein the intelligence "time-to-impact" on the battlefield can take months or years. WTI is a more responsive process focusing on improvised weapons, resulting in a faster "time-to-impact" cycle. It's imperative for the currency of commanders' situational awareness, that WTI enabling capabilities and processes keep pace with adversaries' rapid innovations and changing TTP cycles to determine changes in adversaries' capability and capacity. WTI results are particularly useful when discerning the use of improvised weapon components, such as IED switches and improvised weapon arming and firing systems.[119]

[118] U.S. Joint Chiefs of Staff, *Joint National Intelligence Support to Military Operations*, Joint Publication 2-01, Washington, DC, January 5, 2012, pg. III-39.

[119] (FOUO) Defense Intelligence Agency, *Capstone Concept of Operations for DoD Weapons Technical Intelligence*, paper prepared for Deputy Director for Force Protection, The joint Staff, J8, Washington, DC, December 2009, pg. 13.

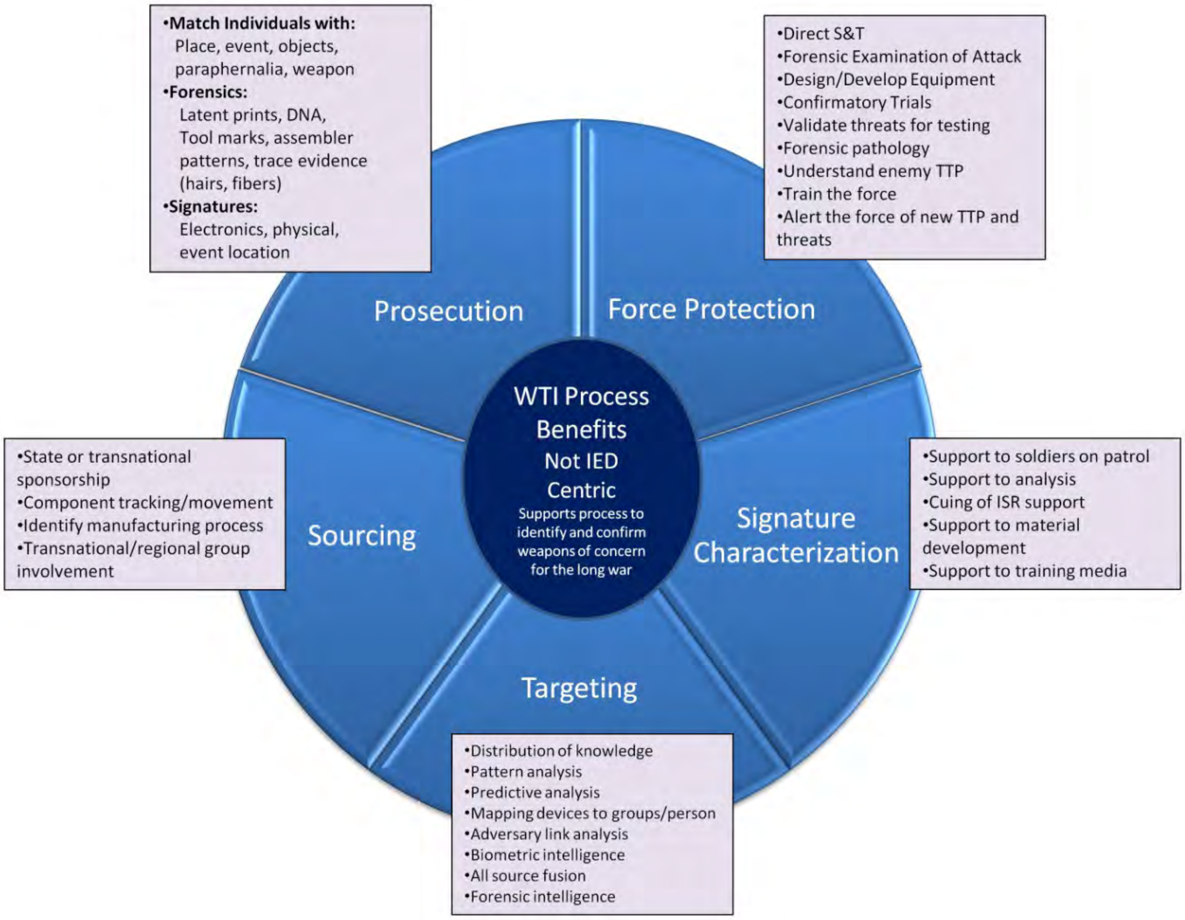

•Match Individuals with:
Place, event, objects, paraphernalia, weapon
•Forensics:
Latent prints, DNA, Tool marks, assembler patterns, trace evidence (hairs, fibers)
•Signatures:
Electronics, physical, event location
•Direct S&T
•Forensic Examination of Attack
•Design/Develop Equipment
•Confirmatory Trials
•Validate threats for testing
•Forensic pathology
•Understand enemy TTP
•Train the force
•Alert the force of new TTP and threats
Prosecution
Force Protection
WTI Process Benefits
Not IED Centric
Supports process to identify and confirm weapons of concern for the long war
•State or transnational sponsorship
•Component tracking/movement
•Identify manufacturing process
•Transnational/regional group involvement
Sourcing
Signature Characterization
•Support to soldiers on patrol
•Support to analysis
•Cuing of ISR support
•Support to material development
•Support to training media
Targeting
•Distribution of knowledge
•Pattern analysis
•Predictive analysis
•Mapping devices to groups/person
•Adversary link analysis
•Biometric intelligence
•All source fusion
•Forensic intelligence

Figure 3-1. WTI Critical Outcomes *(Figure Credit: DIA)*

The WTI process is broader than only technical categorization of improvised weapons; it encompasses the tactical characterization of the location where the improvised weapon or IED was emplaced to better understand insurgent/terrorist targeting criteria and intent. WTI seeks to answer the questions: Why here? Why now? Why is a particular tactical design or technical characterization used? The process supports production of tailored threat assessments for an operational area. This enables WTI analysts to track and study the migration and evolution of technology and enemy TTP. WTI uses technical and forensic methods to gain knowledge about an improvised weapon system, how it was employed, who built it, who employed it, and how to mitigate its effects. WTI accomplishes this by synchronizing and integrating four primary processes: collection, exploitation, analysis, and dissemination. DIA is the DoD lead for WTI, overseeing the processes and capabilities that support C-IED, counterterrorism (CT), counterinsurgency, IrW, and counterproliferation submission areas.[120]

[120] U.S. Joint Chiefs of Staff, *Joint and National Intelligence Support to Military Operations*, Joint Publication 2-01, pg. 15.

3.2 Collection

Collection is defined in Joint Publication 1-02, DoD Dictionary of Military and Associated Terms, as “the acquisition of information and the provision of this information to processing elements.”[121] Collection depends on the ability to detect and identify information and material of possible interest to meet the commander’s information requirements. As illustrated in **Figure 3-2**, collection involves gathering, preserving, documenting, and managing information and material taken from an incident site. Collection also includes the documentation of contextual information and material observed at the incident site or objective, and occurs at any time during processing of information and material. Specialized units, such as EOD, WIT, and site exploitation teams, conduct WTI collection, but other units, such as maritime Visit Board Search and Seizure (VBSS) teams also do it, if properly trained.

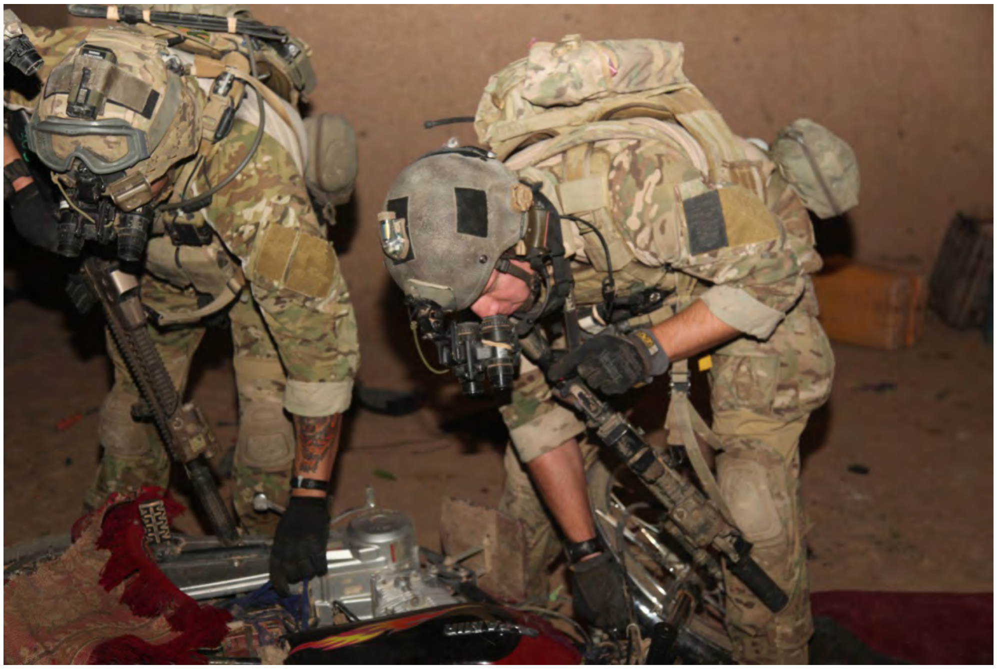


Figure 3-2. Coalition Forces Collect Information and Material During an Operation *(Photo Credit: JIEDDO)*

Collection seeks to obtain information and material to satisfy information requirements at all levels of command, including JIIM organizations. Collected information and material supports intelligence requirements and Host Nations’(HNs’) prosecution efforts. Although all material and documents are considered intelligence, not all intelligence is evidence. Because collected material and documents may be used to support prosecution, collection should follow standardized procedures to prevent corruption of evidence.

Collection efforts usually require EOD Technicians to remediate potential explosive hazards associated with improvised weapon systems, including IEDs or booby traps, to ensure safe collection. While onsite, EOD technicians conduct a post-blast investigation of the scene.

[121] Ibid.

Collection includes documentation of items recovered and data submitted for follow-on exploitation and analysis. Standardized processes for documentation of collected information and material aid in subsequent processing. Documentation includes reports, photographs, contextual information, site sketches, and video recordings. **Figure 3-3** illustrates materials collected onsite that are documented and preserved for follow-on exploitation. This information is of immediate value from tactical to strategic levels, providing timely and actionable feedback to support basic intelligence requirements.

3.3 Exploitation (Processing of Material and Information)

Joint Publication 1-02, DoD Dictionary of Military and Associated Terms, defines exploitation as "taking full advantage of any information that has come to hand for tactical, operational, or strategic purposes."[122] Exploitation occurs throughout the WTI process and involves processing of collected information and material into forms suitable for follow-on analysis (**Figure 3-3**). Exploitation includes synchronization and standardization of timely technical and forensic information to influence the overall WTI process. Exploitation activities capture, organize, sort, translate, extract, convert, prioritize, categorize, and expeditiously disseminate information for follow-on detailed analysis. Exploitation requires a team that possesses an appropriate level of competence in a broad range of scientific and technical disciplines and who use specialized equipment and automated information systems.

Exploitation occurs at the incident site if required capabilities are available, but more often occurs at an offsite location where many of these capabilities can be established in a controlled environment. Forensic and technical capabilities that support the exploitation process are flexible and scalable across the ROMO to address threat and operational requirements.

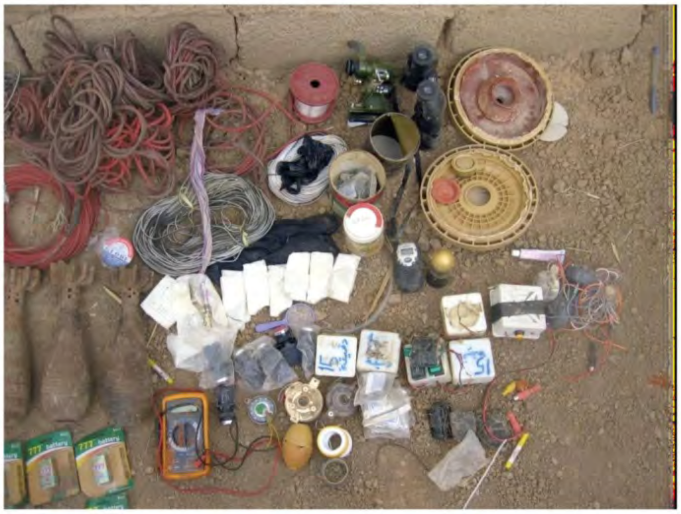


Figure 3-3. Improvised Weapon Material. *Material collected onsite is documented, preserved, and delivered to an exploitation facility for follow-on exploitation and analysis. (Photo Credit: JIEDDO)*

[122] Ibid.

3.4 Analysis

Joint Publication 1-02, DoD Dictionary of Military and Associated Terms, defines analysis as "the conversion of processed information into intelligence through the integration, evaluation, analysis, and interpretation of all-source data."[123] By linking or attributing information, materials, and people to places, things, trends, and patterns, WTI analysts can deduce the tactical through strategic significance of the information and material under analysis. Limited analysis may occur in the field, but more typically analysis occurs in expeditionary or fixed facilities with controlled environments. These facilities are located both CONUS and OCONUS. These facilities have the infrastructure and connectivity to support WTI analytical activities. Facilities that conduct analysis are networked with operational, strategic, and national level analytical organizations that leverage their capabilities and products to support the five WTI outcomes. Analysis also leverages diagnostic capabilities and advanced techniques that support a more detailed scientific examination of materials to further fuse information and intelligence. WTI leverages and feeds information to other intelligence disciplines such as HUMINT, SIGINT, MASINT, TECHINT, OSINT, and complementary intelligence capabilities, such as BEI and FEI. Analysis outputs include formal intelligence products and information to support US tactical operations and partner/HN LE initiatives.

3.5 Dissemination

Joint Publication 1-02, DoD Dictionary of Military and Associated Terms, defines dissemination as "the delivery of intelligence to users in a suitable form and the application of the intelligence to appropriate missions, tasks, and functions."[124] Dissemination involves sharing information and intelligence vertically and horizontally throughout the WTI community of interest (COI). WTI COI is comprised of US, allied, and partner nation organizations involved in the WTI process who share information and products. This information and product sharing permits WTI COI stakeholders to retain threat awareness when physical access to materials is not possible. Effective dissemination provides relevant information and intelligence to the right organizations and individuals in a timely fashion. The sharing of WTI information with host or partner nations helps establish a safe and secure environment and builds or strengthens partnerships.

The WTI process feeds information resulting from exploitation and analysis back down to those who collected it. Dissemination of WTI products generally takes one of two forms: it is "pushed" to user organizations by reports or put on a website where the material is "pulled" by users from databases. WTI products, such as the technical report (TECHREP) in **Figure 3-4,** are pushed out in response to specific requests for information (RFIs) or because OE suggests an organization would benefit from the available material.

[123] Ibid.

[124] Ibid.

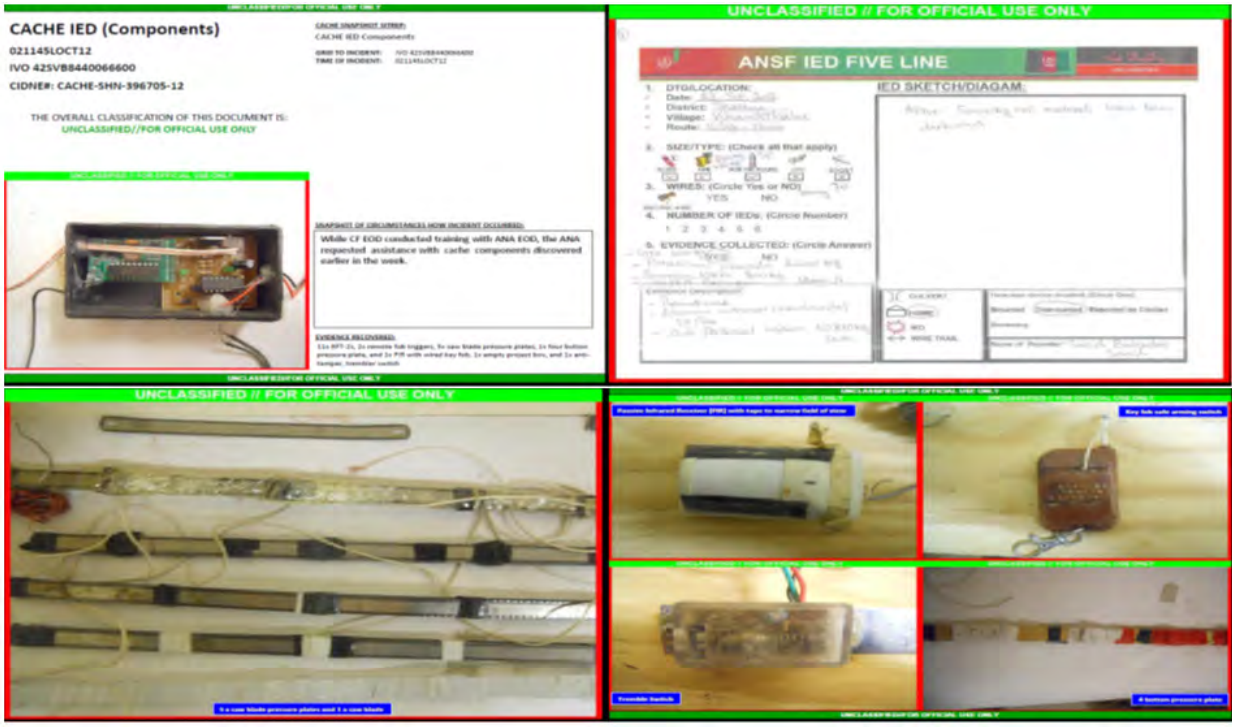

CACHE IED (Components)
021145LOCT12
IVO 42SVB8440066600
CIDNE#: CACHE-SHN-396705-12
THE OVERALL CLASSIFICATION OF THIS DOCUMENT IS:
UNCLASSIFIED//FOR OFFICIAL USE ONLY
While CF EOD conducted training with ANA EOD, the ANA requested assistance with cache components discovered earlier in the week.
UNCLASSIFIED // FOR OFFICIAL USE ONLY
ANSF IED FIVE LINE
1. DTG/LOCATION:
Date:
District:
Village:
Route:
IED SKETCH/DIAGAM:
2. SIZE/TYPE: (Check all that apply)
3. WIRES: (Circle Yes or NO)
YES
NO
4. NUMBER OF IEDs: (Circle Number)
1 2 3 4 5 6
5. EVIDENCE COLLECTED: (Circle Answer)
YES
NO
UNCLASSIFIED // FOR OFFICIAL USE ONLY

Figure 3-4 TECHREP (IED) Storyboard *(Photo Credit CJTF Paladin)*

3.6 Overview of WTI Levels

The concept of operations for DoD WTI describes the WTI process as agile and adaptable based on information priorities, tactical situation, type of mission, and/or required outputs. To achieve this, WTI activities that collect, exploit, analyze, and disseminate information and material are categorized into five distinct WTI levels that support tactical, operational, and strategic environments, as depicted in **Figure 3-5**. Although exploitation and analysis capabilities inherent at each of the five WTI level may be similar, use of the information and intelligence supports varied requirements and intended outcomes of the organization, whether at the tactical, operational, or strategic level. Level 1 activity involves collection, exploitation, and analysis conducted at the tactical level that provides timely and relevant information to help tactical commanders plan and execute current or future operations.

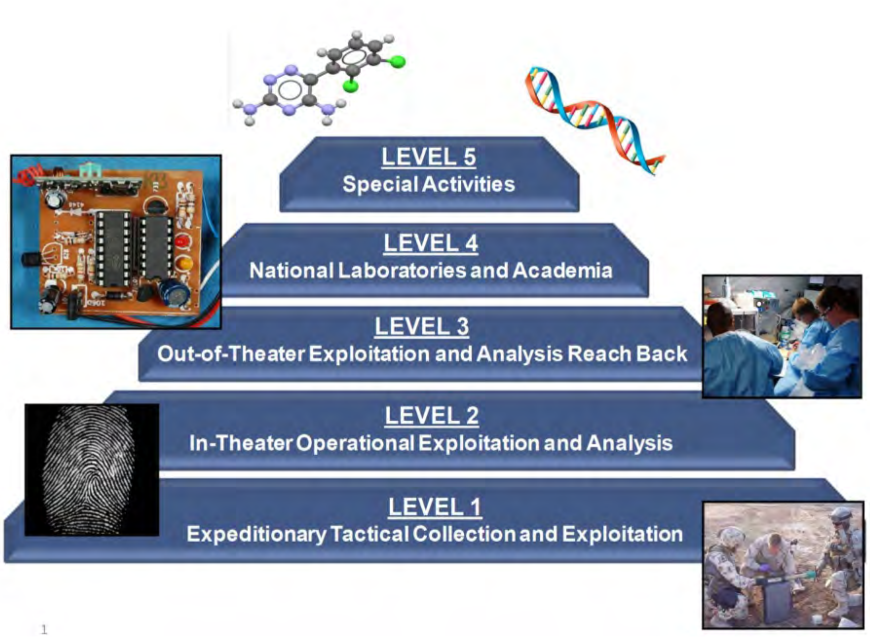

LEVEL 5
Special Activities
LEVEL 4
National Laboratories and Academia
LEVEL 3
Out-of-Theater Exploitation and Analysis Reach Back
LEVEL 2
In-Theater Operational Exploitation and Analysis
LEVEL 1
Expeditionary Tactical Collection and Exploitation
1

Figure 3-5. WTI Exploitation Levels 1 Through 5 *(Figure Credit: JIEDDO)*

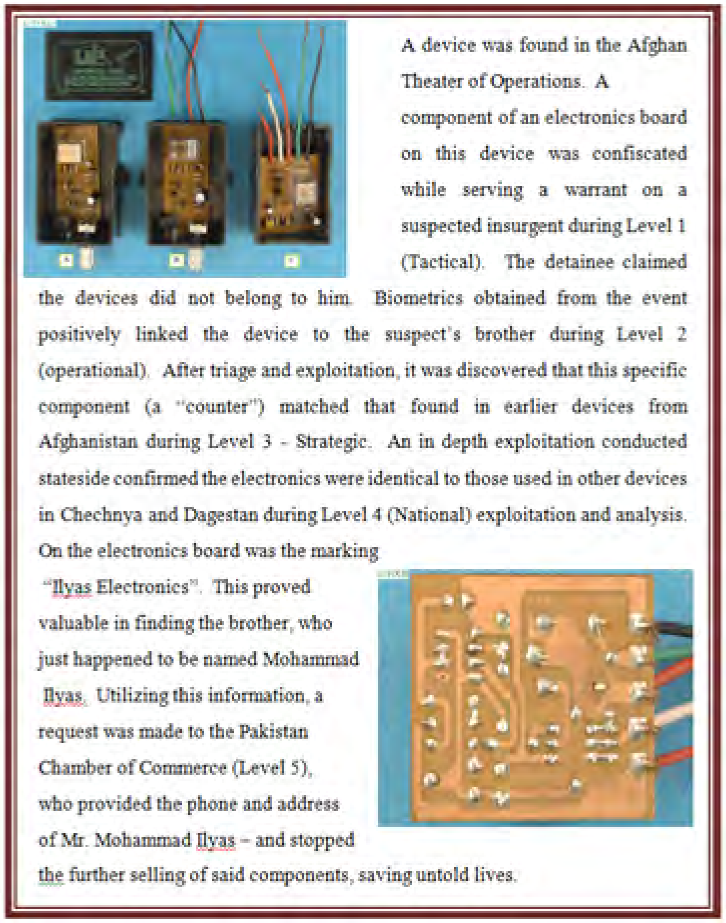
Level 1 occurs at the tactical level, delivering timely and credible information about improvised weapons and those who employ them. Level 1 is the primary source of collected material, which feed Levels 2 and 3.

Level 2 occurs at the operational level, in a deployed environment, delivering exploitation to support commanders' operational requirements, which include evolving adversary TTP, targeting, support to prosecution, and FP.

Level 3 provides an enduring capability that delivers a full spectrum of advanced forensic and technical exploitation and intelligence analysis to support strategic objectives. With interagency and international participation, Level 3 works towards countering the improvised threat around the globe.

The outcomes of strategic-national exploitation derived from Level 4 activities support and combine exploitation and analysis with national policy guidelines, and links laboratories worldwide to exploit items using varied scientific disciplines. This capability provides decision makers technical and sourcing information needed to take action that could have significant diplomatic repercussions or national security implications.

Lastly, Level 5, strategic-special activities, leverages information, intelligence, and products obtained from Levels 1 through 4 activities and from other sources to support strategic initiatives. These activities support sanctions, diplomatic initiatives, or other covert or overt governmental action. WTI levels do not always follow a linear path from Level 1 to Level 5, nor must information and material move through each level for processing.[125] **Figure 3-6** illustrates how WTI exploitation, Levels 1 through 5, work in conjunction with one another to achieve specific outcomes.



A device was found in the Afghan Theater of Operations. A component of an electronics board on this device was confiscated while serving a warrant on a suspected insurgent during Level 1 (Tactical). The detainee claimed the devices did not belong to him. Biometrics obtained from the event positively linked the device to the suspect's brother during Level 2 (operational). After triage and exploitation, it was discovered that this specific component (a "counter") matched that found in earlier devices from Afghanistan during Level 3 - Strategic. An in depth exploitation conducted stateside confirmed the electronics were identical to those used in other devices in Chechnya and Dagestan during Level 4 (National) exploitation and analysis. On the electronics board was the marking "Ilyas Electronics". This proved valuable in finding the brother, who just happened to be named Mohammad Ilyas. Utilizing this information, a request was made to the Pakistan Chamber of Commerce (Level 5), who provided the phone and address of Mr. Mohammad Ilyas – and stopped the further selling of said components, saving untold lives.

Figure 3-6. IED Exploitation Vignette *(Photo Credit: JIEDDO)*

The complexity and purpose of exploitation and analysis determine how quickly information and intelligence products from a given level become usable and available products. Level 1 exploitation often results in important actionable feedback in minutes or hours. Products from Level 2 tend to reach users in days to weeks, while products resulting from the more detailed processes of Levels 3 through 5 can take weeks to months. **Figure 3-7** illustrates estimated WTI exploitation timelines. During each of the five WTI levels, analysts perform triage to assign exploitation priorities to materials and information submitted to the WTI process. Effective triage reduces processing time at all five WTI levels. Representatives from other systems (e.g., those on a tactical intelligence staffs or legal authorities) can also influence priorities assigned to material from a specific event or interrelated series of events.

[125] (FOUO) Defense Intelligence Agency, *Capstone Concept of Operation*, pg. 13.

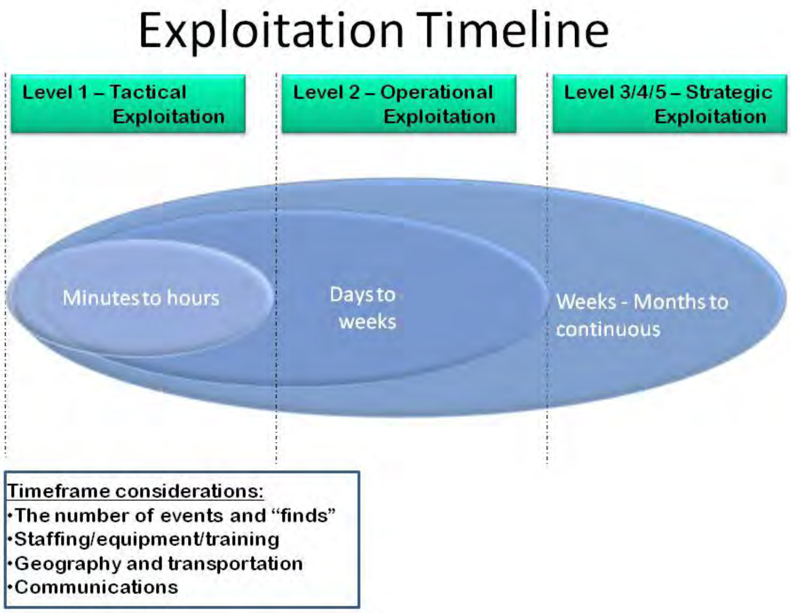

Exploitation Timeline
Level 1 – Tactical Exploitation
Level 2 – Operational Exploitation
Level 3/4/5 – Strategic Exploitation
Minutes to hours
Days to weeks
Weeks - Months to continuous
Timeframe considerations:
•The number of events and "finds"
•Staffing/equipment/training
•Geography and transportation
•Communications

Figure 3-7. WTI Exploitation Timeline *(Figure Credit: JIEDDO)*

Given the worldwide use of improvised weapons, WTI provides a focused whole-of-government effort that synchronizes technical and forensic capabilities and processes to counter a rapidly evolving asymmetric threat. **Figure 3-8** provides an operational view of the WTI framework.

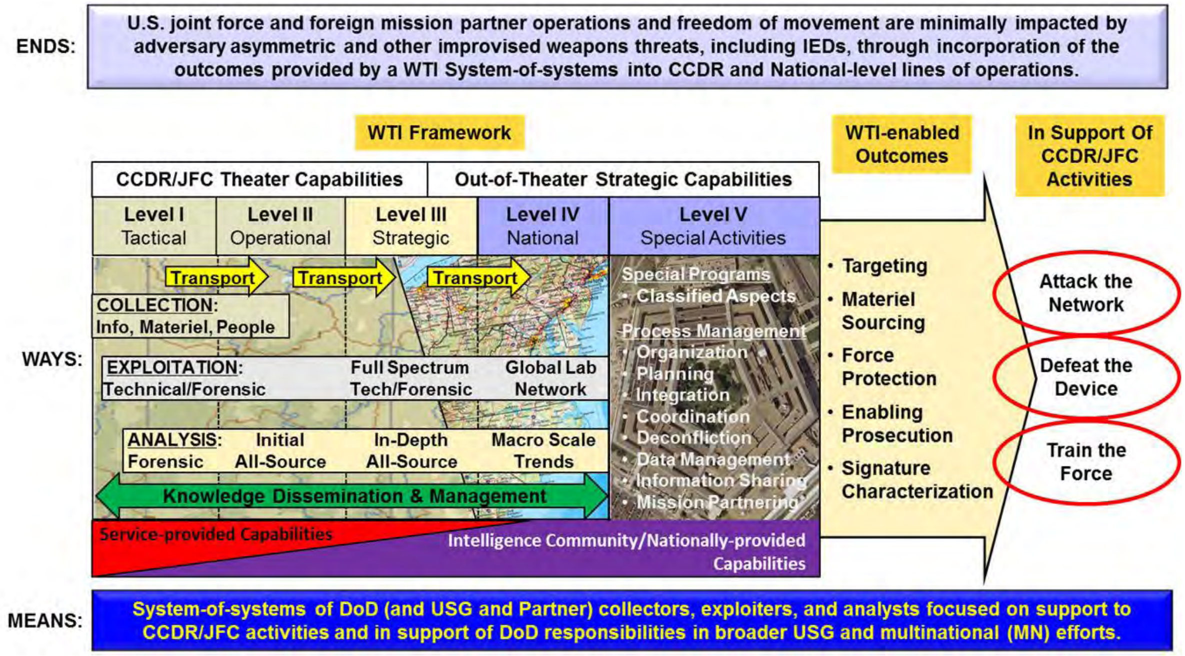

ENDS:
U.S. joint force and foreign mission partner operations and freedom of movement are minimally impacted by adversary asymmetric and other improvised weapons threats, including IEDs, through incorporation of the outcomes provided by a WTI System-of-systems into CCDR and National-level lines of operations.
WTI Framework
WTI-enabled Outcomes
In Support Of CCDR/JFC Activities
CCDR/JFC Theater Capabilities
Out-of-Theater Strategic Capabilities
Level I Tactical
Level II Operational
Level III Strategic
Level IV National
Level V Special Activities
Transport
Transport
Transport
COLLECTION: Info, Materiel, People
WAYS:
EXPLOITATION: Technical/Forensic
Full Spectrum Tech/Forensic
Global Lab Network
ANALYSIS: Forensic
Initial All-Source
In-Depth All-Source
Macro Scale Trends
Knowledge Dissemination & Management
Special Programs
• Classified Aspects
Process Management
• Organization
• Planning
• Integration
• Coordination
• Deconfliction
• Data Management
• Information Sharing
• Mission Partnering
• Targeting
• Materiel Sourcing
• Force Protection
• Enabling Prosecution
• Signature Characterization
Attack the Network
Defeat the Device
Train the Force
Service-provided Capabilities
Intelligence Community/Nationally-provided Capabilities
MEANS:
System-of-systems of DoD (and USG and Partner) collectors, exploiters, and analysts focused on support to CCDR/JFC activities and in support of DoD responsibilities in broader USG and multinational (MN) efforts.

Figure 3-8. WTI Operational View. (Figure Credit: DIA, JIEDDO)

3.7 WTI Across the Range of Military Operations (ROMO)

WTI capabilities vary in scope and complexity, span peacetime to wartime activities, and can be applied throughout the ROMO. As illustrated in **Figure 3-9,** the ROMO is divided into three categories: military engagement, security cooperation, and deterrence activities; crisis response and limited contingency operations; and major operations and campaigns.[126] WTI can be applied across the spectrum of conflict to support US and partner nation interests. Support spans from providing WTI exploitation advice and assistance to a HN during military engagement operations, to the establishment of an operational WTI exploitation facility during limited contingency and major operations.

WTI functional capabilities that support collection, exploitation, analysis, and dissemination of WTI information and material are modular and scalable and are selected independently or in conjunction with other WTI capabilities by the Joint Force Commander (JFC) to fulfill mission requirements. The critical outcomes of WTI (FP, targeting, component and material sourcing, support to prosecution and signature characterization) are in direct support of combatant commands' (CCMDs') ability to attack the network (AtN), defeat the device (DtD), and train the force (TtF). Another critical benefit of WTI is its ability to feed essential information to intelligence activities conducting network analysis and to enhance the common intelligence picture. The JFC can choose to use WTI during major operations and campaigns to support the capture or detention of high-value targets and individuals associated with the production or employment of improvised weapons, including IEDs, associated components, and other weapons systems. After cessation of major combat operations, the JFC can use WTI capabilities to assist HN authorities in exploiting information and material that leads to targeting or prosecution of criminals, terrorists, or insurgents.

Historically, WTI has shown great utility during major combat operations in Iraq and Afghanistan; however, its application throughout the conflict continuum is valuable in supporting operations, such as arms control, counter proliferation, enforcement of sanctions, nation assistance (civil or military), identity resolution/operations, maritime interception operations (MIO), air operations, freedom of navigation, and theater campaigns.

Given the global nature of the adversary, WTI capabilities should be used when conducting operational and contingency planning. WTI is directly dependent on the ability to identify and collect information and material related to a geo-specific weapons threat. Appendix D addresses WTI planning considerations.

[126] U.S. Joint Chiefs of Staff, *Joint Operations Across the Range of Military Operations*, Joint Publication 3-0, Washington, DC, August 11, 2011, pg. I-5.

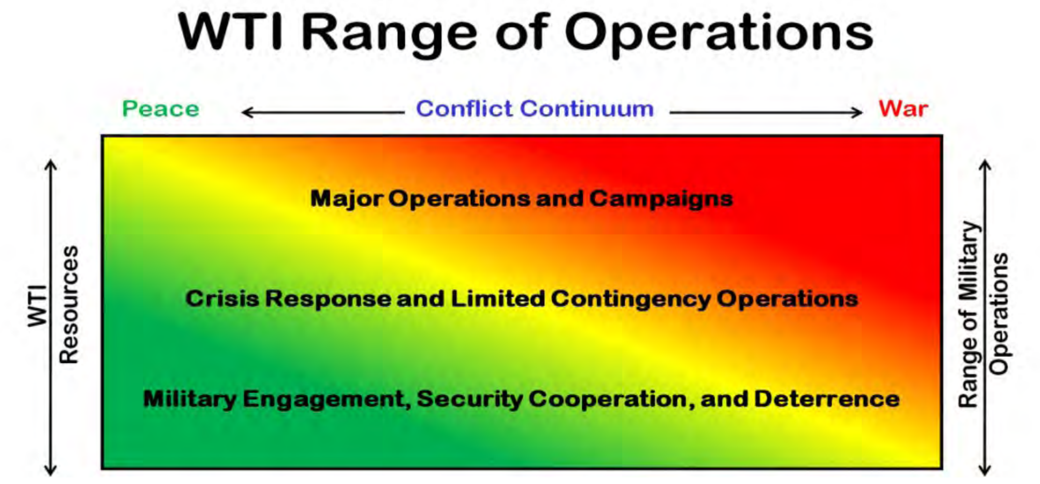

WTI Range of Operations
Peace
Conflict Continuum
War
Major Operations and Campaigns
Crisis Response and Limited Contingency Operations
Military Engagement, Security Cooperation, and Deterrence
WTI Resources
Range of Military Operations

Figure 3-9. WTI Across the Conflict Continuum *(Figure Credit: JIEDO)*

3.7.1 Application to Military Engagement, Security Cooperation, and Deterrence

Use of WTI capabilities during military engagement, security cooperation, and deterrence activities helps to establish, shape, maintain, and refine relations with other nations and domestic civil authorities (e.g., state governors or local LE). WTI actions support the JIIM and protect and enhance national security interests, deter conflict, and set conditions for future contingency operations. Because the Department of State (DoS) is often the lead in this type of OE, the JFC must work closely with the Chief of Mission and US departments and agencies to ensure that applied WTI capabilities are coordinated and synchronized with other governmental initiatives, and consistent with existing legal authorities. In these situations, CCMDs should coordinate closely with interagency partners to ensure mutual understanding of benefits, capabilities, limitations, and consequences of military and nonmilitary actions in support of a whole-of-government solution. A whole-of-government approach integrates the efforts of all interagency partners.

3.7.1.1 Military Engagement

Engagement involves routine contact and interaction between individuals or elements of another nation's armed forces or their domestic civilian authorities or agencies. WTI supports engagement by building HN trust and confidence through sharing of WTI-related information and material and coordination of mutual activities that assist in maintaining US influence in the HN. Engagement occurs as a part of security cooperation and includes interaction with domestic civil authorities.[127] Examples of engagement include routine EOD or WTI collection and exploitation training with HN counterparts. Another example of military engagement is DoD's humanitarian mine action program that seeks to relieve the adverse effects of mines and other discarded or abandoned

[127] U.S. Joint Chiefs of Staff, *Joint Operations Across the Range of Military Operations*, Joint Publication 3-0, pg. V-10.

ordnance while advancing the CCDR's theater campaign plan and US national security objectives as illustrated in **Figure 3-10**.[128]

3.7.1.2 Security Cooperation

Like engagement, security cooperation relies on military interactions with a nation's defense or security organizations to develop its security capability (i.e., internal and external defense) and provide the United States with peacetime contingency access to the HN. Security cooperation seeks to lessen the probability of potential crisis that may require coercive US military intervention.[129] WTI supports a range of activities, including US and HN military to military, military to civilian, and civilian to civilian, depending on the HN environment and US military and DoS goals, and HN laws and OE. WTI security cooperation activities include advising and assisting HNs in development of WTI capabilities, Levels 1 through 5, as appropriate. This includes assistance with development of Level 1 collection and initial exploitation capabilities, including post-blast and site exploitation, and development of Level 2 to 3 technical and forensic exploitation, intelligence analysis, prosecution support, and information dissemination capabilities. Additionally, WTI security cooperation develops the mechanism for the HN to reach out to US and partner nation theater-based exploitation and analysis facilities and databases who can provide analysis of collected WTI materials. The extent of WTI support depends on HN capability and agreement by the two governments. Information obtained through security cooperation operations feeds the intelligence process and enhances the common operational picture (COP).

Figure 3-10. *Engagement Through Training. CJTF Horn of Africa EOD Technician provides unexploded ordnance(UXO) disposal training to Namibian Defense Force and Police Explosive Control Unit. (Photo Credit: USAF)*

3.7.1.3 Deterrence

Deterrence prevents a foreign government from taking action that is contrary to US national interest by making it known that there will be an unfavorable or dire consequence to them if anti-US action is taken. A less known form of deterrence is enhancing a "climate of peaceful cooperation, thus promoting stability."[130] An example of this less known type of deterrence is the development of a HN's WTI capacity and capability that support its efforts to fight subversion, lawlessness, insurgency, terrorism, and other threats to security. Deterrence is accomplished through WTI

[128] U.S. Joint Chiefs of Staff, Department of Defense Support to Humanitarian Mine Action, *Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3207.01C*, September 28, 2013, pg. 1.

[129] U.S. Joint Chiefs of Staff, *Joint Operations Across the Range of Military Operations*, Joint Publication 3-0, Washington, D.C., August 11, 2011, pg. V-10

[130] Ibid.

engagement and security cooperation activities. Information obtained through these operations is also used to feed the intelligence process and to enhance the COP.

WTI planner considerations in support of military engagement, security cooperation, and deterrence include:

- Work with DoS country team to identify current information sharing agreements between the United States and HN and make recommendations for change
- Understand HN laws (military and civil) that permit the collection, exploitation, and analysis of improvised weapons
- Identify host and partner nation capabilities and gaps throughout the five levels of WTI. Examples include enablers who collect, exploit, analyze, and disseminate WTI information and material
- Identify the foreign agency that has primacy for investigating incidents. Identify how forensic evidence is handled and which agency gathers evidence from a scene
- Identify HN EOD team and bomb squad capabilities and training to gather material from a site in a forensically sound manner
- Understand the HN's identity management infrastructure — do they have biometric database or census information?
- Identify what HN organization conducts follow-on Level 2 or 3 exploitation and analysis of material recovered from an event site; not all organization/agencies within a HN communicate or cooperate well with one another
- Understand the current DoJ relationship with the HN because DoJ may have a Legal Attaché (LEGAT) or Special Agent Bomb Technician (SABT) working at the US embassy. SABTs often conduct capability assessments of the HN's LE organizations sponsored by DoS Anti-Terror Assessment Program
- Identify the Defense Attaché and work through US embassies to understand US relationships with HN and our interest in developing capability and/or capacity to collect and exploit improvised weapons
- Understand HN's relationships with neighboring states to identify areas of sanctuary and possible supply lines for illicit materials
- Know who owns the exploitation process (e.g. Ministry of Interior (MOI), Ministry of Defense (MOD), a combination, etc.) and how well they are equipped; a nation's MOD and MOI may have primacy issues regarding exploiting weapons, improvised weapons, and IEDs
- Understand the HN's evidence and LE process for forensically exploiting material, and their relationship with US and other partner nation Level 3 laboratories
- Identify and include WTI capabilities in theater security cooperation plans

3.7.2 Crisis Response and Limited Contingency Operations

"Crisis response and limited contingency operations are typically limited in scope and scale and conducted to achieve a very specific strategic or operational objective in an operational area."[131] In this area of the conflict continuum, an adversary will likely use improvised weapons to inflict casualties, create fear in the local population, and assist in destabilizing the legitimate government. Examples of crisis response and limited contingency operations include noncombatant evacuation operations; expanded maritime interception operations (EMIO); peace operations, including peacekeeping operations, foreign humanitarian assistance, recovery operations, strikes and raids; and homeland defense and defense support to civil authorities.

WTI supports battlespace awareness by affording the JFC and staff the ability to understand the enemy's capabilities, TTP, and vulnerabilities through the exploitation of collected enemy weapons (i.e., tactical characterization and technical categorization) employed by an adversary. WTI provides the JFC capability to target individuals, make associations between individuals and groups, and use intelligence to drive offensive operations against networks and cells. At the strategic level, technical information obtained from the exploitation of these weapons may be used to support enforcement of sanctions that mitigates or stops the proliferation of materials by state or non-state actors into a geographic area. WTI plays a pivotal role in identifying the source of these weapons and the materials used in their construction to determine if there is any state sponsorship that can lead to the enactment of sanctions. Forensic and technical exploitation can help to restore security by rebuilding or developing a HN's technical and forensic capability and capacity. This is accomplished by establishing exploitation facilities or improving the HN's infrastructure so that they can conduct WTI technical and forensic exploitation. The extent to which these modular and scalable WTI capabilities are applied is dependent on the operation's level of complexity, duration, and resources available in the OE.

WTI planner considerations in support of crisis response and limited contingency operations include:

- US WTI capabilities (collection, exploitation, analysis) in Operational Plans (OPLANs) and Operational Orders
- HN military and LE capability and capacity for collecting and exploiting improvised weapons
- Allied forces collection and exploitation processes and capabilities
- Understanding DoD's authorities to conduct WTI missions with the HN (both military and civil organizations)
- Understanding the HN's judiciary system and its acceptance of forensic science in the judiciary process; for example, some countries' judicial systems are not accepting of deoxyribonucleic acid (DNA) evidence, as was initially experienced in Afghanistan and Iraq

[131] U.S. Joint Chiefs of Staff, *Joint Operations Across the Range of Military Operations*, Joint Publication 3-0, Washington, pg. V-20.

- Understanding whether the exchange of information from US forensic facilities (theater and CONUS) are admissible for use within the HN's judiciary process

- Understanding HN and neighboring countries' laws as they pertain to the legal use of explosives

- Scalable and modular WTI exploitation capabilities; US capabilities range from basic harvesting of DNA and latent prints to scientific laboratories; WTI Level 1 and Level 2 capabilities are modular and scalable and can be pushed forward in the battlespace to provide an expeditious response to meet the CCDR's intelligence and operational requirements

3.7.3 Major Operations and Campaigns

Major operations and campaigns are often executed to achieve national strategic objectives or to protect national interests. WTI support provided at this end of the conflict continuum is typically more extensive than what is required earlier in the conflict continuum. WTI supports all aspects of major operations and campaigns, from offensive and defensive operations, to stability operations, often supporting each simultaneously. Outcomes provided by WTI to the JFC permit an understanding of the improvised weapon, allowing the CCMDR to prepare for the asymmetric threat in the OE. Intelligence derived from the WTI process is used to suppress unconventional and asymmetric warfare that accompanies major operations and campaigns. It supports development and refinement of battlespace awareness, targeting packets, missions, and TTP, and supports stability operations that enable civil authorities. Analysis of networks during major operations reduces time traditionally experienced by conventional forces when transitioning from major operations to limited contingency operations. Although operation of robust exploitation laboratories is not typically conducted during major conventional operations, material collection can still be leveraged to feed exploitation and analysis. Flexible expeditionary exploitation capabilities are used modularly on the basis of the threat, requirements, and pre-existing capabilities of the HN and allied partners.

WTI planner considerations in support of major operations and campaigns include:

- Level 1 deployable search and collection capabilities: WIT, Foreign Ordnance Exploitation Cells (FOXC), route clearance teams, CBRNE Response Teams (CRT) and working dogs

- Integration of US and allied deployable Level 2 exploitation laboratories (e.g., Combined Explosive Exploitation Cell [CEXC], Forensic Exploitation Teams [FXTs], Exploitation Analysis Cells [EACs]) that are scalable, modular, and capable of meeting the immediate demand of the tactical commander

- Additional reach back exploitation capacity provided at national Level 3 laboratories to process the expected increase in captured materials

- Transition from collecting improvised weapon material to support military operations to collection that supports the establishment and stabilization of HN civil authority (i.e., transition from Phase IV-Stability Operations to Phase V-Enable Civil Authority)

CHAPTER 4
Level 1 (Tactical) Collection and Exploitation

4.1 General Description

Tactical exploitation delivers timely and credible exploitation and analysis about weapons employed in an asymmetric environment and the people who employ them. Level 1 activity begins at the point of collection. The point of collection includes turnover of material from HN government or civilian personnel, and material and information discovered during a maritime interception operation, cache discovery, raid, IED incident, or post-blast site. This first level encompasses identification, collection, preservation, transportation, and examination of physical material and contextual information from an event site in a land or maritime environment.

Level 1 activities focus on gathering all relevant information and material associated with asymmetric weapons. Limited field exploitation of collected material occurs to meet the immediate needs of tactical units or other vested parties. This level identifies trends in enemy TTP and completes the first tactical characterization of the incident and technical categorization of the materials recovered. Operational exploitation conducted at Level 2 facilities refines the characterizations and categorizations. This first assessment identifies the weapon and its components, the employment method, purpose of device, type of switch, type and amount of explosives, and additional enhancements.

Anyone can collect weapons-related information and/or materials as long as they are properly trained.[132] CCDRs coordinate with non-DoD entities, such as SABTs, HN, nongovernmental organizations, to assist in Level 1 activity because they often have access to materials and information not available to DoD personnel. Multiple enablers accomplish Level 1 activity objectives.

4.2 Level 1 Objectives

- Ensure collection priorities address commander’s critical information requirements (CCIRs)
- Identify cache marking and concealment methods
- Identify ground sign observables and signatures (including “graffiti,” flags, and markers)
- Identify bomb making material discovered on persons of interest (POI)
- Identify systems and components
- Conduct onsite assessment of threat intentions and objectives
- Conduct expedient exploitation of communications and media devices
- Conduct biometric collection/exploitation at the event site
- Collect, protect, and preserve material in a forensically sound manner
- Record lethality, target damage, and tactical effect

[132] NOTE: While anyone can collect WTI information and materials, it is important to understand that EOD must first clear any explosive hazards to preclude inadvertent injury or death.

- Record the scene using drawings, photographs, and video, as appropriate
- Question and record witness statements for later analysis (HUMINT)
- Provide information and intelligence regarding threat TTP or "first-seen" items of technical interest (typically performed by EOD)
- Conduct post-blast investigation at the site (typically performed by EOD or Bomb Technician)
- Assign priorities for additional intelligence collection assets and target planning

4.3 Capabilities

Level 1 capabilities involve a systematic process of collecting, exploiting, analyzing, and disseminating material and/or information, which is obtained at a point of collection or received from a host or partner nation, then exploited and analyzed immediately. Level 1 capabilities rely on the responding organization's ability to collect information and material and address CCIRs. Collection assets conduct limited exploitation, presumptive analysis, and rapidly disseminate material and information recovered at collection point. This includes questioning of suspects and ensuring the safety of those conducting collection operations regarding explosives. CCDRs use information and intelligence derived from these WTI processes to support the production of intelligence products and to refine missions and TTP to meet operational demands.

4.3.1 Collection

Collection assets conduct systematic searches at the point of collection; they recognize material and information of value (e.g., computers and media storage devices, documents, biological materials, firearms, explosives, IED components, drugs, biometrics [**Figure 4-1**]); and adequately document the site using photography, video, and sketching. Collection is done in a forensically correct manner, documented for custody, and properly preserved and protected at the site to prevent inadvertent contamination, loss, or alteration. Potential technical and forensic value can be lost during the exploitation process, making information and material collected unusable to support HN rule of law, without proper collection, custody, and triage of material and information.

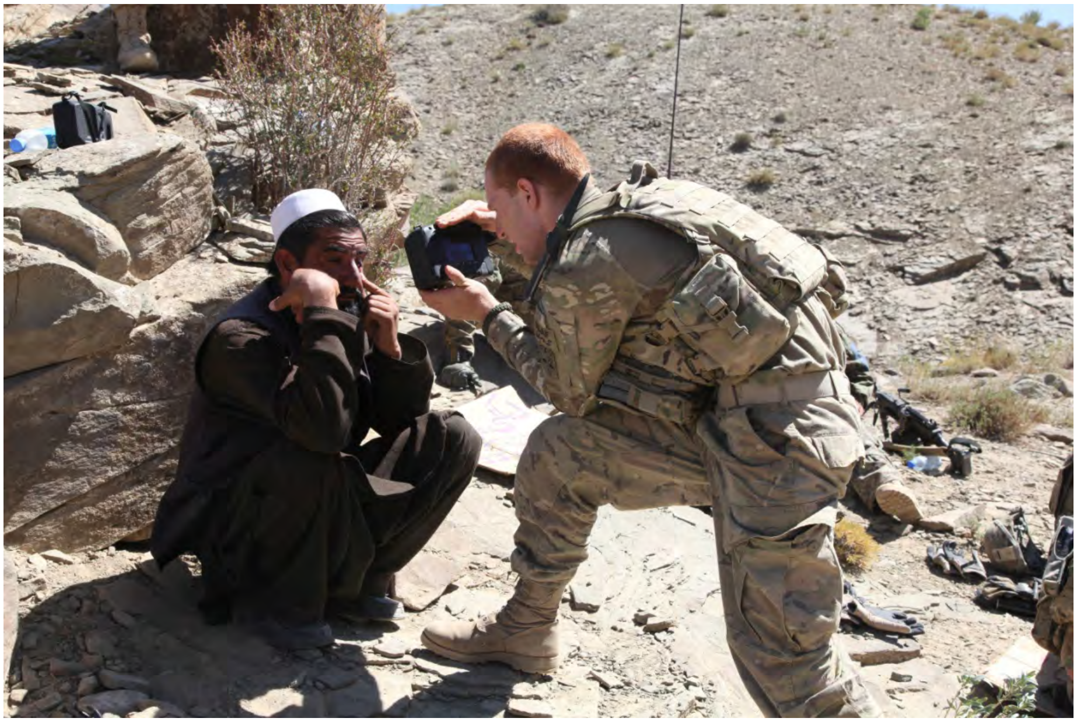


Figure 4-1. Collecting Biometrics. *US Army soldier collects biometric information from a local Afghani in the field. (Photo Credit: US Army).*

4.3.2 Exploitation

Level 1 exploitation (**Figure 4-2**) includes the first tactical characterization/technical categorization (usually conducted by EOD or bomb squad teams) at a collection site to determine a weapon's method of employment, purpose, type of switch, types and amount of explosives (if any), and additional enhancements, including CBRN. Tactical characterization determines how an attack was conducted or was planned to be conducted (the tactical design), and/or how the devices was used or was intended to be used (purpose of the device). Technical categorization describes an improvised weapon using a hierarchical construct to identify its key components, as detailed in the WTI IED Lexicon.[133] Warfighters recover and exploit technical and forensic information from identified weapons, associated components, and precursors. Operators also conduct expedient tactical exploitation of communications and media devices, documents, nonintrusive biometrics, and information derived from personnel at the point of collection at this level. Tactical level exploitation encompasses recording the lethality, target damage, and tactical effect of any attack. Trends in threat TTP are established and further analyzed by a more capable, higher level exploitation activities.

[133] Defense Intelligence Agency/Joint IED Defeat Organization, *WTI IED Lexicon, 4th Edition*, pg. 2.

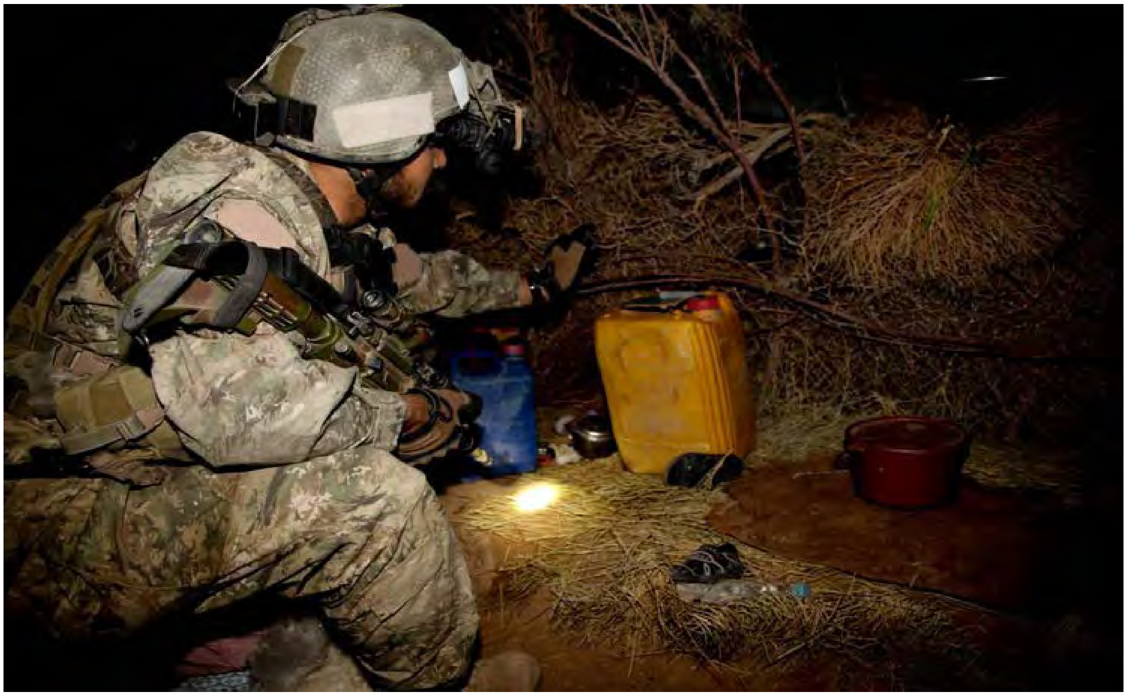


Figure 4-2. Coalition Soldier Conducts Site Exploitation Operations *(Photo Credit: JIEDDO)*

4.3.3 Analysis

Analysis at Level 1 is limited in scope. Although more capable follow-on exploitation activities conduct the majority of analysis of collected material and information, basic analysis of exploited material and information at the collection site can determine if immediate actions are required. Onsite analysis can results in dynamic targeting or development of a threat assessment. Presumptive testing is another form of expedient analysis conducted at the exploitation site to determine the chemical composition of explosive material, precursor, or unknown substance.

4.3.4 Dissemination

Operators properly disseminate collected information to other units in the area and facilitate the transportation of material to the appropriate higher level exploitation activity. Transfer of collected materials and information to an appropriate exploitation activity allows for more complete exploitation and analysis. An enduring Level 3 facility is available to provide timely and tailored exploitation in the absence of a Level 2 facility.[134] Dissemination preserves information and material, follows chain-of-custody protocols, and provides accurate and timely reports to the COI. Dissemination is not complete until proper feedback is pushed down to originating units.

[134] Obama, *Countering the Improvised Explosive Device.*

WTI Level 1 Vignette

Intelligence, surveillance, and reconnaissance (ISR) detected increased enemy activity in the vicinity of a remote village, and a battalion was ordered to conduct a cordon and search. Upon approaching the village, the lead element came under intense small arms and automatic weapons fire, and incurred several casualties. Artillery and air support was requested to suppress enemy fire.

After securing the village, the unit commander initiated a search of all buildings and captured one male person of interest. During the search of a second building, a team discovered potential IEDs, various potential IED components, and two wooden crates with explosive placards. The on-scene commander submitted a 9-line report requesting EOD support and established a cordon. Upon arrival, the EOD team confirmed the existence of IEDs, IED components, and surface-to-air missiles still in their crates. EOD performed render safe procedures on the existing IEDs and determined IED components were being used to construct explosively formed projectile (EFP) arrays. EOD then confirmed no other explosive threats existed, cleared the site, and destroyed the missiles before turning the scene over to the tactical commander for further exploitation.

The unit search team, in collaboration with EOD, obtained forensic and contextual information from the EFP systems, launchers, and crates. The chain of custody was documented and the captured materiel inventoried, photographed, packaged, and transported to the Forward Operating Base (FOB). Biometric data of the captured person was uploaded into a Biometrics Identification System. The captured person was transported to the detention facility for further processing.

Information regarding the materiel recovered onsite was documented in a preliminary technical report (PRETECHREP) by EOD and entered into a Captured Materiel Management System, and associated with a unique, universal case identifier. The initial technical assessment, developed by EOD in coordination with the Electronic Warfare Officer (EWO) and Intelligence Analysts, determined the missile launchers to be anti-aircraft weapons.

The collected materiel was transported to an Expeditionary Exploitation Facility (EEF), an in theater technical and forensic exploitation and analysis laboratory that combines modular capabilities for technical exploitation under a unified command and control structure. Exploitation personnel reviewed the initial onsite assessment and verified that the EFP components were first-seen in the area of responsibility (AOR). Because of a current CCIR concerning the EFP threat in the AOR, the EEF prioritized exploitation of the first-seen circuitry and EFP arrays according to triage protocols. The EEF documented this information into a complementary technical report (COMTECHREP), augmenting the PRETECHREP developed earlier. The EEF then sent the material and COMTECHREP to appropriate national-level laboratories for further processing and exploitation.

Targeting analysts used information obtained from the technical and forensic exploitation of the EFP systems and associated equipment, and information gathered through interrogation of the captured person, to develop a target package that was disseminated to appropriate operational units. Intelligence reports regarding the exploited materiel were developed and disseminated to the COI, and these reports are pushed down to the EEF and collecting units as feedback.

4.4 Enablers

WTI enablers involved in the collection, exploitation, analysis, and dissemination of improvised weapon systems, their components, and associated information are task organized and synchronized.[135] Level 1 enablers include EOD personnel and specialty teams discussed in sections 4.4.1 through 4.4.11.

4.4.1 Explosive Ordnance Disposal (EOD)

EOD personnel serve as one of the primary collectors of WTI-related material from a site (e.g., cache, explosive ordnance, or improvised weapon incident site). EOD personnel are skilled in conducting reconnaissance, detecting and identifying weapons and associated components, neutralizing explosive hazards, conducting render safe procedures (RSPs) and post-blast analysis, and disposing of unexploded ordnance, IEDs, and CBRN hazards (**Figure 4-3**). They evaluate an incidents' tactical characterization, conduct the first technical categorization of a device or weapon, prepare explosive items for transportation, and evacuate them for further exploitation.[136] An EOD team generates an incident report and forwards relevant data and physical material to a location, as directed, for further exploitation, typically to the unit's headquarters, a Level 2 facility, or CONUS exploitation activity. Members of the EOD platoon,

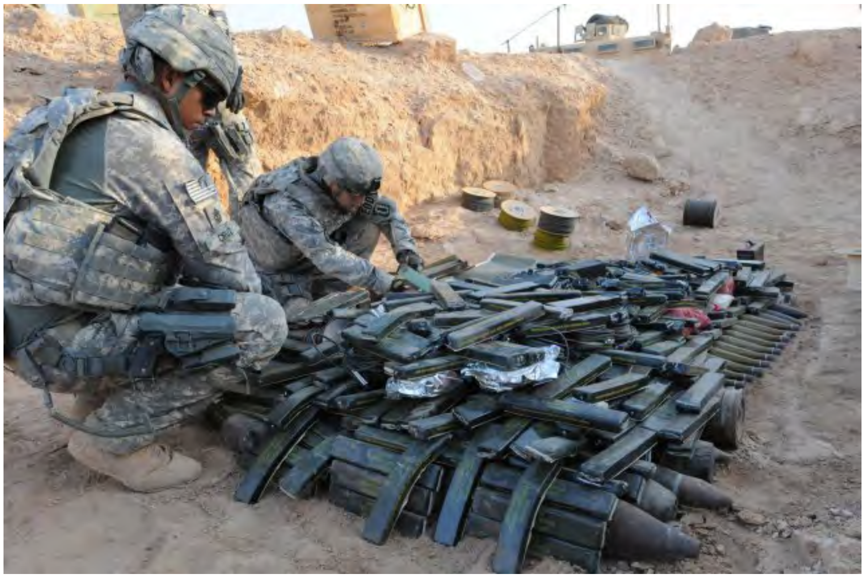


Figure 4-3. Army EOD Technicians Conduct Disposal Operations of Captured Enemy Ordnance *(Photo Credit: USA)*

[135] NOTE: When assisting a sovereign nation, DoD enablers may not have the legal authority to conduct WTI collection, exploitation, and analysis activities within the host nation. In these instances it is important to coordinate with the DoS to develop relationships with the host nation that enable US WTI activities to work in conjunction with partner nation law enforcement authorities to share WTI-related information and material that has resulted during their collection, exploitation, and analysis efforts. This agreement should be codified in writing by both governments.

[136] NOTE: EOD personnel are the only forces within the DoD who are properly trained and equipped to conduct render safe operations.

flight, and/or company simultaneously analyze related theater technical data and pass their analysis forward for pattern and predictive analysis that, in turn, provides products to users in the field. EOD unit members produce IED and other weapons overlays to give units in an area a COP. EOD personnel provide direct support to tactical units who analyze EOD reports and provide consolidated intelligence feedback to their platoons and companies.

4.4.2 Weapons Intelligence Teams (WIT)

WITs are small, specially trained collection teams that provide weapons-focused TECHINT support and are usually task organized within a brigade combat team (BCT). The US Army is the proponent for WIT training, which is conducted Fort Huachuca, AZ. WIT teams support WTI activities across the ROMO and are dispatched according to commanders' intelligence collection requirements. WITs are focused on the exploitation of rendered safe improvised weapons, including IEDs, other weapon systems, and associated components. WITs usually accompany an EOD team, with mutually supporting roles onsite. However, WITs can deploy independently when mission, operational tempo, and availability of security escorts allow.

Although these teams operate as a collection asset, when properly trained, they are capable of going beyond collection to perform exploitation or analysis. EOD Technicians, Intelligence Analysts, and experienced investigators typically comprise a WIT, and members have a W6 Additional Skill Identifier (ASI). WITs are flexible and scalable to support changing commander intelligence requirements. WITs enable information sharing for further exploitation and analysis by those in the field.

The WIT seeks to fully exploit and document sites with potential intelligence value by collecting WTI material; performing tactical questioning; collecting forensic material (including latent fingerprints); preserving and documenting DOMEX, including cell phones and global positioning systems; providing in-depth scene documentation (including making sketches and photographs); evaluating the effects of threat weapons systems; and preparing material for evacuation after cleared as safe by EOD personnel. The processing of collected foreign equipment and material of intelligence value are annotated by WITs in WIT reports.[137] After material collection and initial examination of a scene, WIT members conduct further onsite analysis to:

- Assess the tactical characterization of WTI related events
- Determine threat network intentions in employing a weapon or conducting other activities at a site
- Ascertain intended targets
- Establish responsibility for actions
- Perform onsite forensic collection
- Forensic collection on nonremovable materials
- Recover threat materials

[137] Headquarters, Department of the Army, Army Techniques Publication (ATP) 2-22.4, *Technical Intelligence*, November, 2013. pgs. 5-2.

- Fuse intelligence directly into the intelligence cycle at the lowest tactical levels
- Perform onsite media exploitation (MEDEX)

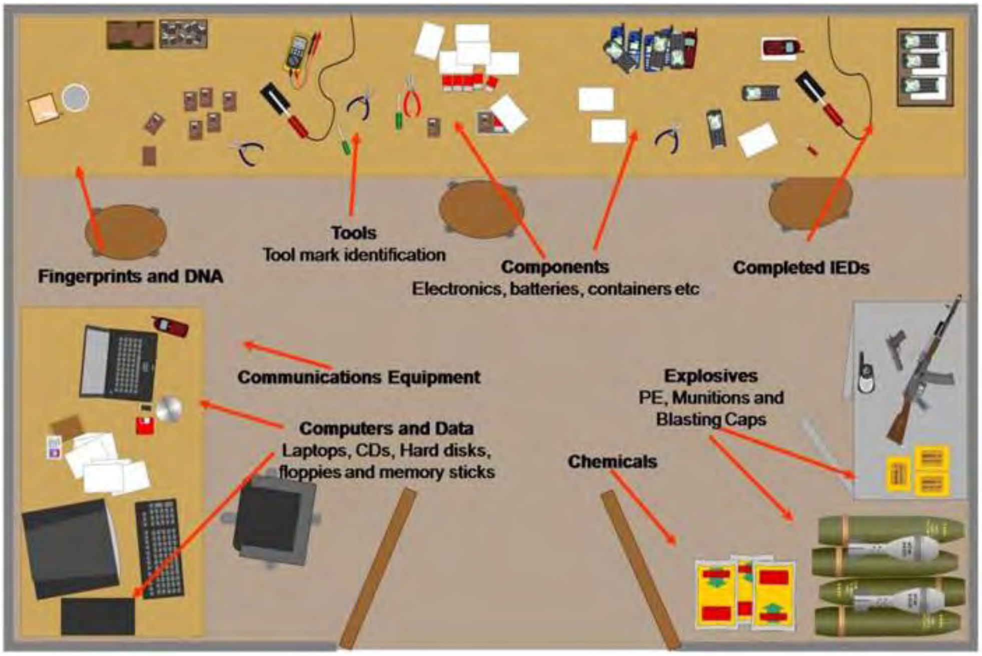


Figure 4-4. Range of Materials and Opportunities for Collection, Exploitation, and Analysis *(Figure Credit: DIA)*

4.4.3 Site Exploitation Teams

These units are task organized teams specifically detailed and trained at the tactical level by the operational commander. The mission of site exploitation teams is to conduct systematic discovery activities and search operations, and properly identify, document, and preserve the point of collection and its material. The team collects material and information of technical and forensic value for further analysis and exploitation, including pattern analysis, trend identification, and rule of law. Unit personnel receive training in formalized forensic collection, and can forensically exploit nontransportable material onsite. Team leaders distribute resultant intelligence laterally and to higher and lower echelons to provide vital insights in a timely manner. **Figure 4-4** illustrates information and materials that can be collected and exploited onsite. **Figure 4-5** shows nighttime site exploitation.

Figure 4-5. US Forces Conduct Site Exploitation at Night. *(Photo Credit: JIEDDO)*

4.4.4 Naval Surface Warfare Center Indian Head Explosive Ordnance Disposal Technology Division (NSWC IHEODTD) Technical Support Detachment (TSD)

The NSWC IHEODTD TSD provides TECHINT personnel who are specially trained and equipped for countering explosive hazards and explosive ordnance across the spectrum of conflict (**Figure 4-6**). The core mission of the TSD is to collect, exploit, and analyze enemy explosive ordnance and explosive hazards (including improvised weapons/IEDs) and their components to provide near-real-time TECHINT. Additionally, the TSD provides deployable TECHINT and Foreign Material Acquisition (FMA) support to individual services, DoD, and national level intelligence activities, as directed by higher authority. The TSD is composed of FMA platoons that support Level 1 activities and CEXC platoons that support Level 1 technical categorization, tactical characterization, and collection activities. TSD also supports Level 2 activities.

4.4.4.1 Combined Explosive Exploitation Cell (CEXC) Platoon

TSD CEXC platoon forward deploys a modular Level 1 exploitation capability that does the following:

- Exploits an incident site; provides post-blat investigation expertise and site exploitation support, including tactical evaluation of incident site
- Recognizes, preserves, and collects items of exploitation value
- Neutralizes remaining explosive hazards
- Conducts initial electronic analysis of post-blast components
- Conducts initial chemical analysis of materials

- Conducts forensics collection from nonremovable materials

Detailed intelligence products resulting from CEXC platoon Level 1 activities aid in the timely development of counter-weaponry TTP and targeting packages.

Figure 4-6. NSWC IHEODTD TSD. *A platoon member uses a mine probe to ensure disturbed dirt around a blast crater is safe. (Photo Credit: USN)*

4.4.4.2 Technical Support Detachment (TSD) Foreign Materials Acquisition (FMA) Platoon

FMA personnel conduct TECHINT operations against conventional military munitions, improvised weapons, and associated components worldwide. Conventional weapons are of interest to the WTI community because of their potential for use in improvised weapons or use in a manner for which they were not designed. FMA operations collect foreign munitions, improvised weapons, and associated components for exploitation by the technical IC and Armed Services S&T laboratories. Collection can require packaging, safe to ship certification, and shipment of hazardous explosive items. NSWC IHEODTD's FMA capability is modular, allowing it to be tailored for specific tasks.

Figure 4-7. A CRT Investigates a CBRN Incident *(Photo Credit: USA)*

4.4.5 CBRN Response Teams (CRT)

CRTs, formerly called technical escort teams, are specially trained and equipped to conduct deliberate site exploitation operations in support of weapons of mass destruction elimination operations (**Figure 4-7**). CRTs are equipped with state-of-the-art technology and employ the latest TTP to identify, neutralize, and dispose of CBRN agents and munitions. CRT members possess the skills necessary to gauge the level of hazards present in clandestine laboratories. Because threat laboratories often contain toxic and caustic chemicals, CRT personnel require a higher level of training and specialized equipment for safe exploitation. This training includes understanding how to properly recognize, preserve, neutralize, and collect hazardous chemical, explosive, or drug-related materials. CRTs have an integrated EOD capability to enhance CBRN activities and mitigate threats.

4.4.6 Law Enforcement Professionals (LEP) Program

LEP program personnel (**Figure 4-8**) support US and coalition military forces by providing a comprehensive understanding of demographic, cultural, and behavioral characteristics of threat networks, including criminal organizations. LEP personnel serve in an advisory role to commanders to advise, assist, mentor, and train personnel and provide experienced LE criminal enterprise analysts to assist in suppressing criminal and other threat networks. LEPs augment Level 1 operations by providing support for site exploitation and material recovery and custody. There are many parallels between insurgent networks and criminal networks in terms of structure, financing, recruiting, and operations. For this reason, LE personnel with gang and crime network experience are useful to tactical units to help them understand and attack critical nodes within threat networks. LEP personnel also provide expertise in customs procedures, border operations, counterinsurgency and counter-drug operations, rule of law, tactical site exploitation, evidence-based operations, support to security forces advisory teams, and guidance regarding evidence preparation, collection, and packaging for use during HN criminal prosecutions.

Figure 4-8. USMC LEP Interacts with a Local National *(Photo Credit: USMC)*

“The LEP program evolved from providing Marines ‘cop on the beat’ training, to sensitive site exploitation and forensic training, to providing ‘detective’ advice and expertise in developing evidence and reports that would support incarceration of insurgents and criminals.”[138]

4.4.7 Maritime Interception Operations (MIO)

Maritime interception enables collection of materials and information during vessel boardings to facilitate target development and identify links between maritime activity and terrorist/criminal networks. There are four basic types of boarding operations, which facilitate naval forces access to potential WTI exploitation opportunities:

[138] Crawford and Tharp, “Role of Law Enforcement Professionals.”

- MIO is used to enforce sanctions or national policies to interdict goods or persons prohibited by lawful sanction
- EMIO broadens VBSS operations to intercept targeted personnel or material that pose an imminent threat to the United States or US interest
- Maritime Counter Proliferation Interdiction (MCPI) is an intelligence-driven interception operation designed to target the spread of WMD components; duel use components and precursors; delivery systems; and munitions
- Counter piracy (CP) boardings to disrupt international piracy

Navy surface combatants, cruiser/destroyer class ships, employ VBSS teams (**Figure 4-9**) to conduct MIOs. VBSS teams are trained in detecting chemical, biological, and radiological materials; collecting biometrics; conducting tactical questioning; and preserving and documenting captured enemy documents and media, including cell phones and contextual and electronic data for DOMEX. Marine Expeditionary Units have specialized Heliborne Visit Board Search and Seizure (HVBSS) teams, which are capable of boarding noncompliant vessels via helicopter insertion techniques. In the CENTCOM AOR, shipboard VBSS teams and United States Marine Corps (USMC) HVBSS teams can be augmented by intelligence exploitation teams (IET) to facilitate HUMINT and tactical site exploitation activities. During EMIO and MCPI boardings, Naval Special Warfare, Marine Special Operations Command forces, USMC HVBSS teams, and EOD personnel can deploy to conduct sensitive site exploitation operations. Forward deployed Navy EOD and TSD CEXC platoons, such as those assigned to United States Naval Forces Central Command Exploitation Laboratory (NEL), support maritime exploitation/boarding operations when IEDs, improvised weapons, or related materials are suspected or encountered.

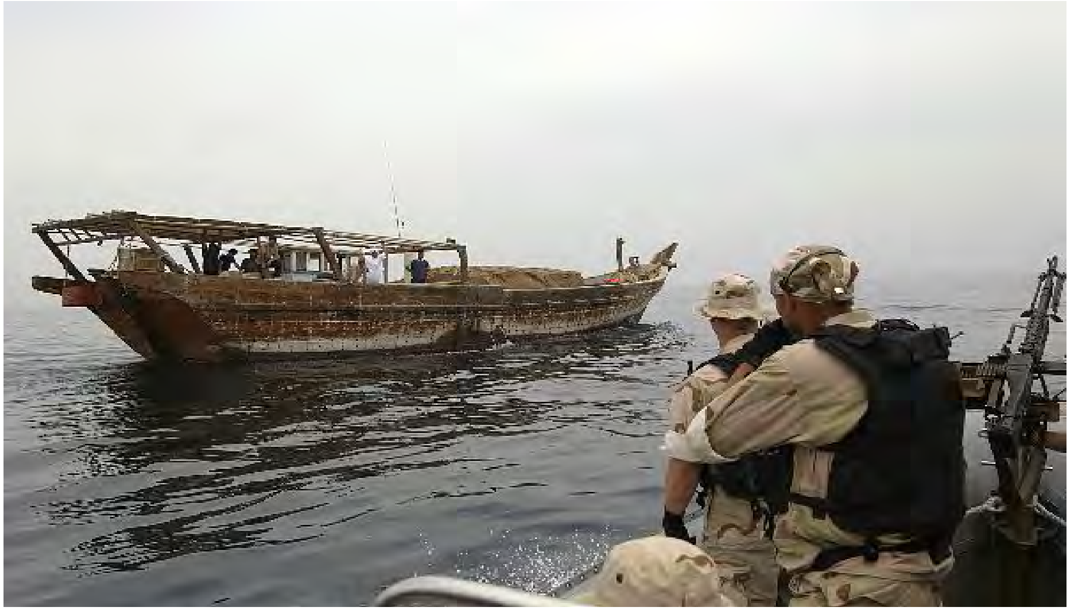


Figure 4-9. US Navy VBSS Team Prepares to Board a Dhow *(Photo Credit: USN)*

4.4.8 National Ground Intelligence Center (NGIC), Combat Incident Analysis Division (CIAD) Technical Intelligence Forensic-Branch (TIF-B)

The NGIC CIAD TIF-B is the US Army's Center of Excellence for Attack Scene Investigation (ASI) and Battlefield Vehicle Forensics (BVF). ASI performs field expedient collection of forensic data from a mounted or dismounted attack scene, with focus on the limitations created by the lack of security, time, and manpower. BVF is the analysis of collected forensic data from a mounted attack scene with the intent to discover and assess the enemy's intent, weapon type, trajectory, range, angle of attack, armor performance, and crew protection.

4.4.9 Working Dogs

Working dogs (**Figure 4-10**) provide a unique search capability to locate weapons, explosives, caches, and track individuals.[139] Working dogs are categorized by their distinct capabilities:

- Specialized search dogs
- Patrol explosive detector dogs
- Mine detector dogs
- Combat tracker dogs

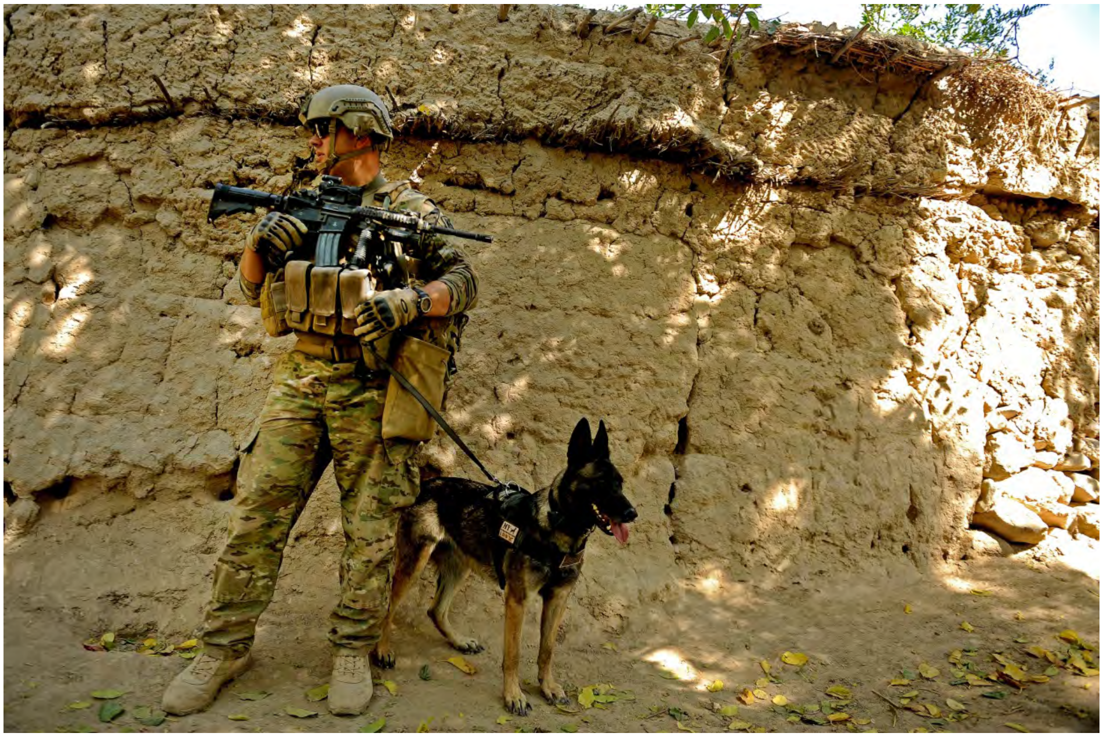


Figure 4-10. US Army Dog Handler with an Explosive Detector Dog *(Photo Credit: JIEDDO)*

[139] NOTE: For a more detailed explanation of Military Working Dog capabilities refer to the Combined Arms Center (CAC) Center for Army Lessons Learned, *Commander's Guide to Military Working Dogs Handbook*, no. 09-09, January 2009.

4.4.10 Special Agent Bomb Technician (SABT)

The SABT program is part of the Federal Bureau of Investigation’s (FBI’s) Hazardous Devices Operations Center, subordinate to the Critical Incident Response Group. SABTs routinely deploy OCONUS on a rotational basis in support of:

- **Capacity Building.** SABTs train local LE and military in evidentiary collection and documentation, improvised explosives, booby traps, enemy TTP, explosive safety, post-blast response, and bomb technician risk assessment. They mentor local LE and military in WTI process, evidentiary accountability, and development of explosive strategy and policy implementation

- **Forensic and Technical Analysis.** SABTs support local LE and military by leveraging HN laboratories and US-issued equipment, submitting IEDs to Terrorist Explosive Device Analytical Center (TEDAC), and examine and analyzing IEDs and components

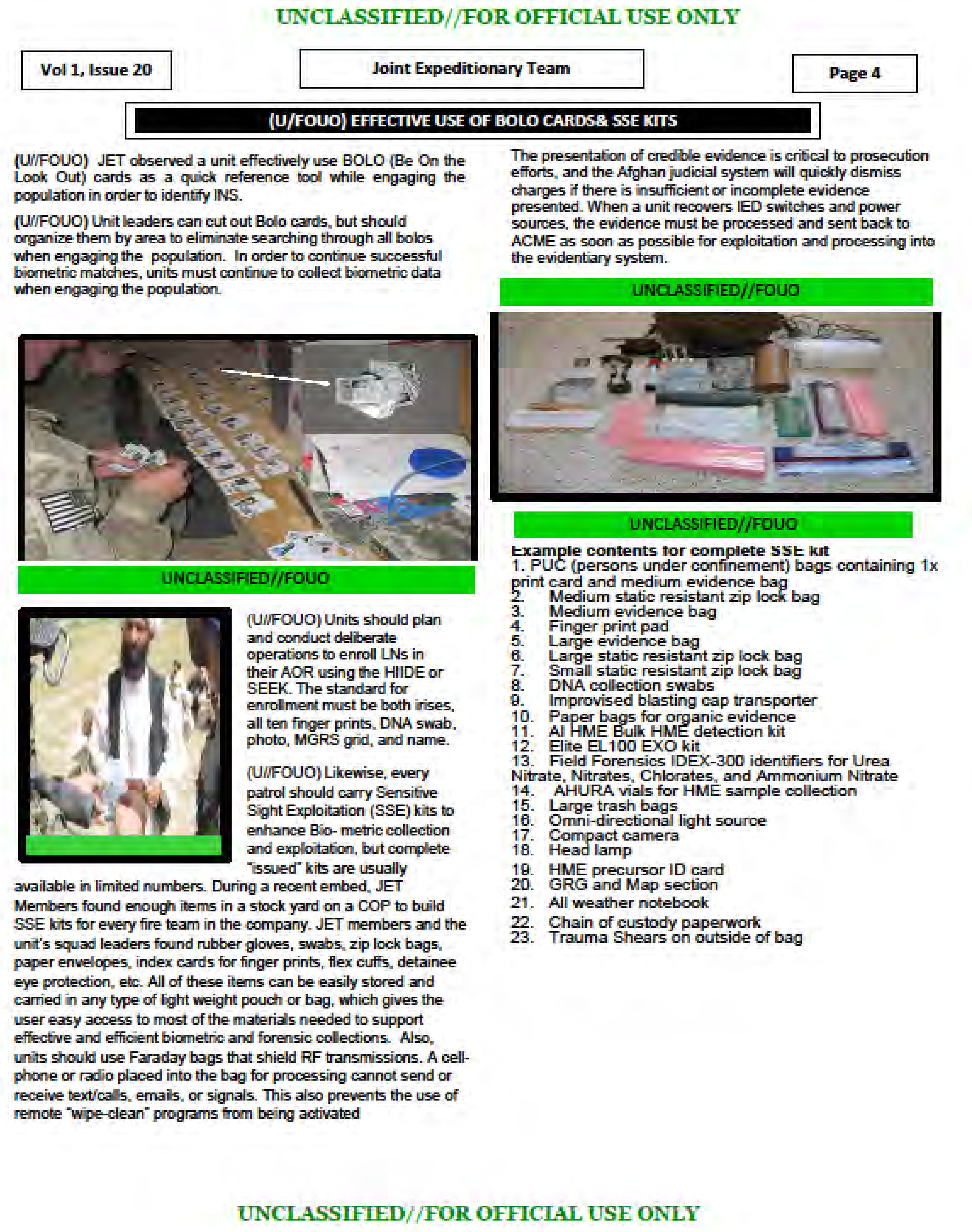
- **Information Collection and Sharing.** Includes witness and suspect interviews; reach back support to TEDAC; TEDAC analysis to HNs; documentation and dissemination of IED and explosive-related intelligence in support of US security

- **Post-Blast Response.** SABTs establish connections and rapport with local LE and military EOD leadership and staff and respond to a bomb scene when required.

- **LEGAT and Field Office Support (as directed by LEGAT).** SABTs are Special Agents first and Bomb Technicians second. They are expected to perform investigation taskings (per LEGAT mission) and are not limited to working bombs and bombings.

4.4.11 Joint Expeditionary Team (JET)

JIEDDO’s JET is a flexible, scalable capability that supports all echelons of the US Armed Services and interagency and US coalition partners to train, advise, observe, analyze, collect, and disseminate TTP, lessons learned, and best practices to mitigate the IED threat, using material and nonmaterial solutions, and enhance C-IED operations, initiatives, and strategies. JET members are primarily retired military, LE, and intelligence subject matter experts (SMEs) who possess a minimum of 10 to 15 years’ experience. JET operates within JIEDDO’s lines of operation, CONUS and OCONUS, including operational personnel embedded in C-IED assistance missions. JET’s observations of best practices, lessons learned, and TTP are primarily disseminated to the COI via a C-IED Advisory Mission Summary (CAMSUM) (**Figure 4-11**).



UNCLASSIFIED//FOR OFFICIAL USE ONLY

Vol 1, Issue 20

Joint Expeditionary Team

Page 4

(U/FOUO) EFFECTIVE USE OF BOLO CARDS& SSE KITS

(U//FOUO) JET observed a unit effectively use BOLO (Be On the Look Out) cards as a quick reference tool while engaging the population in order to identify INS.

(U//FOUO) Unit leaders can cut out Bolo cards, but should organize them by area to eliminate searching through all bolos when engaging the population. In order to continue successful biometric matches, units must continue to collect biometric data when engaging the population.

UNCLASSIFIED//FOUO

(U//FOUO) Units should plan and conduct deliberate operations to enroll LNs in their AOR using the HIIDE or SEEK. The standard for enrollment must be both irises, all ten finger prints, DNA swab, photo, MGRS grid, and name.

(U//FOUO) Likewise, every patrol should carry Sensitive Sight Exploitation (SSE) kits to enhance Bio- metric collection and exploitation, but complete "issued" kits are usually available in limited numbers. During a recent embed, JET Members found enough items in a stock yard on a COP to build SSE kits for every fire team in the company. JET members and the unit's squad leaders found rubber gloves, swabs, zip lock bags, paper envelopes, index cards for finger prints, flex cuffs, detainee eye protection, etc. All of these items can be easily stored and carried in any type of light weight pouch or bag, which gives the user easy access to most of the materials needed to support effective and efficient biometric and forensic collections. Also, units should use Faraday bags that shield RF transmissions. A cell-phone or radio placed into the bag for processing cannot send or receive text/calls, emails, or signals. This also prevents the use of remote "wipe-clean" programs from being activated

The presentation of credible evidence is critical to prosecution efforts, and the Afghan judicial system will quickly dismiss charges if there is insufficient or incomplete evidence presented. When a unit recovers IED switches and power sources, the evidence must be processed and sent back to ACME as soon as possible for exploitation and processing into the evidentiary system.

UNCLASSIFIED//FOUO

UNCLASSIFIED//FOUO

Example contents for complete SSE kit

1. PUC (persons under confinement) bags containing 1x print card and medium evidence bag
2. Medium static resistant zip lock bag
3. Medium evidence bag
4. Finger print pad
5. Large evidence bag
6. Large static resistant zip lock bag
7. Small static resistant zip lock bag
8. DNA collection swabs
9. Improvised blasting cap transporter
10. Paper bags for organic evidence
11. AI HME Bulk HME detection kit
12. Elite EL100 EXO kit
13. Field Forensics IDEX-300 identifiers for Urea Nitrate, Nitrates, Chlorates, and Ammonium Nitrate
14. AHURA vials for HME sample collection
15. Large trash bags
16. Omni-directional light source
17. Compact camera
18. Head lamp
19. HME precursor ID card
20. GRG and Map section
21. All weather notebook
22. Chain of custody paperwork
23. Trauma Shears on outside of bag

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Figure 4-11. Page from a JET C-IED Advisory Mission Summary (CAMSUM) *(Photo Credit: JIEDDO, JET)*

Maritime Interception Vignette

During a MIO, a ship's VBSS team conducted a visit on a ship suspected of transporting illicit materials. Through coordination with the VBSS team's ship and Navy higher headquarters, the VBSS team was directed to conduct a thorough search of the vessel and collect biometrics from the crew. During the search, the team discovered electronic components and containers of unknown chemical compounds. Through reach back support, it was determined that the chemicals were potentially precursors for HME production, and the electronic components could be types that have been used in IEDs. The ship and crew were held, and additional naval assets (i.e., EOD, Naval Criminal Investigation Service [NCIS], and a MIO IET) were deployed to conduct further exploitation of the vessel and tactical questioning of the crew, which Upon further exploitation of the vessel and crew, information was revealed that supported the notion that the vessel was smuggling IED components and precursor materials. Subsequently, the vessel was seized and the crew detained. The materials recovered from the vessel were sent to follow-on exploitation facilities (Level 2, in theater, and Level 3 in CONUS) for further exploitation and analysis.

The follow-on exploitation facilities conducted definitive analysis of the chemicals and determined that they were all precursors to production of HME. Forensic processing and analysis of the materials recovered produced latent prints, trace materials samples, and DNA samples, which were processed and analyzed against known latent prints (the team had collected 10 print cards, buccal swab collections, and DNA profiles). This process produced positive matches to known and unknown latent prints in the Automated Biometric Identification System (ABIS) database, linking them to the materials found. Exploitation of the recovered electronic components and analysis of the information produced linkages of the electronic materials to components used in IEDs in the CCMD and other theaters of operations. Additionally, exploitation of recovered communication devices (e.g., cell phones and computers) led to linkages to other individuals involved in smuggling activities.

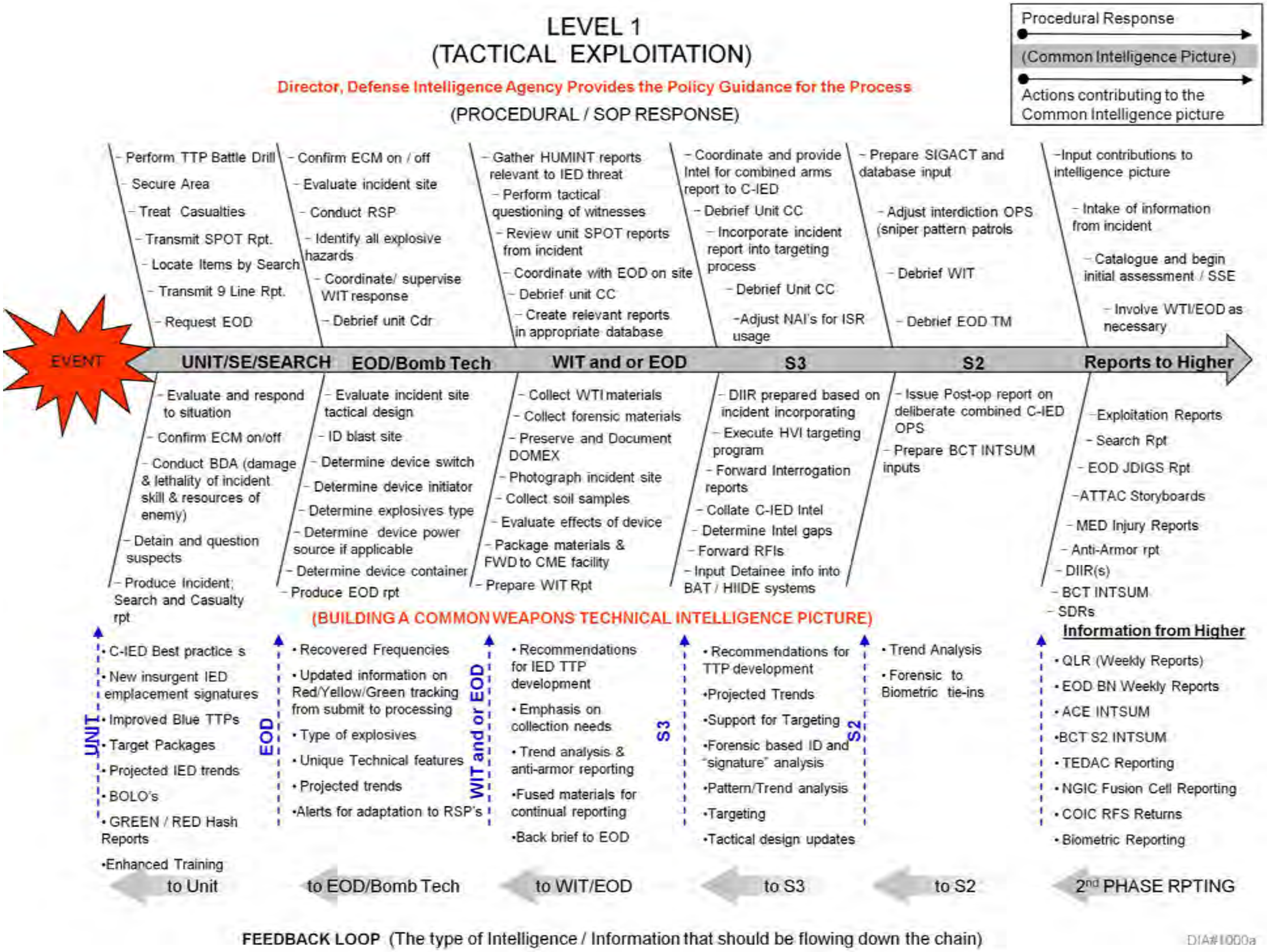
This vignette illustrates one of a myriad of possible scenarios that place MIO teams in situations where they encounter illicit arms/materials being smuggled via the maritime transportation system. While the vignette paints only a conceptual scenario, threat networks exploit weak maritime transportation controls to further their objectives.

Current examples of maritime threats include the following. In December 2012, Yemen authorities arrested three Albanians and seized 180 tons of illicit arms from a cargo vessel entering their country. In January 2013, Yemini Coast Guard officials, with support of the USS FARRAGUT's VBSS team, intercepted a 130-foot fishing dhow attempting to smuggle Iranian-made surface-to-air missiles, 122 mm mortars, rocket-propelled grenades, IED components, and military grade explosives intended to supply the Houthi rebels operating in Yemen.

4.5 Outputs

The specific products associated with exploitation at the tactical level of WTI focus on the tactical commander's capabilities and requirements. The tactical situation determines the level of detail an exploitation asset conducts. The first technical and tactical assessment produces the following information:

- Indicators and warnings of the enemy's introduction of a new or more capable weapon system
- Context regarding how a device or weapon system was used and its intended target
- Battle damage assessments when required
- First reporting of new enemy TTP and devices
- Tactical characterization of how an IED incident was planned and conducted (tactical design) and the intent (purpose of device)
- Initial technical categorization of a weapon system and associated components
- Evaluation of signatures to cue intelligence, surveillance, and reconnaissance (ISR) priorities and provide identifiers regarding other threat activity
- Pattern analysis to identify trends and behaviors and provide analysis regarding possible future threat activity
- Recommendations regarding friendly force TTP adaptation
- Support for follow-on questioning of POI
- Support for dynamic targeting



LEVEL 1
(TACTICAL EXPLOITATION)

Director, Defense Intelligence Agency Provides the Policy Guidance for the Process

(PROCEDURAL / SOP RESPONSE)

Procedural Response

(Common Intelligence Picture)

Actions contributing to the Common Intelligence picture

EVENT

UNIT/SE/SEARCH

- Perform TTP Battle Drill
- Secure Area
- Treat Casualties
- Transmit SPOT Rpt.
- Locate Items by Search
- Transmit 9 Line Rpt.
- Request EOD

- Evaluate and respond to situation
- Confirm ECM on/off
- Conduct BDA (damage & lethality of incident skill & resources of enemy)
- Detain and question suspects
- Produce Incident; Search and Casualty rpt

EOD/Bomb Tech

- Confirm ECM on / off
- Evaluate incident site
- Conduct RSP
- Identify all explosive hazards
- Coordinate/ supervise WIT response
- Debrief unit Cdr

- Evaluate incident site tactical design
- ID blast site
- Determine device switch
- Determine device initiator
- Determine explosives type
- Determine device power source if applicable
- Determine device container
- Produce EOD rpt

WIT and or EOD

- Gather HUMINT reports relevant to IED threat
- Perform tactical questioning of witnesses
- Review unit SPOT reports from incident
- Coordinate with EOD on site
- Debrief unit CC
- Create relevant reports in appropriate database

- Collect WTI materials
- Collect forensic materials
- Preserve and Document DOMEX
- Photograph incident site
- Collect soil samples
- Evaluate effects of device
- Package materials & FWD to CME facility
- Prepare WIT Rpt

S3

- Coordinate and provide Intel for combined arms report to C-IED
- Debrief Unit CC
- Incorporate incident report into targeting process
- Debrief Unit CC
- Adjust NAI's for ISR usage

- DIIR prepared based on incident incorporating
- Execute HVI targeting program
- Forward Interrogation reports
- Collate C-IED Intel
- Determine Intel gaps
- Forward RFIs
- Input Detainee info into BAT / HIIDE systems

S2

- Prepare SIGACT and database input
- Adjust interdiction OPS (sniper pattern patrols
- Debrief WIT
- Debrief EOD TM

- Issue Post-op report on deliberate combined C-IED OPS
- Prepare BCT INTSUM inputs

Reports to Higher

- Input contributions to intelligence picture
- Intake of information from incident
- Catalogue and begin initial assessment / SSE
- Involve WTI/EOD as necessary

- Exploitation Reports
- Search Rpt
- EOD JDIGS Rpt
- ATTAC Storyboards
- MED Injury Reports
- Anti-Armor rpt
- DIIR(s)
- BCT INTSUM
- SDRs

(BUILDING A COMMON WEAPONS TECHNICAL INTELLIGENCE PICTURE)

UNIT

- C-IED Best practice s
- New insurgent IED emplacement signatures
- Improved Blue TTPs
- Target Packages
- Projected IED trends
- BOLO's
- GREEN / RED Hash Reports
- Enhanced Training

to Unit

EOD

- Recovered Frequencies
- Updated information on Red/Yellow/Green tracking from submit to processing
- Type of explosives
- Unique Technical features
- Projected trends
- Alerts for adaptation to RSP's

to EOD/Bomb Tech

WIT and or EOD

- Recommendations for IED TTP development
- Emphasis on collection needs
- Trend analysis & anti-armor reporting
- Fused materials for continual reporting
- Back brief to EOD

to WIT/EOD

S3

- Recommendations for TTP development
- Projected Trends
- Support for Targeting
- Forensic based ID and "signature" analysis
- Pattern/Trend analysis
- Targeting
- Tactical design updates

to S3

S2

- Trend Analysis
- Forensic to Biometric tie-ins

to S2

Information from Higher

- QLR (Weekly Reports)
- EOD BN Weekly Reports
- ACE INTSUM
- BCT S2 INTSUM
- TEDAC Reporting
- NGIC Fusion Cell Reporting
- COIC RFS Returns
- Biometric Reporting

2nd PHASE RPTING

FEEDBACK LOOP (The type of Intelligence / Information that should be flowing down the chain)

DIA#1000a

CHAPTER 5
Level 2 (Operational) Exploitation and Analysis

5.1 General Description

Level 2 exploitation and analysis employs technical and forensic examination techniques and analysis of collected information and material and is conducted by deployed exploitation laboratories in a expeditionary environment. Level 2 exploitation provides feedback and outputs that support WTI's five critical outcomes by identifying technical and forensic characteristics and associations between events, people, and improvised weapons, including IEDs and other weapons employed in an asymmetric environment. Level 2 combines the outputs of Level 1 with Level 2 exploitation results, all-source analysis, and supports more in-depth follow-on exploitation and analysis by injecting timely and relevant forensic and technical design information into the intelligence process to inform CCIRs, support targeting and prosecution, and support material developers for FP and force training objectives.

Deployed exploitation laboratories use advanced capabilities, sophisticated exploitation equipment, and personnel with greater technical and specialized skills than those at the tactical level. Operational level exploitation facilities are typically deployable, flexible, and scalable (plug and play) and are established in a theater of operation relatively close to tactical level assets. Skill sets and equipment associated with Level 2 activity include triage, technical exploitation and analysis, forensic and biometric exploitation/analysis, chemical exploitation/analysis, DOMEX/analysis, information and intelligence fusion, and other functions as required. Level 2 facilities that handle and store explosives must have a written explosive safety management program, be explosively sited, and comply with DoD and service specific explosive safety regulations.[140]

Integration and synchronization of information gleaned from battlefield exploitation capabilities are essential to support military, intelligence, and LE operations in theater. To achieve this, the JFC establishes a Joint Intelligence Exploitation (J2E) staff to provide a theater-level command and control structure to ensure the numerous disparate Level 2 exploitation/analysis capabilities operate as an efficient, coherent, and organized enterprise. A J2E ensures stakeholders and partners, including HNs, are unified in developing focused and fused intelligence and evidentiary information, transparency, and feedback to operations at all levels. Appendix E addresses the J2E in more detail.

5.2 Objectives

- Determine how weapons and devices operate, including identifying radio-controlled IED (RCIED) device frequencies and providing initial analysis of requirements for electronic countermeasures (ECM) equipment

- Conduct forensic and biometric exploitation and analysis, including information to enhance BEI for targeting packages

- Analyze and identify device/weapon components to provide material sourcing information and create searchable theater databases

[140] Department or Defense, *DoD Ammunition and Explosive Safety Standards*, DoD Manual 6055.9-M, Washington, DC, February 29, 2008.

- Identify bomb maker signatures and profiles
- Identify adversary trends in weapons systems development and employment
- Provide input to the intelligence process to identify threat networks
- Evaluate enemy technical capabilities
- Conduct chemical analysis of explosive and enhancement material
- Conduct initial in theater field trials of new threat devices, tactical designs, emplacement geometry, and evaluate existing countermeasures in light of new threat capabilities
- Provide data to support the requirements development process
- Support questioning of POI
- Provide information to assist US, host, and partner nation LE efforts
- Additional exploitation (Level III and higher), if required, will be conducted through reach back means with other laboratories and intelligence agencies.

5.3 Capabilities

Capabilities required at Level 2 facilities to conduct time-sensitive exploitation include the following:

- Triage
- Explosive safety
- Photography
- Case management
- Chemistry
- Technical exploitation
  - Electronic
  - Mechanical
- Forensics exploitation
  - Latent print analysis
  - DNA analysis
  - Firearms and tool marks
  - Trace analysis
  - DOMEX

5.3.1 Triage

Triage is a deliberate process that determines materials' potential value for exploitation, the order it should be processed, and how the device should be exploited to maximize the value of WTI and collected forensic material. During triage, materials are screened for explosive, chemical, radiological, and other physical hazards before being further processed through the exploitation disciplines. This ensures the safety of personnel processing the material. Material being processed is recorded, labeled, entered into a database, and photographed. **Figure 5-1** shows an EOD technician conducting triage at a deployed exploitation laboratory.

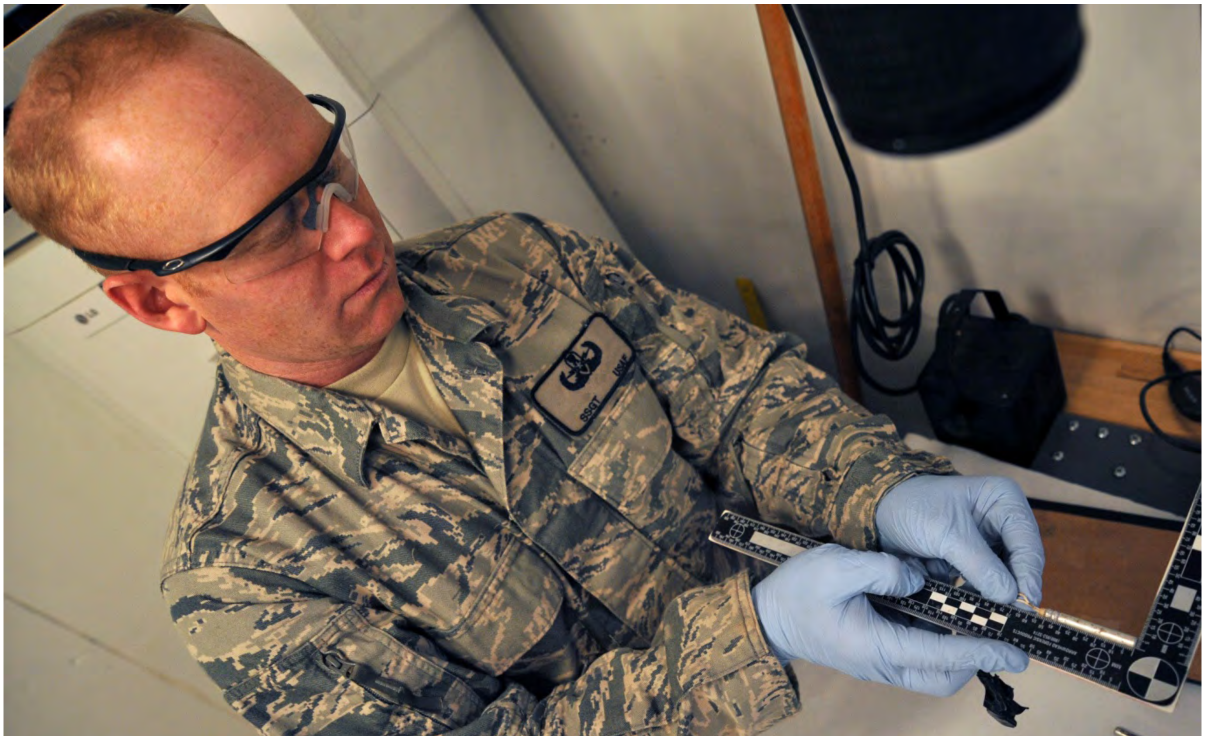


Figure 5-1. Triage. *An EOD Technician measures a blasting cap at CJTF Troy's triage laboratory. (Photo Credit: USAF)*

5.3.2 Explosive Safety

The explosive safety process involves a visual inspection of all received material to determine if any explosive components/materials are hazardous to follow-on exploitation. EOD/certified bomb squad personnel are the only personnel authorized to conduct explosive safety. Materials or items found to be of concern are X-rayed to confirm/deny the presence of explosive materials. Identified hazards are removed from the device so that it can be further exploited by the other disciplines. Explosive samples are taken and forwarded for potential follow-on exploitation.[141]

[141] NOTE: Packaging, certifying, and transporting explosives require the involvement of trained and certified personnel. EOD company and battalion representatives facilitate transportation of explosives by certifying that they are packaged correctly and are safe to ship. The Under Secretary for Intelligence (USD-I) Hazardous Material Transportation Office (HMTO) is another asset qualified to conduct this function.

5.3.3 Photography

Photography (**Figure 5-2**) is one of the first steps in the forensic exploitation process and is used at all levels of exploitation. Photographs are important to inventory and record the original state of an item as identified, collected, and received, and to document its progression through the exploitation process. Detailed photographs are important for examiners and analysts to identify profiling data and signatures, establish links to other devices seen in the operational area, and identify manufacturer information that could lead to identification of supply chains and bomb maker networks. Close-up photographs of an item are used to document individual components, textures, and designs of recovered material for possible use by HN criminal investigation. Photographs are also important to capturing images of latent prints through techniques that include chemical reaction to lasers or ultraviolet light when standard print lifting methods can't be used, or when fuming[142] can't occur because of its incompatibility with the material being exploited. Photographs of devices and components are forwarded to reach back assets to support time-sensitive information requirements.

5.3.4 Case Management

Congruent with triage, case management functions the appropriate handling and processing of materials, which includes chain of custody and proper material flow throughout the exploitation process.

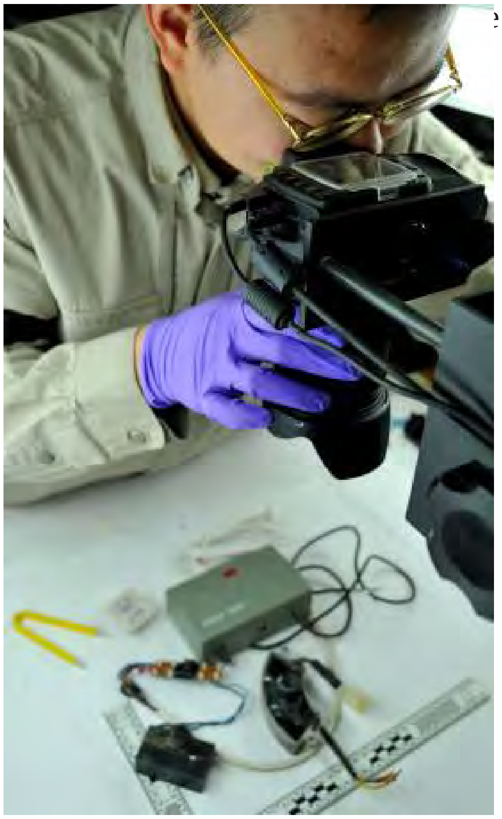


Figure 5-2. CJTF Troy. CEXC Team Member Photographs a Disassembled IED *(Photo Credit: USAF)*

5.3.5 Chemistry

Chemistry encompasses the chemical analysis of bulk or trace material for initial identification of unknown substances or confirmation of substances subjected to presumptive testing during tactical exploitation (Level 1). Chemistry is typically used to identify explosives, explosive precursors, drugs, and poisons. Chemistry personnel sample materials suspected of being involved in the manufacture of HME (e.g., unidentified liquids, solids, and gases). Analysis of the chemical properties of an explosive sample yields the following intelligence, potentially influencing FP, targeting, sourcing, and prosecution:

- Identity of explosives (conventional/HME) or component signatures
- Inform tactical units and HN LE personnel of what to look for during a search
- Identity of specific components and mixtures
- Description of manufacturing processes and material synthesis methods

[142] NOTE: Fuming is a chemical process employed to recover latent prints using super glue.

- Identity of the weapons system for which the explosive is intended, or for which it was used, (e.g., thermobaric, surface-to-air missile, or IED systems)

5.3.6 Technical Exploitation

Technical exploitation includes electronic and mechanical examination and analysis of collected material. This process provides information regarding weapon design, material, and suitability of mechanical and electronic components of IEDs, improvised weapons, and associated components. Technical exploitation involves the relationship of components in comparison to each other and how they function to produce results. Outputs associated with Level 2 technical exploitation include:

- How a switch or other electronic or mechanical elements function
- Arming and firing sequences and related codes
- New capabilities, adaptations, or other evolutions, including new operating frequencies
- Information that supports material sourcing efforts
- Component use and assembler patterns
- Profiles of a weapon and its construction techniques, and equipment used in the process
- The nature of component manufacturing
- Useful information regarding enemy intent
- Confirmation of technical categorization conducted by the tactical unit

5.3.6.1 Electronic Exploitation

Electronic exploitation of improvised weapon material determines how electric components of a device or component function, including switches for arming and firing and their relationship to other features of the weapon system, including the mechanical components. Further exploitation and analysis is conducted to provide a description of the device or components such as switches functions, initial identification of potential sources for the materials recovered, arming and firing sequence and codes, the radio frequency (RF) the device operates on, and a record of functioning times for electronic events.

5.3.6.2 Mechanical Exploitation

Mechanical exploitation of material (mechanical components of improvised weapons and their associated platforms) focuses on devices incorporating manual mechanisms: combinations of physical parts that transmit forces, motion, or energy. It can include things such as evaluation of munitions launch platforms and mechanical components that might be found in an IED, including alarm clock timers, pressure plates, or mechanical anti-tampering devices such as a trip wire. Such analysis — whether encompassing a device, weapon component, or entire system — includes analysis of mechanical components and their relationships with other electrical and explosive elements and subsystems. Examples include the exploitation of the IRAM and victim operated pressure plate devices.

5.3.7 Forensic Exploitation

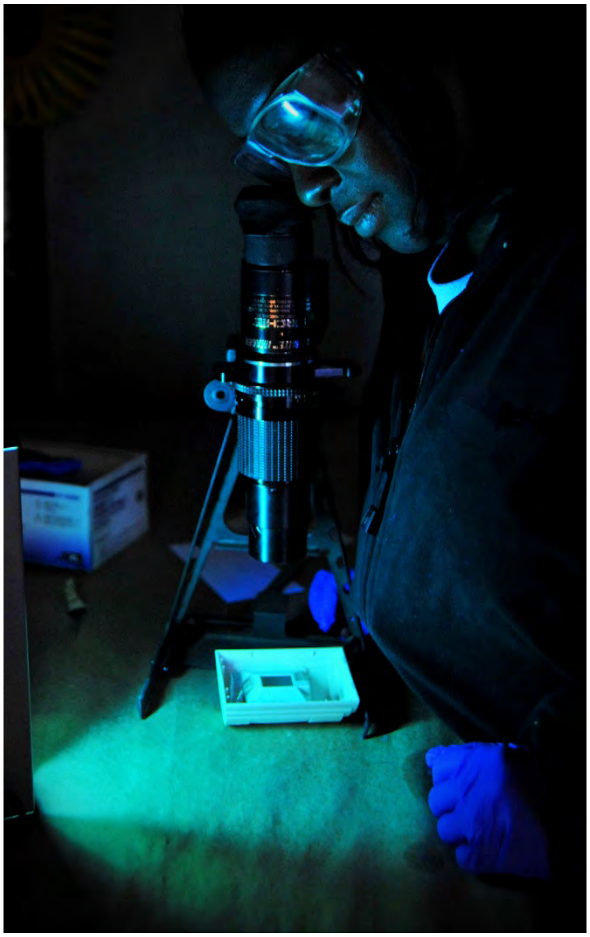


Figure 5-3. Latent Print Examination. *Latent print examiner at a deployed exploitation laboratory uses an reflective ultraviolet imaging system to analyze fingerprints. (Photo Credit: USAF)*

Forensic exploitation is the application of multidisciplinary scientific processes to establish facts. Forensic exploitation applies physical science to link people with locations, events, and material. These methods and processes are used across the ROMO. Forensic exploitation includes:

5.3.7.1 Latent Print Analysis

Latent prints are biometric images of a person's finger, palm, or footprints that are left on material collected. They are the most prolific forensic signature recovered from Level 2 material exploitation and follow-on exploitation processes. The exploitation of latent prints enables biometric identification of people and their association with insurgent, terrorist, or criminal activities, and provides for profiling of events, devices, cells, facilities, and people. Latent print examiners, as shown in **Figure 5-3,** provide specialized experience in harvesting and matching prints from collected materials, as required by the operational commander. Forensic examination of material results in latent prints, which are compared to ABIS holdings to identify a person in a matter of hours. An ABIS match results in notification of NGIC, which produces a Biometric Intelligence Analysis Report (BIAR) and posts it on the Biometric Identity Intelligence Repository (BI2R). The BI2R compiles and associates biometric and forensic data and events to a singular identity, providing the context required to assign an intelligence value and threat level to the individual. Data and events include latent prints and/or DNA recovered from IEDs or site exploitation , and biometric enrollments performed during health and welfare checks, detainment, or detention. BIARs provide further context and basic network associations by including the objective names and other known associates detained or placed in detention during the operation in which the biometric data was collected. Theater commanders leverage BIARs to aid their development of targeting, interrogation, and host/partner nation prosecution support.

5.3.7.2 Deoxyribonucleic Acid (DNA) Analysis

DNA is unique genetic material found within living cells that is collected throughout the exploitation process. Samples of collected DNA are exploited by comparing them against other previously catalogued profiles from post-blast sites, caches, internal and external areas of IED components, bomb makers, detainees and suicide bombers. When results of DNA analysis are fused with other information and intelligence, it can be used to make associations between people, places, and things that aid the development of targeting, interrogation, and host/partner nation prosecution support.

5.3.7.3 Firearms and Tool Marks

Firearm exploitation employs scientific practices to examine firearms, ammunition, ammunition components, gunshot residue, bullet trajectories, and other related material to determine the relationship of a firearm or other object to a person or event. Tool marks analysis involves studying characteristics created during the manufacturing process, such as marks left by machinery or tools, to identify the machinery and tools used to manufacture the device. When conducted by an experienced senior technician, tool marks can determine whether a device was fabricated locally or by a foreign supplier, how many steps were required in the manufacturing process, and the type of machinery involved in making the weapon.

5.3.7.4 Trace Analysis

Trace analysis is the examination and comparison by a variety of disciplines of small particles that include analysis of hairs and fibers, explosive chemistry, trace DNA, and others. Exploitation of improvised weapons and associated components, including IEDs, involves the examination of hairs and textile fibers that have been inadvertently affixed to the device during its construction. Hairs and textile fibers are often found on components within the devices (i.e., command pull, trip lines, battery pack wrapping, lining in main charges). Examination of human hairs from collected material enables mitochondrial or nuclear DNA analysis. Examination and comparison of fibers, fabric, and cordage provide valuable device-device, device-cache, and device-manufacturing location linkage information to help in the elucidation of networks and potential supply lines for networks.

Some trace analysis must be accomplished in a controlled environment which may not be feasible/available in a deployed setting. Tactical commanders must weigh the benefit of employing trace analysis in theater against transporting material to a Level 3 or 4 activity for controlled scientific analysis.

5.3.7.5 Document and Media Exploitation (DOMEX)

WTI activities leverage intelligence capabilities inherent in DOMEX. Documents and media recovered during WTI collection activities, when properly processed and exploited, provide valuable information, such as adversary plans and intentions, force locations, equipment capabilities, and logistical status. Exploitable materials include paper documents such as maps, sketches, letters; or mechanically, electronically, or digitally recorded media such as computer files, hard drives, thumb drives, and cellular phones, as depicted in **Figure 5-4**. When requested, DOMEX support is tailored to the requirement and ranges from a single liaison officer to a robust joint element with a fully staffed Joint Document Exploitation Center (JDEC). The JDEC produces intelligence from all forms of captured adversary documents.[143]

[143] U.S. Joint Chiefs of Staff, *Joint Intelligence*, Joint Publication 1-02, Washington, DC, June 22, 2007.

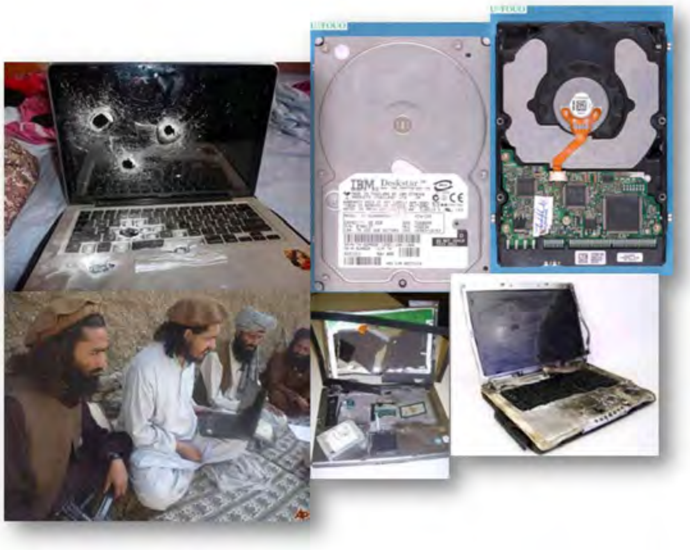


Figure 5-4. Examples of Digital Media Exploited by DOMEX *(Photo Credit: A-TS)*

5.4 Enablers

5.4.1 Joint Task Force (JTF)

Geographic Combatant Commanders may establish a specialized JTF to manage capabilities necessary to combat the enemy's use of improvised weapons. Establishment of a JTF may be deemed appropriate when weapons employed by an adversary in an asymmetric environment exceed the capabilities of the Joint Force Commander or when conducting operations with a joint force would be more efficient. This functional JTF is typically built around a Service (historically Army or Navy) EOD group or battalion/mobile unit (Army/Navy respectively) headquarters and is usually commanded by a senior EOD officer. These headquarters' are uniquely suited with architecture and expertise to provide the core staff upon which to accept additional bolt-on enablers such as expeditionary exploitation laboratories, exploitation teams, operational research/system analysts, and focused intelligence analysts. These enablers provide specialized technical, forensic, biometric, CBRN and intelligence exploitation and analysis expertise not inherent within the core staff. This functional JTF seeks to understand, respond and neutralize the improvised weapon threat, by integrating and coordinating disparate WTI Level 1 and Level 2 enablers that collect, exploit, analyze, and disseminate WTI related material and information. The JTF is normally aligned in direct support of the established theater C2 maneuver structure at each of its echelons and works closely with J2X and J2E staff elements. The JTF provides theater C2 oversight of these ad-hoc and disparate WTI enablers through an established EOD Headquarters. Past examples of this type of JTF include CJTF Troy (Iraq) and CJTF Paladin (Afghanistan) which were employed during Operation Enduring Freedom.

The specialized JTF should be capable of providing the following to enable WTI:

- C2 of EOD and other assets capable of supporting WTI, site exploitation, IED defeat, UXO render safe and recovered munitions disposal

- Analysis and monitoring of enemy improvised weapon TTP and its provision to subordinate tactical units and operational and strategic entities. Provides detailed information on specific adversarial weapon information and improvised weapon trends as well as possible countermeasures.

- Training of in-theater forces on Counter improvised weapon TTP.

- Training to coalition and HN forces on explosive safety and disposal

- Input to the collection plan for materials to be exploited.

- Focus of intelligence collection efforts for captured material and the exploitation of first-seen/recovered improvised weapons and foreign ordnance

- Reliable intelligence and timely indications and warning on the characteristics of adversarial weapons, first-seen ordnance, and potential terrorist threats

- Coordination and synchronization of intelligence collection, exploitation and fusion of WTI

- Synchronization of weapon related intelligence effort across the area of operations (AO) vertically and horizontally, with WTI, all-source, SIGINT, geospatial intelligence, HUMINT, targeting efforts and other agencies and organizations (DoD, National, local, LE)

- Command and control of improvised weapon-related intelligence enablers to help maintain focus and ensure the establishment of improvised weapon Priority Intelligence Requirements

- Focal point for reach back to CONUS concerning WTI and foreign ordnance exploitation

- A focal point for C-IED initiatives and programs, to include programs already in the AO as well as new, untested capabilities.

5.4.2 Naval Surface Warfare Center Indian Head Explosive Ordnance Disposal Technology Division (NSWC IHEODTD) Technical Support Detachment (TSD)

The NSWC IHEODTD TSD provides TECHINT personnel specially trained and equipped to counter explosive hazards and explosive ordnance across the spectrum of conflict. The core mission of the TSD is to collect, exploit, and analyze enemy explosive ordnance, explosive hazards, and their components for the purpose of providing near-real-time TECHINT. Additionally, the TSD provides deployable TECHINT and FMA (e.g., ordnance) support to individual services, DoD, and national level intelligence activities, as directed by higher authority. CEXC and FMA platoons compose the TSD.

Combined Explosive Exploitation Cell (CEXC) Platoon

CEXC platoons are a deployable capability, scalable in skills and size, allowing them to be tailored to meet the commander’s requirements. Scaling can include incorporation of multinational and interagency partners. CEXC platoon members are trained and equipped to conduct TECHINT operations involving recovered weapons systems and provide near-real-time intelligence on weapons systems' construction and employment. CEXC processes provide insights into enemy tactics, identify IED trends and bomb makers, and assist in the development of defensive and offensive C-IED and other weapons defeat measures. Intelligence produced by CEXC supports decision making at all echelons, though the primary customers for its products are tactical and operational commanders. CEXC participates in military exercises with allied and partner nations who seek to provide a focus on WTI missions and capabilities, and supports partner nation capability and capacity building.

When deploying a CEXC platoon to conduct Level 2 exploitation, a TSD provides:

- Triage and explosive safety
- Technical exploitation (electronic and mechanical) of recovered materials
- Chemical analysis of substances
- Intelligence analysis related to the WTI event
- Advice and assistance to US, host, and partner nations organizations
- Support of detainee questioning
- Support of in-country test and evaluation of counter weapons equipment or systems
- Cellular phone exploitation (CELLEX) and MEDEX of cellular phones, computers, hard drives, and media cards

5.4.3 Theater Explosive Exploitation (TEX)

The TEX was established by CJTF Paladin to assist the C-IED fight in the Afghanistan theater of operation. TEX's mission is to coordinate and synchronize improvised weapons and associated components, including IED-related exploitation efforts and WTI, as required, unifying efforts and integrating C-IED capabilities and capacity to ensure freedom of action; protect the population; and enhance the competency, capacity, and credibility of the supported institutions. TEX activities include:

- WTI collection management and dissemination of analysis products
- IED trends, both emerging and migrating
- Joint urgent operational needs statements and in-theater assessment of new materiel solutions
- Guidance on all C-IED technical WTI-related activities
- Training in theater forces on C-IED TTP
- Identifying potential device profiles and leveraging NGIC reach back and/or Level 3 labs for specific device profiles and trends
- A focal point for reach back to CONUS for WTI support
- A focal point for and support to other C-IED initiatives and programs

- Establishing a Joint Prosecution and Exploitation Center (JPEC)

5.4.4 Joint Document Exploitation Center (JDEC) (Forward Deployed Satellite Offices of the National Media Exploitation Center [NMEC] that Conduct DOMEX)

The JDEC exploits captured adversary documents and other media to obtain intelligence. Document exploitation obtains information on topics such as adversary intentions and planning (including deception), locations, dispositions, tactics, communications, logistics, and morale. Coupled with other intelligence sources, document exploitation provides a more complete picture of an unfolding operation and adversary capabilities. The JDEC is activated during periods of hostilities and deploys to the CCMD to manage the recovery, exploitation, automated processing, and disposal of captured adversary documents.

5.4.5 Tactical Document and Media Exploitation (TACDOMEX)

TACDOMEX elements are established to conduct DOMEX operations during hostile conflicts when requested by the CCDR. TACDOMEX provides direct tactical DOMEX support to US combat battalions and brigades using personnel who have been trained to perform the DOMEX mission.

5.4.6 Forensic Exploitation Teams (FXTs)

FXTs are an element of the Defense Forensic Science Center (DFSC). They provide deployable forensic exploitation capability (e.g., personnel, facilities, instrumentation, and HVAC/power generation) as required by the CCMD or JTF CDR. The team includes latent print examiners (**Figure 5-5**), DNA examiners, forensic chemists, firearms/tool marks examiners, and support personnel from a modular pool, task-organized to meet mission requirements. FXTs align critical scientific, technical, and managerial capabilities to increase forensic analytical process efficiency to enhance informed decision making. The FXT reflects the evolution of exploitation capability from large theater laboratories designed to meet Operation Iraqi Freedom (OIF) and Operation Enduring Freedom (OEF) missions. FXTs are scalable and can increase capacity to meet demand. Generally, the FXT deploys two to six-person teams and relies on a robust IT/communications architecture to facilitate in theater exploitation. The FXT operates in conjunction with other capability providers such NSWC IHEODTD.

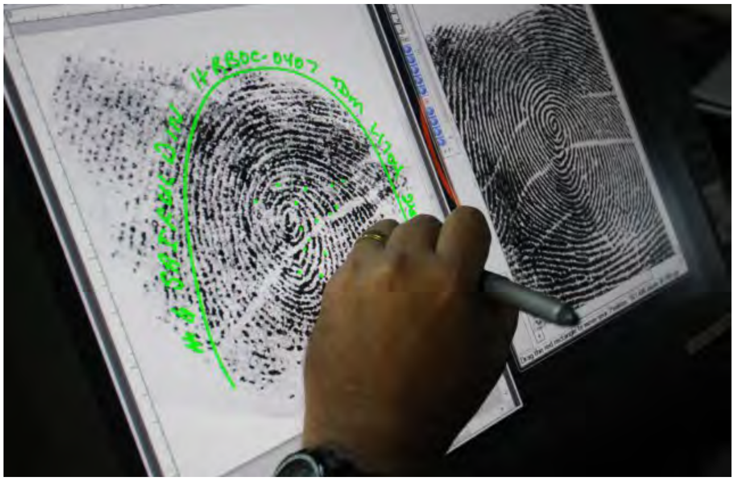


Figure 5-5. A Latent Print Examiner Examines a Fingerprint *(Photo Credit: US Army)*

5.4.7 USMC Exploitation Analysis Cell (EAC)-Lite

The EAC-Lite is an expeditionary Level 2 exploitation capability that supports rapid/near-real-time exploitation, analysis, and forensic examination. It is scalable and employed by the Marine Corps LE detachment that deploys with the Marine Air Ground Task Force (MAGTF) and can be employed in support of VBSS, humanitarian assistance/disaster relief, site exploitation, border control/entry control point operations, and crisis response operations. The capability is designed to quickly exploit all captured enemy material to answer immediate command/security/detention questions and unit's priority intelligence requirements. EAC-Lite has the ability to operate as a Level 2 exploitation operation for the following types of forensic analysis: chemical, media, biometrics (e.g., collection, comparison, storage, sharing), latent print, latent DNA collection, triage, storage, and submission to a follow-on Level 3 exploitation capability. EAC-Lite does not conduct analysis on ballistics, DNA, tool mark comparisons, or technical exploitation. Additional exploitation (Level 3 and higher), if required, will be conducted through reach back with other laboratories and intelligence agencies.

5.4.8 Operations Research Systems Analysts (ORSAs)

ORSAs provide analytical support to tactical units through theater-level commands in Afghanistan and support the military decision making process and planning cycles. ORSAs assist combat leaders and staffs by providing insights that allow them to better define the threat, assess options, and understand complex challenges.

In recent conflicts, the amount of information being collected increased significantly. In Afghanistan, databases related to IEDs, such as the Combined Information Data Network Exchange (CIDNE),[144] WTI exploitation analysis tool (WEAT), and Defense Manpower Data Center, contain terabytes of data. Developing trends and patterns from this data required a unique set of analytical skills and software tools to handle large quantities of often unstructured information without common definitions. ORSAs possess the skill set needed to analyze, define, and structure unstructured data to provide relevant analytics to support the C-IED fight. These skills include analytics and an understanding of C-IED operations, combined with advanced mathematics. The result is the ability to quickly identify emerging friendly and enemy trends, strategically and tactically. ORSAs develop trend information by using multiple statistical and modeling tools to analyze and fuse terabytes of data from multiple databases. This information provides decision makers with an operating picture of IED trends and C-IED progress.

ORSAs provide analytical products and support for the following:

- Threat analysis
- C-IED analysis
- Geospatial analysis
- Trends analysis and forecasting
- Targeting

[144] NOTE: CIDNE is a web enabled database that provides the capability for disparate organizations to capture, manage, and share collected data through a web-browser.

- Casualty assessment and mitigation
- Cost benefit analysis
- Campaign/operational assessment
- Data management
- Qualitative/quantitative assessments
- Route analysis
- Impacts and risk mitigation

5.4.9 Foreign Ordnance Exploitation Cell (FOXC)

The FOXC is a small ad-hoc, task organized TECHINT cell designed to track and analyze the discovery, collection, transportation, and exploitation of foreign ordnance and weapon systems associated with the fabrication and employment of improvised weapons. The cell is comprised of EOD and intelligence professionals from the Army and DIA linked to the IC for reach back assistance and analysis. The cell provides management of captured foreign ordnance to facilitate its exploitation by numerous intelligence agencies and organizations. The FOXC provides analysis on captured foreign ordnance to support WTI, as well as a clear understanding of the ordnance being found. Collocating the FOXC with the C-IED Task Force links collectors and analysts. Additionally, the cell provides a single point of contact for conventional ordnance recovery to fulfill IC and special programs exploitation requirements. The FOXC focuses on the following:

- Maintain and update the Foreign Ordnance Target List
- Provide units with baseline guidance for the recovery of foreign ordnance
- Conduct cache and analysis of foreign ordnance
- Analyze foreign ordnance discoveries in relation to IED attacks
- Analyze foreign ordnance and nation state support to insurgent networks
- Facilitate movement of foreign ordnance
- Monitor special programs
- Provide coalition support

5.5 Outputs

Outputs from these processes also serve to advise and assist US, partner nation, and HN training and doctrine development. The following is a list of additional outcomes associated with operational exploitation.

5.5.1 Intended Outputs of Level 2

Outputs associated with Level 2 focus on a higher level of evaluation and analysis than can be provided at the Level 1. Outputs in the form of reports support the theater commander’s intelligence and prosecution requirements. The emphasis is on enabling offensive operations to identify, track, and target insurgents or terrorists involved in weapons activities and their threat networks. Outputs from these processes also assist with development of FP measures/device countermeasures, and enable operations to identify, track, and target threat actors. The following list includes additional outputs associated with Level 2:

- Information to enhance BEI for targeting packages
- Confirmation and more detailed analysis of the earlier tactical characterization and technical categorization
- IED trends
- IED makers and their links in threat networks
- Bomb maker profiles and signatures to enable pattern analysis and targeting (See Chapters 9 and 10 for details)
- Radio-controlled (RC) frequency tables to enhance electronic warfare (EW)
- New threat technology or new use of technology
- Support for interrogation of IED related detainees

5.5.2 Dissemination

Information obtained during operational exploitation is disseminated horizontally and vertically. Reports created and disseminated to the COI include:

- Triage report
- X-rays, overall device photos, and descriptions
- Electronics report
- Device electronics construction and components, operation, operating frequency, device profile; detailed photos of materials
- Biometrics report
- Latent prints, DNA, trace materials, tool marks recovered and processed; photos of materials recovered
- Chemical analysis report
- Basic confirmation of material type (e.g., explosive, drug, or other)
- Detailed chemical analysis of a substance (e.g., explosive, drug, or other)
- Bulletins: various (e.g., flash reports)
- Alerts on new TTP, new devices, events of significance
- Device profiles

- Categorization of similar devices
- Target and prosecution support packages
- Threat actor profile
- Identification of an individual's weapon making signatures
- Packages developed to support targeting or HN LE activities
- Threat frequency table
- Summary of device frequencies
- Weekly report
- Roll up and summary of exploitation conducted, numbers and types of materials received, exploited, or in process; biometrics and forensic materials recovered and processed; devices added to profiles
- DOMEX reports

Operations Research Systems Analyst (ORSA) Vignettes

ORSA Vignette 1

In Iraq and Afghanistan, ORSAs were assigned to brigades and, in some cases, battalions to provide IED analysis to the most forward warfighters. Products developed by ORSAs allowed patrols to incorporate the most recent IED information into their planning. This gave mounted and dismounted patrols access to the most current information, despite the high volume of significant event data and blue force ops tempo. The brigade ORSAs routinely provided route and trends analysis in support of targeting, assessment of the effects of C-IED operations and equipment, and analysis in support of brigade intelligence (S2).

ORSA Vignette 2

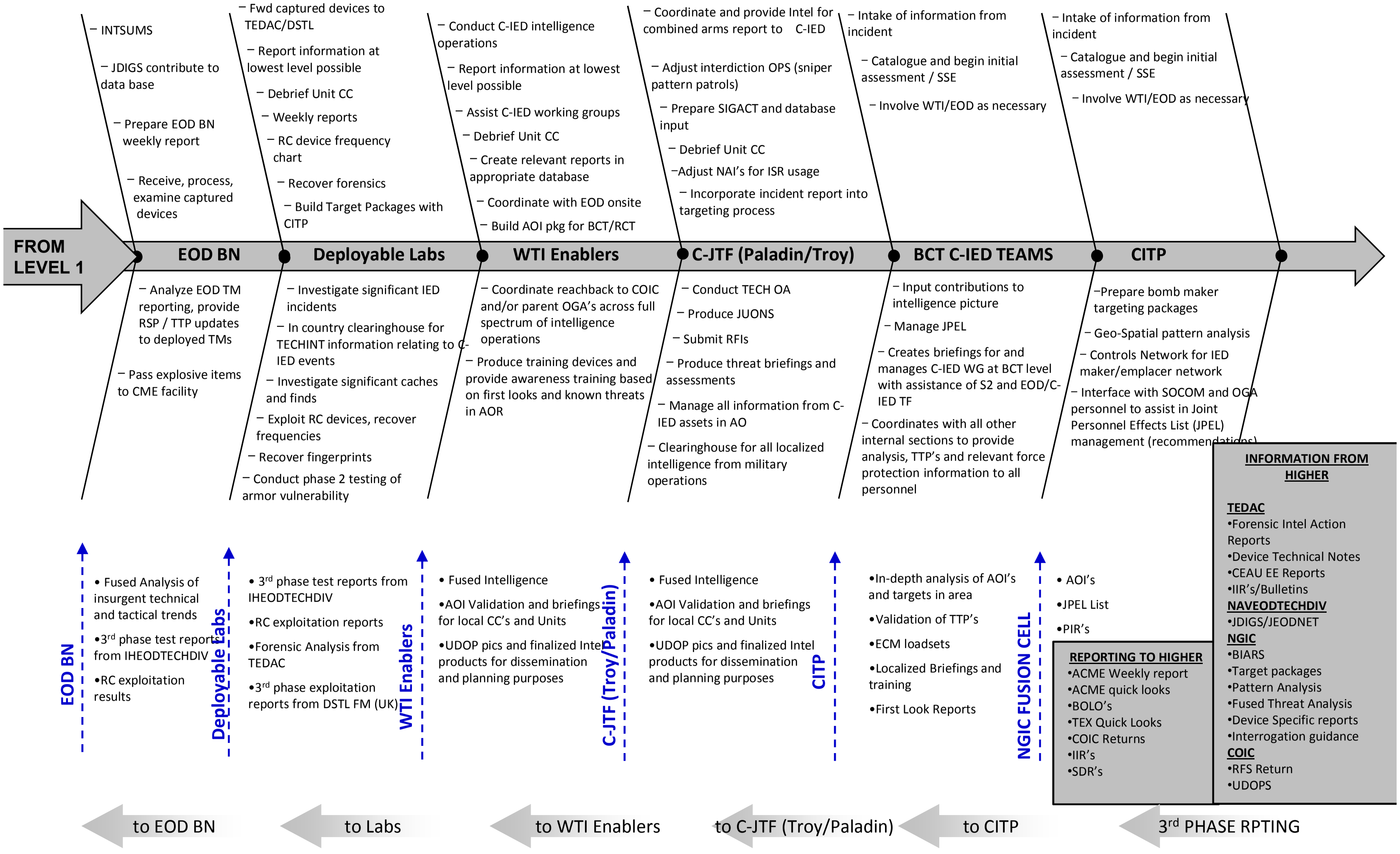
For Iran and Afghanistan, ORSAs established a common set of rules for use at various command levels that was consistently applied across disparate databases that allowed a comparison of IED events to other types of violence. For example, prior to ORSA analysis, violence metrics briefed to senior DoD leaders consistently showed direct fire as the primary form of violence. By linking operational reporting to casualty data, ORSA analysis showed that 60 percent of all US casualties in Iraq and Afghanistan were because of IEDs. Additional analysis that linked medical evacuation reports to significant events and casualty databases allowed the ORSA to show which battlespace owner was sustaining the most severe IED casualties and the types of IEDs that were causing them.

ORSA Vignette 3

When EOD teams conduct post-blast analysis, the reports contain useful information that identifies IED materiel supply trends. For example, the composition of the main charge of an IED device is often included in EOD Level 1 reports. In Afghanistan, reports were entered into CIDNE and provided useful information on specific IED events. ORSAs, working with WTI chemists and the IC community, were able to extract individual chemical reports from Level 1 reporting and identify HME trends across Afghanistan on a weekly basis. Tracking of HME identified ammonium nitrate (AN) as the primary main charge in Afghanistan. This led to a whole-of-government approach to identify where the ammonium nitrate originated and target entities responsible for supplying it to the Taliban.

LEVEL 2
(OPERATIONAL EXPLOITATION)

(PROCEDURAL / SOP RESPONSE)



FROM LEVEL 1

EOD BN

- INTSUMS
- JDIGS contribute to data base
- Prepare EOD BN weekly report
- Receive, process, examine captured devices
- Analyze EOD TM reporting, provide RSP / TTP updates to deployed TMs
- Pass explosive items to CME facility

Deployable Labs

- Fwd captured devices to TEDAC/DSTL
- Report information at lowest level possible
- Debrief Unit CC
- Weekly reports
- RC device frequency chart
- Recover forensics
- Build Target Packages with CITP
- Investigate significant IED incidents
- In country clearinghouse for TECHINT information relating to C-IED events
- Investigate significant caches and finds
- Exploit RC devices, recover frequencies
- Recover fingerprints
- Conduct phase 2 testing of armor vulnerability

WTI Enablers

- Conduct C-IED intelligence operations
- Report information at lowest level possible
- Assist C-IED working groups
- Debrief Unit CC
- Create relevant reports in appropriate database
- Coordinate with EOD onsite
- Build AOI pkg for BCT/RCT
- Coordinate reachback to COIC and/or parent OGA's across full spectrum of intelligence operations
- Produce training devices and provide awareness training based on first looks and known threats in AOR

C-JTF (Paladin/Troy)

- Coordinate and provide Intel for combined arms report to C-IED
- Adjust interdiction OPS (sniper pattern patrols)
- Prepare SIGACT and database input
- Debrief Unit CC
- Adjust NAI's for ISR usage
- Incorporate incident report into targeting process
- Conduct TECH OA
- Produce JUONS
- Submit RFIs
- Produce threat briefings and assessments
- Manage all information from C-IED assets in AO
- Clearinghouse for all localized intelligence from military operations

BCT C-IED TEAMS

- Intake of information from incident
- Catalogue and begin initial assessment / SSE
- Involve WTI/EOD as necessary
- Input contributions to intelligence picture
- Manage JPEL
- Creates briefings for and manages C-IED WG at BCT level with assistance of S2 and EOD/C-IED TF
- Coordinates with all other internal sections to provide analysis, TTP's and relevant force protection information to all personnel

CITP

- Intake of information from incident
- Catalogue and begin initial assessment / SSE
- Involve WTI/EOD as necessary
- Prepare bomb maker targeting packages
- Geo-Spatial pattern analysis
- Controls Network for IED maker/emplacer network
- Interface with SOCOM and OGA personnel to assist in Joint Personnel Effects List (JPEL) management (recommendations)

EOD BN

- Fused Analysis of insurgent technical and tactical trends
- 3rd phase test reports from IHEODTECHDIV
- RC exploitation results

Deployable Labs

- 3rd phase test reports from IHEODTECHDIV
- RC exploitation reports
- Forensic Analysis from TEDAC
- 3rd phase exploitation reports from DSTL FM (UK)

WTI Enablers

- Fused Intelligence
- AOI Validation and briefings for local CC's and Units
- UDOP pics and finalized Intel products for dissemination and planning purposes

C-JTF (Troy/Paladin)

- Fused Intelligence
- AOI Validation and briefings for local CC's and Units
- UDOP pics and finalized Intel products for dissemination and planning purposes

CITP

- In-depth analysis of AOI's and targets in area
- Validation of TTP's
- ECM loadsets
- Localized Briefings and training
- First Look Reports

NGIC FUSION CELL

- AOI's
- JPEL List
- PIR's

REPORTING TO HIGHER

- ACME Weekly report
- ACME quick looks
- BOLO's
- TEX Quick Looks
- COIC Returns
- IIR's
- SDR's

INFORMATION FROM HIGHER

TEDAC
- Forensic Intel Action Reports
- Device Technical Notes
- CEAU EE Reports
- IIR's/Bulletins

NAVEODTECHDIV
- JDIGS/JEODNET

NGIC
- BIARS
- Target packages
- Pattern Analysis
- Fused Threat Analysis
- Device Specific reports
- Interrogation guidance

COIC
- RFS Return
- UDOPS

to EOD BN — to Labs — to WTI Enablers — to C-JTF (Troy/Paladin) — to CITP — 3rd PHASE RPTING

CHAPTER 6
Level 3 (Strategic) Exploitation and Analysis

6.1 General Description

The primary function of Level 3 (strategic) is to further exploit recovered materials and create associations between events, individuals, and weapons. Through additional exploitation of materials and identification and analysis of these associations, Level 3 further enables attack of adversary networks and WTI's critical outcomes of FP, material sourcing, targeting, support to prosecution, and signature characterization. This level of exploitation engages the full spectrum of advanced techniques, equipment, and scientific capabilities to fully understand the nature of the threat by providing in-depth technical, forensic, and intelligence analysis. Level 3 facilities are primarily located in CONUS or with allied or partner nations and provide reach back support to deployed organizations and agencies. Multiple DoD organizations, LE agencies, and intelligence organizations provide Level 3 capabilities that help link WTI and related intelligence drawn from tactical through strategic exploitation processes. From full spectrum exploitation of improvised weapons through the production of finished intelligence products, Level 3 provides specialized, synchronized support to inform strategic decisions.

6.2 Objectives

Level 3 organizations provide precise WTI exploitation and analysis for commanders, interagency partners, material developers, and national level policy makers. With interagency and international participation, Level 3 works towards countering the asymmetric threat by maintaining an understanding of the global improvised weapon. National policymakers use strategic-level WTI in support of national strategy and international policy development. Level 3 supports tactical and operational commanders by providing critical input to aid targeting, material sourcing, and TTP identification throughout the adversary network. Those targeted include material providers and financial supporters, distribution systems, fabricators, and networks worldwide that are linked to those in theater. S&T and research, development, test, and evaluation (RDT&E) stakeholders use Level 3 information to assist the development of material and nonmaterial solutions such as countermeasures and FP measures.

6.3 Capabilities

Capabilities employed at Level 3 facilities include the technical and forensic modalities described in the previous chapter, as well as those more sophisticated capabilities that are impractical or infeasible to deploy OCONUS. These capabilities may include sanitized facilities for exploitation to international scientific standards, or the provision of specialists certified in scientific fields to focus on discrete challenges. Level 3 capabilities involve established laboratory processes, procedures, and state-of-the-art equipment to provide in-depth analysis of the full range of technical, forensic, and biometric functions while incorporating strategic intelligence analysis capabilities and processes.

Afghanistan and Pakistan (AFPAK) 2011 Exploitation

In late 2011, as part of EOD operations in Afghanistan, a cache of improvised antipersonnel devices, AFPAK 2011, were recovered and forwarded to the CEXC in theater for Level 2 exploitation. Forensic processes at CEXC identified manufactures' markings on the AFPAK 2011 and latent fingerprints linking this cache to other IED incidents. The manufactures' markings, at this point, were unintelligible, and a subsample of the mine components was forwarded to the TEDAC for Level 3 exploitation. TEDAC, with support from Headquarters Department of the Army, further exploited the components using various forensic disciplines available at TEDAC and the FBI Laboratory, including latent prints, forensic imaging, questioned documents, tool marks, and chemistry. At the same time, EOD assets in theater, along with CJTF Paladin and NSWC IHEODTD, were working together to identify AFPAK 2011 components, mine nomenclature, and potential RSPs. The information obtained from the analytical practices at TEDAC was forwarded to the NMEC for further examination. This exploitation process was completed in less than 3 months and resulted in information leading to the identification of the source for mine components production. Additionally, Level 3 exploitation promoted additional Level 4 exploitation by research scientists at the US Military Academy (USMA) and encouraged the development/production of specification-grade AFPAK 2011 surrogates by Picatinny Arsenal for post-blast analysis by the G-38 ACES Division and the FBI's Explosive Unit. The information that was gained from these exploitative processes was shared within the IC, with other government agencies and entities, and used for Level V interdiction.

AFPAK 2011 is just one example of how interagency collaborative exploitative efforts are used to affect decisions made by leaders in forward environments. The information exchange and partnership does not stop with information derived from the various levels of exploitation that can be used to influence coalition forces' future adaptations in response to enemy TTPs. In the case of the AFPAK 2011, the information obtained from all levels of operations propelled R&D, affected enemy targeting, initiated surrogate production for training aids, influenced explosive testing/post-blast analysis, and set in motion the start of physical testing for the development of new equipment. The exploitative process starts with personnel on the battlefield, and ends by benefiting personnel on the battlefield.

6.4 Enablers

6.4.1 Terrorist Explosive Device Analytical Center (TEDAC)

TEDAC was formally established in 2004 to serve as the single interagency organization to receive, fully analyze, exploit, and provide a repository for all terrorist IEDs of interest to the United States. TEDAC coordinates efforts of the entire government, including LE, intelligence, and military, to gather and share intelligence about these devices — helping to disarm and disrupt IEDs, link them to their makers, and most importantly, prevent future attacks. To date, TEDAC has received tens of thousands of IED submissions, primarily from Iraq and Afghanistan.

TEDAC consists of a director (FBI), a deputy director (Bureau of Alcohol, Tobacco, Firearms, and Explosives [ATF]), a DoD executive manager (JIEDDO), and supporting units relating to forensics, technical exploitation, intelligence, and investigations. TEDAC includes representatives from DoJ, DoD, international partner agencies, and members of the IC. TEDAC is currently located at the FBI Laboratory in Quantico, VA.

TEDAC provides direct support to broader US government efforts to prevent and mitigate IED attacks by performing advanced exploitation of IEDs through physical examination, resulting in scientific and technical information and valuable intelligence. Through its integration of intelligence resources, TEDAC also provides expeditious reporting of raw and finished intelligence to intelligence and LE partners about device attributes and terrorist TTP to enhance knowledge and understanding of current and future threats.

TEDAC's continued success relies on a whole-of-government approach to addressing the IED threat.[145] By serving as a collaborative, multiagency, single-point advanced IED analytical center, TEDAC is able to identify actionable intelligence, make associations between devices, and communicate findings to a broad customer base of state and local LE, US military, the IC, and partner nations. Through its demonstrated capacity to disseminate raw intelligence, TEDAC serves a key role in broader FBI efforts to acquire, analyze, act on, and share terrorist-related information.

6.4.2 National Ground Intelligence Center (NGIC)

NGIC is the Army Service Intelligence Center, and the DoD lead[146] responsible for conducting in-depth analysis of foreign ground forces, including foreign infantry; insurgent organizations; armor; artillery; logistics; combat support systems; mine/countermeasure; Command, Control, Communications, Computers, and Intelligence; military related research; development, testing, and evaluation; technologies proliferation. It is also responsible for analysis of characteristics and performance of foreign ground force and weapons systems, including IEDs, ground based combat and combat support systems, rotary wing combat and combat support systems; and certain functional areas of biological and chemical weapons systems, emerging and disruptive technologies, and ground forces/weapons denial and deception capabilities. NGIC is the Lead Integrator in the DoD for intelligence analysis of Counterinsurgency Operations (COIN),[147] leads the Identity Intelligence (I2) Tradecraft Working Group for the Service of Common Concern for

[145] Obama, *Countering Improvised Explosive Devices.*

[146] (FOUO) Defense Intelligence Analysis Program, *Management Guidance (Assigned Analytic Subtopics)*, DoD FM/A, August 2011.

[147] (FOUO) Defense Intelligence Analysis Program, *Management Guidance (Key Enterprise Roles)*, DoD FM/A, August 2011.

I2 in the IC, and is assigned as the Manager for the DoD BEWL by the Mission Manager for I2 in the DoD.[148] Under these authorities, NGIC provides analysis of a full range of weapons components, devices, and their related networks. This includes partnering with DoD weapons and WTI communities in testing and evaluation (as Manager of the Army Foreign Material Program), as well as partnering with the forensic and biometric communities to enable matching or to conduct post-match all-source I2 analysis.

NGIC's primary customers for WTI analysis are tactical level US, partner nations, coalition conventional forces, and SOF. WTI analysts are embedded in Level 1 and Level 2 exploitation facilities, with reach back capability resident in Charlottesville, VA, and are an integral part of NGIC's Counter Insurgency Targeting Program (CITP). I2 analysts are embedded[149] within conventional and SOF forces, detention facilities, Level 2 exploitation facilities, and headquarters elements. WTI-related functions within NGIC focused on supporting the warfighter include:

- CITP
- IED/Mines Branch
- CIAD
- DOMEX
- I2 Program
- Foreign Material Program

6.4.2.1 Counter Insurgency Targeting Program (CITP)

The CITP supports targeting, interrogation, and prosecution of insurgents and their networks through the analysis and integration of IED device profiles, insurgent and insurgent network profiles, biometric and other forensic matches, and traditional all-source analysis. CITP leverages FEI, BEI, and I2 activities with the intent of creating technical link pattern and trend analysis for specific individuals and enemy groups. CITP is located at NGIC in Charlottesville, VA, where personnel work closely with NGIC's C-IED and IrW initiatives, including CIAD, I2 Program, IED Branch, DOMEX, and Quiet Storm. CITP consists of two sections with two types of analysts: the WTI analysis team (IED network cell SMEs) and the network analysis team (personality network SMEs). They work together to integrate information from exploited improvised weapons with traditional all-source analysis for all levels of WTI output.

6.4.2.2 NGIC IED/Mines Branch

Members of NGIC IED/Mines Branch determine the extent to which an IED or IED component impacts current and future joint force operations. The branch analyzes munitions technologies to understand how a device functions; determine its effectiveness, likely TTP for its employment,

[148] General Defense Intelligence Program Memo, *BEWL transfer, GDIP Program Manager/ DIA Director*, June 27 2012.

[149] USFOR-A CJ3 BMO, MEMO, *Requirements for AFG Theater Biometrics and Forensic Support Operations*, March 26, 2006.

and how it might be used to defeat existing C-IED technology; and forecast its evolution. Branch products go directly to the warfighter, C-IED developers, and other C-IED organizations. NGIC experts collaborate with those in the CITP and IrW divisions within NGIC.

6.4.2.3 Combat Incident Analysis Division (CIAD)

CIAD is the Army's Center of Excellence for battlefield vehicle forensics, attack scene investigation, and threat to vehicles. Its personnel investigate and analyze attacks by enemy conventional and insurgent forces on armored and non-armored vehicles worldwide. CIAD is regionally focused on areas where US forces are engaged in active combat operations, countries considered potential locations for future US forces involvement (within the next 5 years), and other countries considered to be of special interest. The CIAD maintains the Anti-Armor Incident Database for recording, comparing, and analyzing attacks against armored and nonarmored vehicles in these locations **(Figure 6-1)**. CIAD uses WTI-derived intelligence to identify trends in adversary capabilities development, manufacturing, procurement, and proliferation of anti-armor weapons and TTP.

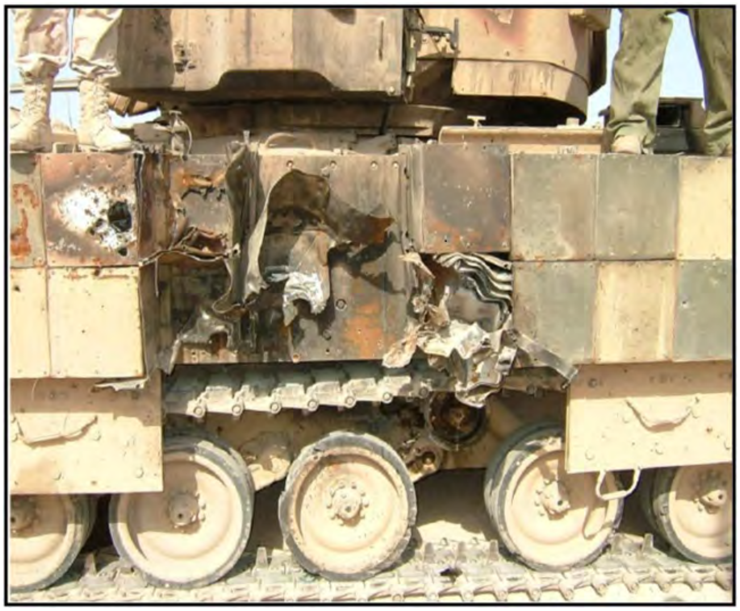


Figure 6-1. Battle Damaged Bradley Fighting Vehicle *(Photo Credit: NGIC CIAD)*

6.4.2.4 NGIC Army DOMEX Program

NGIC is the proponent of the Army's DOMEX program which supports the development of DOMEX capability and enables production of actionable and targetable intelligence responsive to information requirements of forces engaged in operations. Through the collection and analysis of best practices across the community, the Army's DOMEX program develops standardized procedures for collection, processing, and analysis of foreign documents and media, as well as developing and providing training using these standardized procedures. The Army's DOMEX program conducts training at NGIC, through mobile training teams at unit locations, and at the combat training centers (CTCs) to prepare Army elements to conduct DOMEX operations. The Harmony program, also at NGIC, provides the centralized IC repository for storage and dissemination of DOMEX materials and associated reporting through the Harmony database.

6.4.2.5 NGIC I2 Program

NGIC's Identity Intelligence program produces integrated all-source I2 in support of NGIC's Title 10 and Title 50 responsibilities. The NGIC I2 program also assesses foreign biometric capabilities, proliferates I2 tradecraft, manages the DoD BEWL, and sustains enterprise-wide analysis enabling tools and data management services to deny anonymity to our nation's adversaries. I2 functional areas and capabilities that enable the WTI process include:

- Post-Biometric Match All-Source I2 Analysis - NGIC's I2 conduct post-biometric match all-source identity intelligence analysis related to latent fingerprints and DNA.150
- I2 Fusion - NGIC's I2 Counterinsurgency Team provides reach back I2 support and assists driving theater operations and biometric collections by established relationships with deployed forces/commands through embedded I2 SMEs.
- Facial Search and Analysis - The NGIC I2 Facial Search and Analysis Team brokers image-based RFIs from deployed customers to the organization best able to affect the match.
- BEWL -The BEWL is used to identify POI at the point of biometric enrollment for DoD elements worldwide by fusing POI biometric data with all-source intelligence, and sharing DoD BEWL information with interagency and authorized partner nations.
- I2 Analysis - I2 results from the fusion of identity attributes (e.g., biologic, biographic, behavioral, and reputational information related to individuals) and other information and intelligence associated with those attributes collected across all intelligence disciplines. I2 operations combine the synchronized application of biometrics, forensics, and DOMEX capabilities with intelligence and identity management processes to establish identity, affiliations, and authorizations in order to deny anonymity to the adversary and protect US/partner nation assets, facilities, and forces. The I2 operations process results in discovery of true identities; links identities to events, locations, and networks; and reveals hostile intent.
- Enterprise-Wide Analysis Enabling Tools151 - NGIC manages/sustains the BI2R , an automated system that ingests biometrically-related intelligence data into its repository. The BI2R provides positive identification and tracking of individuals' data for intelligence products.

[150] DIA Message, *Defense Joint Operations Center(DJIOC) Support to JIEDDO DTG 230612ZMay06*, DIA Director, May 23, 2006.

[151] MEMO Through DA-G2 for CG INSCOM, *INSCOM Roles with Regard to BEI and Analysis Tools Supporting the DoD Biometrics Executive Agent*, DA Deputy Chief of Staff (G-3/5/7), May 2, 2007.

6.4.2.6 NGIC Army Foreign Material Program

NGIC manages the Foreign Material program for the Army, providing highly technical assessment of equipment and technologies in support of operational commanders, national decision makers, and force and material developers.

6.4.3 JIEDDO Counter-IED Operations/Intelligence Integration Center (COIC)

In support of all geographic CCMDs, the COIC harnesses, masses, and fuses information analysis, technology, interagency collaboration, and training support to enable more precise attacks to defeat networks that employ IEDs. The COIC provides analytical support and enemy network information to other USG organizations and multinational partners.

The COIC integrates and analyzes information from multiple intelligence databases and fuses it into products that answer a strategic, operational, and tactical commander’s request for support (RFS). COIC answers RFS directly from joint and Service members to alleviate hours of organizational intelligence staff work. The COIC maintains a federated architecture, which leverages the expertise from the IC, national laboratories, and academia. Products forwarded from COIC include comprehensive persistent views of networks employing IEDs; pattern analysis; geospatial analysis; network dynamics analysis; social network analysis; complex adaptive systems analysis; and products that support targeting packages. All focus on defining and enabling the commander to have more lethal and nonlethal effects on networks that employ IEDs.

6.4.4 Naval Surface Warfare Center Carderock Division’s (NSWCCD’s), Survivability and Weapons Effects Department

NSWCCD’s Survivability and Weapons Effects department, located in Carderock, MD, investigates and analyzes the effects of weapons attacks on military and commercial vessels, aircraft, and transportation conveyances worldwide. The information derived from their analysis of structural damage, coupled with other exploitation processes such as post-blast analysis and technical and forensic exploitation, provides a comprehensive picture of the event and supports attribution of the event to state or non-state actors.

6.4.5 Naval Surface Warfare Center Indian Head Explosive Ordnance Disposal Technology Division (NSWC IHEODTD)

NSWC IHEODTD’s mission is to provide research, development, engineering, manufacturing, test, evaluation, and in-service support of energetic and energetic materials (e.g., chemicals, propellants, and explosives) for ordnance, warheads, propulsion systems, pyrotechnic devices, fusing, electronic devices, cartridge actuated and propellant actuated devices, packaging, handling, storage, transportation, gun systems, and special weapons for Navy, joint forces, and the nation. NSWC IHEODTD develops and delivers EOD technology, knowledge, tools, and equipment and their life cycle support through an expeditionary workforce that meets the needs of the DoD, CCDRs, and our foreign and interagency partners. NSWC IHEODTD is assigned as the Executive Manager for EOD technology and training and executes other responsibilities as assigned by the Commander, NSWC.

The NSWC IHEODTD core joint Service EOD technology functions include:

- Develop EOD procedures to counter threat munitions, IEDs, and other adversary weaponry

- Develop tools and equipment to meet EOD operational needs
- Perform in-the-field engineering expertise for EOD tools and equipment
- Provide depot level management and repair for EOD tools and equipment

Some of the other IHEODTD programs that support the WTI process are:

6.4.5.1 Explosive Detection Equipment (EDE) Program

IHEODTD is the DoD's EDE RDT&E program for antiterrorism and security applications. The EDE program develops equipment that effectively and economically finds energetic materials, precursors, IEDs, and/or IED components, and provides RDT&E, technical support, and sustainment for EDE.

6.4.5.2 Hemlock Electronic Forensics Program

Hemlock is a cyber C-IED program that conducts electronic forensics on IEDs in support of US and allied EOD and intelligence communities in partnership with NSWC IHEODTD, Naval Cyber Warfare Development Group, Naval Research Lab, and NCIS. Hemlock collects, reverse engineers, and exploits IED software, firmware, and hardware designs. It produces and maintains electronic forensic hardware and software tools that are used by the IED exploitation and the IC to enable them to AtN, DtD, and TtF.

6.4.5.3 NSWC IHEODTD Research Department

Investigates a broad spectrum of research areas focusing on the C-IED mission. It performs advanced chemical exploitation and analysis of energetic materials to provide technical assessments that can be used to reverse engineer a material composition, a likely method of preparation, or intended use. The department's capabilities include the development of laboratory, field, and pilot-scale preparation of HME threat materials and theater-relevant formulations. Explosive performance is evaluated in laboratory grade indoor testing facilities and at field detonation ranges. Detonation testing is conducted to study terminal effects of known and predicted HME threats to understand the potential of the threats and inform the warfighter. Teams provide training on HME production methods using authentic or surrogate materials. They provide chemical exploitation methodologies and define chemical signatures/observables for use at tactical, operational, and strategic levels. The Research Department works in partnership with the IC to anticipate warfighter requirements and future threats.

6.4.6 Joint IED Defeat Organization (JIEDDO)

JIEDDO leads all DoD actions to rapidly provide C-IED capabilities in support of the CCDRs and to enable the defeat of the IED as a weapon of strategic influence. JIEDDO leverages other agencies' information and intelligence through information sharing, exchange of liaison personnel, and participation in working groups, boards and senior leader engagements. JIEDDO leads an effective C-IED effort, which provides specific and integrated capabilities that address threat networks and devices. In a partnership with DIA, JIEDDO provides oversight of WTI activities to provide the ability to collect and exploit information from individuals, IEDs, and components to understand threat networks, IEDs, and components. By providing a whole-of-government approach, JIEDDO is developing future capabilities that must be scalable, affordable, adaptable, and expeditionary. These capabilities should be capable of being employed in a domestic environment.

6.4.7 United Kingdom Defence Exploitation Facility (UK DEF)

Founded in 2009, UK DEF is a relatively new capability. Its current focus is almost exclusively to provide exploitation support to ongoing operations in Afghanistan. In line with the current UK Ministry of Defence (MoD) concept of employment for exploitation, items identified for materiel and personnel exploitation (MPE) recovered within UK areas of operation in Afghanistan are returned to the UK DEF for Level 3 exploitation.

The receipt, movement, and reporting of exploitation materiel within the UK DEF is managed by the Exploitation Coordination, Liaison, and Triage team. UK DEF technical teams conduct detailed MPE in four major categories: forensics and biometrics (including biometric data management), technical exploitation, seized media analysis, and chemical exploitation. A dedicated analytical capability, to fuse outputs from these four technical areas, is provided by the Multi-Source Fusion and Analysis team.

Supporting the UK DEF (and for capability planning purposes considered a core part of the UK DEF), the Technical Threat Exploitation Fusion and Analysis Cell provides a vital function in bridging the technical exploitation community and the individual research and equipment capabilities they support. Ingesting the outputs of detailed technical and multi-source analysis from reported CT threats globally, it provides further analysis of the impacts of identified and tested threats on existing and planned UK MoD capabilities.

6.4.8 Other Level 3 Supporting Entities

Level 3 support agencies and department capabilities provide access to personnel with specialized expertise, unique collection capabilities, and specialized equipment from a variety of US and allied government agencies, departments, and academic facilities. The following is a representative list of supporting entities that might be tasked to support WTI missions:

- Coalition armed forces and national police
- ATF
- Central Intelligence Agency (CIA)
- U.S. Drug Enforcement Agency (DEA)
- Department of Commerce
- Department of Homeland Security
- DoJ
- DoS
- Department of Treasury
- FBI
- US National Security Agency (NSA)
- US university departments

- Federally Funded Research and Development Centers (FFRDC) (e.g., RAND Corp, CNA, etc.)
- US DoD agencies and departments

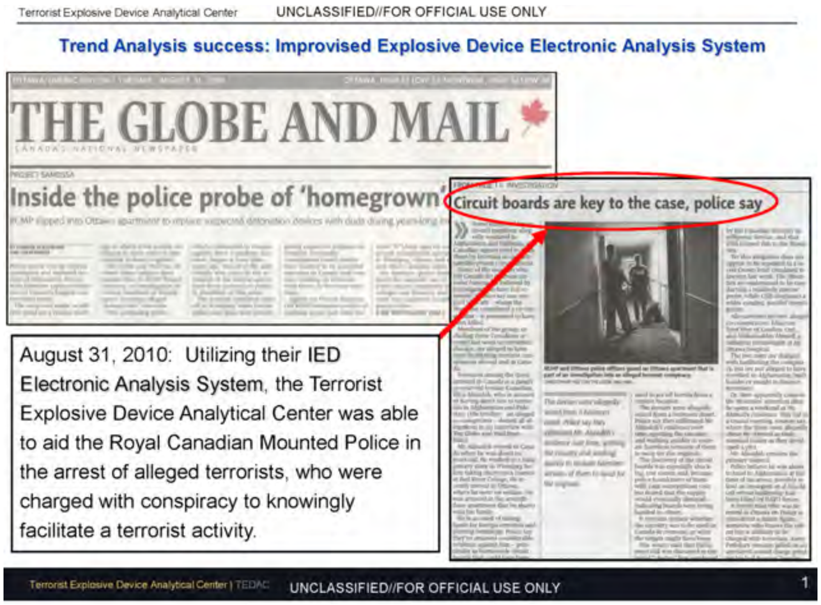
6.5 Outputs

- Identify trends, assembler patterns, and profiles from materials received; determine circumstances behind threat employment of weapons systems
- Detect threat improvements or first-seen weapons systems
- Determine the nature of and map threat networks and identify supporting organizations that provide funding, equipment, and training
- Conduct chemical analysis of explosive and enhancement material
- Conduct biometric and DNA analysis
- Forward material and related data to or from Level 3 facilities to HN military and LE personnel, as directed, in support of prosecution
- Provide advanced firearm and tool mark exploitation
- Collect and analyze trace materials from items forwarded from Levels 1 or 2
- Provide advanced video and photographic collection and analysis
- Support advanced human remains identification beyond Level 2 capabilities
- Provide advanced forensics chemistry analysis
- Physically measure all material as received
- Identify enemy employment TTP
- In support of the entire community, from every device, provide standard data from the collection, analysis, profiling, and reporting of electronic frequency measurements and the operation of electronic circuits in a nonintrusive manner
- Collect weapons system integrated circuit component information, circuit design, and operating details to pass to Level 4 for detailed analysis
- Analyze information in ORSA’s database
- Perform all-source intelligence data fusion
- Gather information and intelligence useful for training allied and HN forces to deal effectively with asymmetric network threats
- Gather TTP and recommendations to mitigate the effects of specific weapons of concern
- Provide all-source intelligence data fusion and reporting in support of AtN within an area of operations and worldwide

- Degrade key terrorist standing with followers and potential recruits on a worldwide basis
- Deny communications and movement within network cells
- Protect US communications and movement within and outside an AOR
- Attack network safe havens
- Provide HN rule of law
- Detect and inhibit IED funding sources

The majority of Level 3 outputs are in the form of reports. Level 3 processes include products supporting the following outputs or activities:

- Advanced technical, forensic, and intelligence exploitation of devices, components, and improvised weapons beyond Level 2 capabilities
- Provision of a worldwide view of adversary weapons systems manufacturing, processing, and component sourcing
- Intelligence regarding in-depth global associations between collected and forensically-examined materials over an extended period of time to support future military, LE, and other civil activities
- Maintain a historical repository of exploited material for use in higher levels of exploitation
- Provide a searchable database of this material that allows tracking of case files
- Provide detailed reverse engineering of improvised weapons and components for the identification of new threats and vulnerabilities
- Process, translate, analyze, and disseminate data and electronic data recovery from electronic media (e.g., hard drives, flash drives, videos)
- Signaling duration for electronic events and means of functioning, arming, and firing sequences and related codes for FP
- Construction characteristics to support trend analysis to enable individual and network targeting (**Figure 6-2**)
- Identification of new capabilities, adaptations, or other evolutions for FP
- Sources of components for component and material sourcing



Terrorist Explosive Device Analytical Center UNCLASSIFIED//FOR OFFICIAL USE ONLY

Trend Analysis success: Improvised Explosive Device Electronic Analysis System

THE GLOBE AND MAIL

CANADA'S NATIONAL NEWSPAPER

PROJECT SAMOSSA

Inside the police probe of 'homegrown'

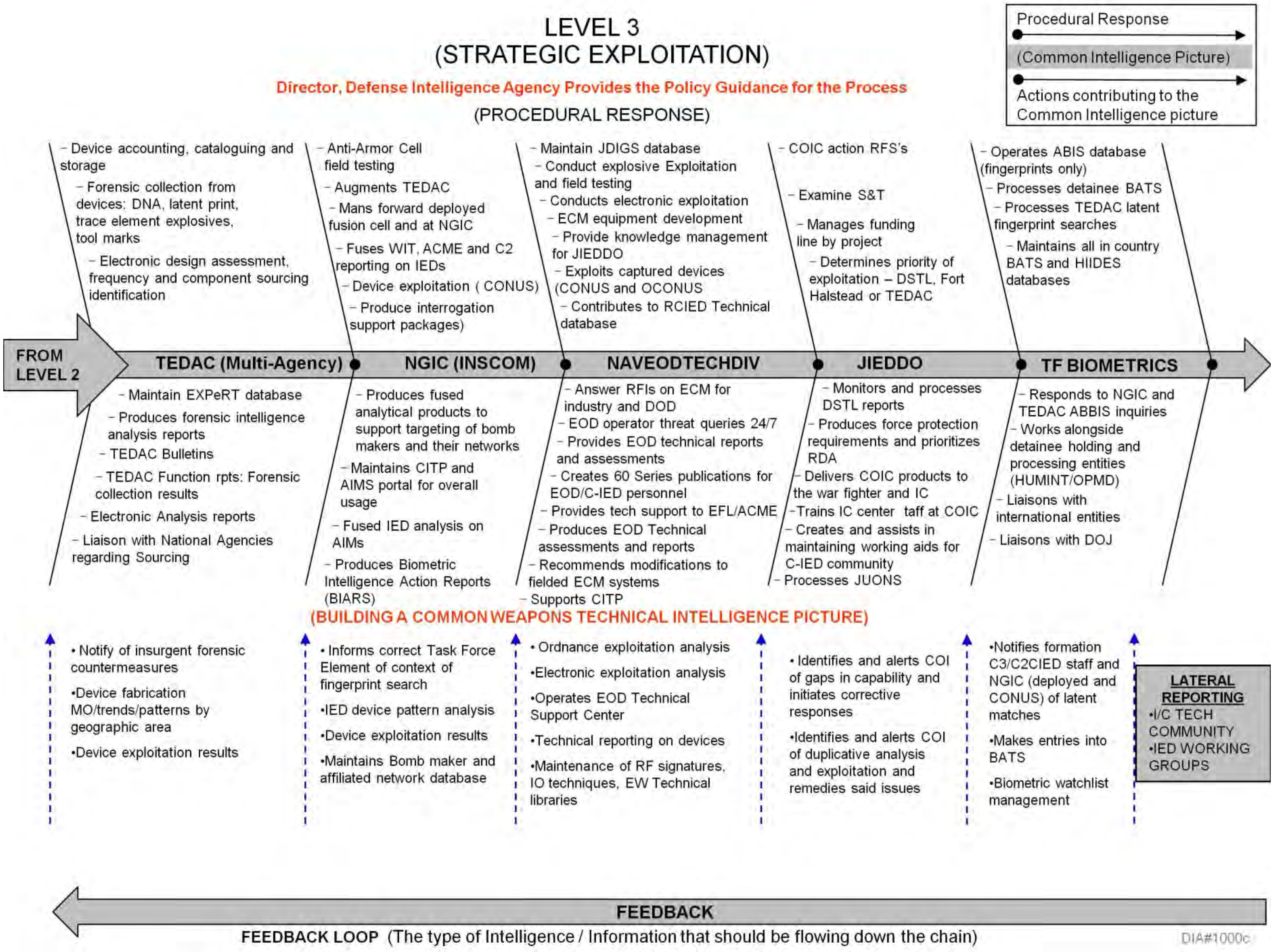
RCMP slipped into Ottawa apartment to replace suspected detonation devices with duds during year-long in

Circuit boards are key to the case, police say

August 31, 2010: Utilizing their IED Electronic Analysis System, the Terrorist Explosive Device Analytical Center was able to aid the Royal Canadian Mounted Police in the arrest of alleged terrorists, who were charged with conspiracy to knowingly facilitate a terrorist activity.

Terrorist Explosive Device Analytical Center | TEDAC UNCLASSIFIED//FOR OFFICIAL USE ONLY 1

Figure 6-2. Example of Construction Materials and Characteristics Used to Identify and Target Individuals and Networks *(Photo Credit: TEDAC)*



LEVEL 3
(STRATEGIC EXPLOITATION)

Director, Defense Intelligence Agency Provides the Policy Guidance for the Process

(PROCEDURAL RESPONSE)

Procedural Response

(Common Intelligence Picture)

Actions contributing to the Common Intelligence picture

FROM LEVEL 2

TEDAC (Multi-Agency)

- Device accounting, cataloguing and storage
- Forensic collection from devices: DNA, latent print, trace element explosives, tool marks
- Electronic design assessment, frequency and component sourcing identification
- Maintain EXPeRT database
- Produces forensic intelligence analysis reports
- TEDAC Bulletins
- TEDAC Function rpts: Forensic collection results
- Electronic Analysis reports
- Liaison with National Agencies regarding Sourcing

NGIC (INSCOM)

- Anti-Armor Cell field testing
- Augments TEDAC
- Mans forward deployed fusion cell and at NGIC
- Fuses WIT, ACME and C2 reporting on IEDs
- Device exploitation (CONUS)
- Produce interrogation support packages)
- Produces fused analytical products to support targeting of bomb makers and their networks
- Maintains CITP and AIMS portal for overall usage
- Fused IED analysis on AIMs
- Produces Biometric Intelligence Action Reports (BIARS)

NAVEODTECHDIV

- Maintain JDIGS database
- Conduct explosive Exploitation and field testing
- Conducts electronic exploitation
- ECM equipment development
- Provide knowledge management for JIEDDO
- Exploits captured devices (CONUS and OCONUS
- Contributes to RCIED Technical database
- Answer RFIs on ECM for industry and DOD
- EOD operator threat queries 24/7
- Provides EOD technical reports and assessments
- Creates 60 Series publications for EOD/C-IED personnel
- Provides tech support to EFL/ACME
- Produces EOD Technical assessments and reports
- Recommends modifications to fielded ECM systems
- Supports CITP

JIEDDO

- COIC action RFS's
- Examine S&T
- Manages funding line by project
- Determines priority of exploitation – DSTL, Fort Halstead or TEDAC
- Monitors and processes DSTL reports
- Produces force protection requirements and prioritizes RDA
- Delivers COIC products to the war fighter and IC
- Trains IC center taff at COIC
- Creates and assists in maintaining working aids for C-IED community
- Processes JUONS

TF BIOMETRICS

- Operates ABIS database (fingerprints only)
- Processes detainee BATS
- Processes TEDAC latent fingerprint searches
- Maintains all in country BATS and HIIDES databases
- Responds to NGIC and TEDAC ABBIS inquiries
- Works alongside detainee holding and processing entities (HUMINT/OPMD)
- Liaisons with international entities
- Liaisons with DOJ

(BUILDING A COMMON WEAPONS TECHNICAL INTELLIGENCE PICTURE)

- Notify of insurgent forensic countermeasures
- Device fabrication MO/trends/patterns by geographic area
- Device exploitation results

- Informs correct Task Force Element of context of fingerprint search
- IED device pattern analysis
- Device exploitation results
- Maintains Bomb maker and affiliated network database

- Ordnance exploitation analysis
- Electronic exploitation analysis
- Operates EOD Technical Support Center
- Technical reporting on devices
- Maintenance of RF signatures, IO techniques, EW Technical libraries

- Identifies and alerts COI of gaps in capability and initiates corrective responses
- Identifies and alerts COI of duplicative analysis and exploitation and remedies said issues

- Notifies formation C3/C2CIED staff and NGIC (deployed and CONUS) of latent matches
- Makes entries into BATS
- Biometric watchlist management

LATERAL REPORTING

- I/C TECH COMMUNITY
- IED WORKING GROUPS

FEEDBACK

FEEDBACK LOOP (The type of Intelligence / Information that should be flowing down the chain)

CHAPTER 7
Level 4 (National) Exploitation and Analysis

7.1 General Description

Level 4 combines collection, exploitation, analysis, and reporting with national policy direction, planning, and support. National exploitation focuses on very specific technology and intelligence problem sets that concern national security. This level of exploitation involves the synthesis of multidisciplinary scientific, forensic, financial, and commercial intelligence information that exceeds the capabilities and time constraints inherent at Levels 1, 2, or 3. The primary intended outcomes of Level 4 exploitation are the development of intelligence collection technologies, improved FP, and the creation of training materials to defeat the improvised threat worldwide. These outcomes are provided to stakeholders at the lower levels of the WTI community to further their analysis on a short-turn time frame or on a long-term basis.

National exploitation involves the coordinated efforts of various US government-sponsored labs, DoD and private industry R&D labs, and universities to investigate specific items of interest across a range of scientific specialties. The range of skill sets for Level 4 include doctorate level engineering research, in addition to the use of advanced testing instruments, test ranges, and electronic test chambers that are capable of in-depth research on a broad range of complex problems associated with improvised weapon technology. Level 4 exploitation solicits federal sponsorship and support from US government and allied agencies and departments to provide the most detailed reporting possible on current and projected threat technologies. Additionally, various DoD test ranges work collectively to evaluate reported findings and provide feedback prior to production and deployment of materiel solutions used to mitigate IEDs.

Follow-on actions resulting from Level 4 exploitation and analysis are used to target specific threat weapon system and/or those personnel who manufacture or employ them. Level 4 outputs include reporting on the specific functions of a device, the device's perceived use, and the development and sophistication of the networks using the device and/or its components. Level 4 analyses seek to confirm or identify the source of the improvised weapon or its components, to support targeting, HN LE initiatives, or other actions that quell the flow of materials.

7.2 Objectives

Level 4 exploitation addresses the information needs of commanders, national policy makers, and other strategic decision makers in a scientific manner. These efforts support the development, fielding, and sustainment of advanced technologies to DtD, AtN and TtF, which include:

- Technical forensic exploitation of recovered materiel and information to support AtN efforts
- WTI support of tactical, strategic, and national operations
- Techniques development and countermeasure support
- Collection of device data for testing and prototyping
- Global IED trend analysis
- Predictive global IED technology and TTP analysis

- Technical RFI response
- Gap analysis
- Prioritization of threats for countermeasure and collection asset development
- Standardized technical data and analytical reports to support global C-IED requirements
- High fidelity replication of threat devices to support testing and development
- Signals analysis support to command, control, communication, and computers, intelligence, surveillance, and reconnaissance (C4ISR) development and testing
- Testing and development of material countermeasures solutions
- Support to "supply chain defeat" analysis for follow-on actions

7.3 Focus Areas

Level 4 organizations focus on specific problem sets that require advanced analytical and scientific capabilities. These in-depth research and analytical capabilities are tailored to address each specific problem set. These problem sets necessitate a collaborative pursuit involving experts across national engineering, intelligence, and academic pursuits. Analysts from Level 4 organizations often collaborate with allied nations and international organization counterparts to resolve complex areas of mutual concern. Focus areas at the national level that have emerged since OIF and OEF include:

7.3.1 Electronic Exploitation

Level 4 electronic exploitation focuses on thorough and, in most cases, invasive, special purpose electronic exploitation of threat materials identified in Level 3 as a new device or as a device with an anomaly. From the exploitation of a threat circuit and its RF transmission or reception capabilities, to the specifics of its signaling and data structure, this level of effort supports the needs of the reverse engineering and replication, test and evaluation, and materiel development communities. High fidelity data gleaned through Level 4 exploitation enables the development and enhancement of strategic and tactical FP systems.

Level 4 electronic exploitation seeks to determine the following regarding threat materials entering WTI investigation that have one or more electronic components:

- Means of functioning
- Signaling duration for electronic events
- Arming and firing sequences and related codes
- Identification of new capabilities, adaptations, or other evolutions
- Sources of components
- Construction characteristics
- Construction techniques or processes

7.3.2 Terrorist and Insurgent Financing Exploitation

Threat finance efforts analyze and target organizations, cells, and individuals directly linked to terrorism. Terrorists use a quickly evolving series of TTP to transfer money throughout their networks, from sophisticated electronic bank transactions to low-tech/no-tech means such as couriers. From a strategic standpoint, threat finance efforts aim to “deny terrorists the resources they need to operate and survive.” WTI exploitation and analysis identifies key components that need to be sourced and, when tracked, provide linking data that assists in confirming where financing and purchases originate and end. Although actual currency is critical to global terrorist activities resources and must be denied and disrupted as funds travel from one set of hands to another, threat finance activities aim to disrupt or influence several other resources that are equally important to the adversary including:

- Capture/kill leadership
- Deny or disrupt access to geographic and virtual safe havens
- Deny communications and movement
- Deny access to WMD and weapons; counter asymmetric use of technologies
- Counter the proliferation of extremist ideology
- Protect potential US and allied targets
- Delegitimize extremism.

7.3.3 Signals Analysis

Level 4 analysis focuses on signals development, threat network analysis, threat technology trends, and commercial communication infrastructure. After a RC device has been recovered, advanced signals analysis discerns the remaining unique operational characteristics of the device. These characteristics include:

- Operating frequencies
- External modulation parameters
- Signal recognition and processing capabilities
- Protocol analysis
- Pulse duration and repetition intervals

Signals analysis is an important component of the WTI process and informs the design, modification, and optimization of C4ISR assets against an evolving global adversary. The signals analysis efforts applied to this threat are a collaborative venture of multiple community stakeholder agencies and labs.

7.3.4 Threat Replication

Technical data retrieved from Level 2 and 3 technical forensics laboratories is used to produce electro-mechanical threat device replicas. The T&E community uses these replica devices for

C4ISR system performance testing in destructive and nondestructive conditions. TECHINT/WTI data derived from a Technical Forensic Exploitation (TFE) asset ensures that the replica looks and functions like the actual device or improvised weapon, affording T&E and military EOD training elements an opportunity to fully interact with a known threat device, while preserving the integrity of the technical and biometric data from the original improvised weapon or component.

UNCLASSIFIED//FOUO

Technical Forensic Exploitation of an Emerging Threat

In 2007, Intelligence and Information Warfare Division (I2WD) received intelligence from another government agency that indicated the adversaries' intended nefarious use of mesh capable, frequency hopping spread spectrum, and COTS transceivers in IEDs. At the time of this reporting, these transceivers represented a dramatic improvement in the sophistication of switches used to initiate IEDs in Iraq. Reporting indicated that Middle Eastern front companies were purchasing these devices for use in IEDs. Given its observed association with EFPs and IRAMs, the device was of immediate strategic interest from a FP and collection standpoint.

I2WD acquired the transceiver in question and performed in-depth technical characterization of the device. This exploitation included reverse engineering and signals analysis, and resulted in development of algorithms for detection platforms. I2WD analysis also enabled development of EW systems and load sets to offer FP against the threat before it was used on the battlefield. The collaborative efforts of several agencies, leveraging national capabilities in a proactive manner, represented a paradigm shift in the fight against IEDs. The initiative proved the value of global IED supply chain monitoring and analysis, and the criticality of technical forensic exploitation as an enabler to C4ISR capabilities. I2WD's ability to relay this emerging threat's unique identifier to the responsible collection assets resulted in unparalleled insight into the threat's proliferation and incorporation into the IED supply chain. The subsequent detection and location of IED engineering and manufacturing facilities associated with this threat was a key victory in the effort to disrupt the global IED supply chain.

UNCLASSIFIED//FOUO

7.4 Enablers: Representative Organizations/Staffs That Conduct or Support the Level 4 WTI Process

Organizations performing Level 4 analyses possess significant technical expertise and include national level research laboratories and test ranges in addition to international collaboration. Because of the classification level of many of the Level 4 capabilities, the following organizations represent only a sampling of those that conduct or support Level 4 exploitation and analyses.

7.4.1 Intelligence and Information Warfare Division (I2WD)

I2WD is a part of US Army Communications Electronics Research and Engineering Center. Its mission is: "By identifying, developing, evaluating, tailoring and inserting emerging information technologies into operational systems, I2WD provides our warfighters effective intelligence and information warfare tools that equip America's warfighter with the superior integrated systems needed to ensure information dominance."[152] The I2WD TFE team conducts technical characterization and replication of globally collected threat material. As the sole DoD Level 4 electronic exploitation facility, I2WD TFE shepherds threat materials through reverse engineering, firmware, electromagnetic interference, antenna, RF signals analysis, and replication in support of T&E; countermeasure development; and R&D communities, all under the purview of its organic programs. TFE supports the WTI process by providing TECHINT analysis and research in support of C4ISR systems development and national IC architecture initiatives. I2WD intelligence staff members track the dissemination and development of adversary networks, threat materials, TTP, and technologies across the globe. I2WD also provides support to first responders (e.g., SABTs, ATF, SOF, and EOD), forward laboratories, DFSC, and TEDAC, in the form of SMEs electrical engineers and hardware solutions, such as the Advanced Aggregate Data Extraction tool, which was designed to provide a forward deployed, in-depth electronic technical forensic exploitation capability spanning Levels 2 through 4.

7.4.2 Global Threat Integration Program (GTIP)

The GTIP is a joint consortium of stakeholder organizations from across the operational, test, and R&D communities of interest. This group meets quarterly to exchange information on current and emerging trends in threat technology and TTP worldwide. This information and the briefings presented to the community at large support the development, modification, and optimization of C4ISR systems, capitalizing on the knowledge of each agency as it pertains to the five levels of WTI. This group is co chaired by I2WD and NGIC.

7.4.3 Defense Intelligence Agency (DIA)

DIA is first in all-source defense intelligence focused on preventing strategic surprise and delivering a decision advantage to warfighters, defense planners, and policymakers. DIA personnel deploy globally alongside warfighters and interagency partners to defend America's national security interests. The DIA is organized into three directorates and five regional centers. The Director DIA, on behalf of the Undersecretary of Defense for Intelligence (USD [I]), directs, monitors, and modifies WTI requirements and processes in coordination with JIEDDO to adapt to evolving circumstances and emerging threats associated with improvised weapons and IEDs. The following DIA offices have direct ties with the WTI community:

- Office of Collection and Exploitation
- Joint Material Program Office
- National MASINT Office
- NMEC

[152] US Army Research and Development and Engineering Command, Intelligence and Information Warfare Directorate, "Mission," as of December 5, 2013, http://ww.cerdec.army.mil/directorates/i2wd.asp

7.4.4 National Security Agency

"The National Security Agency is an element of the US intelligence community charged with collecting and reporting intelligence for foreign intelligence and counterintelligence purposes. NSA performs this mission by engaging in the collection of 'signals intelligence,' which quite literally, is the production of foreign intelligence through the collection, processing, and analysis of communications or other data, passed or accessible by radio, wire, or other electromagnetic means. Every intelligence activity NSA undertakes is necessarily constrained to these central foreign intelligence and counterintelligence purposes."[153] NSA has a symbiotic relationship with the WTI community and obtains from and provides to the WTI community classic SIGINT, dual tone multi-frequency, autonomic, and cell phone reports for technical fusion with other related data. NSA identifies foreign entities and develops networks with which they or their organizations belong. NSA also helps protect national security by providing policy makers and military commanders with the intelligence information needed to do their jobs.

7.4.5 Department of Justice (DoJ)

The DoJ enforces the law and defends the interests of the United States according to the law; to ensure public safety against threats foreign and domestic; to provide federal leadership in preventing and controlling crime; to seek just punishment for those guilty of unlawful behavior; and to ensure fair and impartial administration of justice for all Americans.[154] Within the DoJ there are 53 agencies, four of which have obvious ties to the WTI community, including:

7.4.5.1 Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF)

The mission of ATF is to conduct criminal investigations, regulate the firearms and explosives industries, and assist other law enforcement agencies. This work is undertaken to prevent terrorism, reduce violent crime, and protect the public in a manner that is faithful to the constitution and the laws of the United States.[155]

7.4.5.2 Federal Bureau of Investigation (FBI)

The FBI is an intelligence-driven and a threat-focused national security organization with both intelligence and LE responsibilities. The mission of the FBI is to protect and defend the United States against terrorist and foreign intelligence threats, to uphold and enforce the criminal laws of the United States, and to provide leadership and criminal justice services to federal, state, municipal, and international agencies and partners.[156] The DoD WTI community is connected to the FBI through its affiliation with TEDAC.

[153] National Security Agency Memo, *The National Security Agency: Missions, Authorities, Oversight and Partnerships*, August 9, 2013.

[154] Department of Justice, "About DOJ, Our Mission," as of December 5, 2013, http://www.justice.gov/about/about.html

[155] Department of Justice, "Departments of Justice Agencies, ATF," as of December 5, 2013, http://www.justice.gov/agencies/index-list.html#ATF

[156] Department of Justice, "Departments of Justice Agencies, FBI," as of December 5, 2013, http://www.justice.gov/agencies/index-list.html#FBI

7.4.5.3 International Criminal Police Organization (INTERPOL) Washington

INTERPOL facilitates the exchange of information to assist LE agencies in the United States and throughout the world in detecting and deterring international crime and terrorism through a network of 187 member countries. Each INTERPOL member country establishes a National Central Bureau (NCB) to serve as its liaison between the member country's LE agencies and INTERPOL. NCBs work with the police authorities in their countries to transmit, respond to, and execute RFIs and assistance in criminal investigations and police matters to and from other countries' NCBs via the INTERPOL communications network.

"The mission of INTERPOL Washington is to facilitate LE cooperation as the United States representative to INTERPOL on behalf of the Attorney General."157 WTI support has involved tracing vehicle registration numbers from various incidents to locate the vehicles' country of origin, identify route to the scene, and purchasing record.

7.4.5.4 Drug Enforcement Administration (DEA)

"The mission of the DEA is to enforce the controlled substances laws and regulations of the United States and to bring to the criminal and civil justice systems of the United States, or any other competent jurisdiction, those organizations, and principal members of organizations, involved in the growing, manufacture, or distribution of controlled substances appearing in or destined for illicit traffic in the United States; and to recommend and support non-enforcement programs aimed at reducing the availability of and demand for illicit controlled substances on the domestic front." [158] DEA supports WTI through identification and differentiation between processes and materials used in HME and drug production.

7.4.6 Department of Energy (DoE) National Laboratories and Technical Facilities

The US Department of Energy national laboratories and technology centers are a system of facilities and laboratories overseen by the DoE for the purpose of advancing science and technology. Together, the 17 DoE laboratories comprise a preeminent federal research system that provides the nation with strategic scientific and technological capabilities. The laboratories:[159]

- Execute long-term government scientific and technological missions, often with complex security, safety, project management, or other operational challenges
- Develop unique, often multidisciplinary, scientific capabilities beyond the scope of academic and industrial institutions, to benefit the nation's researchers and national strategic priorities
- Develop and sustain critical scientific and technical capabilities to which the government requires assured access

[157] Department of Justice, "Departments of Justice Agencies, INTERPOL Washington," as of December 5, 2013, http://www.justice.gov/interpol-washington/about.html

[158] Department of Justice, "Departments of Justice Agencies, DEA," as of December 5, 2013, http://www.justice.gov/agencies/index-list.html#DEA

[159] Department of Energy (DoE), "The Office of Science Laboratories," as of December 5, 2013, http://science.energy.gov/laboratories/

Of the 17 DoE national laboratories, 16 are administered, managed, operated, and staffed by private-sector organizations under management and operating contracts with DoE. The following establishments support WTI through in-depth exploitation and analysis.

- DoE National Laboratories:
- Sandia National Laboratories
- Los Alamos National Laboratory
- Lawrence Livermore National Laboratory
- Idaho National Laboratory
- Technical Facilities:
- Kansas City Plant

7.4.7 Research Laboratories and Federally Funded Research and Development Centers (FFRDCs)

Although DoD and academia research laboratories are not dedicated WTI entities or stakeholders, Level 4 exploitation relies on them to assist in answering some of the nation's most difficult R&D and FP questions. Some examples of these laboratories are:

- Army Research Laboratories
- Air Force Research Laboratories
- Navy Research Laboratories
- Johns Hopkins University
- FFRDCs (e.g., RAND Corp, CNA, etc.)

7.4.8 National Test Ranges

Level 4 exploitation efforts rely on the ability to verify their results and solutions at standardized testing facilities. These test ranges use Level 4 replication efforts to provide baseline threats for systems performance testing. The following are examples of such national test ranges:

- Yuma Proving Ground, AZ
- Dugway Proving Ground, UT
- China Lake Proving Ground, CA

7.5 Outputs

Level 4 exploitation processes provide customers with insight required to support improvements to FP, targeting, network engagement, battlefield forensic analysis, and exploitation. As new techniques are developed and fielded, dissemination of data and lessons learned to tactical, strategic, and national consumers is crucial to keep pace with the global weapons threat in the OE.

Modeling and simulation of RCIED threat systems and blue C4ISR systems support automated testing. The goal of this analysis is to simulate the improvised weapon/IED threat, and enhance performance of the C4ISR system under development. The replication of captured threat devices and prototyping of circuits and systems assist the efforts of the R&D and T&E communities whose areas of investigation include the following:

- Technology designed to reduce the effects of IED detonations
- Technology development disruption activities throughout the adversary network via enhanced intelligence collection, surveillance, reconnaissance, information operations, device technical and forensic exploitation, disposal of unexploded and captured ordnance, and persistent surveillance
- Training equipment and materials that include counters to new threat network weaponry, improved information management and dissemination technologies, and strategic communications
- Worldwide intelligence data fusion that links threat network weapons system component sourcing, design, and tracking
- Advanced forensic engineering support
- New C-IED equipment and TTP training for deployed and deploying US and allied military forces, including HN military and police
- SIGINT support for DtD, AtN, and FP
- Improved explosive residue detection equipment used in a field environment
- Improved body armor protection materials
- Improved vehicle operation in improvised weapon/IED threat environments
- Improved remote exploitation and render safe technologies using robotics
- Improved forensic techniques and equipment
- Improved computer-based training capabilities and training aids
- Improved DOMEX/MEDEX equipment
- Integrated software technologies for data fusion of ISR capabilities
- Collection of data used across the IC/C-IED community in support of analysis and standardization FP ECM testing and support
- Improved vehicle armor and vehicle mechanics against IED attacks
- Improved FP equipment

CHAPTER 8
Level 5 (Strategic Oversight and Special Activities)

Governance and Policy for Weapons Exploitation and Action

8.1 General Description

The highest levels of US, international government organizations, and special activities conduct Level 5 exploitation to support unique collection and investigations of national importance. Level 5 activities include clandestine or covert operations authorized by the President and focused on precise challenges and developmental projects to enhance collection efforts and focus exploitation across the spectrum of ROMO. The production of information at Level 5 informs national level initiatives.

8.2 Objectives

Level 5 objectives include collection, analysis, and research by government agencies that enable national level activities to take strategic action against improvised weapons and the networks that use them. These activities include overt strategic action, such as issuance of a demarche, or to move or create sanctions against a state sponsor of an improvised weapon threat. Level 5 provides synchronization and coordination of departmental activities that support national level initiatives.

8.3 Focus Areas

Level 5 focus areas include national level program management and policy development, requirements identification and resourcing, and conflict resolution and facilitation of coordinated activity across multiple international agencies, departments, and military services. This level includes collection, analysis, and research by government agencies and private agencies/research firms.

8.4 Enablers

To be successful, WTI must remain networked, integrated, and synchronized across governmental agencies, military services, theaters, and other organizations. Some of the goals of these organizations are the identification of state sponsors and counter proliferation.

8.4.1 Office of the Director of National Intelligence (ODNI)

The ODNI stood up on April 21, 2005, and is led by a Director of National Intelligence (DNI). Post-9/11 investigations proposed sweeping change in the IC, resulting in Congressional passage of the Intelligence Reform and Terrorism Prevention Act of 2004. The ODNI oversees a 17-organization IC and improves information sharing, promotes a strategic, unified direction, and ensures integration across the nation's IC. Governance of WTI is implied through the National Intelligence Plan via the Director DIA.[160]

[160] Office of the Director of National Intelligence, "Mission, Vision and Goals," as of December 4, 2013, http://www.odni.gov/index.php/about/mission

8.4.1.1 The Central Intelligence Agency (CIA)

The CIA is part of the IC. Its primary mission is to collect, evaluate, and disseminate foreign intelligence to assist the President and senior US government policymakers in making decisions relating to national security. The CIA does not make policy; it is an independent source of foreign intelligence information for those who do. The CIA may also engage in covert action at the President's direction in accordance with applicable law. Its offices use elements of WTI analysis within their mission sets.

8.4.2 National Counter Terrorism Center (NCTC)

NCTC serves as the primary US organization for integrating and analyzing all intelligence pertaining to terrorism possessed or acquired by the US government (except purely domestic terrorism); serves as the central and shared knowledge bank on terrorism information; provides all-source intelligence support to government-wide CT activities; establishes the information technology system and architectures within the NCTC and between the NCTC and other agencies that enable access to, as well as integration, dissemination, and use of terrorism information.[161] The NCTC ensures that agencies receive all-source intelligence support needed to execute their CT plans or to perform independent, alternative analysis, and receive the intelligence needed to accomplish their assigned activities. WTI is one source of information and all-source analysis integrated and further analyzed by the NCTC to support its counterterrorism mission.

8.4.3 Department of State (DoS)

The DoS advances freedom for the benefit of the American people and the international community by helping to build and sustain a more democratic, secure, and prosperous world composed of well-governed states that respond to the needs of their people, reduce widespread poverty, and act responsibly within the international system.[162] Representative organizations within DoS that benefit from WTI activities include: the Political-Military Affairs office that integrates diplomacy and defense issues and forges strong international partnerships to meet shared security challenges; and the DoS Bureau of CT that forges partnerships with non-state actors, multilateral organizations, and foreign governments to advance CT objectives and national security of the United States. CT takes a leading role in developing coordinated strategies to defeat terrorists abroad and in securing the cooperation of international partners.[163]

8.4.3.1 Homemade Explosives (HME) Task Force (TF)

The HME TF has three co chairs, the Deputy Special Representative to Afghanistan Pakistan (DoS); the Director of the JIEDDO (DoD); and the Deputy Assistant Secretary of Defense for Afghanistan, Pakistan, and Central Asia (DoD). The HME TF was specifically established to counter and abate the proliferation of materials (**Figure 8-1**) used in the manufacture of HME and in IED main charges and initiators. Disrupting the flow of HME and its precursors requires a whole-of-government approach in coordination with the international community and private sector. HME precursors are often readily available and easy to obtain legitimately in most countries. The community of action

[161] National Counter Terrorism Center (NCTC), "What We Do," as of December 4, 2013, http://www.nctc.gov/about_us/what_we_do

[162] Department of State, "Mission," as of December 4, 2013, http://www.state.gov/s/d/rm/index.htm#mission

[163] Department of State, Bureau of Counterterrorism, as of December 4, 2013, http://www.state.gov/j/ct/index.htm

December 12, 2012

Homemade Explosives (HME) Task Force (TF)

Background: The signature weapon of choice used by the insurgency in Afghanistan is the IED. IEDs play a significant role in the combat environment and represent the most significant threat to the success of the coalition's strategy in Afghanistan. In 2012, approximately 2,000 US combat casualties were caused by IEDs, accounting for 63 percent of all US combat casualties.

Approximately 88 percent of IEDs in Afghanistan are made using HME as the main charge, and approximately 71 percent of HME IEDs are AN-based. Hence, 62 percent of IEDs are AN-based. The primary precursor for AN-based HME is the fertilizer calcium ammonium nitrate (CAN), which is illegal in Afghanistan but legal in Pakistan. The vast majority of IED components, including commercial explosives, radio-control triggers, and HME precursors are sourced from and/or transmitted through Pakistan, making Pakistan the center of gravity for the C-IED effort in Afghanistan. A complex, global network of licit and illicit activities facilitates the flow of lethal aid into Afghanistan from Pakistan. Unfortunately, the HME nodes of activity in Pakistan are difficult to influence given recent events.

Eliminating the use of CAN in HME, if possible, would not solve the IED problem in Afghanistan, but is a critical first step in affecting the enemy's ability to use HME against US and coalition forces. Because no single interagency or international organization has capabilities or full authority to limit enemy access to HME precursors, countering HME in Pakistan and Afghanistan requires an approach that combines multinational, whole-of-government, and private sector capabilities. The HME TF brings together a community of action to leverage all of these resources.

The three co chairs of the HME TF are the Director of JIEDDO; the Deputy Assistant Secretary of Defense for Afghanistan, Pakistan, and Central Asia; and the Deputy Special Representative to Afghanistan Pakistan. The community of action includes participation across the DoD, DHS, DoS, DoJ, and Departments of Treasury and Commerce. The TF's multinational members include the United Kingdom, Canada, Australia, and New Zealand, and its private sector partners include the International Fertilizer Association and The Fertilizer Institute.

The purpose of the HME TF is to reduce the flow of HME precursors into Afghanistan, thereby reducing effective attacks against US and coalition forces. Disrupting the enemy's HME pipeline requires identification of vulnerabilities within HME networks that produce IEDs and taking action against those vulnerabilities using the full capabilities of this multinational, whole-of-government, and private TF.

Current Status: The HME TF is developing a robust intelligence picture that allows a common understanding of the HME problem set. In addition, the HME TF is reviewing those policies that enable or limit the ability of HME TF member organizations to take action against HME networks. There has been tremendous support and involvement across the multinational interagency and private sector to coordinate, collaborate, and implement measures to reduce the HME threat. The US-Pakistan bilateral relationship remains strained after the November 26, 2011 cross-border incident, which limits our ability to engage with the Government of Pakistan on C-IED cooperation.

Challenges and Way Ahead: The HME problem continues because of a lack of HME precursor control measures, strained relations with Pakistan, and unopposed insurgent networks operating in safe havens within Pakistan and Afghanistan. Limited intelligence collection and analysis resources, competing priorities within the multinational interagency, and unclear or limiting policies challenge our ability to identify and take actions to disrupt the HME pipeline.

includes participation across the DoS, DoD, DHS, DoJ, and the Departments of Treasury and Commerce. Its multinational members include the United Kingdom, Canada, Australia, and New Zealand and private sector partners from the International Fertilizer Association and the Fertilizer Institute.

Figure 8-1. HME Materials. *Terrorists and insurgents commonly use ammonium nitrate (AN)-based fertilizer to make HME. (Photo Credit: JIEDDO)*

8.4.4 Department of Homeland Security (DHS)

DHS duties are wide-ranging, but the goal is clear: a safer, more secure America, which is resilient against terrorism and other potential threats. WTI information and analytical products help to inform DHS in the conduct of their mission. DHS has the following five homeland security missions:[164]

- Prevent terrorism and enhance security
- Secure and manage borders
- Administer immigration laws
- Safeguard and secure cyberspace
- Ensure resilience to disasters

8.4.4.1 Office for Bombing Prevention

The Office for Bombing Prevention (OBP) leads the DHS' efforts to implement the national policy for countering IEDs and enhance the nation's ability to prevent, protect against, respond to, and mitigate the terrorist use of explosives against critical infrastructure, the private sector, and federal, state, local, tribal, and territorial entities. OBP conducts focused portfolio activities to coordinate national and intergovernmental bombing prevention efforts; enhance C-IED capabilities through

[164] Department of Homeland Security, "Mission," as of December 4, 2013, http://www.dhs.gov/our-mission.htm

requirements and gap analysis; and increase IED awareness and information sharing among federal, state, local and private sector partners.[165]

8.4.5 Department of Justice (DoJ)

The DoJ enforces the law and defends the interests of the United States according to the law; to ensure public safety against threats foreign and domestic; to provide federal leadership in preventing and controlling crime; to seek just punishment for those guilty of unlawful behavior; and to ensure fair and impartial administration of justice for all Americans.[166] Within the DoJ there are 53 agencies, many of which have direct ties to WTI and include the ATF, FBI, and INTERPOL Washington.

8.4.5.1 Joint Program Office for Countering IEDs (JPO C-IED)

The JPO C-IED, administered by the Attorney General through the FBI, is an interagency group that is overseen by an executive council of senior executives from DoJ/FBI, DoD/OSD, and the Joint Staff, DoS, DHS, and the National CT Center. The JPO C-IED Implementation Committee of Program Managers (PMs) and SMEs from federal departments and agencies meets monthly to coordinate, track, and review progress of the White House's plan to counter the IED threat by the doing following:[167]

- Increase domestic and international engagement
- Effectively exploit information and materials from IED attacks
- Advance our intelligence and information analysis
- Maintain our deployable C-IED resources
- Screen detect, and protect our people, facilities, transportation systems, critical infrastructure, as well as the flow of legitimate commerce
- Safeguard explosives and select precursor materials
- Coordinate and standardize training and equipment
- Enhance our operational planning

8.4.5.2 National Explosives Task Force (NETF)

The US government established a NETF to enhance C-IED activities and advance the implementation of the national strategy for countering IEDs. The FBI administers the NETF, whose mission is to coordinate rapid integration of explosives expertise with intelligence and LE information to support operational decisions by those responsible for preventing terrorist or criminal use of explosives. The mission of the NETF is to centrally coordinate the provision of explosives expertise to investigations and to ensure the coordination of a whole-of-government effort to

[165] Department of Homeland Security, "Office of Bombing Prevention," as of December 4, 2013, http://www.dhs.gov/obp

[166] Department of Justice, "About DOJ, Our Mission Statement," as of December, ,4 2013, http://www.justice.gov/about/about.html

[167] The White House, *Countering the Explosive Device*, pgs. 1-3.

deter, prevent, detect, protect against, and respond to the threat posed by terrorist or criminally inspired attacks using explosives in the United States or against US interests abroad. NETF is the central communication and coordination point for ATF and the FBI, at the Headquarters level, for explosives response coordination and intelligence matters. NETF is also instrumental in the intelligence gathering functions of both agencies as they relate to the exploitation of information from IEDs. The NETF is staffed with intelligence specialists, investigators, and bomb technicians. NETF also works with the National Security Staff and the JPO to align ATF's mission, resources, and expertise with the national strategy to counter IEDs.[168]

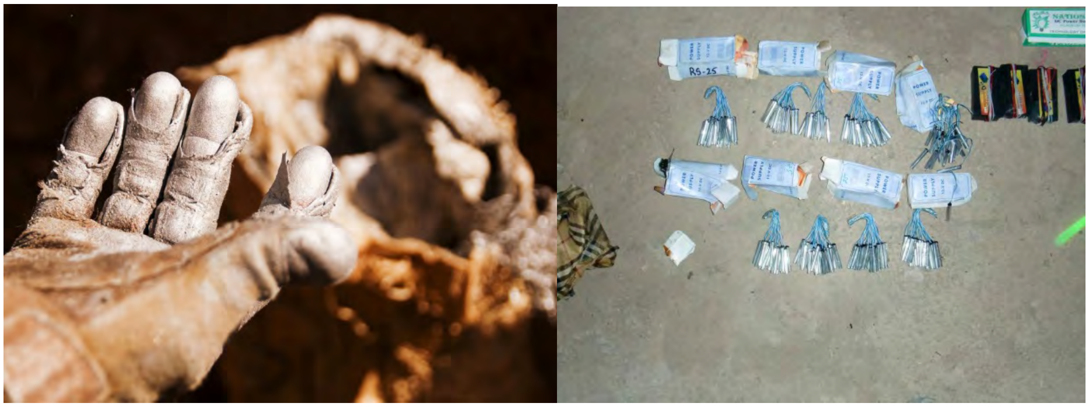


Figure 8-2. Components Commonly Associated with IEDs. *Aluminum powder is used as a precursor material to enhance the explosive effect of HME and commercial blasting caps and other paraphernalia can be purchased on the open market. (Photo Credit: JIEDDO)*

8.5 Outputs

Level 5 WTI outputs include the revision of policy and governance for improvised weapons related strategic issues and bilateral agreements with partners.

While several organizations and activities are listed in this chapter, it must be noted that many activities that occur at Level 5 are conducted in classified environments, and occur between members of the IC, diplomatic corps, and partner nations and could not be included in this handbook.

Counter Proliferation of IED Materials

Multiple governmental organizations work in conjunction with one another to severely curtail or monitor the purchase of explosive or CBRN precursor materials and paraphernalia on the open market. They ensure compliance with existing international trade agreements and laws and track components that are commonly associated with IEDs **(Figure 8-2)**.

[168] Bureau of Alcohol, Tobacco, Firearms and Explosives, "National Explosives Task Force," as of December 4, 2013, http://www.atf.gov/content/explosives/explosives-enforcement/national-explosives-task-force

CHAPTER 9
CRITICAL OUTCOMES

Products associated with WTI (**Figure 9-1**) provide relevant and timely information to commanders and staffs to allow them to make decisions and adjust operations. Many of these products are associated with actionable intelligence that is required to apply constant pressure on the enemy and networks. The following are examples of typical WTI-related products and reports produced by and shared with organizations throughout the WTI process:

Tactical	**Operational**	**Strategic – Special Activities**
• Collection reports • Quick Look reports • Targeting Support Packages • Detainee Interrogation Support Packages • Be-on-the- Lookout (BOLO) reports • QA/QC Feedback reports • Forensic Material Log • Witness statements • Intelligence reports • Anti-Armor Incident reports • COIC products resulting from requests for support	• RC Device Threat Frequency Chart • CEXC reports • IED Flash and Awareness reports • Technical Exploitation reports • Named Area of Interest (NAI) reports • Biometrics/Forensics reports • Insurgent technical and tactical trends • CIAD trend analysis • Quick Look reports • Targeting Support Packages • Detainee Interrogation Support Packages	• TEDAC reports • Electronic assessments • Interrogation Support Packages • ECM development • BIARs • Bomb maker/insurgent organizational intelligence • CIAD TECHREPs • DoD BEWLs

Figure 9-1. WTI Reports and Products

These products and reports provide critical inputs that drive predictive and pattern analysis that continuously feeds intelligence preparation of the OE (IPOE). IPOE is the commander's main tool to predict enemy activity and develop courses of action. WTI products allow US and coalition forces to quickly recognize and adapt to enemy TTP by using modern tools and techniques to produce information and factual reports and to enable continuous countermeasures updates based on enemy reactions.

Typically, the first report generated in the WTI process is a technical assessment of an improvised weapon. These provide the technical information necessary to complete a WIT report, inform pattern analysis, and produce an improvised weapon (or conventional weapon) overlay. This first technical assessment helps EOD staffs determine if EOD RSPs and FP measures require adjustments. Overall, WTI supports the five critical outcomes: FP, targeting, sourcing, support to prosecution, and signature characterization.

9.1 Force Protection (FP)

The technical categorization and tactical characterization of IED materials enables FP through countermeasures development, identification of observables and signatures, and tip and cue information for collection.[169] Tip and cue refers to detecting information/intelligence areas of interest that can be used to focus collection efforts. The exploitation and analysis of information and material from an incident support WTI FP outcomes by informing warfighters of developments or adjustments to TTP, providing battle damage assessments, identifying useful indicators and warnings, and providing information and analysis critical to the development of essential equipment.

Force Protection Vignette

Abdul Rahman applied for a local national military position at a coalition FOB. During the initial screening process, a 10-print enrollment (i.e., he was fingerprinted) was submitted as a prerequisite for Abdul's employment. Upon collection, his prints were transmitted to the CENTCOM Forward Server (CFS) containing the DoD BEWL and simultaneously to the ABIS database in West Virginia that maintains collected known and latent print data. The CFS provided a latent print match to the screening official within 2 minutes, with ABIS confirming the match 1 minute later.

The subject was immediately detained during the initial employment screening process, preventing him from infiltrating the military training program and/or posing a green-on-blue threat to coalition forces. Subsequent investigation and analysis tied the subject to multiple IED-related incidents in the prior year, resulting in enhanced HN prosecution proceedings under the rule of law.

CENTCOM used a CFS in Afghanistan beginning in 2011, providing a repository of wanted individuals and encoded latent prints for near-real-time biometrics (NRTB) operations. Units were able to obtain a match/no-match response in minutes versus non-NRTB units that often did not find out they had an insurgent in their custody until returning to the FOB and downloading the enrollments to the ABIS. NRTB ensures units detain upon first encounter and eliminate the suspect's ability to return to insurgent operations.

9.1.1 Tactics, Techniques and Procedures (TTP)

The collection, processing, and analysis of the improvised weapon (including IEDs and other weapons) and its employment has a significant and immediate impact on how deployed forces operate in a given area of operations. For example, US and coalition forces have determined that the human eye is the most effective tool for identifying weapons and environmental indicators of improvised weapon/IED activity. During tactical operations warfighters use lists of device

[169] Army Doctrine Reference Publication 2-0, *Intelligence*, August 2012, pgs. 4-8.

indicators, containing observables and signatures developed through previous documentation of how a new improvised weapon/IED was located, what it looked like, and how it was emplaced. These indicators are shared during patrol briefs, incorporated during rehearsals, and checked by leadership during pre-combat checks and pre-combat inspections. Additionally, WTI information informs changes to Counter Radio-Controlled IED Electronic Warfare (CREW) systems and load set updates. For example, post-patrol briefs and Level 1 reports provide valuable information that informs adjustments to tactical employment of a CREW system on the basis of its effectiveness against a certain IED. Technical exploitation reports provided by CEXC, TEDAC, and I2WD to the battalion EWO ensure CREW systems are operating with the correct ECM load sets.

WTI information and analysis has a direct effect on how CTCs and Major Subordinate Commands prepare warfighters for deployment. WTI feeds the production of after action reports best practices, lessons learned, and intelligence summaries used to adjust training and blue TTP. Information sharing between deployed assets and CONUS-based training commands is often accomplished through mobile training teams, video and online training aids, and field guides to facilitate rapid incorporation into training.

9.1.2 Battle Damage Assessment

Battle damage assessments provide important information to analysts and SMEs regarding the lethality of enemy weapon systems in context of the targeted vehicle, vessel, and crew. WIT and EOD conduct battle damage assessments (**Figure 9-2**) onsite to determine the type of improvised weapon or conventional weapon used in an attack. This information leads to characterization of the overall damage or effect of the improvised weapon against the intended target by analyzing the tactical design of the event. The results are further examined to verify the technical category of a weapon or device used in an attack and how effective US and coalition vehicles and equipment are in protecting personnel and contents. For ground vehicle attacks, this information is forwarded to CIAD where personnel conducts studies and compile data to enhance materiel development and validate test requirements and threats. For attacks against maritime targets (i.e., surface vessels or maritime structures), information from battle damage assessments is forwarded to NSWCCD. These reports produce significant data for PMs responsible for improvement of US vehicle and ship survivability and allows senior leaders to prioritize resources on the basis of hard data. Analysis of battle damage assessments determines exploitable weaknesses and advancements in enemy weapon design and TTP. This analysis equates to changes in friendly TTP and visibility into friendly TTP vulnerabilities.

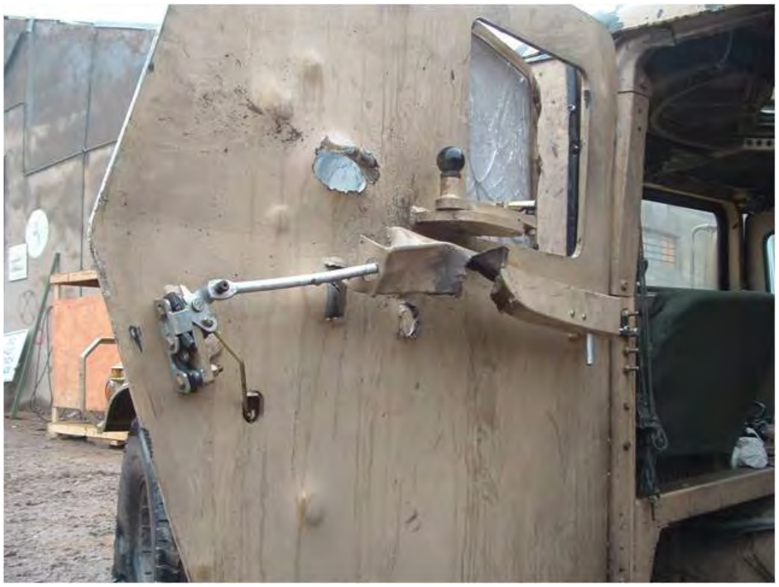


Figure 9-2. Battle Damage. *This damage was caused by an anti-armor IED and documented for further analysis by CIAD. (Photo Credit: CJTF Troy)*

9.1.3 Indications and Warnings

WTI produces useful indicators and warnings associated with the tactical design and technical characterization of an improvised weapon and its associated event (**Figure 9-3**). Indicators are observable and measurable. They point out or point to an improvised weapon, including an IED or enemy activity (e.g., a stack of rocks or empty bag used as an aiming point). Through continuous exploitation of improvised weapons in a particular OE, EOD Technicians and WIT members are able to build a COP of the most commonly used improvised weapon/IED components to educate personnel. For example, prior to conducting dismounted patrols in urban areas, units are shown common components (e.g., wires, batteries, base stations) that, if seen in a search or for sale in a local shop, will cue further investigation. Incorporating indicators into training ensures warfighters respond appropriately to the enemy's activity and use of improvised weapons. Educating the warfighter on the tactical design of improvised weapons/IEDs through the use of photographs and/or training aids assists Service members in understanding emplacement techniques and environmental conditions to identify similar situations where these types of weapons may be encountered.

WTI products include contextual data of IED events using tactical design and technical categorization from previously found and cleared devices, explosions, caches, hoaxes, and false alarms to help locate future IEDs, enhance training lanes, and predict how the enemy will conceal IEDs in the future. WTI products also provide the ability to train personnel who monitor unmanned aerial vehicle feeds to identify IED emplacement and HME production activities.

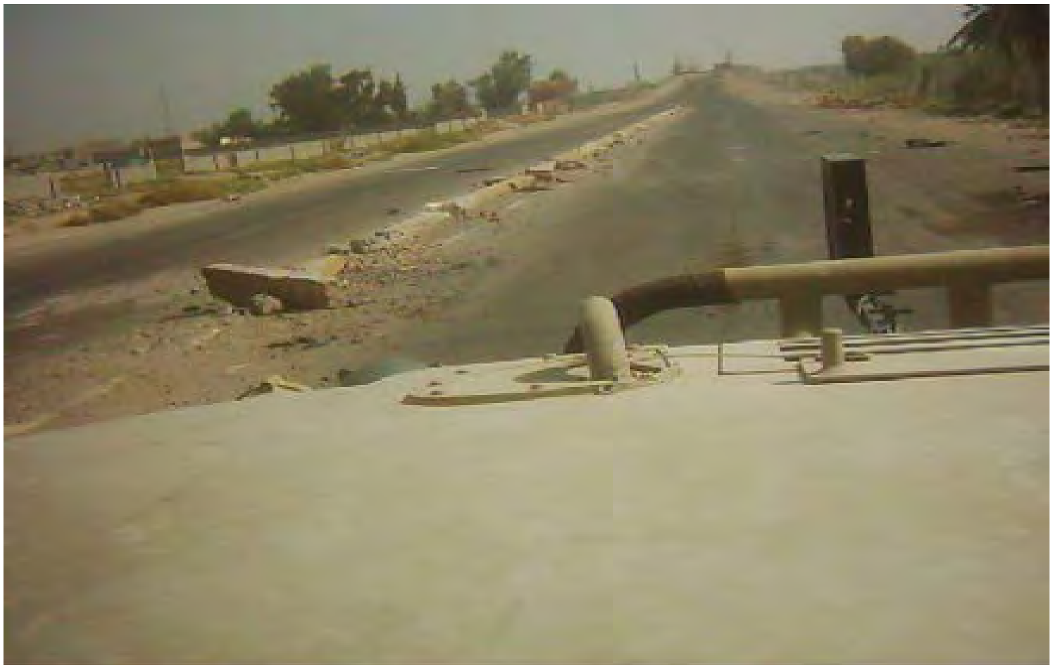


Figure 9-3. WTI Analysis Helps Warfighters Recognize IEDs in Complex Terrain. *Insurgents hide foam-encased EFPs in roadside rubble. (Photo Credit: CJTF Troy)*

9.1.4 Equipment Development

Information and intelligence obtained from WTI activities is used to help design, develop, and test equipment and countermeasures to reduce the effectiveness of enemy weapons, improvised weapons, and IEDs. WTI enables US material developers to understand current weapons threats and ensure the accuracy of RDT&E by providing timely factual data to develop material solutions, EOD RSPs and tools, CREW devices, and enhanced armor protection. In 2005, collection, exploitation, and analysis efforts were effectively used to determine that the enemy was employing passive infrared (PIR) sensors to initiate EFPs. Many different equipment solutions have since been developed and tested to defeat PIRs and to pre-detonate these improvised weapons. WTI products were also paramount to determining the size of EFPs being employed during the development of resistant armor for HMMWVs and the Mine Resistant Ambush Protective vehicle. Since 2005, CIAD analysis has positively impacted US materiel development programs and provided numerous tactical recommendations to unit commanders.[35]

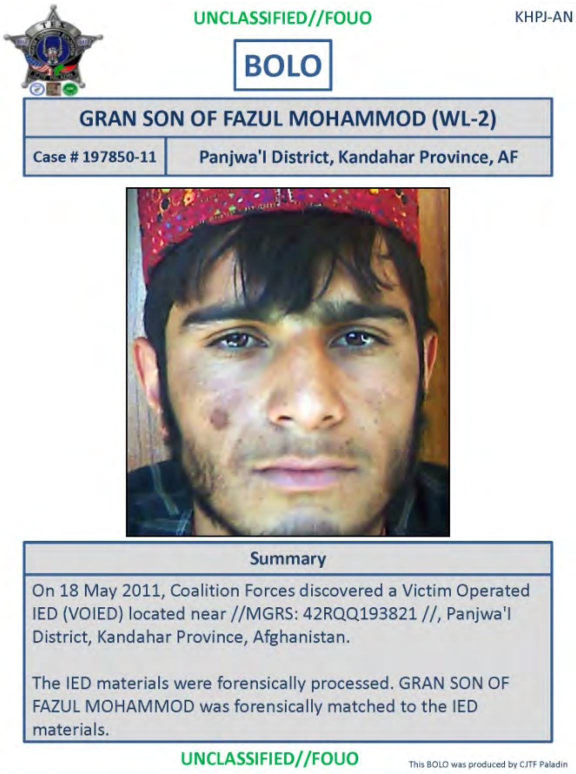
9.2 Targeting

9.2.1 Dynamic Targeting

Dynamic targeting allows users to rapidly gather information from one target, identify a follow-on time-sensitive target, and conduct an immediate raid on the next site. For example, site exploitation results and examination of the IED components collected onsite have led to the discovery and neutralization of IEDs and bomb makers before they had a chance to strike again. Warfighters have experienced successes by quickly recovering information from cell phones and global positioning systems from IED caches and detainees and using it to conduct dynamic targeting. Warfighters trained in WTI and site exploitation collection and processing skills provide a distinct advantage during patrols, raids, searches, and site exploitation operations by enabling dynamic targeting.

9.2.2 Targeting in Support of Network Attack

WTI is a key element to effectively target individual, networks, and sites involved in enemy activities. WTI provides information critical to the find, fix, finish, exploit, analyze, decide (F3EAD) targeting cycle. WTI supports both lethal and nonlethal targeting through the analysis of the technical and forensic information that is turned into intelligence. WTI is fused with all-source intelligence to create targeting packages and determine intelligence gaps used by commanders to prioritize targets and match an appropriate response. Commanders decide whether to apply tactical patience on the basis of the level of detail regarding a target. WTI assists the commander's staff in cueing ISR assets that locate and track individuals, refining targeting information, and tying enemy activity to possible insurgents. Forensic information from an improvised weapon also may produce BEI, which facilitates the identification and targeting of enemy personnel, including high-value individuals. This information is fused with all-source intelligence to create targeting packages. **Figure 9-4** is a BOLO package generated to assist targeting of personnel of interest. Targeting packages are reviewed and analyzed during targeting meetings designed to identify and address intelligence gaps and produce intelligence requirements necessary to improve the targeting package.



UNCLASSIFIED//FOUO

KHPJ-AN

BOLO

GRAN SON OF FAZUL MOHAMMOD (WL-2)

Case # 197850-11	Panjwa'I District, Kandahar Province, AF

Summary

On 18 May 2011, Coalition Forces discovered a Victim Operated IED (VOIED) located near //MGRS: 42RQQ193821 //, Panjwa'I District, Kandahar Province, Afghanistan.

The IED materials were forensically processed. GRAN SON OF FAZUL MOHAMMOD was forensically matched to the IED materials.

UNCLASSIFIED//FOUO

This BOLO was produced by CJTF Paladin

Figure 9-4. Be-on-the-Lookout (BOLO) Report *(Photo Credit: CJTF Paladin)*

The WTI process produces conclusive information to attribute specific individuals to a group or network and produce more valuable targeting information. WTI process results can support pattern analysis, establishing the operational boundaries of a threat network. WTI exploitation methods help identify and determine signatures for each bomb maker on the basis of the type of event and IED fabrication methods used and the type of components the bomb maker used, creating profiles that are accorded NAIs. For instance, most EFPs recovered in Iraq were associated with Shia insurgent networks, while the signature of Sunni attacks is highlighted by use of large vehicle IEDs. However, many networks have attempted to fabricate and employ IEDs similar to their adversaries in an attempt to create confusion. Exploitation and analysis of captured information and material during the WTI process allows US forces to discern the difference.

Material collected from IED sites and caches and exploited at tactical and operational levels provide forensic data to link identities with activity, material, and locations. When fused with other forms of intelligence, the result is a more refined and informative targeting package. Additionally, this information allows US and coalition forces to identify which networks have formed coalitions and which networks are state-sponsored. It presents a picture of the global networks participating in an insurgency or terrorist activity and with whom they're aligned. This type of information formed the cornerstone of targeting individual bomb makers in Iraq and Afghanistan. WTI products enabled visualization of the insurgency and terrorist activity in Iraq and Afghanistan, which led to comprehensive network mapping that facilitated targeting. NGIC and COIC AtN products were valuable resources for tactical and operational level commanders and staff to leverage when conducting targeting.

9.3 Component and Material Sourcing

9.3.1 Internal to Theater

Identifying the source of material, components, munitions, and the type of explosives in main charges used in IEDs is a challenging process. Expeditionary exploitation laboratories attempt to identify the source of material at a location close to the point of collection. However, due to time constraints, an expeditionary laboratory may not have the capability and/or capacity to exploit information and material and forward it to another more capable exploitation facility. Therefore, technical exploitation personnel collect and record all serial numbers, manufacturing information, and parametric data required to identify and link sources of improvised weapon material. This information is fused with other intelligence collected from caches, improvised weapon fabrication sites, and all-source intelligence to identify individuals and networks responsible for purchasing, transporting, and storing these materials. Many of these improvised weapon suppliers are part of independent criminal networks that are directly connected to other cells and enemy networks. WTI provides the means for intelligence organizations to identify linkages between networks and cells so that they can understand, exploit, and attack them. WTI makes the process and enablers that collect, exploit, analyze, store, and share weapons related information available to further identify international and state-sponsored sources.

9.3.2 External to Theater

TEDAC is the US government's singular strategic level exploitation and analysis capability and the repository for globally collected improvised weapons. TEDAC works with other strategic, national, and international exploitation organizations to analyze and help identify the sources of IED components and precursors. Information and intelligence derived at TEDAC leads to a better understanding of insurgent and terrorist network affiliations with international sponsors, assists in understanding emerging enemy characteristics, and allows the United States and its allies to develop an effective information campaign.

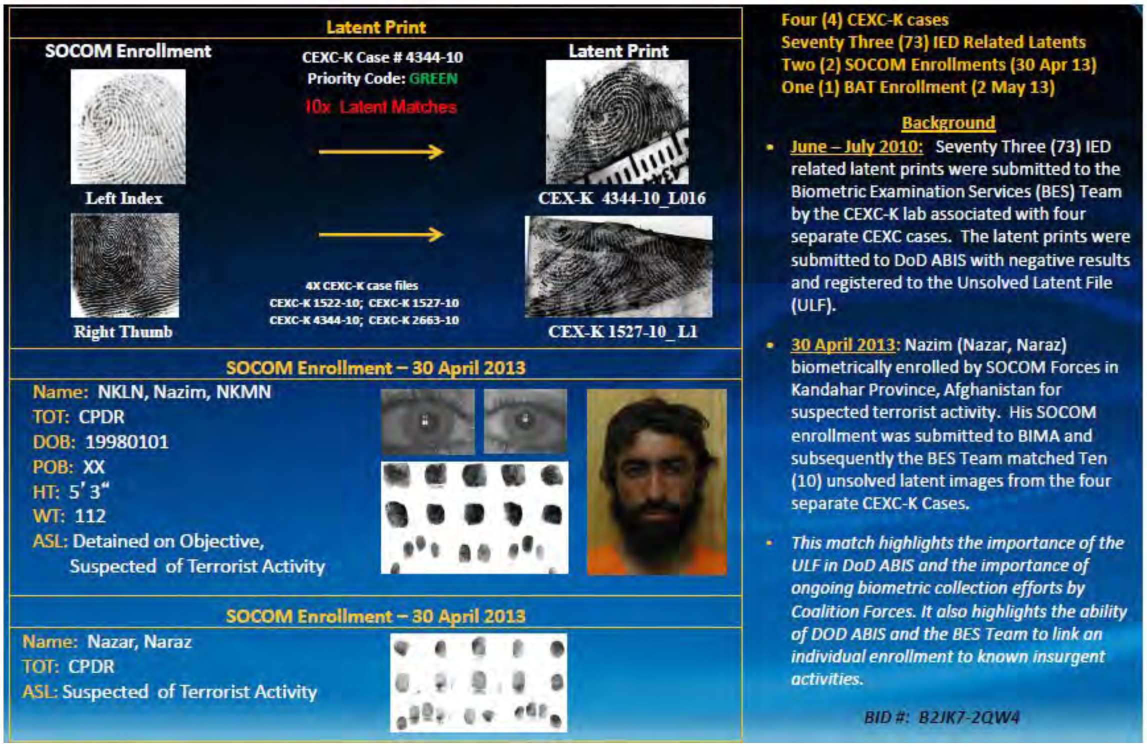
9.3.3 Support to Attack the Network (AtN)

Identifying sources of IED supplies and materials is a component of AtN. It further refines mapping of human connections inside and outside enemy networks and allows us to understand them more clearly. Many insurgents have pre-existing connections with enabling entities (e.g., black market, commercial sources, criminal networks, financial networks, and state sponsors,). WTI enables us to make connections between these entities, insurgents, and terrorists. WTI results also allow targeting of supply shipments, which reduces the amount of attacks by breaking the IED cycle while supporting efforts to provide security for local nationals.

9.4 Support to Prosecution (HN and CONUS)

Information derived from exploited improvised weapons has been critical to support the prosecution of detainees in Iraq, Afghanistan, and CONUS. Increasingly, HN judges allow and rely on WTI-related information to secure the prosecution of insurgents and detainees involved in IED events. Photographs, sketches, diagrams, and other physical material secured during site exploitation may be used as evidence in a court of law. WTI collected and processed material provides latent fingerprints, DNA, and tool marks — technical matches, profiles, and trace explosive residue results that are used successfully as evidence in HN judicial systems. As seen in Iraq and Afghanistan, much of the success stemmed from training HN judges and the understanding and confidence gained by fostering a close working relationship between them and US LE professionals, technical specialists, and forensic examiners. Advanced training of HN military and LE entities must occur to ensure prosecutorial skills and capability transition to enable civil authorities.

Local judges from some countries must be trained on the process and reliability of forensic evidence. The operational situation dictates collection methods employed, time allotted for onsite forensic processing, and the need to preserve the evidentiary integrity of collected material to secure a conviction in a HN and CONUS court of law. When US and allied forces are no longer in the lead, HN sovereignty issues could make collection of WTI information and material more challenging. Therefore, it is important to establish and foster a strong relationship with HN judges to understand what information is acceptable for a warrant. As illustrated in **Figure 9-5**, a collaborative effort between unit intelligence (S2), EOD, WIT, FXT, CEXC, CITP, or other expeditionary exploitation activity is necessary to effectively collect and exploit WTI information and create an enduring HN capability.



Latent Print

SOCOM Enrollment

CEXC-K Case # 4344-10
Priority Code: GREEN
10x Latent Matches

Latent Print

Left Index

CEX-K 4344-10_L016

Right Thumb

4X CEXC-K case files
CEXC-K 1522-10; CEXC-K 1527-10
CEXC-K 4344-10; CEXC-K 2663-10

CEX-K 1527-10_L1

SOCOM Enrollment – 30 April 2013

Name: NKLN, Nazim, NKMN
TOT: CPDR
DOB: 19980101
POB: XX
HT: 5' 3"
WT: 112
ASL: Detained on Objective,
Suspected of Terrorist Activity

SOCOM Enrollment – 30 April 2013

Name: Nazar, Naraz
TOT: CPDR
ASL: Suspected of Terrorist Activity

Four (4) CEXC-K cases
Seventy Three (73) IED Related Latents
Two (2) SOCOM Enrollments (30 Apr 13)
One (1) BAT Enrollment (2 May 13)

Background

- June – July 2010: Seventy Three (73) IED related latent prints were submitted to the Biometric Examination Services (BES) Team by the CEXC-K lab associated with four separate CEXC cases. The latent prints were submitted to DoD ABIS with negative results and registered to the Unsolved Latent File (ULF).
- 30 April 2013: Nazim (Nazar, Naraz) biometrically enrolled by SOCOM Forces in Kandahar Province, Afghanistan for suspected terrorist activity. His SOCOM enrollment was submitted to BIMA and subsequently the BES Team matched Ten (10) unsolved latent images from the four separate CEXC-K Cases.
- *This match highlights the importance of the ULF in DoD ABIS and the importance of ongoing biometric collection efforts by Coalition Forces. It also highlights the ability of DOD ABIS and the BES Team to link an individual enrollment to known insurgent activities.*

BID #: B2JK7-2QW4

Figure 9-5. Latent Hit of the Week Reports. *These are distributed to highlight successful matches of latent prints to people, places, things, and events in support HN or CONUS LE effort. (Photo Credit: BIMA)*

9.4.1 Detainee Operations

WTI analysis at the tactical and operational levels provides the commander with direct support when making hold/release decisions for detainees. Actionable intelligence is collected from detainees, providing technical questioning support to assist with interrogation. Interrogators often determine whether an individual is involved in improvised weapon making or attacks on the basis of WTI material exploited from the site and collected from the individual. Material found on a detainee is properly marked, packaged, and reviewed prior to evacuation to a storage location.

Commanders must create a systematic process to manage "pocket litter"[170] from detainees. This material is critical to classifying a detainee as bomb related or not and could produce actionable intelligence and guide additional tactical questioning and interrogation. WTI analysis is the foundation of the BOLO process currently in operation.

[170] NOTE: Pocket litter is all material collected from a detainees pocket when being held for questioning or interrogation.

9.5 Signature Characterization

This WTI output reflects how bottom-up and top-down information derived from various nontraditional and intelligence-based activities related to the improvised weapons and explosives threats is used to support warfighters, commanders, material developers, and others.

Current and future operations require forces to recognize, evaluate, disrupt, and destroy improvised weapons; their manufacture and employment; and their associated patterns of activity, processes, materials, and networks. A correlation between people, materials, processes, and locations surrounding these activities must be developed to articulate specific, identifiable "indicators," which will be used to detect and collect future signatures. These activities have challenged traditional intelligence processes and capabilities, complicating the ability to detect the adversary's indicators from the ground and air. Warfighters are less familiar with these indicators (**Figure 9-6**) because they are deliberately hidden and difficult to distinguish from other background activities. Therefore, many of these observables can only be inferred through direct observation, indirect observation, or technical measurements.

9.5.1 Indicators

Indicators provide confirmation that a certain condition exists or certain results have or have not been attained. Indicators consist of observables and signatures. For example, observables at an HME production facility may include illegal bags of fertilizer, large cooking pots, propane tanks, tarps, strong ammonia smell, plastic jugs, and outside drying areas.

9.5.2Observable.

An observable is a directly or indirectly identifiable indicator. For example, a patrol witnessing an IED being emplaced would be a direct observable of IED emplacement, while a patrol who observes anomalies in the terrain, such as aiming markers or trails of rocks, disturbed ground, changes in the color of the earth, or flags would be considered indirect observables.

9.5.3 Signature.

A signature is the detected and recorded measurement of an observable from a sensor or collection platform. A signature is a distinctive basic characteristic or set of characteristics that consistently recur and uniquely identify a piece of equipment, material, activity, individual, or event.

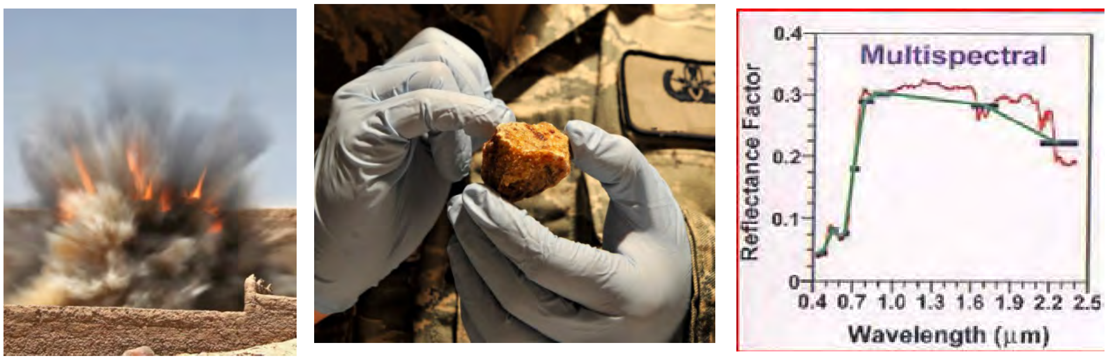


Figure 9-6. Indicators, Observables, and Signatures. *Explosions, explosive material, and spectral and chemical analyses provide useful information can be used for operational planning and aid decision making. (Photo Credit: DoD)*

9.5.4 Using Sensors for Signature Characterization

Sensors used for signature characterization respond to a physical stimulus (e.g., heat, light, sound, pressure, chemical, magnetism, or a particular motion) and transmits a resulting impulse (for measurement or operating a control).[171] There are many different types of sensors that are capable of analyzing a myriad of differing signatures. Information and data obtained throughout the WTI process (i.e., collection, exploitation, and analysis) has proven instrumental in determining the type of sensors required to identify improvised weapons and those individuals or groups who make and employ them. Since different sensors are used to analyze unique signatures, it is important to understand what stimulus is required to achieve the desired measurement or result. Examples of sensor types used in signature characterization are as follows:

9.5.4.1 Spectral.

Refers to electromagnetic signatures that emit, reflect, or absorb radiation such as gamma radiation, X-ray radiation, ultraviolet radiation, visible light, infrared radiation, microwave radiation, radio waves, and more. Electromagnetic signatures are as unique as fingerprints and enable sensors and analysts to detect observables and targets. Detailed observation and documentation of adversarial activities, equipment and materials used, and TTP is key to signature characterization. Knowledge gained through detailed WTI reports and exploitation and analysis of recovered materials is fundamental to identifying signatures that influence sensor and ISR platform selection used to detect and discriminate adversarial materials and activity. When equipment, material, and TTP used by our adversary is known, sensors can be selected and calibrated to detect them. Information about what objects were found at a site and how materials were discovered provide valuable context. Signature identification resulting from material analysis can help pinpoint its origin or facts related to its manufacture and fabrication. Signature characterization drives further intelligence collection and enables improved material detection and intelligence production. Examples of sensors used to detect spectral signatures include:

9.5.4.1.1 Infrared.

Infrared signatures measure thermal variation across the target and background. Target material properties and environmental factors, such as solar loading and other atmospheric conditions contribute to the target's thermal signature. These factors help create contrast useful to discriminate the target from its background. Generally, improvised weapons are detectable using thermal imaging camera throughout the day. However, periods of greatest contrast occur during early morning, just after sunrise, and at night after sunset. During mid/late morning and mid/late afternoon, the least amount of contrast occurs because the improvised weapon and the background generally are equal in temperature. The signature of one improvised weapons is not representative of all improvised weapons. Knowledge of the material properties of an improvised weapon play an important role in producing the target-to-background contrast since differences in materials produce varying results.

9.5.4.1.2 Radar.

Radar is an all-weather sensing capability that measures reflected energy from the target and is common on numerous ISR platforms. The radar signature is very sensitive to the sensor to target geometry, sensor specifications, and target-to-ground interactions. Typically, interpretation of radar signatures is an expertise that is developed with specialized training. Radar can identify human

[171] Merriam-Webster Online, s.v. accessed December 2013, http://www.merriam-webster.com/dictionary/sensor

activity, command wires, and anomalous targets in the scene. As an example, synthetic aperture radar has been used successfully to detect the presence of specific substances in bulk or in residues (such as HME precursors) left behind, as depicted in **Figure 9-7**.

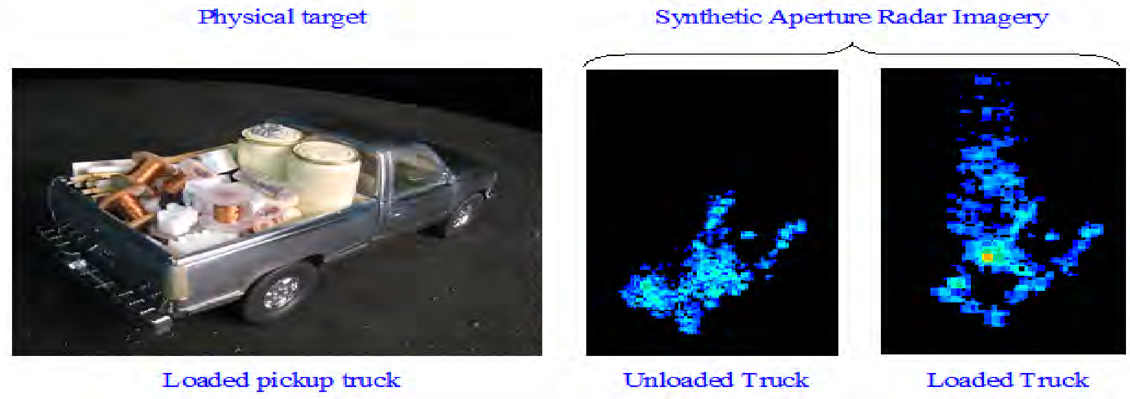


Figure 9-7. Radar Imagery. *Radar imagery detects bulk HME and its residue in the back of a pickup truck. (Photo Credit: NGIC)*

9.5.2 Support to the Warfighters.

WTI-based indicators and observables are used to brief individuals prior to operations and to create training materials for a squad/team patrols (e.g., what to look for, what to expect, and what information/samples to collect when appropriate). An example is DIA's HME Handbook (**Figure 9-8**). Other examples include US Army training videos used to train warfighters on patrol about WTI ground signs (observables) and indicators to look out for when locating HME while on patrol in Afghanistan (**Figure 9-9**).

DEFENSE INTELLIGENCE AGENCY

UNCLASSIFIED//FOUO

HOMEMADE EXPLOSIVES

Updated August 2012

UNCLASSIFIED//FOUO

Committed to Excellence in Defense of the Nation

Figure 9-8. DIA's Homemade Explosives Handbook *(Photo Credit DIA)*

Weapons Technical Intelligence

Locating HME - ANAL (CAN26/AI) on Patrol in Afghanistan

https://www.milsuite.mil/video/watch/new video/4708

Weapons Technical Intelligence

IED - Ground Sign (Indicators & Observables) on Patrol in Afghanistan

https://www.milsuite.mil/video/watch/new video/4785

Figure 9-9. US Army Training Videos. *These address the use of indicators and observables while on patrol. (Photo Credit: USA TRADOC)*

9.5.3 Support to Commander.

WTI supports the commander and staff in AtN by assisting in identification of:

- People, by title , who are members of an organization/insurgent cell. WTI links people to an activity or membership in a group through exploitation of DNA and latent fingerprints from collected material or from incident sites
- Processes used by the adversary (e.g., manufacture of HME and electronic switch fabrication [i.e., WTI analysis]) that reveal consistent patterns of assembly and device fabrication
- Material (in all forms) required by the adversary to fabricate weapons (e.g., make, develop, and deploy RF switches [WTI analysis-supply chain] that are used on a consistent basis and can be traced back to their source)
- Locations where the adversary lives, stores materials, manufactures items, and attacks US and partner nation forces (e.g., unit and EOD/WIT reports) that, when recorded systematically over time, can reveal patterns of activity and bias in the enemy's choices regarding use of terrain.

9.5.4 WTI Cueing Intelligence, Surveillance, and Reconnaissance (ISR) Support for Operational Staff

An important element in development of indicators that support detection of threat activity is a baseline understanding of the weapons threat that includes improvised weapon makeup, manufacture, and tactical design. Indicators are based on what is routine for the geographic area or region — whether it be patterns of daily life or manufacturing processes associated with local legal and illegal commercial activity. After the norm is established as the baseline, it is easier to discern anomalies in patterns that indicate enemy activity. A challenge in Afghanistan has been distinguishing drug-related processing from HME manufacture. Analysts identified unique indicators and programmed ISR systems to discriminate between the two, cueing the commander to locations of HME fabrication versus drug laboratory activity. The identification of WTI-based signatures that indicate specific enemy activity directly supported ISR collection strategies. This ensured that the appropriate system was tasked to discover the activity. Indicators are normally a composite of several observables and signatures that, when layered, improve detection probability. For example, HME production involves a series of discrete steps, executed in a specific sequence, with each element of the manufacturing process creating a unique observable that, when combined, make the intent of the activity clear and its discovery by ISR systems more likely.

9.5.5 Support to the Material Developer

WTI data supports signature development through:

9.5.5.1 RF Signature Analysis.

RF signatures typically refer to unintended radiation emanating from electronic components. Detection of RF energy in isolated areas, or identification of the source using its signature, can tell the operator a great deal about the threat environment. Full characterization of RF signatures allows the material developer to support development of countermeasures and sensors to optimize standoff range, system bandwidth, system sensitivity, and antenna design for a faster design cycle to respond to change in current and future RF threats.

9.5.5.2 HME Signature Analysis.

HME signature analysis is analysis of activities that reflect the manufacture of HME and transportation of HME and precursors. Analysis considers caching and emplacement indicators that result from production equipment/tools and residual evidence (such as stains or unique vapors) that allow for determination and validation of HME signatures during various stages of IED life cycle. Validated signatures are necessary for material developers to support development of sensors with effective sensor modalities, frequencies, and sensitivities for addressing current and future HME threats.

9.5.5.3 Biometric.

Biometric signatures are deduced from biometric samples taken from a subject. They are distinctive, measureable characteristics used to identify individuals and match them to an item, locations, activities, or other individuals. Identity attributes are biographic, biologic, and behavioral characteristics by which an individual, person, persona, system, or discrete groups thereof can be distinctively recognized or known. Biologic attributes are related to the shape of the body, and include fingerprint, face recognition, DNA, palm print, hand geometry, iris recognition (which has largely replaced retina), and odor/scent. In WTI, latent fingerprints, DNA, and other signatures recovered from material is used to scientifically fix an individual's biometrics to an item or hostile event. Use of FP biometrics is then used to identify the responsible individual.

9.5.6 Signature Support to Others

Provision of WTI information assists in field testing and training. It provides media and reports to governmental science and technical intelligence and R&D training programs and the biometric enrollment of witnesses, specifically:

- WTI information and material collected in theater aids ISR field testing in support of CCIRs. ISR field testing ensures correct sensor development and selection of sensor, interpretation of data, and blending of products within the targeting process
- WTI information is used in the production of training DVDs and courses that provide the current battlefield picture for those executing and preparing for operations
- WTI analysis provides crucial data used to identify technical requirements that support countermeasure and signature development
- WTI analysis provides information used to produce biometric matches, which enable placement of individuals on watch lists

CHAPTER 10
WTI Analysis and the Intelligence Process

"Successful use of ISR against insurgent IED efforts requires organizational structures and processes that allow information to be acted upon quickly enough to be effective."[172]

"As a relatively inexperienced Battalion Intelligence Officer, I deployed to Helmand Province, Afghanistan, the year the Marine Corps led the largest air-ground operation since the Vietnam War. Operation Moshtarak targeted Marjah in early 2010 as key terrain for controlling the fertile Helmand River Valley. The region financially supported the insurgency through the lucrative opium trade and Marjah was single largest poppy-producing area in the world. Marjah was a melting pot of sorts; not just for people but also for information, ideas, and insurgent TTP. Before Operation Moshtarak, coalition forces remained noticeably absent in Marjah and the area became a breeding ground for storing, fabricating, and transporting IED material and components.

As a young Intelligence Officer assigned to an infantry battalion … my job was to serve the Marines and the commander with timely and accurate intelligence about the enemy, terrain (including the human and political), and the weather. I also understood that IEDs would be a significant and persistent threat to our operations.

What I did not understand and what I was not prepared to do was leverage existing frameworks and methodologies to target the number one killer of Marines and sailors in our battalion. I was comfortable with creating collection plans that targeted named areas of interest based on rudimentary pattern analysis overlaid with the other intelligence or collection capabilities … (e.g., HUMINT, SIGINT, Scout Snipers, and Ground Sensor platoon). However, I was completely unaware of how we, as a maneuver battalion, were providing the raw materials for much larger collection efforts in support of the WTI process.

It was not until I started receiving feedback from the IED materials our Marines and EOD attachments bagged, tagged, and forwarded to regiment. The raw inputs our battalion was providing facilitated biometric and forensic matches both within and outside our area of operation. All of a sudden … bags of IED components had a name and face. Just as I was starting to understand how it all worked, sporadic matches every couple months turned into weekly occurrences by the end of the deployment. My hope is that there will be a First Lieutenant, a young Intelligence Officer that gets to read this handbook and learn just how important this process is. WTI is a capability that removes our adversaries' greatest advantage — their anonymity."

Captain Eric Chase, USMC

Captain Eric Chase served as the Battalion Intelligence Officer in 1st Battalion, 6th Marine Regiment from 2009 to 2010. The battalion deployed to Marjah, Afghanistan in support of Operation Enduring Freedom in 2010.

[172] Jackson, B., Frelinger D., et al., *Intelligence Support to Counter IED Operations*, RAND Corporation, National Security Research Division, October 2005

10.1 General Description

This chapter describes how WTI analysis fits into the current intelligence process and across the ROMO in future OEs. WTI analytic capabilities and processes are modular, flexible, scalable, customizable, and are forward deployed to support WTI analytical requirements to meet the needs of operational commanders.

WTI analysis follows a fusion-based model to generate weapons threat information and intelligence to affect a wide spectrum of military operations. The intelligence process used in an asymmetric environment requires a dynamic and comprehensive process to transform raw data into actionable intelligence and helps to ascertain enemy capabilities, and operational tempo. WTI information and intelligence is derived from analysis of raw data and materials obtained at the point of collection, from operational exploitation and from analytical exchanges. WTI incorporates analysis from a variety of intelligence disciplines (HUMINT, SIGINT, TECHINT, etc.) and collateral data sources (**Figure 10-1**) to develop specific adversarial weapons-related threat products. These products, when fused into the intelligence and operational planning process (S/J-2&3), assist the commander in decision making by providing historic and current enemy threats and capabilities. WTI analysis also attempts to predict the future impact of improvised weapons and IEDs used in an asymmetric environment.

The WTI intelligence process is active and flexible to adapt to the enemies' continually changing TTP and support commanders' tactical and operational requirement for rapid decision making. WTI analysis expedites interpretation of raw data to produce actionable intelligence that determines enemies, their capabilities, and intentions. The speed of WTI analysis is critical in transitioning from a reactive and primarily defensive posture, to a proactive, offensive posture.

The Value of Intelligence Analysis in WTI

"In October 2011, the Department of Justice unsealed an indictment describing the illegal export of electronic devices to Iran. Four men from Singapore had purchased 6,000 radio frequency (RF) modules through a Singapore front company which were forwarded to Iran through third countries and ended up in IEDs in Iraq. Between 2008 and 2010, the U.S. military had recovered 16 of the RF modules from IEDs in Iraq. By exploiting the recovered IEDs, the U.S. government was able to trace the RF modules by serial number from the United States to Iran and then to the IEDs in Iraq. This success is a good example of the strategic implications of technical exploitation — in this case exposing third country support to an insurgency — and the importance of a continuum from collection through out-of-theater exploitation with linages to the broader intelligence community."[173]

10.2 Joint Intelligence Preparation of the Operational Environment (JIPOE)

JIPOE is a systematic and continuous process of evaluating the threat and environment of a specific area. WTI plays a significant role in the JIPOE process and allows the IC to better "see the

[173] R3 Strategic Support Group, "The Value of Technical and Forensic Exploitation," draft paper prepared for the Commanding Officer, Naval EOD Technology Division, undated.

Enemy” and understand the threat. Evaluating the threat of improvised weapons and IEDs relies heavily on the information gleaned from EOD and WIT collecting material and determining the tactical characterization and technical categorization. This information is valuable for producing a realistic intelligence assessment to include an evaluation of the threat’s strengths, weaknesses and vulnerabilities. JIPOE is a continuous reassessment of the ever-changing WTI architecture to include HN judicial JIPOE.

WTI assists in characterizing the OE by determining the types of improvised weapons and IEDs used in the AO and associating them to specific insurgent organizations. As an example, characterizing the electronic environment produces known cellular communications systems and other electromagnetic signatures insurgents can use to program switches in IEDs. Describing the effects of the OE and synchronizing it with electronic warfare analysis provides another layer of technical information linked to threat analysis to enhance FP measures. Linking improvised weapon device switches with tactical design and terrain analysis helps identify likely areas the enemy will employ similar improvised weapons and enables predictive analysis. Further terrain analysis is helpful to identify choke points and areas that allow the enemy to employ hoax devices to target first responders with secondary and tertiary devices.

The benefits of WTI allow the commander’s staff to evaluate the threat and develop threat models and threat analysis layers. Threat models linked to IEDs and improvised weapon systems with characteristics of the battlefield, and, more importantly terrain and civilian demographics, enables staff members to narrow down the type of improvised weapons and their respective tactical employment in their AO. The use of WTI data enables the commander to determine enemy network size and link key individuals, using factual data, to a place and time. His information is time sensitive relative to the commander’s targeting cycle.

10.3 Tools and Data Sources

WTI analysis fuses scientific, technical, and forensic examination of recovered information and material with other sources of information and intelligence to produce formal intelligence products used to support targeting, FP, material component sourcing, support to prosecution, and signature characterization. Intelligence products that address CCIR and priority intelligence requirements and that may result in recommendations to adjust collection plans at the tactical level may also incorporate WTI. Leaders at the operational and strategic levels use WTI analysis, often fused with other IC products when reviewing OPLANs, orders, and standing policies.

Figure 10-1 depicts the range of data sources currently available and used by WTI analysts to produce WTI products.

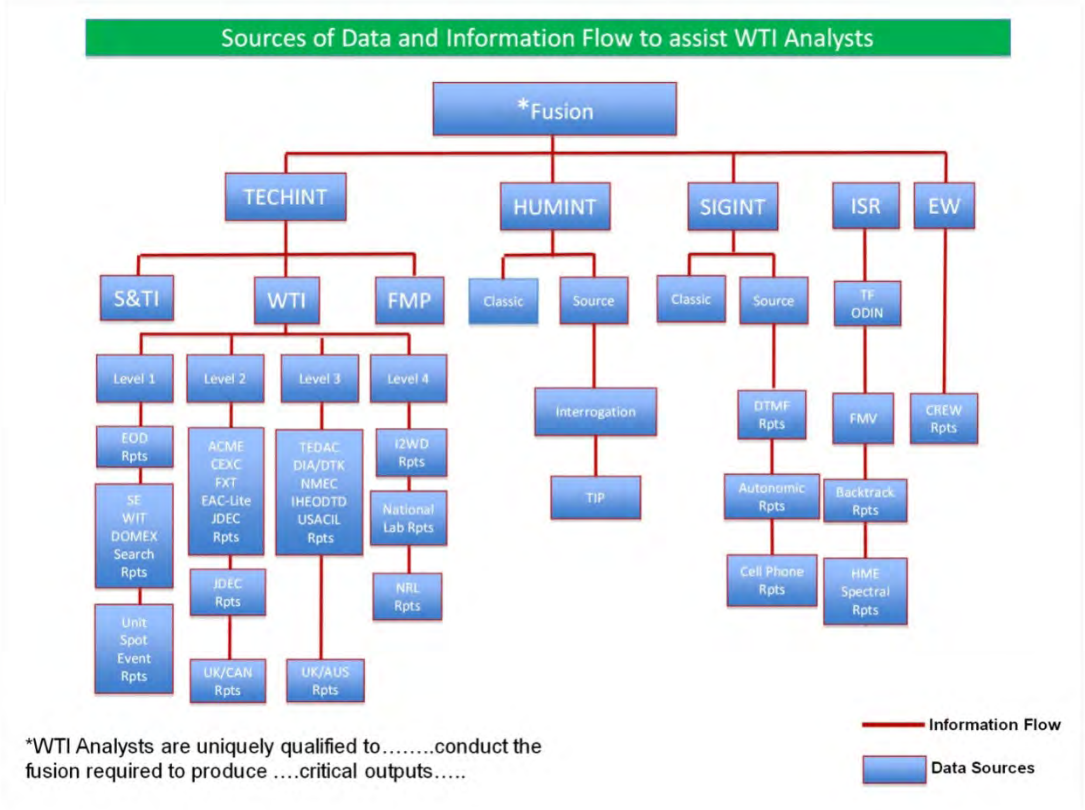


Figure 10-1. WTI Data Sources. *WTI fusion of exploitation information and traditional all-source analysis produces intelligence that supports the critical outcomes of WTI.*

10.3.1 Enabling Reports, Data Sources, and Tools Used for WTI Analysis

10.3.1.1 Tactical

- SPOT and incident reports in Tactical Ground Reporting system, Command Post of the Future, CIDNE
- Search and Site Exploitation reports created on Asymmetric Threat and Technical Analysis Casebook (ATTAC)[174]
- EOD reports (Level 1) created on ATTAC; stored in CIDNE

10.3.1.2 Operational

- FXT and EAC-Lite reports in CIDNE and Special Operations Exploitation (SOFEX)
- Joint Task Force Augmentation Cell (JTFAC) in Special Operations Command

[174] ATTAC provides the operator an automated capability to document and storyboard an incident. ATTAC goes beyond diagramming, providing a full field reporting solution that includes data entry, digital evidence management, satellite imagery, diagramming, and quick, thorough reports output for the government sector

- DOMEX (CELLEX, MEDEX, and Document Exploitation [DOCEX]) reports in Harmony
- Interrogation reports
- SIGINT TECHREPs
- HUMINT reports
- Afghanistan Captured Material Exploitation; CEXC reports in CIDNE/WTI Exploitation Analysis Tool (WEAT)

10.3.1.3 Strategic

- Distributed Common Ground System-Army (DCGS-A)
- Harmony
- BI2R
- NGIC Worldwide IED Incident database
- TEDAC data in the Explosive Reference Tool
- ATF worldwide IED data in DFuze
- I2WD Intelligence Data Elements Authorized Standards (IDEAS) and NSWC IHEODTD support to CREW
- National research labs
- Current Tools and Data Sources in Use
- NGIC Profile and network analysis database
- Joint EOD Decision Support System
- Analyst Notebook
- WEBTAS
- Palantir
- ORA Software for SNA, dynamic network analysis, link analysis
- IED Electronic Analysis System (IEDEAS)

10.3.1.4 Tools in Development

- DCGS-A JIST)
- MAP HT
- Globally Leveraged Integrated Data Explorer for Research (GLIDR)

10.4 WTI Analysis Objectives

- Provide commander with timely intelligence and data to support the decision making process. Information provided includes historical and current adversarial weapons systems, improvised weapons, the overall IED threat in an AOR, weapons tactical characterization and technical categorization
- Provide specific weapons-based (e.g., conventional, improvised WMD) intelligence to address critical command issues such as FP, targeting, material movement and facilitation, and support to prosecution outcomes within the lines of operation
- Extract and combine relevant technical, forensic, and biometric data to produce specific products that attribute an individual or entity to a specific incident(s) or weapon system
- Support ISR collection tasking and considerations
- Support identification; re-affirm, or deny NAI within AOR. An NAI is a point or area along a particular avenue of approach, through which enemy activity is expected to occur. Activity or lack of activity within an NAI helps to confirm or deny a particular course of action
- Develop technical link pattern and trend analysis to identify, track, and target a specific individual and associated enemy groups
- Identify technical advancements or degradation of improvised weapon and IED technology
- Influence and inform the acquisition and material development process.

10.5 Intent

The intent and focus of a WTI analyst can be divided into two subsets:

- Situational awareness
- Attribution

Outputs in each subset directly or indirectly influence the outputs of each other. Additionally, certain outputs from one subset may not be obtainable until requirements of the other are met.

10.5.1 Situational Awareness

WTI situational awareness is fluid and requires current and predictive knowledge of an incident or event, including signature analysis. The framework and methodology currently in use was established and continually adjusted during OIF and OEF. Future conflict poses unique challenges that will alter this methodology. The basic methods discussed below are flexible and apply to any conflict or operation. WTI situational awareness breaks down into the following sub-categories:

- Profiling
- Pattern analysis
- Route assessments

- Area assessments
- Migration of device

10.5.1.1 Profiling

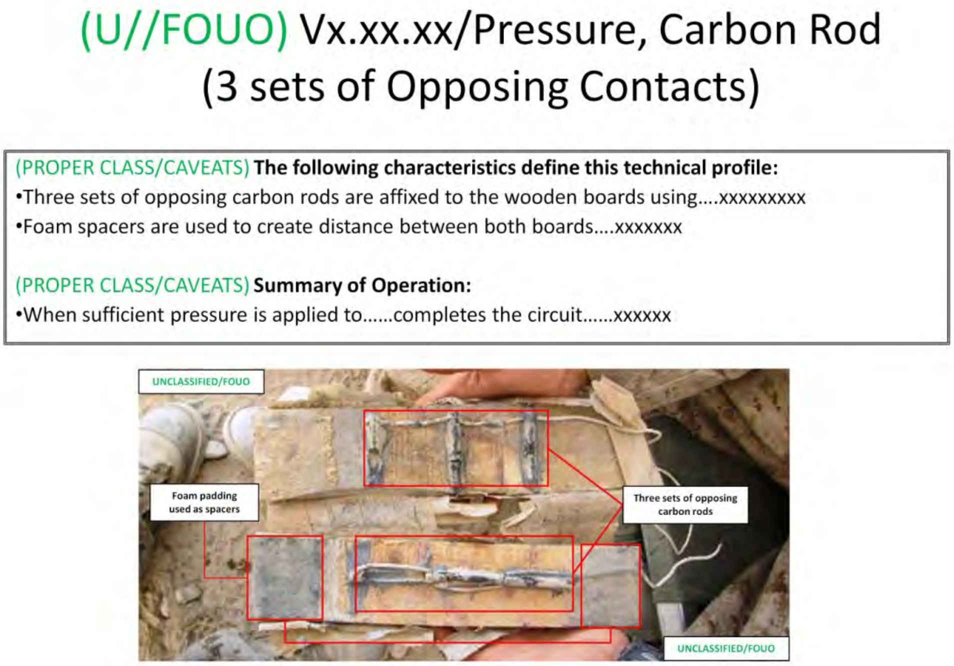
During the WTI planning phase a device profile and naming convention using the WTI IED Lexicon is established. Although there currently is no joint/interagency universal naming convention within the IC, LE community or the Armed Services, CITP/WTI developed a switch profile naming schema that is widely accepted and used in Afghanistan and throughout the WTI community.

Device profiling technically structures and categorizes IED information and data using the WTI IED Lexicon and a universal schema — a relational database used to identify specific signatures associated with improvised devices. Use of the WTI IED Lexicon and an accepted universal schema provides a common framework and vocabulary to address the broad spectrum of IED employment scenarios, the variety of IED devices and their critical components (such as types of switch, initiator, main charge, container and power source), distinguishing features, construction techniques, TTP, etc. Although device profiling was created for IEDs, it is also applicable to other improvised weapons.

A common framework for conducting device profiling ensures standardized data and reporting, and reduces ambiguity when analyzing multiple or similar devices and components. During detailed technical categorization of improvised weapon systems and explosives, groups of signatures are identified that enable analysts to determine unique components and construction techniques and to assist in determining attribution and material sourcing.

The most commonly analyzed IED component is the switch. The device profile is often represented using an alphanumeric code ascribed to key features of each component as depicted in **Figures 10-2 and Figure 10-3**. The compilation of key features creates a unique and discernible profile. This profile may include notable unique construction methods that may be associated or disassociated with previously analyzed components from other devices.

Establishing device profiles is typically the first step in establishing the current operational picture within an AOR. Basic device categorizations are elemental to all products that support commanders' situational awareness. In addition to developing commanders' situational awareness, WTI analysts use products developed through device profiling when conducting signature analysis to identify improvised weapon makers.



(U//FOUO) Vx.xx.xx/Pressure, Carbon Rod (3 sets of Opposing Contacts)

(PROPER CLASS/CAVEATS) **The following characteristics define this technical profile:**

•Three sets of opposing carbon rods are affixed to the wooden boards using….xxxxxxxxx

•Foam spacers are used to create distance between both boards….xxxxxxx

(PROPER CLASS/CAVEATS) **Summary of Operation:**

•When sufficient pressure is applied to……completes the circuit……xxxxxx

UNCLASSIFIED/FOUO
Foam padding used as spacers
Three sets of opposing carbon rods
UNCLASSIFIED/FOUO

Figure 10-2 Generic Example of a Switch Profile *(Photo Credit: NGIC)*

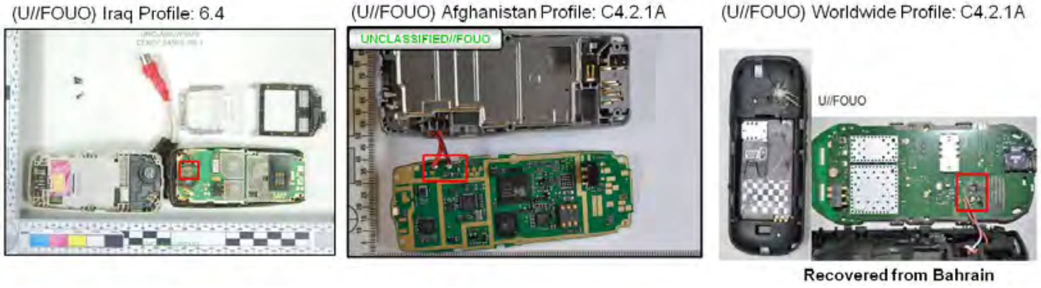

(U//FOUO) Iraq Profile: 6.4
(U//FOUO) Afghanistan Profile: C4.2.1A
UNCLASSIFIED//FOUO
(U//FOUO) Worldwide Profile: C4.2.1A
U//FOUO
Recovered from Bahrain

Figure 10-3. IED Switch Profile. *This shows Notional Universal Alphanumeric Profiling Methodology to depict similarities in device types, functioning, construction techniques and construction materials. (Photo Credit: NGIC CITP)*

10.5.1.2 Pattern Analysis

Contextual data collected from Level 1 reports (e.g., SPOT reports, patrol debriefs, site exploitation reports, PRETECHREP, COMTECREP, EOD, and WIT reports) provide essential information to enable command and staff to detect, determine, and help categorize enemy activity. The data contains technical and tactical information the staffs can break down into categories. Each data category presents specific enemy patterns that US and coalition forces can exploit to predict future actions. The enemy targets specific formations, vehicles, and infrastructure with precise devices in prescribed areas because of intent, opportunity, and capability. Pattern analysis is a method to break down each occurrence to study and analyze friendly and enemy cycles to prevent future attacks, target the enemy, and break the cycle. Pattern analysis becomes less useful when information gaps develop as a result of transitioning responsibilities and LE functions to HN as was experienced in Iraq and currently in Afghanistan. Liaisons, trainers, and good relationships can help mitigate these gaps.

There are several different ways to conduct pattern analysis. This handbook does not cover all methods. One method is use of a circle plot chart (**Figure 10-4**), which is a visual matrix displaying the time of an event and how it relates to other events in the AO. Another is an area map that displays where an event occurred in relation to other activity such as cache finds, site exploitations, and the locations of other related intelligence. These charts provide a visual representation of possible supply routes, enemy reconnaissance positions, and cellular telephone towers; all provide valuable information to determine enemy intent, opportunity, and capabilities for future attacks.

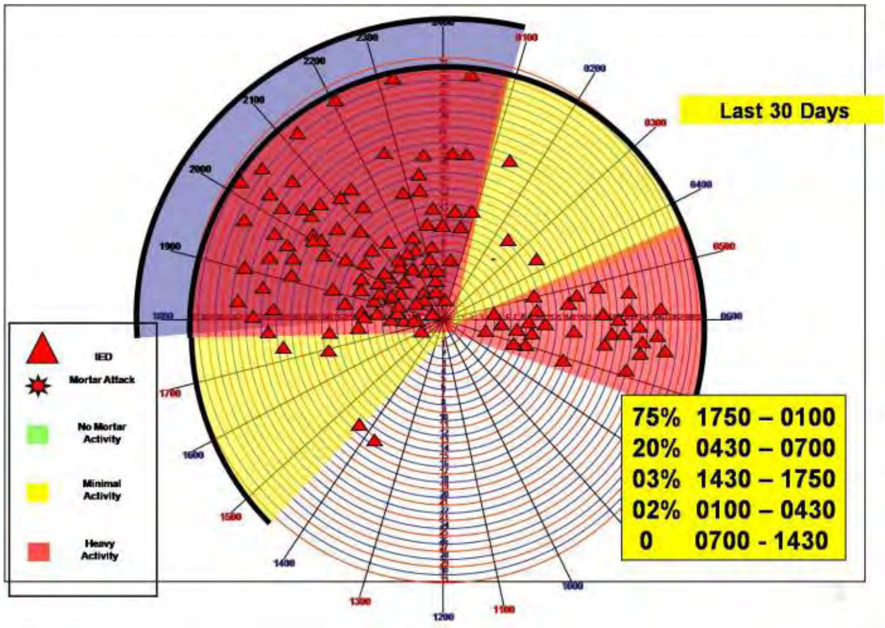
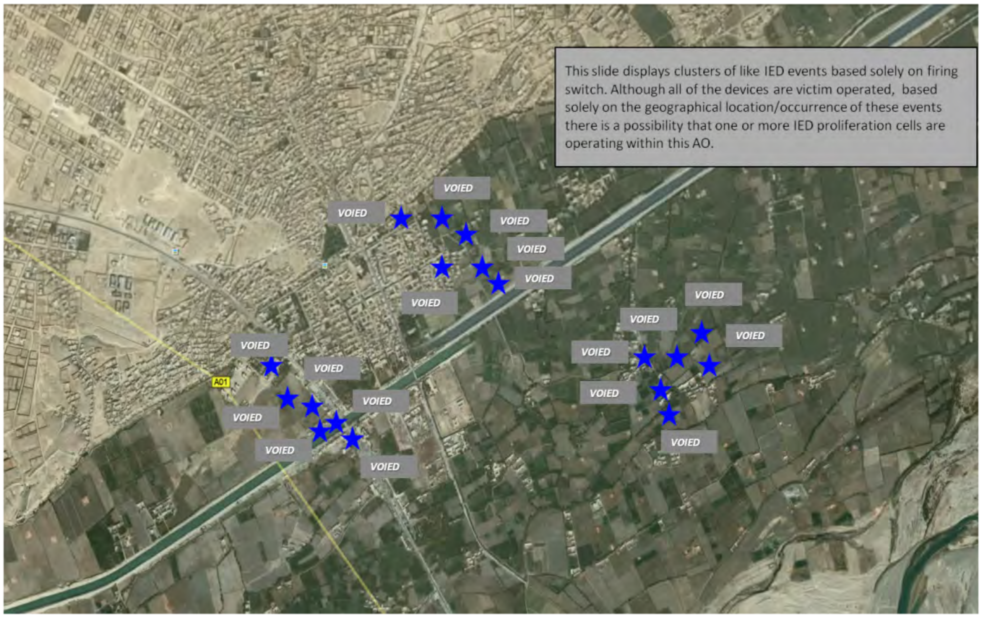


Figure 10-4. Circle Plot Chart. *Pattern analysis helps discern the frequency and timing of IED activity in an NAI. (Figure Credit: CJTF Troy)*

Through WTI analysis, known geographic locations of exploited devices, caches, etc. and their associated device profiles are overlaid on charts to depict weapon activity in a region (**Figures 10-5 and 10-6**) and to help define NAI and target areas of interest (TAI) boundaries. As previously stated, NAIs are geographical areas where enemy activity is expected to occur. TAIs are geographical areas where friendly forces can acquire and engage high-value targets. TAIs are not typically assigned to C-IED activity but focus on high-value insurgents such as those who provide C2 and operational guidance to improvised weapon assemblers, emplacers, and employers.

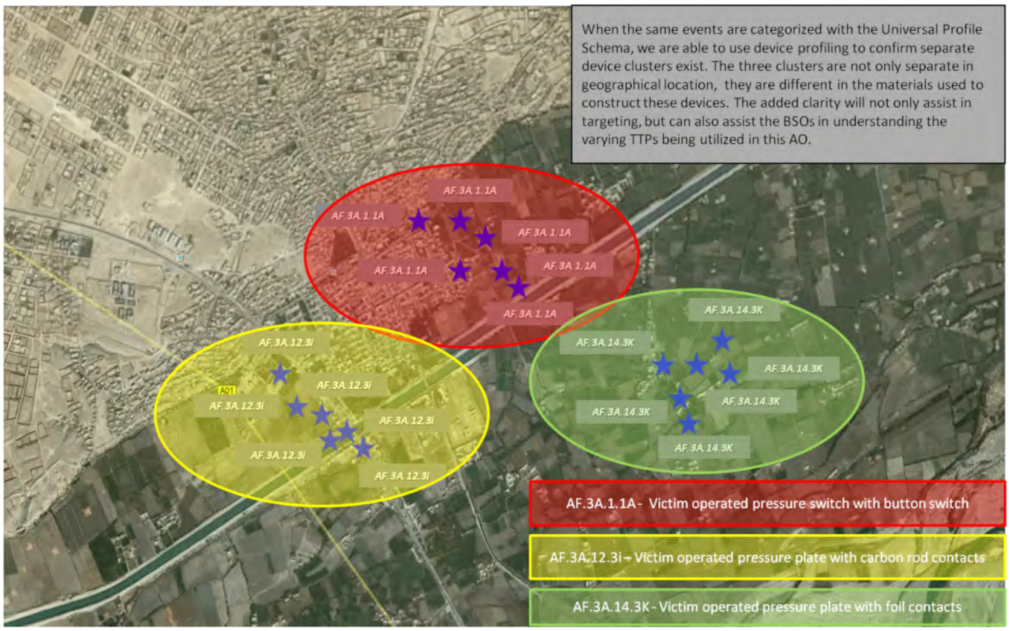
Through analysis of statistical information provided by reach back capabilities, in theater analysts such as those that stood up and surged to support OIF and OEF (CITP and ORSA), can better delineate NAIs. ORSA access multiple databases and modeling tools to conflate and analyze data to provide decision makers and analysts with a near-real-time operating picture of improvised weapon trends and insight into C-IED effectiveness. Additionally, the COIC provides in-depth products that detail pattern of life analysis, compounds of interest, and significant activities

(SIGACT) monitoring to compile other in-depth products supporting AtN operations in theater. This information, when tied to database information entered by WTI analysts who discern device profile characterization, enables network pattern analysis and targeting. This shows correlations between devices, attacks, and personnel to develop a picture of networks, and their support arms to target associated personnel and IED cells.



This slide displays clusters of like IED events based solely on firing switch. Although all of the devices are victim operated, based solely on the geographical location/occurrence of these events there is a possibility that one or more IED proliferation cells are operating within this AO.

Figure 10-5. WTI Event Plot Using Pattern Analysis to Depict Locations of IED Activity *(Graphic Credit: A-T Solutions)*



When the same events are categorized with the Universal Profile Schema, we are able to use device profiling to confirm separate device clusters exist. The three clusters are not only separate in geographical location, they are different in the materials used to construct these devices. The added clarity will not only assist in targeting, but can also assist the BSOs in understanding the varying TTPs being utilized in this AO.

AF.3A.1.1A - Victim operated pressure switch with button switch

AF.3A.12.3i – Victim operated pressure plate with carbon rod contacts

AF.3A.14.3K - Victim operated pressure plate with foil contacts

Figure 10-6. Map of IED-Related NAI *(Graphic Credit: A-T Solutions)*

10.5.1.3 Route Assessments

Route assessments give a commander situational awareness of improvised weapon activity within a given AOR. Level 1 and Level 2 WTI exploitation reports help to determine the most likely enemy course of action for a route. Geographic conditions along the planned route are also taken into consideration when assessing routes. Analyst use this information to identify probable natural and manmade ambush points, chokepoints, enemy spotting positions, and cover and concealment possibilities. The combination of Level 1 and 2 reports from past improvised weapon incidents, geographic considerations, and pattern analysis assists the WTI analyst in depicting the most recent improvised weapon operational picture and probable enemy targeted areas. They also assist commanders in developing ISR considerations for an operation.

10.5.1.4 Area Assessment

An area assessment encompasses a range of topics and is dependent on the commander's intent and taskings. The parameters of any area assessment are modified based on intent and available resources. An area assessment is tailored to include tactical through strategic level exploitation reports, insurgent network structure, and political climate. At a minimum, an improvised weapon-centric area study for a particular time period and area includes historical data regarding number of improvised weapons attacks, improvised weapon find/cache sites and hoaxes, and enemy targeting; the three to five most prolific improvised weapon switches; most casualty producing switches; average explosive composition and weight of main charge; anomalous improvised weapon incidents; ambush/choke points; known categorized complex attacks; and recent biometrics. An area assessment depicts these findings on a map or image with known blue force points of interest (e.g., main supply route, FOB, Contingency Operating Base) identified to help clarify and identify the IED problem within the commander's prescribed area.

The two photographs depicted in **Figure 10-7** provide similar data; however, the photograph on the right organizes the data by switch profile; the blue highlighted areas employed victim operated, pressure, crush wire switches; the red area employed pressure plates using saw blades, and the yellow area employed the use of passive infrared sensors. Profiling identifies device construction methods, and materials, as well as the devices' methods of operation. At the tactical level, device profiling informs the patrol leader who is then better prepared to plan and execute his mission because he or she more fully understands the threat. In addition, profiling provides increased awareness needed to target engagement areas, update TTP, and efficiently distribute and employ countermeasures. When resources allow, the WTI analyst provides the enemy's most likely course of action/most dangerous course of action (MLCOA/MDCOA) within the area.

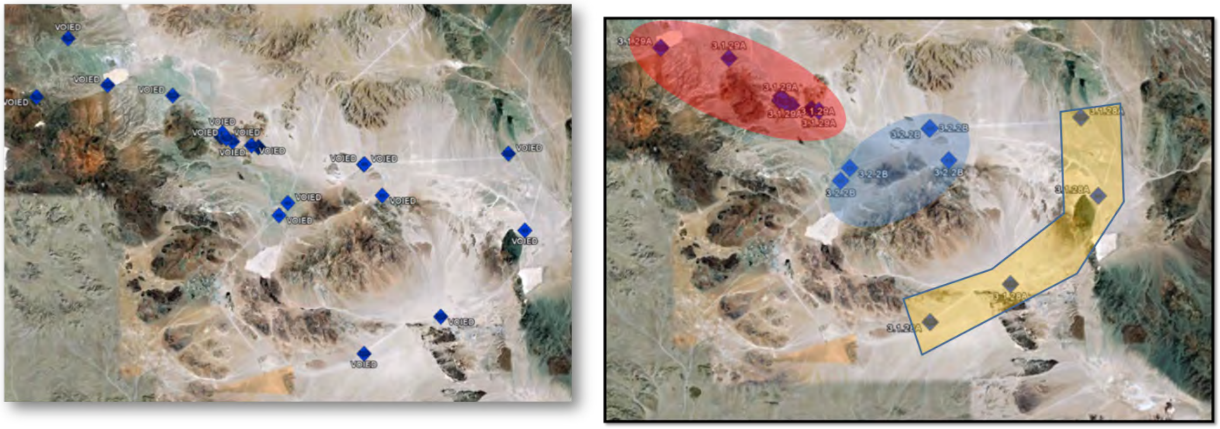


Figure 10-7. Area Assessments. *Devices found and labeled using the WTI IED standard naming convention (left); device profiles make improvised weapon patterns more apparent (right). (Photo Credit: A-T Solutions)*

10.5.1.5 Migration of Device

Migration of device, either affirms or negates the presence of a previously unseen device within an area. Migration of device functionally falls under area assessment. To accomplish this, a general improvised weapon picture for an area must be established. After the analyst knows the historical patterns and resources for an area, he/she conducts a similar area assessment for different periods of time. The analyst notes anomalous but repeated circumstances and IED switches that appear in one assessment but not the other. The anomalous device should be seen more than once because in insurgent warfare, a single, sporadic incident is probable. If a previously unseen device is identified in an area, the analyst attempts to ascertain its origin. At a minimum, analysts examine areas that border their focus area, historical intelligence reports, and other information pertaining to new individuals that have recently moved into the area. They also examine legacy cache sites in the prescribed areas and within the border areas.

Migration of device into new areas will more than likely exhibit different associated TTP and resources. A newly migrated device can change facilitation routes, personnel, and trainers. Analysts advise commanders about migration of device assessments quickly to give them time to adjust FP measures and possible targeting efforts.

Situational awareness outputs and contributions include:

- Identification and categorization of incidents, devices and associated components
- FP enhanced by area assessments
- Improvised weapon and enemy TTP migration and evolution
- Cache assessment
- Route assessment and planning
- Future operations planning support by providing identification of the improvised weapons' MLCOA/MDCOA

- WTI and improvised weapon and IED-specific NAIs
- Identification of training and manufacturing facilities
- Development and improvement of material and equipment such as ECM and armor

10.5.2 Attribution

Attribution is the process of establishing an insurgent or insurgent groups' signature by identifying device and incident characteristics and linking them through traditional all-source analysis, forensic and biometrics enabled intelligence. This handbook contains information derived from the lessons learned during OIF and OEF and focuses on signature analysis that leads to the following:

- Establishment of individual or group improvised weapon maker signatures
- Evolution and migration of individual or group improvised weapon maker skill set
- Identification/recognition of the introduction of or migration of improvised weapon maker or group into a new area (e.g., immediate or global)
- Identification of device profiles and later weapon maker signatures
- Identification of technically specific source directed requests (SDRs) during the interrogation process
- Identification of the dynamics of the associated group with the specific threats and the people, places, and materials associated with the profile
- Support to prosecutorial efforts by providing technical, individual, and group signature and incident specific information
- Identification of the sourcing of improvised weapon systems and/or their components

10.5.2.1 Establishment of Individual Signatures

WTI analysts determine unique weapon-maker signatures by analyzing specific exploited weapon information and material and linking it to a person through forensics and/or other all-source intelligence. Unique similarities in device construction techniques and methodologies, materials used in device construction, in conjunction with TTP used for its employment and its intended target, create unique signatures for that specific weapon assembler or emplacer. WTI device profiles establish the foundation for initial comparison with other devices as depicted in **Figure 10-8.** The device profile provides the analyst a smaller subset of incident information to mine for unique individual signatures.

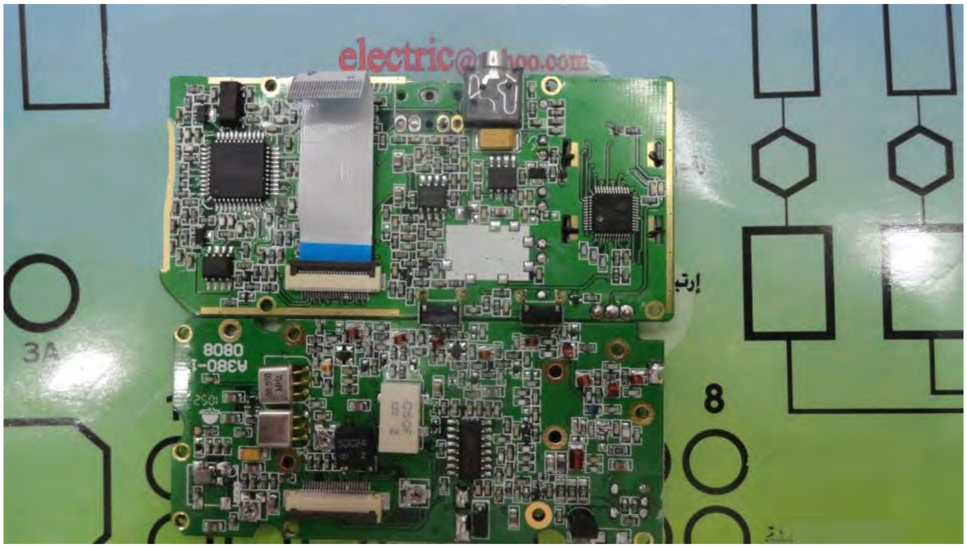


Figure 10-8. Example Circuit Board. *Videos for use by Syrian Rebels to produce electronic initiation and arming systems for IEDs feature this circuit board. (Photo Credit: RAPID Report 2304-1)*

Attribution can result from comparison and matching of forensically collected fingerprints and/or DNA from a weapon or collection site with known base samples maintained in a biometric database. While a device with a biometric match to an individual is the simplest way to establish attribution, other intelligence disciplines (e.g., HUMINT, SIGINT) and technical and forensic exploitation such as latent-to-latent fingerprint analysis, may also provide sufficient information to identify an improvised weapon maker's signature.

Often prints and DNA recovered during exploitation are attributed to an Unknown Biometric Identity (UBI) or someone with which identification cannot be attributed within the biometric databases. Although the identity of the individual may be unknown, his prints or DNA are often attributed to other devices or events within that area. This information reaffirms the signature association and the area of operation for the UBI. This defined area is used to direct biometric collection operations, potentially identifying the UBI for future targeting.

After the improvised weapon incident and related material has been exploited, the WTI analyst applies a holistic approach to determine the weapon maker's signature. The WTI analyst defines the individual's signature by identifying distinct values resulting from some of the following questions:

- Basic dimensions of device?
- Graphical markings on the inner or outer portion of device (e.g., pen or pencil markings)?
- What is used to secure the components of device together (e.g., hot glue, tape, or wire)?
- How is the device constructed?
- How is the glue, tape, or wire used?
- What type of wire is used?

- Is the wire sheathing shaved back from the wire contact points? If so, how far back is it shaved?
- Are there any visible notches in device components?
- If there are visible notches, what is spacing pattern between each notch?
- Are wires spliced?
- If there are electronic components, what is the original nature of the components (e.g., COTS, custom made, or COTS that have been modified)?
- If there is an electronic component that uses radio frequencies, what are the specifics of the electronic components that control activation of the signal, and what are the specifics of the signal?
- How is the tape wrapped around the device?
- How are the wire contacts attached to the switch?
- Exactly where are the fingerprints and/or DNA found on the device? (The placement of fingerprints and/or DNA is critical to determining the individual's role and influence of the improvised weapon.)
- Type and make of the initiator (igniter or detonator)?
- Type and size of main charge?
- Type and voltage of power source?
- Type of container?
- Type of any enhancement used?
- Explosive composition (HME versus military munitions)

The above are just some of the variables used to determine a signature.

After a WTI analyst identifies and characterizes enough weapon related variables, he can begin to determine a signature. Using the signature, the analyst queries multiple databases (i.e., WEAT, CIDNE) to identify other devices with the same or similar signatures for a given area and time period. After an analyst has confidently attributed other devices and events to a specific person/network, the analyst maps the insurgent network using simple tools such as Analyst Notebook, illustrated in **Figure 10-9**. The WTI analyst graphically represents the role and relationship an individual has with a particular device and potentially associated persons, groups, or similar events, and creates a graphic product which can be used to support targeting, prosecution and network analysis.

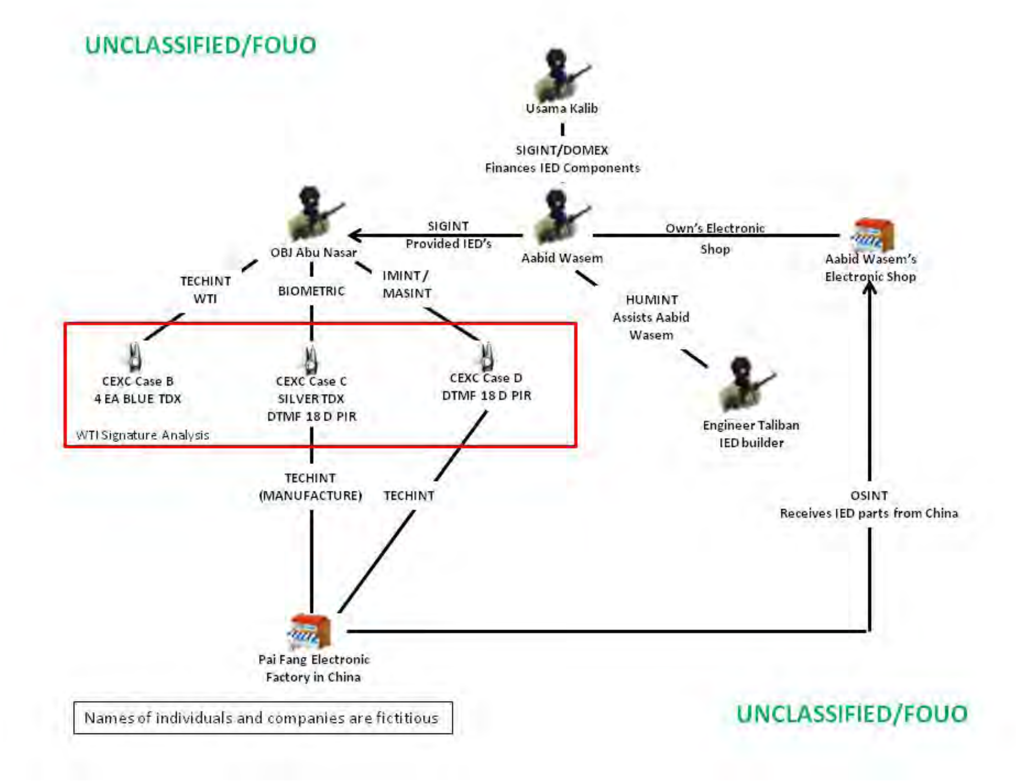


Figure 10-9. Page from Analyst Notebook Detailing Links Between Individuals and Improvised Weapons *(Figure Credit: NGIC)*

The marked physical characteristics of a device alone do not always determine the signature of the individual or group who made or emplaced the improvised weapon; TTP employed for placement, terrain, and target selection also play a critical role in determining attribution. For proficiency and safety reasons, these TTP are often mimicked by all the members within the same group who are typically trained by the same trainer. To make apparent the more nuanced characteristics or discernible behavioral patterns of a signature, the WTI analyst uses all levels (1 through 5) of exploitation. Other sources of attribution information include:

- Reliably sourced HUMINT (e.g., interrogation reports) with a clear description of the device and/or incident
- SIGINT (e.g., landline and cell phone plus striping of data) traffic with a clear description of the device or incident and association to an individual
- MEDEX imagery (e.g., video) of a person or persons constructing or emplacing a device, IED printed circuit board software, and insurgent IED/improvised weapon manuals and schematics with corresponding assessments

10.5.2.2 Identification of Group or Cell Signatures

The location a device was discovered, along with its identifiable signatures, whether cached or emplaced for attack, helps to define geographic boundaries of insurgent groups and, potentially, the members of these groups. Cache analysis is a key component to determining insurgent cell and group boundaries. A cache, whether temporary or permanent, usually contains multiple devices from multiple assemblers, and these devices are all being used and emplaced by the same groupg. The type of cache can indicate the size and complexity of the group using the devices.

Likewise, an area of operations defined through other intelligence disciplines for a group or cell can provide attribution to a device signature in this defined area. Although differences exist between the OIF and OEF theaters, enemy groups or cells often occupied and operated within specific territories. Even though the group in one territory works with a group in a neighboring area, the group with territorial responsibility controls almost all operations that occur inside its borders. Thus, IED operations are often attributed to the same group responsible for other criminal or insurgent activities inside the territory, as reported in the other intelligence disciplines.

10.5.2.3 Evolution of Improvised Weapon Construction

For safety and proficiency reasons, low to moderately skilled improvised weapon makers typically adhere to the same production methodology until they gain a level of comfort, experience a change in resource availability, or until blue force TTP, or countermeasures necessitate their change. Because of a bomb maker's comfort and familiarity with the weapons construction process, weapon modifications or enhancements are usually insignificant and seldom change the functionality of the weapon. Similarly, changes in resource (components and materials) availability often results in material substitutions that rarely alter the functionality or basic design of the improvised weapon. Although adaptations resulting from enemy observation of blue force TTP or countermeasures can be extreme (such as abandonment of a specific device design in a particular area), minimal changes in weapons design may be all that is required for successful adaptation in the evolution process.

10.5.2.4 WTI Contribution to HUMINT Collection

A WTI analyst contributes to SDR and HUMINT Directed Requirements to gain information from HUMINT collection that can lead to the identification of facilitation routes, key personnel, hierarchal connections, and planned enemy actions. Although those involved with HUMINT collection operations are generally aware of collection priorities through established standing collection requirements, this information does not always meet the needs of analysts to provide a meaningful assessment. The analyst often provides context, background, or technical expertise to the collection officer to help guide his line of questioning. If a source, whether a detainee or someone paid for information, has access to needed information, the analyst creates a SDR to provide questioning guidance about what the source already knows or what information he may be able to acquire. The WTI analyst, in particular, has a specialized knowledge of improvised weapons that most in the IC do not. As a result, the WTI analyst provides critical guidance through SDRs to interrogation support packages of known improvised weapons producers or sources in place and with access. In turn, information obtained from SDRs assists in ISR collection efforts, information operations, basic battlespace owner situational awareness, and the prosecutorial process.[175]

[175] NOTE: There exists a need for the classified addendum, and focused training on WTI against the asymmetric weapon in today's complex technical fight. The US Army has no billet or a training plan for the WTI discipline, despite the improvised weapon being the primary weapon used against coalition forces in OIF and OEF. Today, the IED is a global weapon, employed in any nation, against any chosen target. Certain nation states support use of the IED, and the capability is disseminated freely on the Internet and in writing. The global fight can only be managed with a full understanding of the history of devices, complete data and tools for analysts, and the IC's ability to share information between parties, including conventional and special operators, LE, and other US agencies.

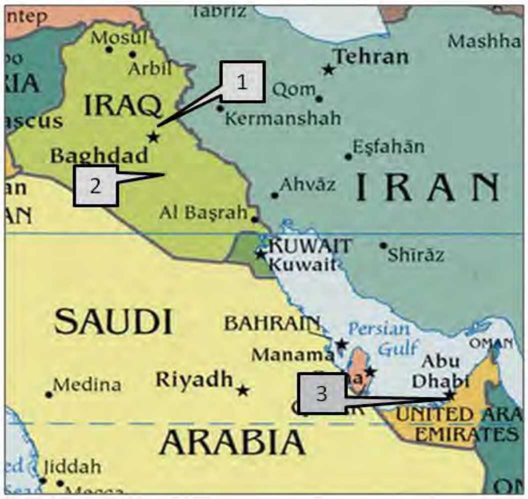
10.5.2.5 Component Tracking Analysis

When an improvised weapon or an IED configuration uses COTS components, analysts use component tracking analysis to support WTI's critical outcome of material sourcing. Component tracking analysis enables analysts to identify improvised weapon construction and facilitation by tracking established supply routes and then linking them to key personnel and nodes. Component tracking is conducted on dual use items such as PVC couplers or microcontrollers, illustrated in **Figure 10-10.** These couplers are common in hardware stores; however, origin labels on their shipping boxes are unique.

Figure 10-10. Typical COTS Microcontroller Component

Civilian companies do not make parts with the intent of them being used in IEDS, so technical information about a component is easily accessible. WTI analytical products inform legitimate manufacturers of potential illegitimate uses for their products and technologies. Intelligence and LE agencies, such as DoS, Department of Transportation, Commerce Department, and FBI, contribute to component tracking analysis efforts (**Figure 10-11)**.

Collaborative Component Tracking



1. May 2007 large EFP cache was received at CEXC. Within the cache with PVC couplers used for EFP's. The couplers were recovered in original shipping boxes with "A&B Group" labels with an origin of UAE on them.
   - Analysts conducted an OSINT search on A and B group with a analysis determination that it was a front company.
2. Extensive search of exploitation db CEXC data base revealed that a piece of a identical label was recovered from a found and cleared EFP in Hilla in 2006
3. WTI analyst collaborated with strategic Intelligence assets and DoS and a Demarche was issued in UAE against A and B group.

Figure 10-11. How Component Tracking Works *(Figure Credit: TECHINT Solutions)*

10.6 The WTI Analyst

Successful WTI analysts have a basic understanding of each of the intelligence fields (e.g., BEI, FEI, SIGINT, HUMINT, and TECHINT) and are skilled at fusing intelligence from each of these fields into cohesive actionable intelligence. WTI analysts play an important role at influencing new methods of collection and exploitation to keep ahead of the ever-changing OE and serve as the conduit between intelligence and the tactical environment. Development of a formalized WTI training program will ensure the WTI analyst skills will be maintained and evolve to meet the future asymmetric threats.

10.7 Interagency Use of WTI-Based Analysis at the 2013 Boston Marathon

In response to the Boston Marathon, federal representatives from the TEDAC and the National Explosive Task Force (NETF) relied on technical and forensic knowledge to examine key photographs, evidence and on-scene reports to identify and exploit key IED components recovered from the incident site. The NETF, comprised of representatives from DoJ, DHS, DoD, and ODNI played an instrumental role in coordinating the rapid integration of explosive expertise with the ongoing LE investigation.

Preliminary exploitation of the crime scenes resulted in identifying components used to fabricate the IEDs, how the devices may have been constructed, and how they likely functioned. Early findings revealed that the two devices detonated less than a block apart and functioned within approximately 10-15 seconds of one another. Rapid technical exploitation determined that each of the two devices likely consisted of a pressure cooker containng a low explosive main chanrge, an electrical fuzing system using components from RC toy cars, electronic speed controllers used as a switch mechanism, and sub-C rechargeable battery packs as the power source. Additional, chemical analysis indicated that the low explosive main charge was consitent with a blend containing nitrate and perchlorate-based oxidizers.[176]

WTI skills and knowledge proved useful in quickly identifying bomb components and their associated operating capabilities which played a significant role in providing expeditious leads, and resulted in early case breakthroughs. **Figure 10-12 and 10-13** are photograhps of evidence collected at the bomb site **(Figure 10-14)** and during further investigation**.**

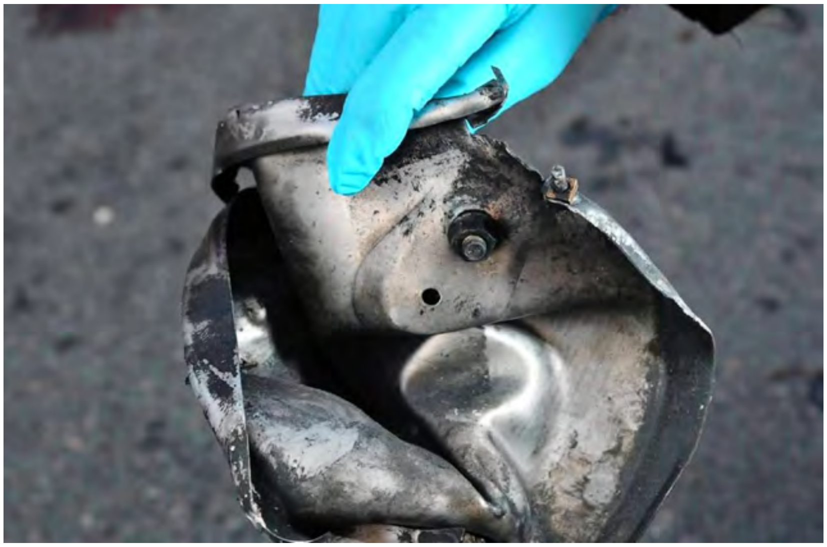


Figure 10-12. Boston Marathon Bomb Scene Picture. *Taken by investigator, this picture shows the remains of a pressure cooker used to contain the IED. (Photo Credit: FBI - DHS Joint Security Bulletin)*

[176] FBI – DHS Joint Intelligence Bulletin, *Updated Information Regarding Likely Components used in Boston Marathon Devices*, April 23, 2013.

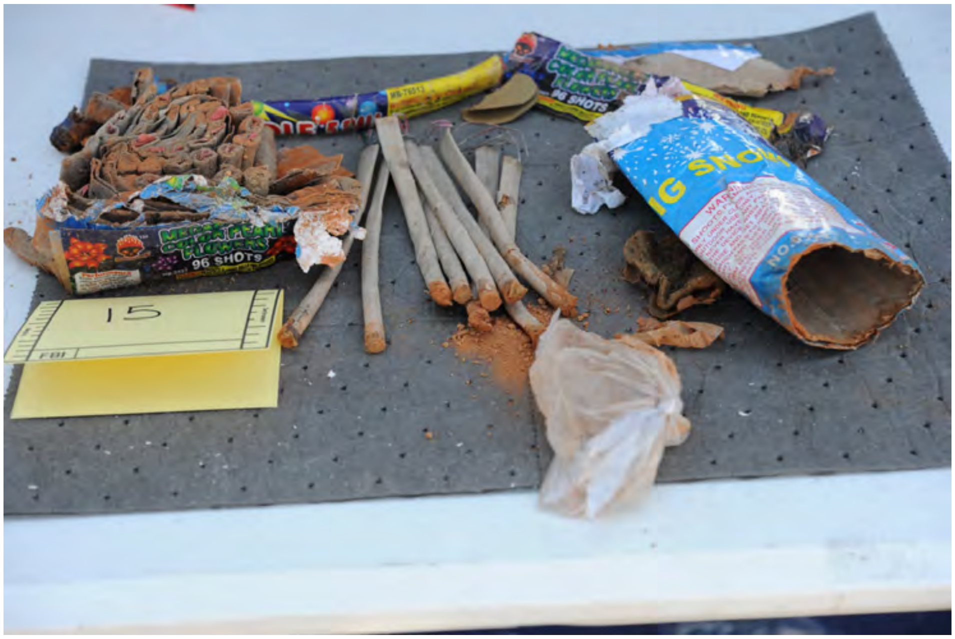


Figure 10-13. Boston Marathon Bomb Site Evidence. *Opened and emptied fireworks were found in the dormitory room of an acquaintance of the suspected marathon bomber. The individual was charged with conspiracy to obstruct justice by conspiring to destroy, conceal, and cover up tangible objects belonging to suspected marathon bomber. (Photo Credit: U.S. Attorney's Office)*

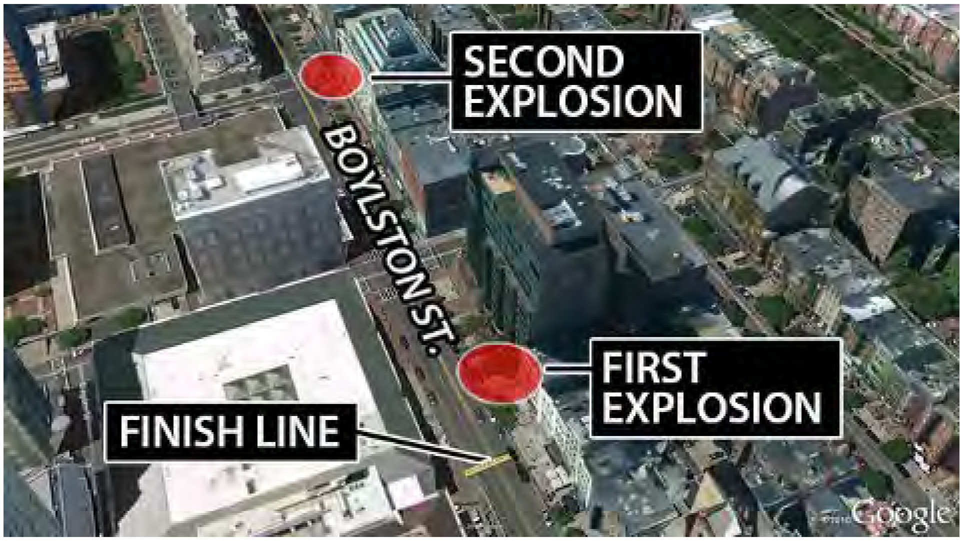


Figure 10-14. Downtown Boston Location of the Two April 2013 Boston Marathon IED Detonations
(Photo Credit: Google)

10.8 Conclusion

WTI analysts provide commanders, at all levels of operation, with timely decision making technical and scientifically supported intelligence and data relevant to the weapons, improvised weapons, overall IED threat and related threat networks in their AOR. This is achieved by:

- Providing specific intelligence products from a range of sources to address FP, component sourcing, targeting, and support to prosecution outcomes within the lines of operation
- Assisting with ISR collection assets tasking and considerations
- Network identification, tracking, and support to subsequent attack
- Creating technical link pattern and trend analysis for specific individuals and larger enemy group identification and placement at an incident

WTI analysts and their skill set are essential to address the full range of conventional, improvised weapons, and WMD on the domestic or international stage.

CHAPTER 11
WTI Information Sharing

11.1 General Description

"Our national security depends on our ability to share the right information, with the right people, at the right time. This information sharing mandate requires sustained and responsible collaboration between federal, state, local, tribal, territorial, private sector, and foreign partners."[177]

The attacks of 9/11 and subsequent terrorist and insurgent activities in Iraq and Afghanistan and around the globe highlight the need to expeditiously and openly share information and intelligence. The sharing of information must occur throughout the DoD and horizontally with the US LE, IC, and international partners. Information sharing enables DoD and its interagency and foreign partners to achieve dynamic situational awareness, enhance decision making, and promote unity of effort at all levels of government when responding to an evolving adversary.[178]

Our adversary's ability to rapidly learn and evolve requires us to understand their motives and methods quickly. This requires a coordinated and synchronized effort throughout the DoD and in conjunction with our interagency and foreign partners. It requires the ability to expeditiously leverage all available information and intelligence to counter the threat. Today's adversaries *"freely communicate, obtain training, share information on tactics, gathering intelligence on potential targets, spread propaganda, and proselytize."*[179] The DoD must be capable of moving faster than its adversaries and be capable of leveraging all sources of information and intelligence to defeat them.

Success against the asymmetric threat at the tactical, operational, and strategic levels will be effective only when WTI data is collected, exploited, analyzed, and disseminated to the greatest extent possible. This requires an information sharing process that facilitates, deconflicts, and coordinates WTI information sharing during collection, exploitation, and analysis, throughout the JIIM community, following a unified process to ensure consistent, comprehensive exploitation and analysis of improvised weapons. Additionally, where appropriate legal authority exits, the sharing of event-related biometric and forensic information offers enhanced opportunity to identify IED threat networks. Information sharing or systems granting greater visibility or confidence facilitate a systematic approach and quality control (e.g., data integrity, perish ability, data duplication) of information and intelligence to support the JIIM community.

Processes, arrangements, and agreements between partner and HNs enhance information sharing and collaboration on DoD initiatives. Any WTI information shared with partner and HNs must be continuously assessed to ensure reliability for use by judiciary, intelligence, military, and other governmental organizations. When possible, WTI products should be developed in HN languages and provided during the transition process to enable civil authorities to continue the fight. WTI products should be developed to support collection, analysis, and dissemination of WTI data for the following:

[177] Office of the President of the United States, *National Strategy for Information Sharing and Safeguarding*, Executive Summary, December 2012, pg. 1.

[178] Department of Defense, *DoD Information Sharing Strategy*, May 14, 2007

[179] National Intelligence Community, *Intelligence Community Information Sharing Strategy*, February 2008, pg. 5.

- Tactical characterization of IED incidents to facilitate the development of C-IED TTP
- Technical categorization of IEDs to facilitate the development of technical countermeasures
- Confirmation of suspects' identities to help support targeting
- Match individual suspects to particular locations, events, or devices
- Link exploited material to provide a picture of origin and movement of components and suspected networks

11.2 Common Language

The growing number and wide variety of communities contributing to the fight against use of improvised weapons (e.g., operational units, IC agencies, EOD community, allied and coalition nations, DHS and DoJ) bring together organizations that have rarely worked together previously, and who have no agreed upon definitions for the terms they use to describe tactical characterization or technical categorization of improvised weapons. Lack of a common lexicon resulted in same or similar terms having quite different meanings, depending on who was speaking. Establishment of a common language for use by all of these varied contributing organizations is the key to WTI information sharing. Several WTI products have been, or are being developed to create this common language, which consists of a lexicon (i.e., precise terminology), a metadata schema, and map marking symbology.

11.3 Lexicon

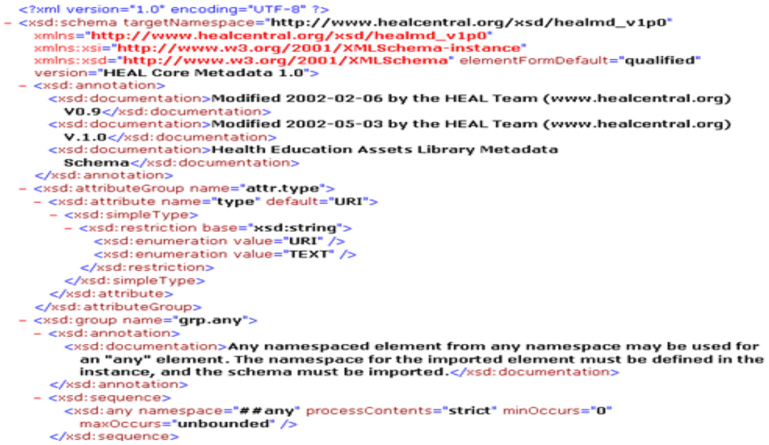
The WTI IED Lexicon (**Figure 11-1**) provides an agreed upon and coherent conceptual framework and a controlled operational vocabulary to address the IED threat worldwide, standardize IED reporting, improve database content management, and enable IED-related education and training and information sharing with federal, state, local, and international partners. The lexicon enables warfighters and LE personnel to use unambiguous words to describe an IED and associated event(s). These words are traceable and recoverable in structured reports that can be searched and aggregated electronically.

Weapons Technical Intelligence (WTI)
Improvised Explosive Device (IED) Lexicon
4th Edition

Figure 11-1. Cover of the DIA/JIEDDO WTI IED Lexicon. *(Photo Credit: DIA/JIEDDO)*

11.4 XML Metadata Schema

Derived from the WTI IED Lexicon, the metadata schema serves as a “Rosetta Stone” to enable the comparison of WTI data elements between databases with incompatible data formats. The schema was developed and is maintained by the JIEDDO sponsored C-IED Information Sharing Community of Interest. It is shared through the DoD Metadata Registry. A uniformly accepted XML Metadata Schema (**Figure 11-2**) makes it possible to cross-correlate WTI data elements across multiple databases, in and outside of DoD, which significantly increases the amount of exploitable WTI data and fosters analysis aimed at connecting events, materials, and people in enemy networks to each other.



```
  <?xml version="1.0" encoding="UTF-8" ?>
- <xsd:schema targetNamespace="http://www.healcentral.org/xsd/healmd_v1p0"
    xmlns="http://www.healcentral.org/xsd/healmd_v1p0"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:xsd="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified"
    version="HEAL Core Metadata 1.0">
  - <xsd:annotation>
      <xsd:documentation>Modified 2002-02-06 by the HEAL Team (www.healcentral.org)
        V0.9</xsd:documentation>
      <xsd:documentation>Modified 2002-05-03 by the HEAL Team (www.healcentral.org)
        V.1.0</xsd:documentation>
      <xsd:documentation>Health Education Assets Library Metadata
        Schema</xsd:documentation>
    </xsd:annotation>
  - <xsd:attributeGroup name="attr.type">
    - <xsd:attribute name="type" default="URI">
      - <xsd:simpleType>
        - <xsd:restriction base="xsd:string">
            <xsd:enumeration value="URI" />
            <xsd:enumeration value="TEXT" />
          </xsd:restriction>
        </xsd:simpleType>
      </xsd:attribute>
    </xsd:attributeGroup>
  - <xsd:group name="grp.any">
    - <xsd:annotation>
        <xsd:documentation>Any namespaced element from any namespace may be used for
          an "any" element. The namespace for the imported element must be defined in the
          instance, and the schema must be imported.</xsd:documentation>
      </xsd:annotation>
    - <xsd:sequence>
        <xsd:any namespace="##any" processContents="strict" minOccurs="0"
          maxOccurs="unbounded" />
      </xsd:sequence>
```

Figure 11-2. Example of an XML Schema *(Figure Credit: JIEDDO and DIA)*

11.5 Map Symbols

This set of graphical representations of IEDs, explosions, finds, caches, hoaxes, and false alarms serve the same purpose for graphical representations as the WTI IED Lexicon does for textual data. These symbols were staffed through the DoD Symbology Standards Management Committee in accordance with Military Standard 2525c, which has representation from all four services and NGA. Approved symbols were incorporated into US Army field manuals and have been and are being coded into the Force XXI Battle Command Brigade and Below FBCB2 software. With these symbols, examples of which are shown in **Figure 11-3,** ground units can generate unambiguous and automated situational awareness reports of known and suspected IEDs on tactical level battlefield command and control displays.

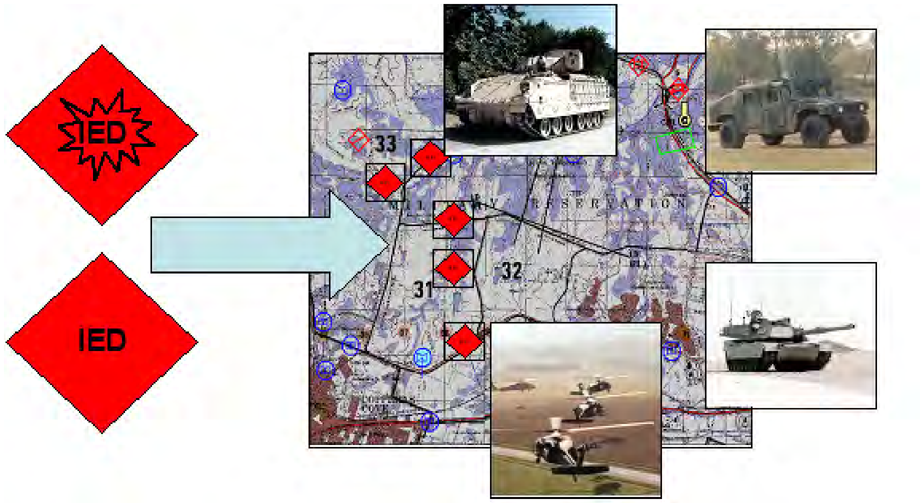


Figure 11.3. Sample of Approved IED Symbols in FBCB-2 *(Figure Credit: JIEDDO and DIA)*

11.6 Federated Architecture

The DoD is working toward a federated architecture that will have federated search capabilities and can cross-correlate data across previously incompatible databases and IED reports. Currently, intelligence collectors and analysts use a common and universally accepted nomenclature that facilitates data exchange (i.e., DoD Discovery Metadata Specification V4) and makes WTI data useful to the many communities that contribute to the C-IED fight.

11.7 Planning Considerations

- Implement a database to capture improvised weapon events and SIGACTS
- Acquire existing and required information sharing agreements with foreign nations
- Develop relationships with partner nation and HN bomb data centers
- Explore solutions to move data between domains
- Establish connectivity to ensure near-real-time feedback of biometric matches

Appendix A.
Acronyms

ABIS – Automated Biometric Information System

AFPAK – Afghanistan and Pakistan as a Single Theater of Operations

AN – Ammonium Nitrate

AO – Area of Operations

AOR – Area of Responsibility

ATF – Bureau of Alcohol, Tobacco, Firearms and Explosives

AtN – Attack the Network

BCT – Brigade Combat Team

BEI – Biometric Enabled Intelligence

BI2R – Biometric Identity Intelligence Repository

BIAR – Biometric Intelligence Analysis Report

BOLO – Be-on-the-Lookout

BVF – Battlefield Vehicle Forensics

C4ISR – Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance

CAMSUM – C-IED Assistance Mission Summary

CAN – Calcium Ammonium Nitrate

CBRN – Chemical, Biological, Radiological, and Nuclear

CCDR – Combatant Commander

CCIR – Commander's Critical Information Requirement

CCMD – Combatant Command

CELLEX – Cellular Phone Exploitation

CENTCOM – Central Command

CEXC – Combined Explosive Exploitation Cell

CFS – CENTCOM Forward Server

CIA – Central Intelligence Agency

CIAD – Combat Incident Analysis Division

CIDNE – Combined Information Data Network Exchange

C-IED – Counter-Improvised Explosive Device

CITP – Counter IED Targeting Program

CJTF – Combined Joint Task Force

CME – Captured Material Exploitation

COI – Community of Interest

COIC – C-IED Operations and Integration Center

COIN – Counterinsurgency Operations

COMTECHREP – Complimentary Technical Report

CONUS – Continental United States

COP – Common Operational Picture

COTS – Commercial Off-The-Shelf

CREW – Counter Radio Control IED Electronic Warfare

CRT – CBRNE Response Teams

CT – Counterterrorism

CTC – Combat Training Center

DCGS-A – Distributed Common Ground System-Army (DCGS-A)

DEA – Drug Enforcement Agency

DFE – Defense Forensic Enterprise

DFSC – Defense Forensic Science Center

DIA – Defense Intelligence Agency

DNA – Deoxyribonucleic Acid

DoD – Department of Defense

DoE – Department of Energy

DoJ – Department of Justice

DOMEX – Document and Media Exploitation

DoS – Department of State

DtD – Defeat the Device

EAC- Lite– Exploitation Analysis Cell

ECM – Electronic Countermeasures

EDE – Explosive Detection Equipment

EEF – Expeditionary Exploitation Facility

EFP – Explosively Formed Projectile

EMIO – Expanded Maritime Interception Operations

EOD – Explosive Ordnance Disposal

EW – Electronic Warfare

EWO – Electronic Warfare Officer

FARC – Fuerzas Armads Revolutionarias De Colombia

FBI – Federal Bureau of Investigation

FEI – Forensic Enabled Intelligence

FMA – Foreign Material Acquisition

FOB – Forward Operating Base

FP – Force Protection

FOXC – Foreign Ordnance Exploitation Cell

FXT – Forensic Exploitation Team

GFXC – Global Forensics Exploitation Center

GTIP – Global Threat Integration Program

HME – Homemade Explosives

HMMWV – High-Mobility Multipurpose Wheeled Vehicle

HMTO – Hazardous Material Transportation Office

HN – Host Nation

HUMINT – Human Intelligence

HVBSS – Heliborne Visit Board Search and Seizure

I2 – Identity Intelligence

I2P – Identity Intelligence Program

I2WD – Intelligence and Information Warfare Division

IC – Intelligence Community

IED – Improvised Explosive Device

IET – Intelligence Exploitation Team

IND – Improvised Nuclear Device

INTERPOL – International Criminal Police Organization

IPOE – Intelligence Preparation of the Operational Environment

IR – Intelligence Requirement

IRAM – Improvised Rocket Assisted Mortar

IrW – Irregular Warfare

ISR – Intelligence, Surveillance, and Reconnaissance

I2WD – Intelligence and Information Warfare Division

J2E – Joint Intelligence Exploitation

JDEC – Joint Document Exploitation Center

JET – Joint Expeditionary Team

JFC – Joint Force Commander

JIEDDO – Joint IED Defeat Organization

JIIM – Joint, Interagency, Intergovernmental, Multinational

JIPOE – Joint Intelligence Preparation of the Operational Environment

JMRC – Joint Maneuver Readiness Center

JPEC – Joint Prosecution and Exploitation Center

JPO C-IED – Joint Program Office for Countering IEDs

JRTC – Joint Readiness Training Center

KIA – Killed in Action

LE – Law Enforcement

LEGAT – Legal Attaché

LEP – Law Enforcement Professionals

LOC – Lines of Communication

MAGTF – Marine Air Ground Task Force

MANPADS – Man Portable Air Defense Systems

MASINT – Measures Intelligence

MCPI – Maritime Counter Proliferation Interdiction (MCPI)

MDCOA – Most Dangerous Course of Action

MEDEX – Media Exploitation

MIO – Maritime Interception Operations

MLCOA – Most Likely Course Of Action

MOD – Ministry of Defense

MOI – Ministry of Interior

MRAP – Mine Resistant Ambush Protective

NAI – Named Area of Interest

NCB – National Central Bureau

NCIS – Naval Criminal Investigation Service

NCTC – National Counter Terrorism Center

NEO – Noncombatant Evacuation Operations

NETF – National Explosives Task Force

NGIC – National Ground Intelligence Center

NMEC – National Media Exploitation Center

NRTB – Near-Real-Time Biometrics

NSA – National Security Agency

NSWCCD – Naval Surface Warfare Center Carderock Division

NSWC IHEODTD – Naval Surface Warfare Center Indian Head Explosive Ordnance Disposal Technology Division

NTC – National Training Center

OBP – Office for Bombing Prevention

ODNI – Office of the Director of National Intelligence

OE – Operational Environment

OEF – Operation Enduring Freedom

OIF – Operation Iraqi Freedom

OPLAN – Operational Plan

ORSA – Operational Research Systems Analysts

OSD – Office of the Secretary of Defense

PIR – Passive Infrared

PIRA – Provincial Irish Republican Army

PKO – Peacekeeping Operations

PM – Program Manager

POI – Persons of Interest

PRETECHREP – Preliminary Technical Report

R&D – Research and Development

RBOC – Reach Back Operations Center

RC – Radio Controlled

RCIED – Radio-Controlled IED

RDT&E – Research, Development, Test, and Evaluation

RDD – Radiological Dispersal Device

RF – Radio Frequency

RFI – Request for Information

RFS – Request for Service

RM – Recovered Munitions

ROMO – Range of Military Operations

RPG – Rocket Propelled Grenade

RSP – Render Safe Procedure

S&T – Science and Technology

SABT – Special Agent Bomb Technician

SDR – Source Directed Requests

SIGACT – Significant Activities

SIGINT – Signals Intelligence

SME – Subject Matter Expert

SOF – Special Operations Forces

SSE – Sensitive Site Exploitation

TACDOMEX – Tactical Document and Media Exploitation

TBOC – Training Brain Operations Center

TECHINT – Technical Intelligence

TECHREP – Technical Report

TEDAC – Terrorist Explosive Device Analytical Center

TEX – Theater Explosive Exploitation

TF – Task Force

TFE – Technical Forensic Exploitation

TIF-B – Technical Intelligence Forensics Branch

TSD – Technical Support Detachment

TtF – Train the Force

TTP- Tactics, techniques and procedures

UBI – Unknown Biometric Identity

UK DEF – United Kingdom Defence Exploitation Facility

USD-I – Undersecretary of Defense for Intelligence

USMA – US Military Academy

USMC – United States Marine Corps

UXO – Unexploded Ordnance

VBIED – Vehicle Borne IED

VBSS – Visit Board Search and Seizure

WEAT – Weapons Technical Intelligence (WTI) Exploitation Analysis Tool

WIA – Wounded in Action

WIT – Weapons Intelligence team

WMD – Weapons of Mass Destruction

WTI – Weapons Technical Intelligence

Appendix B.
Glossary

analysis and production — In intelligence usage, the conversion of processed information into intelligence through the integration, evaluation, analysis, and interpretation of all-source data and the preparation of intelligence products in support of known or anticipated user requirements. See also **intelligence process.** (JP 2-01)

anti-aircraft — An IED primarily intended to damage or destroy aircraft and/or their payload. (WTI IED Lexicon)

anti-armor — An IED that uses a directional explosive effect primarily intended to penetrate armored vehicles. (WTI IED Lexicon)

anti-vehicle — An IED primarily intended to damage or destroy vehicles-excluding armored vehicles-and/or their cargo as well as to kill or wound individuals inside such vehicles. (WTI IED Lexicon)

arming switch — A switch that prevents an IED from arming until an acceptable setoff criteria has occurred and subsequently effects arming and allows functioning. (WTI IED Lexicon)

area of responsibility — The geographical area associated with a CCMD within which a geographic CCDR has authority to plan and conduct operations. Also called **AOR.** (JP 1)

asymmetric — In military operations the application of dissimilar strategies, tactics, capabilities, and methods to circumvent or negate an opponent’s strengths while exploiting his weaknesses. (JP 3-15.1)

attack the network operations — Lethal and nonlethal actions and operations against networks conducted continuously and simultaneously at multiple levels (tactical, operational, and strategic) that capitalizes on or creates key vulnerabilities and disrupt activities to eliminate the enemy’s ability to function to enable success of the operation or campaign. Also called **AtN operations.** (JP 3-15.1)

biological agent — A microorganism that causes disease in personnel, plants, or animals or causes the deterioration of material. (JP 3-11)

biological weapon — An item of material which projects, disperses, or disseminates a biological agent including arthropod vectors. (JP 3-11)

biometric — Measurable physical characteristic or personal behavior trait used to recognize the identity or verify the claimed identity of an individual. (JP 2-0)

biometrics — The process of recognizing an individual based on measurable anatomical, physiological, and behavioral characteristics. (JP 2-0)

blasting cap/detonator — A device containing a sensitive explosive intended to produce a detonation wave. Can be either electric or nonelectric.

brigade combat team — As combined arms teams, brigade combat teams form the basic building block of the Army's tactical formations. They are the principal means of executing engagements. Three standardized brigade combat teams designs exist; heavy, infantry, and Stryker. Battalion-sized maneuver, fires, reconnaissance, and sustainment units are organic to a brigade combat team. Also called **BCT.** (JP 3-31)

cache — A source of subsistence and supplies, typically containing items such as food, water, medical items, and/or communications equipment, packaged to prevent damage from exposure and hidden in isolated locations by such methods as burial, concealment, and/or submersion, to support isolated personnel. See also evader; evasion; recovery; recovery operations. (JP 3-50)

campaign — A series of related major operations aimed at achieving strategic and operational objectives within a given time and space. (JP 5-0)

chain of command — The succession of commanding officers from a superior to a subordinate through which command is exercised. (JP 3-0)

chemical, biological, radiological, or nuclear weapon — A fully engineered assembly designed for employment to cause the release of a chemical or biological agent or radiological material onto a chosen target or to generate a nuclear detonation. Also called **CBRN weapon.** (JP 3-11)

chemical weapon — Together or separately, (a) a toxic chemical and its precursors, except when intended for a purpose not prohibited under the Chemical Weapons Convention; (b) a munition or device, specifically designed to cause death or other harm through toxic properties of those chemicals specified in (a), above, which would be released as a result of the employment of such munition or device; (c) any equipment specifically designed for use directly in connection with the employment of munitions or devices specified in (b), above. (JP 3-11)

coalition — An arrangement between two or more nations for common action. (JP 2-01)

collection — In intelligence usage, the acquisition of information and the provision of this information to processing elements. (JP 2-01)

collection requirement — 1. An intelligence need considered in the allocation of intelligence resources. Within the Department of Defense, these collection requirements fulfill the essential elements of information and other intelligence needs of a commander, or an agency. 2. An established intelligence need, validated against the appropriate allocation of intelligence resources (as a requirement) to fulfill the essential elements of information and other intelligence needs of an intelligence consumer. (JP 2-01.2)

combatant command — A unified or specified command with a broad continuing mission under a single commander established and so designated by the President, through the Secretary of Defense and with the advice and assistance of the Chairman of the Joint Chiefs of Staff. CCMDs typically have geographic or functional responsibilities. Also called **COCOM** (JP 5-0)

combatant commander — A commander of one of the unified or specified combatant commands established by the President. Also called **CCDR.** (JP 3-0)

combatant command (command authority) — Nontransferable command authority established by Title 10 (“Armed Forces”), United States Code, Section 164, exercised only by commanders of unified or specified combatant commands unless otherwise directed by the President or the Secretary of Defense. Combatant command (command authority) cannot be delegated and is the authority of a combatant commander to perform those functions of command over assigned forces involving organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction over all aspects of military operations, joint training, and logistics necessary to accomplish the missions assigned to the command. Combatant command (command authority) should be exercised through the commanders of subordinate organizations. Normally this authority is exercised through subordinate joint force commanders and Service and/or functional component commanders. Combatant command (command authority) provides full authority to organize and employ commands and forces as the combatant commander considers necessary to accomplish assigned missions. Operational control is inherent in combatant command (command authority). (JP 1)

commander’s critical information requirement — An information requirement identified by the commander as being critical to facilitating timely decision making. Also called **CCIR.** (JP 3-0)

common operational picture — A single identical display of relevant information shared by more than one command that facilitates collaborative planning and assists all echelons to achieve situational awareness. Also called **COP.** (JP 3-0)

command wire IED — A switch where the firing point and contact point are separate but joined together by a length of wire. A command wire may contain multiple power sources located near both the firing point and the contact point to overcome the resistance of the length of wire. Also called **CWIED**. (WTI IED Lexicon)

concept of operations — A verbal or graphic statement that clearly and concisely expresses what the joint force commander intends to accomplish and how it will be done using available resources. Also called **CONOPS.** (JP 5-0)

continental United States — United States territory, including the adjacent territorial waters, located within North America between Canada and Mexico. Also called **CONUS.**

counter-improvised explosive device operations — The organization, integration, and synchronization of capabilities that enable offensive, defensive, stability, and support operations across all phases of operations or campaigns to defeat improvised explosive devices as operational and strategic weapons of influence. Also called **C-IED operations.** (JP 3-15.1)

counterinsurgency — Comprehensive civilian and military efforts taken to defeat an insurgency and to address any core grievances. Also called **COIN.** (JP 3-24)

counterterrorism — Actions taken directly against terrorist networks and indirectly to influence and render global and regional environments inhospitable to terrorist networks. Also called **CT.** (JP 3-26)

country team — The senior, in-country, US coordinating and supervising body, headed by the chief of the US diplomatic mission, and composed of the senior member of each represented US department or agency, as desired by the chief of the US diplomatic mission. Also called **CT.** (JP 3-07.4)

defense support of civil authorities — Support provided by US Federal military forces, Department of Defense civilians, Department of Defense contract personnel, Department of Defense component assets, and National Guard forces (when the Secretary of Defense, in coordination with the governors of the affected states, elects and requests to use those forces in Title 32, United States Code, status) in response to requests for assistance from civil authorities for domestic emergencies, LE support, and other domestic activities, or from qualifying entities for special events. Also called **DSCA**. (DODD 3025.18)

dissemination and integration — In intelligence usage, the delivery of intelligence to users in a suitable form and the application of the intelligence to appropriate missions, tasks, and functions. (JP 2-01)

electric — An initiator who's function is initiated by an electrical impulse that creates heat or a spark (WTI IED Lexicon)

electronic warfare — Military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. Also called **EW.** (JP 3-13.1)

electronic warfare frequency deconfliction — Actions taken to integrate those frequencies used by electronic warfare systems into the overall frequency deconfliction process. (JP 3-13.1)

enhancements — An optional, deliberately added component as opposed to a secondary hazard which modifies the effects of the IED. The IED would be effective, yet produce a different measureable result if this material were not added. The effect can be additional physical destruction, proliferation of dangerous substances (radiation, chemicals, etc.), or other results to enhance the effect of the IED. **(WTI IED Lexicon)**

expeditionary force — An armed force organized to accomplish a specific objective in a foreign country. (JP 3-0)

exploitation — 1. Taking full advantage of success in military operations, following up initial gains, and making permanent the temporary effects already achieved. 2. Taking full advantage of any information that has come to hand for tactical, operational, or strategic purposes. 3. An offensive operation that usually follows a successful attack and is designed to disorganize the enemy in depth. (JP 2-01.3)

explosion — A nuclear, chemical or physical process leading to the sudden release of energy. (WTI IED Lexicon)

explosively formed projectile — Specially designed main charge configuration incorporating an explosive charge with a concave metal liner which by the force of the charge reshapes the plate into a high velocity metal slug capable of penetrating armor. Also called **EFP**. (WTI IED Lexicon)

explosive ordnance — All munitions containing explosives, nuclear fission or fusion materials, and biological and chemical agents. (JP 3-34)

explosive ordnance disposal — The detection, identification, on-site evaluation, rendering safe, recovery, and final disposal of unexploded explosive ordnance. Also called **EOD.** (JP 3-34)

false — An incident that is incorrectly identified through reported in good faith as an IED, which is subsequently categorized as a false alarm after positive EOD action. (WTI IED Lexicon)

firing switch — Component that initiates the firing train. (WTI IED Lexicon)

force protection — Preventive measures taken to mitigate hostile actions against Department of Defense personnel (to include family members), resources, facilities, and critical information. Also called **FP.** (JP 3-0)

fusion — In intelligence usage, the process of examining all sources of intelligence and information to derive a complete assessment of activity. (JP 2-0)

geospatial intelligence — The exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on the Earth. Geospatial intelligence consists of imagery, imagery intelligence, and geospatial information.

hoax — An IED related incident that involves a device fabricated to look like an IED and that is intended to simulate one to elicit a response. (WTI IED Lexicon)

homeland defense — The protection of United States sovereignty, territory, domestic population, and critical defense infrastructure against external threats and aggression or other threats as directed by the President. Also called **HD.** (JP 3-27)

homeland security — A concerted national effort to prevent terrorist attacks within the United States; reduce America's vulnerability to terrorism, major disasters, and other emergencies; and minimize the damage and recover from attacks, major disasters, and other emergencies that occur. Also called **HS.** (JP 3-28)

host nation — A nation which receives the forces and/or supplies of allied nations and/or NATO organizations to be located on, to operate in, or to transit through its territory. Also called **HN.** (JP 3-57)

human intelligence — A category of intelligence derived from information collected and provided by human sources. Also called **HUMINT.** (JP 2-0)

improvised explosive device — A weapon that is fabricated or emplaced in an unconventional manner incorporating destructive, lethal, noxious, pyrotechnic or incendiary chemicals and designed to kill, destroy, incapacitate, harass deny mobility, or distract. Refers to a type of IED incident that involves a complete functioning device. Also called **IED. (JP 1-02)**

improvised/homemade explosives — Nonstandard explosive mixtures/compounds which have been formulated/synthesized from available ingredients. Most often used in the absence of commercial/military explosives. Also called **IE/HME** (WTI IED Lexicon)

improvised mortar — An improvised weapon, using military or homemade components, designed to launch an explosive charge to the target. (WTI IED Lexicon)

improvised Rocket — An improvised weapon, military or homemade, designed to propel an explosive charge to the target. (WTI IED Lexicon)

improvised rocket assisted munition — A projected explosive device made from a canister filled with explosives, which is delivered by propellant. (WTI IED Lexicon)

Improvised Weapon — Weapons constructed in an improvised manner designed to destroy, incapacitate, harass or distract. (WTI IED Lexicon)

incident — An occurrence, caused by either human action or natural phenomena, that requires action to prevent or minimize loss of life or damage to property and/or natural resources. See also information operations. (JP 3-28)

indications and warning — Those intelligence activities intended to detect and report time sensitive intelligence information on foreign developments that could involve a threat to the United States or allied and/or coalition military, political, or economic interests or to US citizens abroad. It includes forewarning of hostile actions or intentions against the United States, its activities, overseas forces, or allied and/or coalition nations. Also called **I&W.** (JP 2-0)

initiator — Any component that may be used to start a detonation or deflagration. An initiator will be categorized as either a detonator or an igniter. (WTI IED Lexicon)

insurgency — The organized use of subversion and violence by a group or movement that seeks to overthrow or force change of a governing authority. Insurgency can also refer to the group itself. (JP 3-24)

intelligence — The product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations. The term is also applied to the activity which results in the product and to the organizations engaged in such activity.

intelligence process — The process by which information is converted into intelligence and made available to users, consisting of the six interrelated intelligence operations: planning and direction, collection, processing and exploitation, analysis and production, dissemination and integration, and evaluation and feedback.

interagency — Of or pertaining to United States Government agencies and departments, including the Department of Defense. See also **interagency coordination**. (JP 3-08)

irregular warfare — A violent struggle among state and non-state actors for legitimacy and influence over the relevant population(s). Irregular warfare favors indirect and asymmetric approaches, though it may employ the full range of military and other capacities, to erode an adversary's power, influence, and will. Also called **IrW.** (JP 1)

joint captured materiel exploitation center — An element responsible for deriving intelligence information from captured enemy materiel. It is normally subordinate to the intelligence directorate of a joint staff. Also called **JCMEC.** (JP 2-01)

joint intelligence preparation of the operational environment — The analytical process used by joint intelligence organizations to produce intelligence estimates and other intelligence products in support of the joint force commander's decision-making process. It is a continuous process that includes defining the operational environment; describing the impact of the operational environment; evaluating the adversary; and determining adversary courses of action. Also called **JIPOE.** (JP 2-01.3)

law enforcement agency — Any of a number of agencies (outside the Department of Defense) chartered and empowered to enforce US laws in the following jurisdictions: The United States, a state (or political subdivision) of the United States, a territory (or political subdivision) of the United States, a federally recognized Native American tribe or Alaskan Native Village, or within the borders of a HN. Also called **LEA.** (JP 3-28)

leverage — In the context of joint operation planning, a relative advantage in combat power and/or other circumstances against the adversary across one or more domains or the information environment sufficient to exploit that advantage. (JP 5-0)

line of communications — A route, either land, water, and/or air, that connects an operating military force with a base of operations and along which supplies and military forces move. Also called **LOC.** (JP 2-01.3)

maritime interception operations — Efforts to monitor, query, and board merchant vessels in international waters to enforce sanctions against other nations such as those in support of United Nations Security Council Resolutions and/or prevent the transport of restricted goods. Also called **MIO.** (JP 3-03)

measurement and signature intelligence — Intelligence obtained by quantitative and qualitative analysis of data (metric, angle, spatial, wavelength, time dependence, modulation, plasma, and hydromagnetic) derived from specific technical sensors for the purpose of identifying any distinctive features associated with the emitter or sender, and to facilitate subsequent identification and/or measurement of the same. The detected feature may be either reflected or emitted. Also called **MASINT.** (JP 2-0)

multinational — Between two or more forces or agencies of two or more nations or coalition partners. (JP 5-0)

nuclear weapon — A complete assembly (i.e., implosion type, gun type, or thermonuclear type), in its intended ultimate configuration which, upon completion of the prescribed arming, fusing, and firing sequence, is capable of producing the intended nuclear reaction and release of energy. (JP 3-11)

operation order — A directive issued by a commander to subordinate commanders for the purpose of effecting the coordinated execution of an operation. (JP 5-0)

operation plan — 1. Any plan for the conduct of military operations prepared in response to actual and potential contingencies. 2. A complete and detailed joint plan containing a full description of the concept of operations, all annexes applicable to the plan, and a time-phased force and deployment data. Also called **OPLAN.** (JP 5-0)

ordnance — Explosives, chemicals, pyrotechnics, and similar stores, e.g., bombs, guns and ammunition, flares, smoke, or napalm. (JP 3-15)

partner nation — Those nations that the United States works with to disrupt the production, transportation, distribution, and sale of illicit drugs, as well as the money involved with this illicit activity. Also called **PN.** (JP 3-07.4)

peace operations — A broad term that encompasses multiagency and multinational crisis response and limited contingency operations involving all instruments of national power with military missions to contain conflict, redress the peace, and shape the environment to support reconciliation and rebuilding and facilitate the transition to legitimate governance. Also called **PO.** (JP 3-07.3)

power source — A device that either stores or releases electrical or mechanical energy. The key elements of information about a power source are its type/source, number of batteries and their configuration (series or parallel), its voltage (if electrical) and how it is connected to close an IED switch. **(WTI IED Lexicon)**

pressure — A switch designed to function when pressure is applied in a predetermined direction (plate, tube, plunger, crush wire). (WTI IED Lexicon)

priority intelligence requirement — An intelligence requirement, stated as a priority for intelligence support, that the commander and staff need to understand the adversary or other aspects of the operational environment. Also called **PIR.** (JP 2-01)

proliferation — The transfer of weapons of mass destruction, related materials, technology, and expertise from suppliers to hostile state or non-state actors. (JP 3-40)

radio-controlled IED — A switch initiated electronically by wireless means consisting of a transmitter/receiver. Also called as RCIED (WTI IED Lexicon)

radiological dispersal device — An improvised assembly or process, other than a nuclear explosive device, designed to disseminate radioactive material to cause destruction, damage, or injury. Also called **RDD**. (WTI IED Lexicon)

render safe procedures — The portion of the explosive ordnance disposal procedures involving the application of special explosive ordnance disposal methods and tools to provide for the interruption of functions or separation of essential components of unexploded explosive ordnance to prevent an unacceptable detonation. Also called **RSP**. (JP 3-15.1)

rocket — Self-propelled ordnance that uses gas pressure from rapidly burning propellant to transport a payload (warhead) to a desired target. **(WTI IED Lexicon)**

scientific and technical intelligence — The product resulting from the collection, evaluation, analysis, and interpretation of foreign scientific and technical information that covers: a. foreign developments in basic and applied research and in applied engineering techniques; and b. scientific and technical characteristics, capabilities, and limitations of all foreign military systems, weapons, weapon systems, and materiel; the R&D related thereto; and the production methods employed for their manufacture.

sensitive site — A geographically limited area that contains, but is not limited to, adversary information systems, war crimes sites, critical government facilities, and areas suspected of containing high value targets. (JP 3-31)

signals intelligence — 1. A category of intelligence comprising either individually or in combination all communications intelligence, electronic intelligence, and foreign instrumentation signals intelligence, however transmitted. 2. Intelligence derived from communications, electronic, and foreign instrumentation signals. Also called **SIGINT.** (JP 2-0)

site exploitation — A series of activities to recognize, collect, process, preserve, and analyze information, personnel, and/or materiel found during the conduct of operations. Also called **SE.** (JP 3-31)

source — 1. A person, thing, or activity from which information is obtained. 2. In clandestine activities, a person (agent), normally a foreign national, in the employ of an intelligence activity for intelligence purposes. 3. In interrogation activities, any person who furnishes information, either with or without the knowledge that the information is being used for intelligence purposes. (JP 2-01)

stability operations — An overarching term encompassing various military missions, tasks, and activities conducted outside the United States in coordination with other instruments of national power to maintain or reestablish a safe and secure environment, provide essential governmental services, emergency infrastructure reconstruction, and humanitarian relief. (JP 3-0)

strategic intelligence — Intelligence required for the formation of policy and military plans at national and international levels. Strategic intelligence and tactical intelligence differ primarily in level of application, but may also vary in terms of scope and detail. (JP 2-01.2)

support to prosecution — The process of associating related people, places, devices, or equipment to an individual for evidentiary purposes in a recognized court of law. (WTI IED Lexicon)

switch — A device for making, breaking, or changing a connection in an IED. A single switch can have multiple functions (i.e., arming and firing. (WTI IED Lexicon)

tactical design — The specific design of an IED attack – including but not limited to: position of the IED, the type of IED, method of actuation, type of road segment used, concealment technique, use of secondary devices, the time of day, etc. Tactical design addresses the questions of "why here, why now, and why in this way." Terms used to describe a specific type of device or component of a device (e.g., VBIED) are often used to describe all or part of the tactical design. (WTI IED Lexicon)

tactical questioning — Direct questioning by any Department of Defense personnel of a captured or detained person to obtain time-sensitive tactical intelligence information, at or near the point of capture or detention and consistent with applicable law. Also called **TQ.** (JP 3-63)

Tactics, techniques and procedures development — Using lessons learned from an IED attack to refine and improve the tools and methods used during all missions in which an IED may be encountered (e.g., convoys, tactical suppression efforts, ISR, C-IED missions, etc. (WTI IED Lexicon)

target — 1. An entity or object that performs a function for the adversary considered for possible engagement or other action. 2. In intelligence usage, a country, area, installation, agency, or person against which intelligence operations are directed. 3. An area designated and numbered for future firing. 4. In gunfire support usage, an impact burst that hits the target. See also **objective area.** (JP 3-60)

target analysis — An examination of potential targets to determine military importance, priority of attack, and weapons required to obtain a desired level of damage or casualties. See also **target acquisition.** (JP 3-60)

targeting — The process of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities. (JP 3-0)

technical intelligence — Intelligence derived from the collection, processing, analysis, and exploitation of data and information pertaining to foreign equipment and materiel for the purposes of preventing technological surprise, assessing foreign scientific and technical capabilities, and developing countermeasures designed to neutralize an adversary's technological advantages. Also called **TECHINT.** (JP 2-0)

terrorism — The unlawful use of violence or threat of violence to instill fear and coerce governments or societies. Terrorism is often motivated by religious, political, or other ideological beliefs and committed in the pursuit of goals that are usually political. (JP 3-07.2)

toxic industrial chemical — A chemical developed or manufactured for use in industrial operations or research by industry, government, or academia. For example: pesticides, petrochemicals, fertilizers, corrosives, poisons, etc. These chemicals are not primarily manufactured for the specific purpose of producing human casualties or rendering equipment, facilities, or areas dangerous for human use. Hydrogen cyanide, cyanogen chloride, phosgene, and chloropicrin are industrial chemicals that also can be military chemical agents. Also called **TIC.** (JP 3-11)

toxic industrial material — A generic term for toxic or radioactive substances in solid, liquid, aerosolized, or gaseous form that may be used, or stored for use, for industrial, commercial, medical, military, or domestic purposes. Toxic industrial material may be chemical, biological, or radioactive and described as toxic industrial chemical, toxic industrial biological, or toxic industrial radiological. Also called **TIM.** (JP 3-11)

toxic industrial radiological — Any radiological material manufactured, used, transported, or stored by industrial, medical, or commercial processes. For example: spent fuel rods, medical sources, etc. Also called **TIR.** (JP 3-11)

toxin — Poisonous substances that may be produced naturally (by bacteria)

transnational threat — Any activity, individual, or group not tied to a particular country or region that operates across international boundaries and threatens US national security or interests.(JP 3-26)

unexploded explosive ordnance — Explosive ordnance which has been primed, fused, armed or otherwise prepared for action, and which has been fired, dropped, launched, projected, or placed in such a manner as to constitute a hazard to operations, installations, personnel, or material and remains unexploded either by malfunction or design or for any other cause. Also called **UXO.** (JP 3-15)

weapons of mass destruction — Chemical, biological, radiological, or nuclear weapons capable of a high order of destruction or causing mass casualties and exclude the means of transporting or propelling the weapon where such means is a separable and divisible part from the weapon. Also called **WMD.** (JP 3-40)

weapons technical intelligence — A category of intelligence and processes derived from the technical and forensic collection and exploitation of improvised explosive devices, associated components, improvised weapons, and other weapon systems. Also called **WTI.** (JP 3-15.1)

weapon system — A combination of one or more weapons with all related equipment, materials, services, personnel, and means of delivery and deployment (if applicable) required for self-sufficiency. (JP 3-0)

working group — An enduring or ad hoc organization within a joint force commander's headquarters consisting of a core functional group and other staff and component representatives whose purpose is to provide analysis on the specific function to users. Also called **WG.** (JP 3-33)

IED Incident Planning Considerations

November 26, 2013

POST BLAST

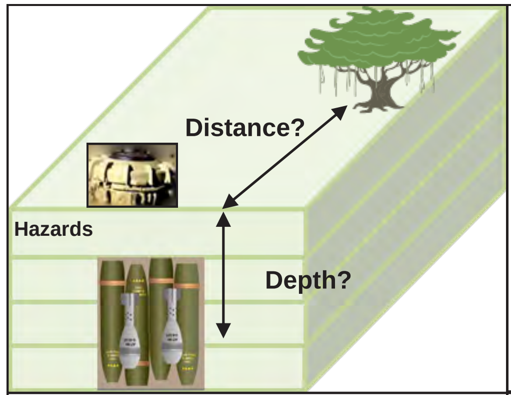
Threat Assessment:
- Secondary Devices
- Improvised Weapon
- Chem/BIO/Rad Hazards
- Ambush
- Toxic Industrial Chemicals

Planning Considerations:
- RSP as Required
- Site Survey
- Post Blast Exploitation
- Vehicle/Building Damage **Assessment**
- Crater Analysis
- Soil Sampling
- Fragmentation Collection
- Question Observers

Initial Required Forces:
- EOD/SABT
- Security Element

Required Forces Follow-On:
- WIT (If High Profile Event)
- Working Dogs
- UAV Support
- CRT (If CBRN Event)
- CEXC (If Meets Requirement)

FIND/CACHE



Threat Assessment:
- VOIEDs
- Booby Traps
- First Seen Improvised Weapon
- Explosive Ordnance
- Chem/BIO/Rad Hazards
- Ambush
- Explosive precursors

Planning Considerations:
- Long Term Cache
- Transit Cache
- Short Term Cache
- GPS/CELLEX
- Search Kit/HIIDE/BATS
- Explosive Detection

Initially Required Forces:
- Search Team
- EOD
- Security Element

Required Forces Follow-On:
- WIT
- Working Dogs
- UAV Support
- CRT (If CBRN Present)

SITE EXPLOITATION

M
E
T
T
-
T
C
-
C

Mission Analysis
- Purpose
- Task
- Constraints

Enemy Analysis
- Skilled Bomb Maker or Trained Technician
- Insurgent Cell
- Criminal Organization

Terrain and Weather
- Obstacles, Avenues of approach, Key terrain, Observation and fields of fire, Cover and concealment (OAKOC)
- Terrain Analysis
- Rain, Wind
- Begin Morning Nautical Twilight (BMNT), End Evening Nautical Twilight (EENT)

Troop Analysis
- Search
- EOD
- WIT (If used)
- TSE
- Transportation
- Working Dogs
- Interpreters
- Law Enforcement

Time Analysis
- Movement
- Render Safe Operations
- Search
- Collection Operations
- Exploitation Operations
- Triage

Civilian Considerations
- Areas, Structures, Capabilities, Organizations, People and Events (ASCOPE)
- Local Leaders

CCIR
- Priority Intelligence Requirements (PIR)
- Friendly Forces Intelligence Requirements (FFIR)
- Latest Time Information is Of Value (LTIOV)

LOCATE/RSP IED

Threat Assessment:
- Secondary Devices
- Hoax Device with Enemy ISR
- Hoax Device w/Ambush
- First Seen Improvised Weapon
- Chem/BIO/Rad Hazards to include Toxic Industrial Chemicals
- Explosive precursors

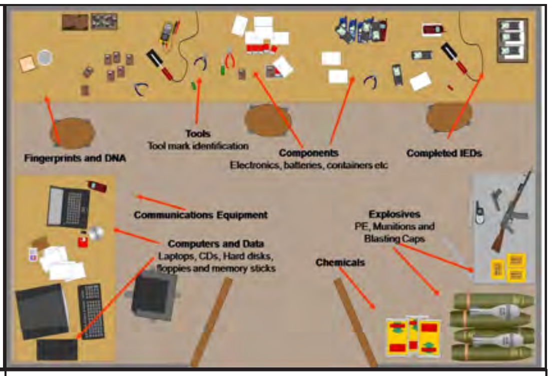
Planning Considerations:
- Size of IED/VBIED
- Site Security
- Past IED Events
- New TTP or Device
  - Switches and initiators
  - Power sources
  - Main Charges
  - Containers
  - Enhancements

Initially Required Forces:
- EOD
- Security Element

Required Forces Follow-On:
- WIT (If Required)
- Working Dogs
- UAV Support
- CRT (If CBRN Event)
- CEXC (If Meets Requirement)

FABRICATION FACILITY

Threat Assessment:
- VOIED's
- Home Security System IED's
- First Seen Improvised Weapon
- Unknown Explosives
- Explosive Precursors
- Chem/BIO/Rad Hazards
- Toxic Industrial Chemicals



Planning Considerations:
- Complete Improvised Weapons
- Under Construction Improvised Weapons
- "As Is" Photographs/Sketches
- Materiel Identification
- Circuit Diagrams
- Biometrics Collection
- Fabrication Tools and Methods
- Material Receipts

Initially Required Forces:
- EOD
- Security Element

Required Forces Follow-On:
- WIT (If Required)
- Working Dogs
- UAV Support
- CRT (If CBRN Present)

WTI Collection Considerations

IED Incident

- **Systematic Examination of the Site:**
  - Experience
  - Current Intelligence
  - Known devices in AO
  - Enemy TTP
- **Search Pattern selection**
- **Scene Sketch**:
  - Key features (houses, buildings, roads, paths, fences, markers, obstacles, firing points, aiming points, vehicles).
- **Identify Witnesses**
- **Photograph:**
  - Scene Overview
  - Scene towards 4 cardinal directions
  - Blast Seat/Emplacement Site
  - Damage/Debris
  - Onlookers/Witnesses
  - Triggerman/Attacker View
  - Firing Point
  - Observation Points
  - Timing Method
  - Devices/items of interest
  - Detainees and Suspects
  - Searched targets (entry, rooms, items of interest, cabinets)
- **Identify and collect WTI material and components**
- **Sample Blast Seat and obtain Control Sample**
- **Sample Residue**
- **GPS ALL locations for structured reports**
- **Collect Latent Prints from non-removable objects, detainees, persons of interest, enemy KIA**
- **Tactical question/interview witnesses, victims, detainees, persons of interest**
- **Exploit cell phones from detainees** (cell phones from IEDs exploited at Level 2)
- **Friendly Information:**
  - Convoy/Patrol composition (vehicle type and C-IED capabilities)
  - Order of movement
  - Direction and speed
  - Location of vehicles on road (shoulder, center, median, off-road)
  - Actions prior to contact
  - Actions after contact
  - How the IED/weapon was spotted
  - Who spotted the IED
  - Details of wounds, injuries, deaths
  - Contact information from unit for future contact

Movement of Material

Evacuation Considerations:

- Safe to handle/Transport
- Triage Materials
- Commanders Guidance
- Assets Available
- Chain of Custody
- Packaging Requirements

November 26, 2013

Tactical Data

- Method of Identification
- Method of Employment
- Method of Emplacement
- Method of Attachment
- Sensor Defeat
- Role of IED
- Attack Geography
- Incident Environmental Conditions
- Incident Atmospherics

Technical Data

- Switch type
- Initiator
- Main Charge
- Power Source
- Container type
- Enhancement Type
- Arming/Firing Method
- Device Signature

Forensic Signatures

- Photography
- Biometric
    - Latent Fingerprints
    - DNA
    - Iris
    - Facial
    - Voice
- Trace
- Explosives
    - Conventional
    - Home-Made

IED Event Data Exploitation

Tactical Level-1 Exploitation

WTI Exploitation :

Tactical:

- Date, time, location device was emplaced, found, functioned, recovered
- Concealment method utilized by the emplacer
- Timeline for emplacer to be effective
- Environmental conditions
- How long to Emplace/Bury
- Emplacement signatures based on known events
- New enemy TTP based on successful enemy ISR

Technical:

- Fragmentation and debris pattern
- Brisance (1) and detonation speed based on effects
- Type of device based on effects to vehicles, personnel, site
- Detailed technical properties:
    - – Switch
    - – Initiator
    - – Main charge
    - – Power Source
    - – Container
    - – Enhancements
    - – Construction methods
    - – Device method of operation
    - – Frequency of R/C switch

Forensic:

- Suspect or Detainees on Watch List?
- Previous detention or links to insurgent/criminal groups?
- New insurgents in the AO?
- Associations to other devices and events (Areas of Interest)

Critical Information:

- How is the enemy learning and adapting?

Follow-on Tasks:

◊ Write and disseminate a detailed EOD and WIT report based on Level 1 exploitation/analysis

◊ Process and evacuate materiel for further exploitation, analysis and reporting

◊ Track materiel evacuated, follow-up on results, integrate results into assessments and historical/technical records

- ∗ Similar emplacement and components to previous incidents?
- ∗ New cell in AOR or "Learning Enemy?"
- ∗ Use of secondary devices to entrap first responders?
- ∗ Make first technical assessment of device and its emplacement design.
- ∗ Prioritize for exploitation.

WTI Report Production

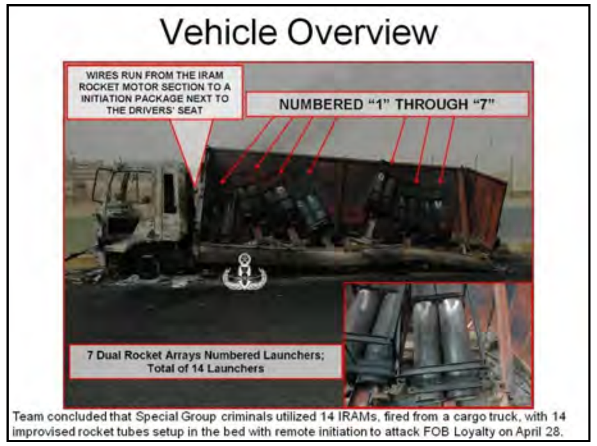
Reports to the BCT Commander Within 24 Hours

EOD Report

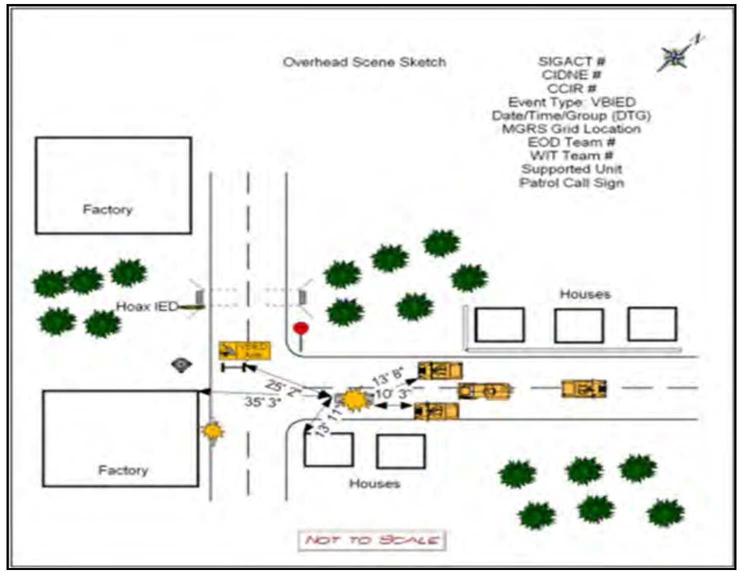
WIT Report

CIDNE

Level 1 Reporting


Vehicle Overview
WIRES RUN FROM THE IRAM ROCKET MOTOR SECTION TO A INITIATION PACKAGE NEXT TO THE DRIVERS' SEAT
NUMBERED "1" THROUGH "7"
7 Dual Rocket Arrays Numbered Launchers; Total of 14 Launchers

Team concluded that Special Group criminals utilized 14 IRAMs, fired from a cargo truck, with 14 improvised rocket tubes setup in the bed with remote initiation to attack FOB Loyalty on April 28.



November 26, 2013

WTI Analysis

WTI Collection Management and Dissemination

Planning and Direction:
- Develop collection and processing framework
- Develop collection plan and assign responsibilities
- Assign WTI Collection Manager
- Integrate WTI process with Intelligence Process (Collect, Exploit, Analyze)

Collection:
- Priorities and synchronization of efforts
- Triage to support Commander's priorities

Processing and Exploitation:
- Contextual data and physical material
- First Technical Assessment
- EOD and WIT Analysis

Production:
- Analysis of raw data to develop a final product
- Pattern Analysis, Predictive Analysis, Network Analysis, Device Analysis
- Route Analysis, Area Analysis

Dissemination and Evaluation:
- "Push" and "Pull" methods
- Web Site posting
- RFI Management

Site Exploitation Data

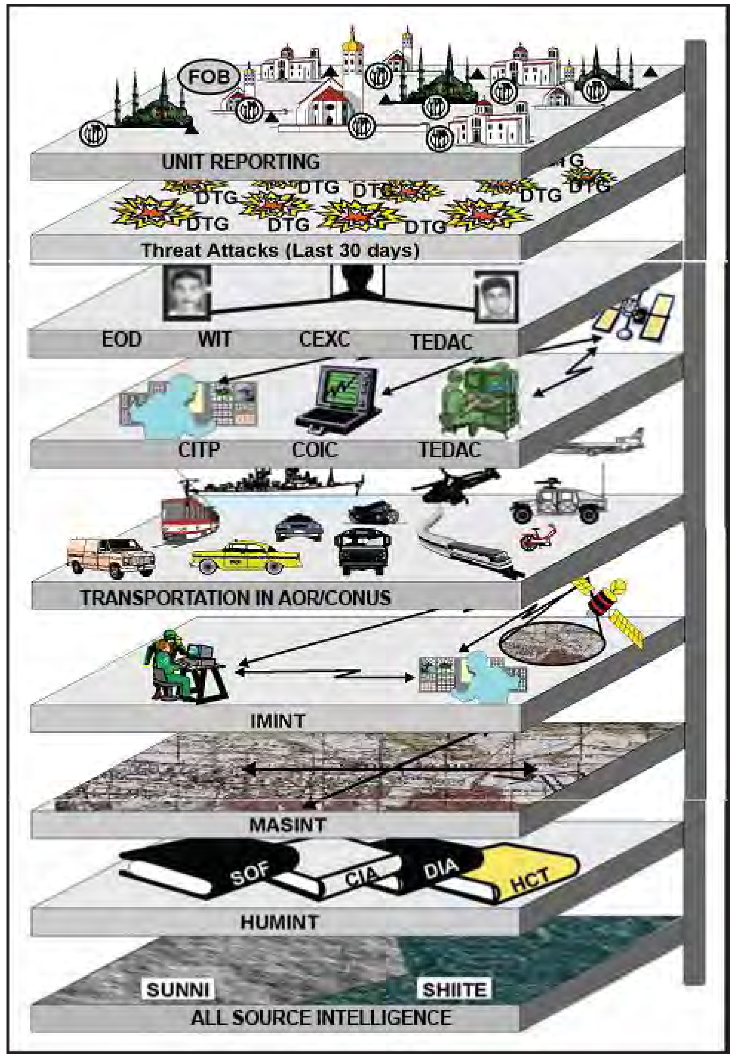
Non-Device Data

- 9 Line IED Report
- EOD Report
- WIT Report
- Post-IED Patrol Debrief
- UXO Data Base
- Witness Statements
- Interrogation Report
- CREW Download

Device Data

- EOD First Technical Assessment
- Biometrics
- Switch
- Initiator
- Main Charge
- Power Source
- Container
- Enhancements
- Home-Made Explosive
- DOMEX
- Electronic Frequency

FUSION AND ANALYSIS



COLLECT

EXPLOIT

ANALYZE

FUSE

WTI

ALL SOURCE

WTI PRODUCTS

EFP Event Analysis

Route Analysis

Area Analysis

Intelligence Reports

Interrogation Support

Monthly EFP Analysis

Subordinate Unit RFIs

ASR / MSR Synch Effort

Event Analysis

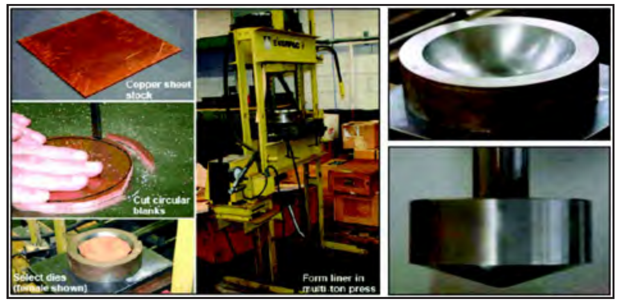
WTI Outputs

FORCE PROTECTION

Materiel Solu-

TARGETING

SOURCING



Signature Characterization

PROSECUTION

November 26, 2013

IED Exploitation

RULE SET TO ESTABLISH CONDITIONS FOR LEVEL 2

LEVEL 1 ACTIVITY

Collection of relevant explosive and non-explosive material by:

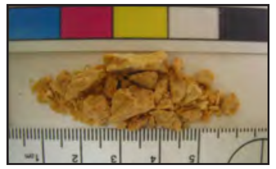
- Unit Search/SE Team
- EOD/SABT
- WIT
- C-IED Team
- Photographs and sketch record of event/scene made
- Items recorded, bagged, and tagged
- Material moved to FOB for transfer to Level 2

First Technical Assessment Made by EOD

Collection:

Probability of Value
(Pay off—What has our experience taught us?)

MAIN CHARGE



30 gms of suspected compound.
Wrappers and Containers.
Who handled explosive residue from crater and fragmentation control samples from site. Level 2 →

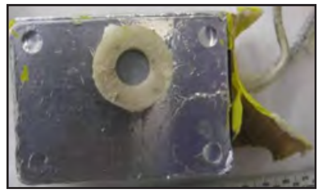
MIL Level 3 → Confirm country of Origin
COM Level 3 → Confirm manufacturer and use
HME Level 2 → Locally produced? Yes/No

INITIATOR

Complete item for physical characteristics detailed breakdown.
Containers and wrapping.
Electrical integrity, functioning.
Fragments/Assessment of type.

Level 2 →
Level 3/4 → Level 3/4 → Manufacturer
Who has handled?

SWITCH



Complete items.
Fragments or description from post blast.
Wrapping paper.
Shipping container:
- External packaging
- Photograph with scale
- Relationship to other components

Level 2 →
Level 3/4 →

POWER SOURCE

Complete item with tape
Who handled the item?
Trace under tape if soil sample is taken at the scene.
Fragments for item ID/pattern analysis.

Level 2 →
Level 3/4 →
Level 2 →

CONTAINER

Estimate size of the device, damage/effect.
Complexity of manufacture.
IED network capability.

Level 2 →
Level 3 →

ENHANCEMENTS

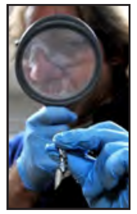
Sample from blast seat.
Qualitative and Quantitative.
Type of material and hazards.

Level 2 →
Level 3 →

DESIRED OUTCOMES

TIME CONSIDERATIONS
- **TACTICAL**
- **OPERATIONAL**
- **STRATEGIC**

Is it a new device?

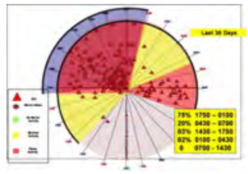


Exterior/Interior
- **Tape**
- **Prints**
- **DNA**

TRIAGE DECISION? → **TECHNICAL PROCESS** → **FORENSIC PROCESS**

What is the Commander's priority?
Force Protection OR targeting?

Level 1/2 Task



PATTERN ANALYSIS →

COMMON THREAT PICTURE →

INDICATIONS AND WARNINGS

FORCE PROTECTION **Level 1** →

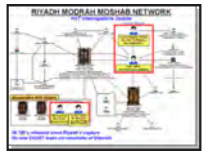
TTP's

Level 3 →

PM Requirements

NAI

TARGETING **Levels 1/2/3/4** →



COMPONENT MATERIAL SOURCING
- **Level 1/2** → **Support Search/TSE/EOD**
- **Levels 2/3/4** → **Origin of Manufacture/Supply**

SIGNATURE CHARACTERIZATION
- → **Cue ISR Assets/Spt to Matl Developers**
- → **Biometric Identity**

SUPPORT TO PROSECUTION

Latest Time Information is of Value?
How long to process?
Priority? Red, Amber, Green

What physical material is needed for court?

What biometric evidence is needed for court?

24 hrs | **48 hrs** | **72 hrs** | **CONTINUOUS**

Switch Exploitation

November 26, 2013

Electronic and Mechanical SWITCH EXPLOITATION

	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4
WHO:	EOD, CEXC Platoon SABT	Expeditionary Exploitation Facility, CEXC Platoon	TEDAC, IHEODTD, NGIC, DSTO, DSTL	NSA, OGA, FFRDC. I2WD
WHAT:	• Identify Switch during Technical Categorization	• Confirm Level 1 • Switch Type by Function (mechanical/ electronic) • Includes arming/firing • Operating Frequency • Current/Voltage Required to function	• Confirm Level 2 • Circuit design • Integrated circuit info • Frequency Analysis • Component ID • Micro-Controller • Firmware	• ID Manufacturer • Source of components • PIC Reading • Construction techniques or processes • Arming/firing sequences and related codes • Construction characteristics
WHERE:	On-Site/FOB	Lab in AOR	Out of Theater	Out of Theater
WHEN:	Time of Incident	Red - within 24 hrs Amber - within 72 hrs Green - within 30 days	Red - within 5 days Amber - within 30 days Green - within 120 days	Within 30 days of receipt

NOTE: Examples current as of Sept 2013

NOTE: Times are Notional

COMMAND

SAMPLES/COLLECTION REQUIREMENTS

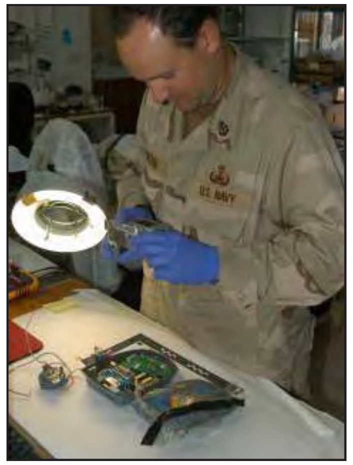
MECHANICAL:

- Whole Item
- Components from RSP or Post Blast

ELECTRONIC:

- Whole Item—Non invasive
- Components from RSP or Post Blast

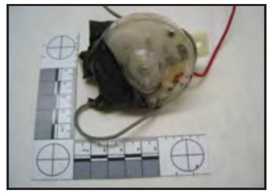
Level 2 Assessment



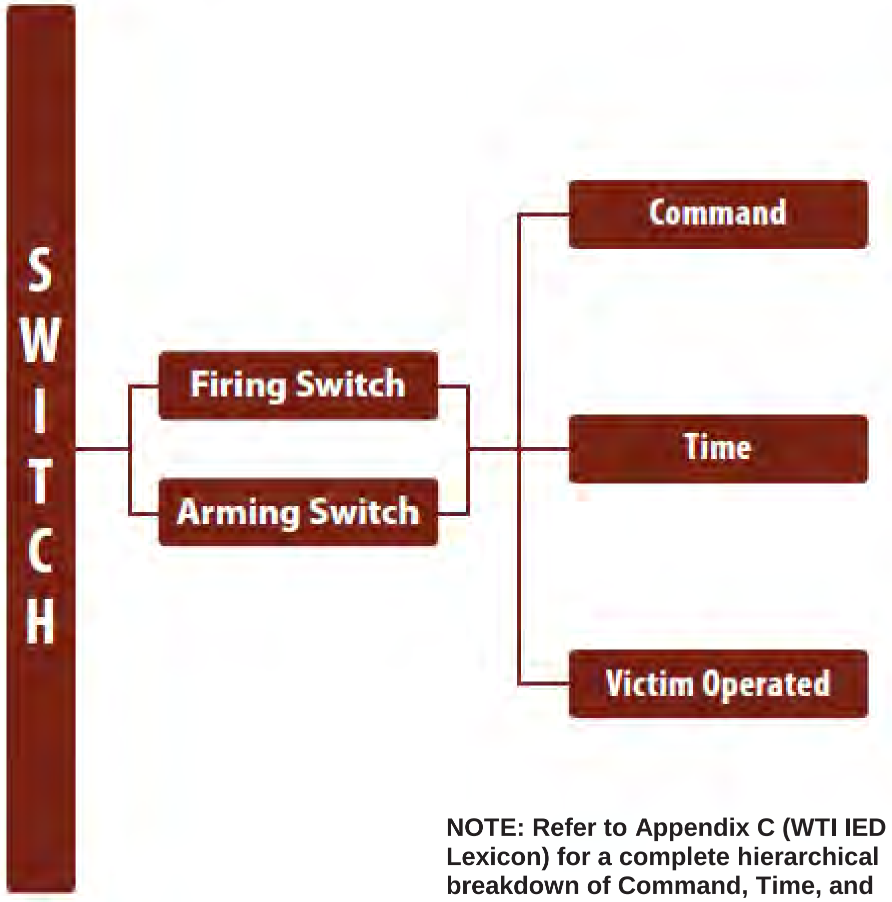
TRIAGE

- Sealed Package—X-ray for hazardous components
  - → Pass to Technical Exploitation (mechanical/electronic)
    - → Confirm Switch/Further exploit and if necessary, dispatch for follow-on Level 3 and 4 exploitation and analysis

TIME

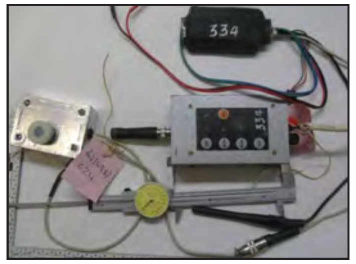


VICTIM OPERATED



NOTE: Refer to Appendix C (WTI IED Lexicon) for a complete hierarchical breakdown of Command, Time, and Victim Operated switches.

COMMAND ARMED VICTIM OPERATED



DIAGNOSTIC EQUIPMENT

Initiator Exploitation

November 26, 2013

INITIATOR EXPLOITATION

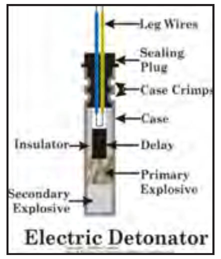
	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4
WHO:	EOD	Expeditionary Exploitation Facility, CEXC Platoon	TEDAC IHEODTD	Picatinny Arsenal NRL
WHAT:	• Complete Item • Fragments • Description • Photographs • Wrapping and Packaging	• Photography • Characteristics • Continuity • Manufacturing • Nomenclature	• Energetic Assessment • Confirm Voltage/Current Requirements • Country of Origin • Age	• Internal Characteristics
WHERE:	**On-Site/FOB**	**Lab in AOR**	**CONUS**	**CONUS**
WHEN:	Time of Incident	Within 72 Hours	0 –120 Days	Within 30 days of receipt

NOTE: current examples as of Sept 2013

NOTE: Times are Notional

ELECTRIC DETONATOR

NONELECTRIC DETONATOR



INITIATOR SAMPLE COLLECTION, EXPLOITATION AND ANALYSIS

I. Individual items separated from explosive train and prepared for transportation

- Electric Blasting Cap
- Non-Electric Blasting Cap
- Improvised Initiator
- Radiography of Circuit

II. Input data into level 2 report

- Body Length
- Diameter
- Material
- Base Stampings
- Crimp/Plug (Material, color)
- Markings
- Wire Length, Color, Type (Strands)
- Origin of Manufacture

III. Energetic assessment of the initiator. Confirm voltage/current requirements, country of origin, estimation of age.

IV. Characteristics of internal components and explosive compound, Level 3 and 4 reports.

V. Samples/Collection Requirements.

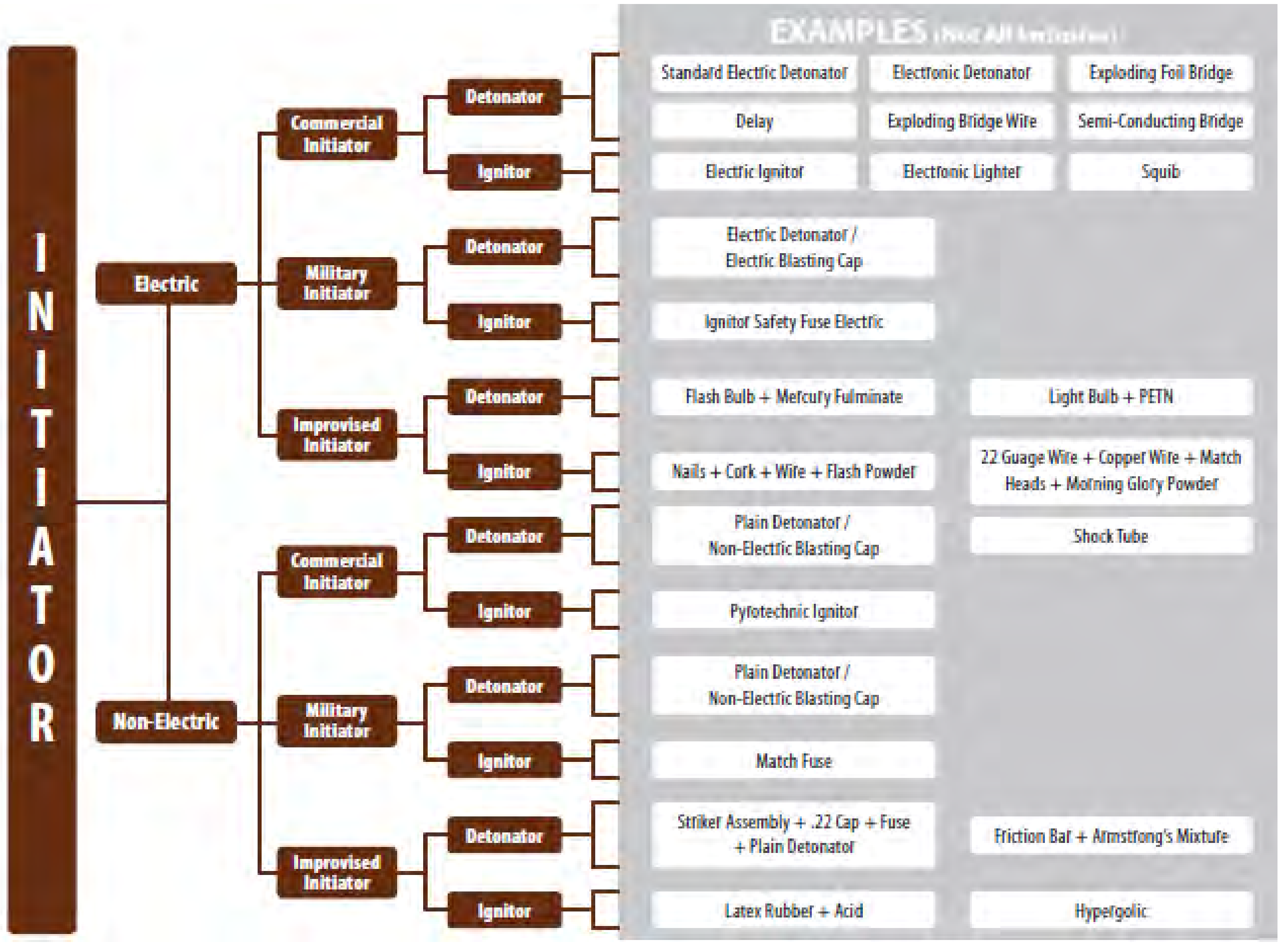
- Complete Items
- Fragments or description from post blast (Leg Wires, Plugs, Metal, Fragments)
- Wrapping Paper
- Shipping Containers
    - External Packaging
    - Photograph with scale
    - Cardinal Directions and relationship to other components

DETONATOR I.D. FEATURES

WIRES AND PLUGS

CRIMPING

MARKINGS



INITIATOR

EXAMPLES (Not All Inclusive)

Electric	Commercial Initiator	Detonator	Standard Electric Detonator Delay	Electronic Detonator Exploding Bridge Wire	Exploding Foil Bridge Semi-Conducting Bridge
		Ignitor	Electric Ignitor	Electronic Lighter	Squib
	Military Initiator	Detonator	Electric Detonator / Electric Blasting Cap		
		Ignitor	Ignitor Safety Fuse Electric		
	Improvised Initiator	Detonator	Flash Bulb + Mercury Fulminate	Light Bulb + PETN	
		Ignitor	Nails + Cork + Wire + Flash Powder	22 Guage Wire + Copper Wire + Match Heads + Morning Glory Powder	
Non-Electric	Commercial Initiator	Detonator	Plain Detonator / Non-Electric Blasting Cap	Shock Tube	
		Ignitor	Pyrotechnic Ignitor		
	Military Initiator	Detonator	Plain Detonator / Non-Electric Blasting Cap		
		Ignitor	Match Fuse		
	Improvised Initiator	Detonator	Striker Assembly + .22 Cap + Fuse + Plain Detonator	Friction Bar + Armstrong's Mixture	
		Ignitor	Latex Rubber + Acid	Hypergolic	

IMPROVISED DETONATORS

Main Charge Exploitation

November 26, 2013

MAIN CHARGE EXPLOITATION

	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4
WHO: (2013)	EOD, WIT, C-IED TEAM	Expeditionary Exploitation Facility, CEXC Platoon	DTK, TEDAC, NSWC IHEODTD	OGA
WHAT:	Presumptive analysis of explosive filler	Identify IEDs consistent components	Organic/Inorganic Quantitative/ Qualitative breakdown By percentage	Identification of trace organic/inorganic material at surface
WHERE:	On site/FOB	Laboratory in AOR	Laboratories CONUS/OCONUS	Laboratory CONUS
WHEN:	Time of incident Initial Evacuation	Within 72 hours	Within 24 hours to 90 days	Within 90 days
TYPE OF DETECTION:	**AHURA/HAZMAT ID**	**AHURA/HAZMAT ID**	**FTIR, IT/MS, GC/MS, LC/MS**	

NOTE: current examples as of Sept 2013

NOTE: Times are Notional

SEMTEX-H

SAMPLES COLLECTION REQUIREMENTS

Collection

- -30gm sample of main charge
- -30 gm sample of explosive residue from crater
- Sample of explosive residue from fragmentation
- Sample of suspect explosive materials from a find, cache, or fabrication site.
- Sample of suspect explosive material wrappers or containers
- Samples from detainee clothing
- Samples from skin
- Complete Improvised Main Charge and X-rays

Controls

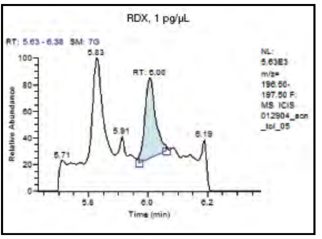
– 30 gm samples of Military, Commercial explosives indentified from general usage in a theater of operation

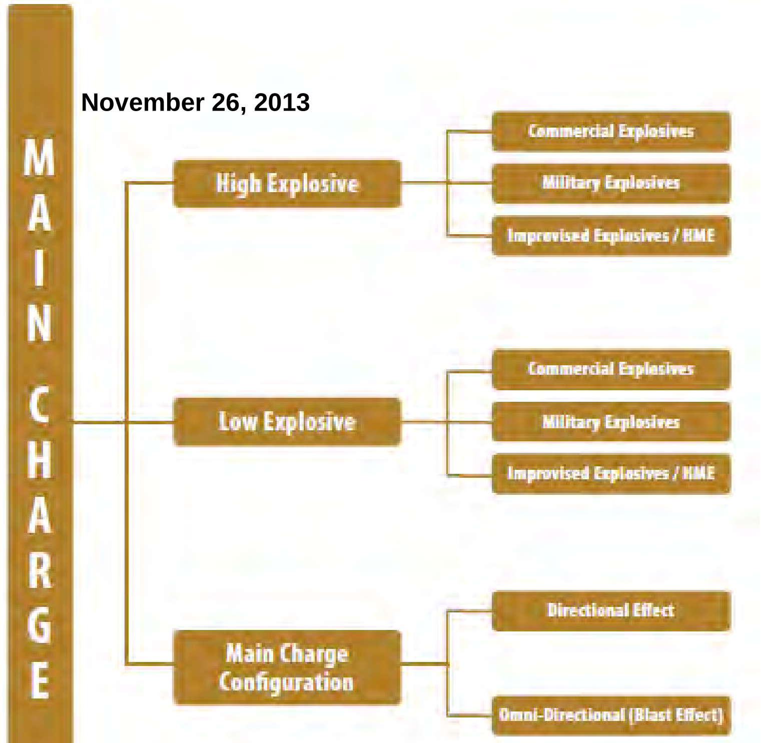
– 30 gm samples of HME

Associated Samples

HOME-MADE EXPLOSIVE PRECURSORS

EXPLOITATION AND ANALYSIS





November 26, 2013

NOTE: Refer to Appendix C (WTI IED Lexicon) for a complete hierarchical breakdown of main charges

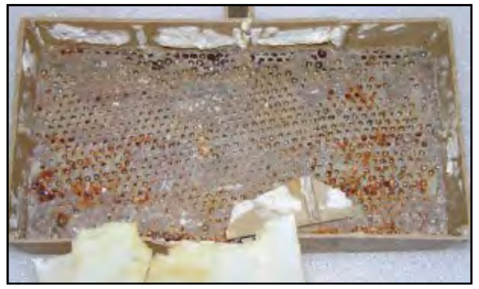
COPPER LINED EFP

IMPROVISED SHAPE CHARGE

TWO TYPES OF LARGE SHAPED CHARGES.

ONE WITH A PVC CASING AND ONE WITH A METAL CASING. BOTH HAVE A COPPER SHAPE CHARGE CONE.

DIRECTIONAL FRAGMENTATION CHARGE



Power Source Exploitation

November 26, 2013

POWER SOURCE EXPLOITATION

	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4
WHO:	EOD, WIT, C-IED	ExpeCEXC Platoon	TEDAC	
WHAT:	• Complete Item • How Connected to Device • Description • Photographs • Wrapping and Packaging	• Photography • Characteristics • Name and Type • Manufacturing • Nomenclature	• Confirm Characteristics • Schematics of Device	• Source Information
WHERE:	On-Site/FOB	Lab in AOR	CONUS	CONUS
WHEN:	Time of Incident	After Biometrics	0 –120 Days	Within 30 days of receipt

NOTE: current examples as of Sept 2013

NOTE: Times are Notional

POWER SOURCE COLLECTION, EXPLOITATION AND ANALYSIS

I. Identify the power source—AC or DC.

II. Positively identify the power source

- Type/Voltage
- Configuration of power pack (series, parallel
- Position within the circuit

III. Confirm position of power source within the device.

IV. Produce a schematic

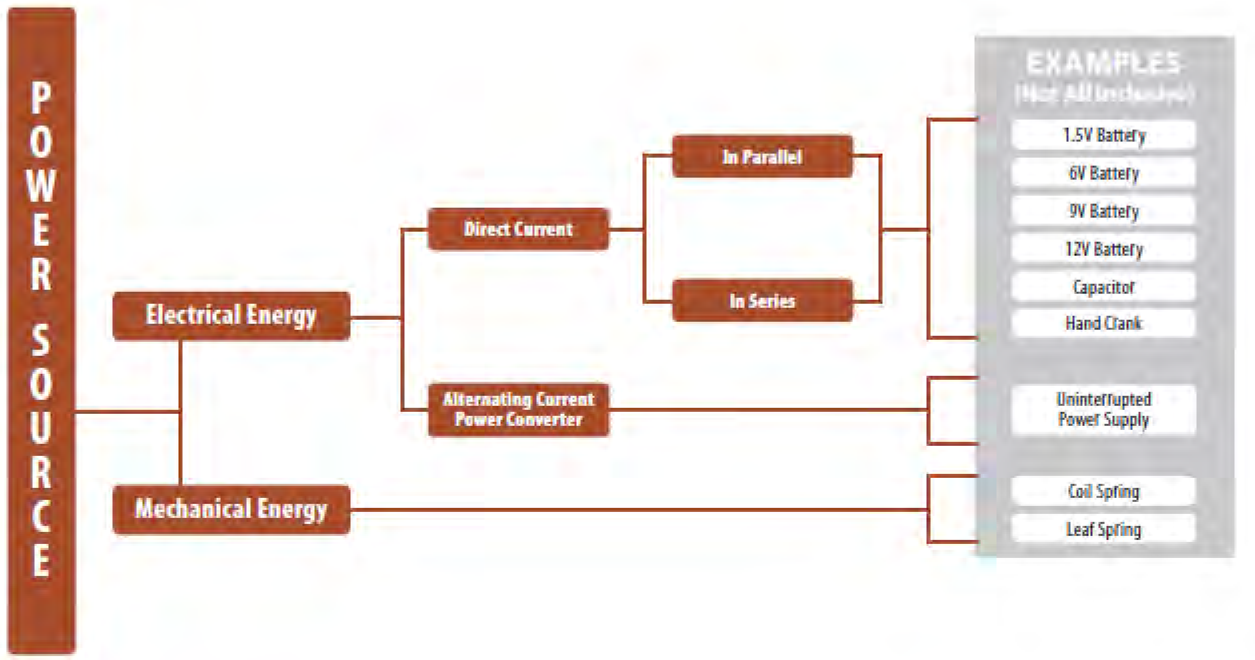
V. **SAMPLES/COLLECTION REQUIREMENTS**

- Firing Packs Complete
- Separate Batteries
- Photograph, including connection
- Disrupted battery components and material
- Post blast battery components

POWER PACKS

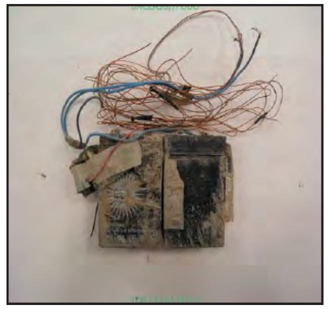
UNINTERRUPTED POWER SUPPLY

CAPACITOR BANK



12 VOLT BATTERY

6 VOLT BATTERY



9 VOLT BATTERY

Container Exploitation

November 26, 2013

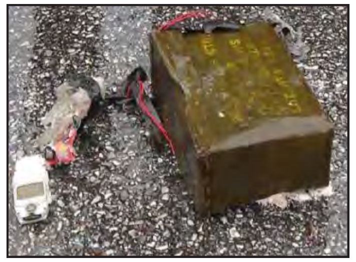
CONTAINER EXPLOITATION

	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4
WHO:	EOD, WIT, C-IED	Expeditionary Exploitation Facility, CEXC Platoon	TEDAC	
WHAT:	• Complete Item • Description • Photographs • Wrapping and Packaging	• Photography • Characteristics • Name and Type • Manufacturing • Nomenclature	• Confirm Characteristics • Line Drawings of Device • Metallurgy Data	• Source Identification
WHERE:	**On-Site/FOB**	**Lab in AOR**	**CONUS**	**CONUS**
WHEN:	Time of Incident	Within 30 days of receipt	After Biometrics	0 –120 Days

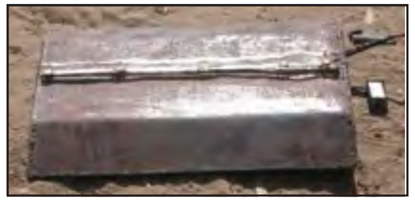
NOTE: current examples as of Sept 2013

NOTE: Times are Notional

AMMUNITION CAN USED FOR AN IED CONTAINER



SPEED BUMP CONTAINER



CONTAINER EXPLOITATION AND ANALYSIS

I. Identify type of container used.

II. Identify container components and

III. Samples/Collection Requirements.

- Complete Items
- Fragments or description from post blast
- Remnants from RSP or BIP

PIPE USED FOR IED CONTAINER

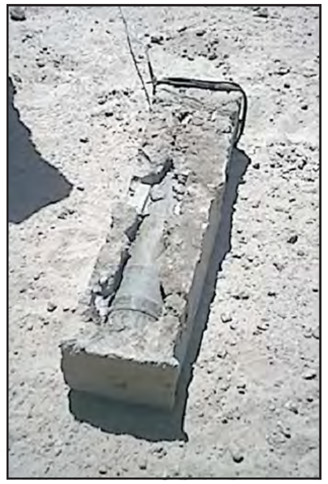
PROPANE TANK USED FOR IED CONTAINER

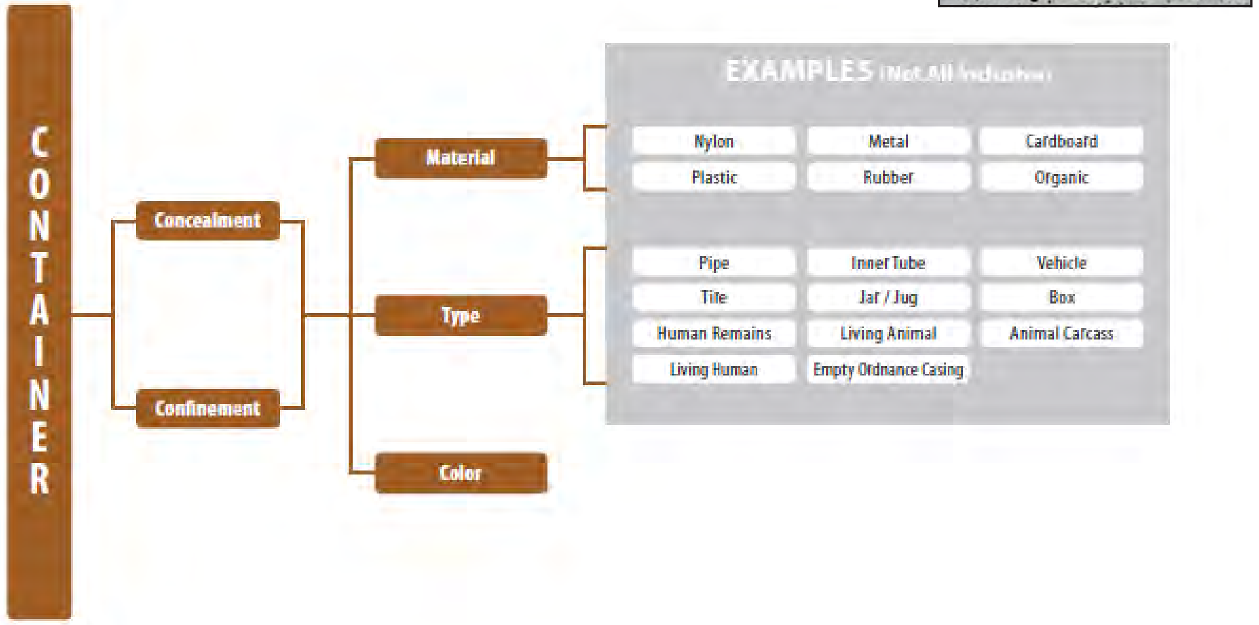
WATER BOTTLE CONTAINER

VEHICLE USED AS CONTAINER

FIRE EXTINGUISHER USED FOR IED CONTAINER

CONCRETE ENCASED





CONTAINER

Concealment

Confinement

Material

Type

Color

EXAMPLES (Not All Inclusive)

Nylon | Metal | Cardboard
Plastic | Rubber | Organic

Pipe | Inner Tube | Vehicle
Tire | Jar / Jug | Box
Human Remains | Living Animal | Animal Carcass
Living Human | Empty Ordnance Casing

CARCASS AS A CONTAINER

ORDNANCE IN A VBIED

WATER-BORNE VBIED

Enhancement Exploitation

November 26, 2013

ENHANCEMENT EXPLOITATION

	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4
WHO:	EOD, WIT, CRT	DTK or 20TH SUPCOM LAB	ECBC	OGA, National Laboratory
WHAT:	- Presumptive Analysis - Container Photos - Container Characteristics - Environmental Data - Sketches	- Photography - Characteristics - Confirmatory Analysis	- Confirmatory Analysis - Qualitative/Quantitative Analysis - Source Strength - Volatility - Processing Method	- Source Identification - Processing and Weaponization Signatures
WHERE:	**On-Site/FOB**	**Lab in AOR**	**CONUS**	**CONUS**
WHEN:	Time of Incident	Within 24 to 72 hrs **Depending on Priority**	0 –120 Days	Within 30 days of receipt
TYPE OF DETECTION	**M8, M256, ICAM, PINS HazMat ID, FirstDefender**	**GC/MS**	**GC/MS**	

NOTE: current examples as of Sept 2013 **NOTE: Times are Notional**

FUEL ENHANCEMENT

CYANIDE ENHANCEMENT

(U//FOUO) Demonstration of a mubtakar release.

CHLORINE GAS ENHANCEMENT

ENHANCEMENT COLLECTION AND ANALYSIS

I. Identify the type and amount of enhancement.

II. Identify the type of container and weaponization method.

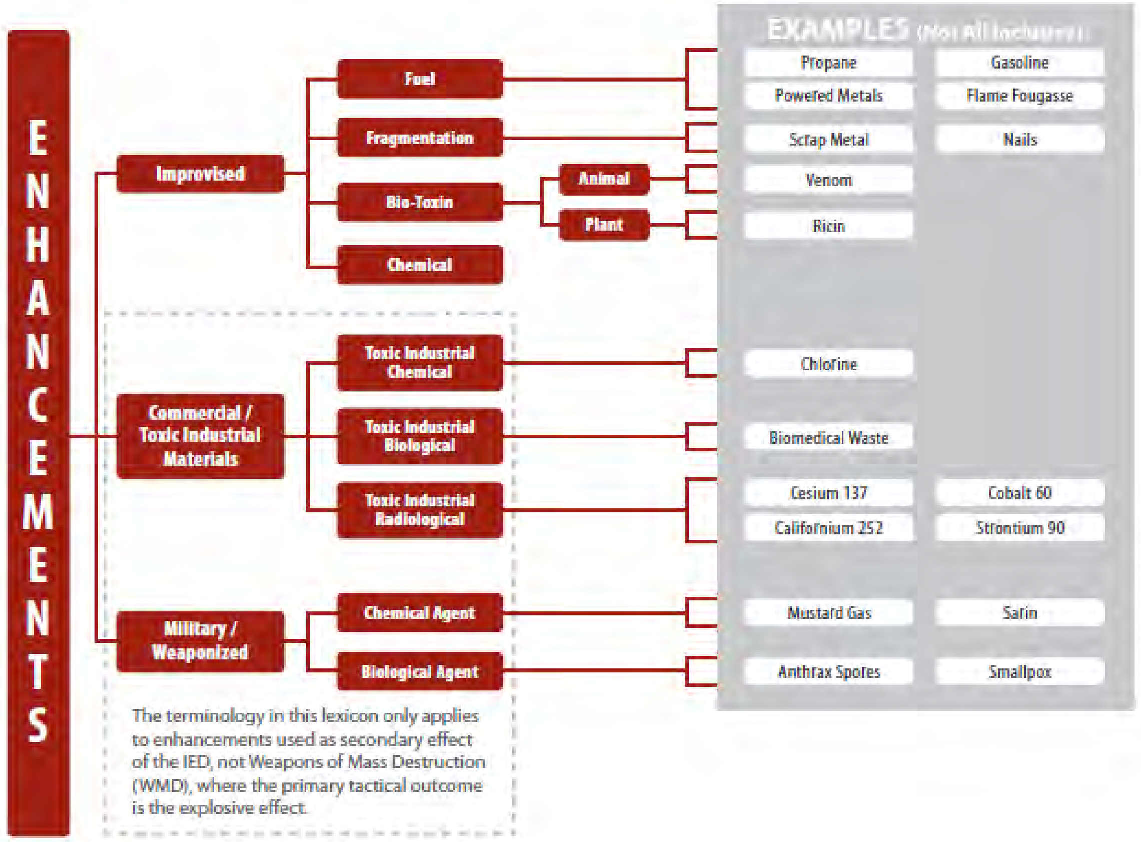
III. Identify tactical employment and environmental conditions.

IV. Samples/Collection Requirements:

- Sample from container
- Sample from Blast Seat
- Sample from fragmentation and debris
- Control sample

PERSONAL PROTECTION DURING COLLECTION

CHEMICAL ENHANCEMENT

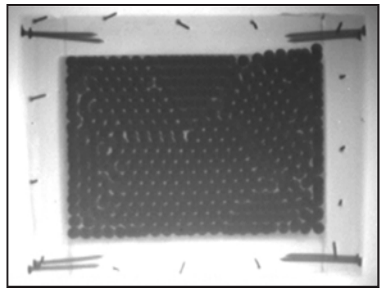


The terminology in this lexicon only applies to enhancements used as secondary effect of the IED, not Weapons of Mass Destruction (WMD), where the primary tactical outcome is the explosive effect.

REBAR FRAGMENTATION ENHANCEMENT

FRAGMENTATION ENHANCEMENT

BALL BEARING ENHANCEMENT



Appendix D.

WTI Capability Assessment Matrix

Weapons Technical Intelligence (WTI) Capability Matrix
Potential Establishment of WTI Capabilities with Other Nations

General Factor	Detailed Factor	Criticality/Importance
Part One - Assessment of Threat and Need		
1. Location	(a). Is the country located in a part of the world already subject to asymmetric attacks?	If attacks are not occurring, are they anticipated? Should resources be committed? Consider impact on US interests if attacks were to start.
	(b). Is it located close to countries that have an active insurgent or terrorist campaign ongoing?	Insurgent groups have a history of using satellite countries as "safe havens" and as part of their supply chain for the procurement of IEDs, weapons, and equipment.
	(c). Are the borders porous?	Countries with indistinct or porous borders lacking proper control measures are more usable by insurgents/terrorists.
	(d). Is the country being used as a "staging post" or transit route into a country already experiencing an active terrorist campaign?	Such countries are often also used to base training facilities, stage caches for immediate use, and as stepping off points for operations in other countries. Such countries will also be used as part of a larger transit route for materials and personnel. Access to the WTI material from such a country can give valuable insights into terrorists' current capability and future aspirations or intentions.
2. Political Situation	(a). How stable is the country? Do neighboring countries have an anti-US/coalition agenda and are they politically motivated to provide support to the terrorists/insurgents?	Limited security force activity on borders in stable countries is advantageous to insurgents/terrorists. In unstable countries, security forces already committed to internal operations elsewhere and unable to secure all borders are advantageous to insurgents/terrorists.
	(b). Is the country a member of the Coalition Against Terror (CAT)?	It has already been demonstrated that countries supporting the United States have themselves become the target of internal elements, either acting alone or under external direction, to destabilize their support and weaken the coalition.
	(c). If not a member of the CAT, what is its record for support of the United States and the other CAT nations?	Same as above, but not as likely as attacks against active supporters.
	(d). Does this country provide troops to Coalition Forces in support of military operations?	Such overt support leads to direct attacks that will seek to undermine the political will of the country thereby reducing support. This situation is often made more fragile if there is only limited support from the public.

NOTE: Information contained in this appendix was derived from a TSWG commissioned project entitled "*A Mechanism for Establishing the Potential for Transfer of Weapons Intelligence (WEPINT) Capability to Other Nations.*" August 01, 2007.

General Factor	**Detailed Factor**	**Criticality/Importance**
	(f). Does the current government have a record of carrying out policies that might be construed as being at odds with the aspirations or values of an indigenous religious minority?	Such indigenous religious minorities may embark on attacks as payback for perceived internal maltreatment of their religious community.
	(g). What are the broad aims, intentions, and political aspirations of the terrorist group?	Consider whether their aspirations relate to internal issues or are an element of wider external movement.
	(h). Are they aligned to a wider movement of unrest?	Consider whether there are already elements of the civil population willing to provide active or tacit support to the terrorists/insurgents?
	(i). What are their demands?	Are these realistic and able to be met by the government?
	(j). Are they a religion-centric organization?	Consider whether the group is aligned to a particular religious group and also the proportion of this group within the population.
3. History of Attacks	(a). Has the country been subjected to terrorist attacks?	
	(b). What targets were attacked?	
	(c). What is the average yearly and seasonal occurrence of IED incidents?	Consider whether this is increasing, stable, or decreasing compared to previous years.
	(d). What is the effectiveness of the terrorist campaign?	Consider number of devices, number of casualties, targets destroyed or damaged, and effect on the capacity of the security forces to maintain law and order.
	(e). What have been the aims of these attacks?	Are the attacks designed to make a statement without causing unnecessary casualties, or are there clear aims to inflict maximum casualties? Do aims change depending on the target selected? Some groups will provide warnings when attacking shopping or commercial areas to limit casualties, but give no warning, and seek to maximize casualties when attacking security forces.

Weapons Technical Intelligence (WTI) Capability Matrix
Potential Establishment of WTI Capabilities with Other Nations

General Factor	Detailed Factor	Criticality/Importance
	(f). Were the targets linked to the policies and aspirations of the ruling government?	Consider effects and likely changes of policy that could result. Also consider whether the government has a policy for dealing with terrorist groups (openly or through intermediaries).
	(g). Were the targets linked (even tenuously) to the United States?	Consider all possibilities and even tenuous links. Include commercial interests owned or partly owned by US companies.
	(h). Are the targets military, police, government, commercial, random, or the recognized representatives of another country?	
	(i). Are foreign embassies being attacked?	Consider also aborted or disrupted attacks where the possibility of an embassy being the target was indicated by intelligence.
4. Likely Targets	(a). What targets exist in the country?	Consider all likely targets, including government, commercial, and judiciary related targets.
	(b). How many of these are linked to American interests?	
	(c). Are there iconic structures such as skyscrapers, bridges or towers that would provide a particularly photogenic and media friendly target for terrorists?	
	(d). Are US forces based in the country?	Consider size, location, the role of the base (may be linked to the ongoing War on Terror), the attitude of the local population to US presence, and any history of such attacks in the region.
	(e). Do US commercial interests own high profile key locations in the country?	
	(f). Are there unique, US-owned or run industries based in the country?	Consider if the country in question is the sole provider of a particular mineral or commodity that, if sources were to be disrupted, would impact US interests or global supply.

General Factor	Detailed Factor	Criticality/Importance
5. Device Switch Types, Time Devices	(a). Do we have an understanding of terrorists' modus operandi relating directly to their use of timed switch type IEDs?	Consider all aspects of device design, construction, and placement and the planned effect. Timed switch types are categorized in the WTI Lexicon as Time Mechanical, Time Chemical, and Time Electronic.
	(b). Are warnings given?	This can relate to overall intention. Warnings are normally given to allow evacuation to take place and reduce casualties, although a disadvantage is the likelihood that EOD teams will be able to render safe the device during the time delay. By close observation, the terrorist will identify the likely window of opportunity so that evacuation can take place, but first responders will not be able to take further action.
	(c). What is the technical level and construction quality of the devices?	Devices built to low quality standards are likely to malfunction and, as a result, may be more likely to be rendered safe. There is also a possibility of premature initiation.
	(d). Are mechanical timers used?	These types of timers may be simple to construct but can afford a degree of reliability.
	(e). If mechanical timers are being used, is there an established record of the use of a particular type of timer, or are a number of varying mechanical time delays being used?	A record of response timelines for particular timers can inform the design of equipment and procedures for first responders.
	(f). Do we have enough information to establish safe waiting periods for EOD teams at incidents?	
	(g). Are electronic timers used?	These timers can be used for accurate long or short delay attacks, depending on the scenario.
	(h). When electronic timers are used, are the timers wholly improvised or are existing timing components modified with add-on firing circuits?	The type of electronic timer used can be an indicator of technical sophistication. Simple add-on firing circuits and off-the-shelf timers are relatively easy to produce, while custom timers assembled from basic components may require more skill and knowledge of timer design.

General Factor	Detailed Factor	Criticality/Importance
	(i). Are there any indications that time delays are being manipulated to take advantage of current security force TTP and reactions?	A study of response timelines and accurate record of explosion times related to warnings given and times of discovery will indicate whether this is the case. This will also provide valuable input into equipment and TTP development for EOD resources.
	(j). Is there any evidence of secondary (left behind) timers being used to deter reactive follow up by security forces?	Record the time delays normally used during such attacks from the time of the initial attacks and when primary devices are discovered. This trend will indicate a desire to disrupt the efforts of first responders, including EOD and follow-up investigators.
	(k). Are long delay timers (time measured in hours or days rather than minutes) being used, and, if so, what are the targets for these types of devices?	Historically, these types of devices have been used to attack venues or events that are likely to be subject to some form of security search prior to their occurrence. The intention is to place the device in a hidden location so that it's unlikely to be discovered during preemptive search operations.
6. Device Switch Types, Victim Operated IEDs (VOIED) Devices	(a). Are VOIEDs being used in isolation or as part of larger scenarios?	Also examine whether VOIEDs are being used to target specific individuals or likely responders. VOIED switches are categorized in the WTI Lexicon as being initiated by pressure, pressure release, pressure/pressure release, sensor, tension, tension release, collapsing circuit, and membrane switch.
	(b). Is there evidence that terrorists are carrying out elaborate tactical design (i.e., designing scenarios and events to draw security forces into the area of VOIEDs built to match the scenario?)	Consider whether a degree of tactical design is being used by the terrorists to place the VOIEDs where they are likely to be triggered by first responders or investigators following an initial attack or event.
	(c). What is the sophistication level of the actual devices?	VOIEDs can be very simple in construction (e.g., trip wires, pressure pads, tilt switches) or sophisticated (e.g., Passive Infrared [PIR], active infrared, vibration sensors, light-sensitive devices). Consider also the elements of tactical design applied by the terrorist to make the device work regardless of its apparent sophistication.

General Factor	Detailed Factor	Criticality/Importance
	(d). Is there evidence of sophisticated intruder alarm sensors, such as passive infra-red, active infrared, microwave, or ultrasonic sensors being used?	If this is the case, identify models used, sensor ranges, and likely supply chains.
	(e). Are terrorists making use of whole alarm systems as devices?	An unusual trend that may indicate a high level of sophistication. The majority of alarm-based VOIEDs or command IEDs use only key components such as sensors or the actual arming system such as car alarm arming and disarming radio key fobs. Whole alarm systems are rarely used as IED circuits, although their method of operation and use lend them to use as victim operated IEDs (VOIEDs).
	(f). What types and sizes of explosive charges are being used with VOIED devices?	This varies depending on the target selected and the sensing area of the actual device. A device that can sense the presence of the target and can trigger when the target is still fairly remote may require a large main charge. This is also the case when a larger target, such as a military or police patrol, is being targeted. Smaller charges may be used when the terrorist can be confident that the target will be in close proximity or may even handle the VOIED.
	(g). Are the devices small and designed to kill an individual, or do they incorporate large charges designed to damage a larger group such as a police or army patrol?	See (a) above.
	(h). Are EOD Technicians being deliberately targeted by VOIEDs, and, if so, are these devices successful?	This is a trend normally linked to the overall success rate of the bomb technician. Terrorists recognize that EOD teams form part of the response force and have a part to play in the prosecution of terrorists following the recovery of IED components. EOD Techs are also seen as high value targets that cannot be readily replaced, unlike other first responders. Also, examine the relative sophistication of such attacks and whether they are exploiting weaknesses in EOD SOP or equipment.

General Factor	Detailed Factor	Criticality/Importance
7. Device Switch Types, Command Devices	(a). What types of command switches are being used?	The WTI Lexicon categorizes command switches into the following categories: Command Wire (CWIED), Pull, Radio Controlled (RCIED), Optical, Active Infrared, and Command Projectile.
	(b). Does the type of switch vary depending on the target being engaged?	
	(c). Are radio control switches being used?	Will determine if ECM is required
	(d). At what ranges are the common command switches in each main group (RCIED and CWIED) being used?	Are these distances assessed or confirmed? What evidence was found?
	(e). What is the assessed source of the technology involved?	Consider where the switches were made, whether available for sale in the target country, and likely routes of supply.
	(f). Is there any evidence that custom circuits are being used, or are switches based on existing transmitter and receiver technology?	Custom switches might indicate some sort of internal construction capability, with specific switches being fabricated to address specific conditions. Switches based on existing radio equipment can be relatively unsophisticated, making use of readily available transmitters and receivers adapted with simple add on firing circuits.
	(g). Is there any evidence that electronic counter measures (ECM) are being countered by the design, method of operation, or placement of RC devices?	This can be a long process but it is possible to identify a progression of switch types encountered and tactics used by terrorist as ECM starts to reduce the effectiveness of RC devices. Transition into other areas of the radio spectrum, such as that which uses microwaves or light triggering, may indicate that the terrorists are becoming frustrated by their attacks being disrupted by ECM effectiveness. A shift to other targets not equipped with ECM and use of enhanced tactics and placement to negate ECM coverage may also be identified.
	(h). Have the terrorists developed identifiable safety and control features such as dual tone multi-frequency (DTMF) coding as a result of device failures?	DTMF coding provides a "key code" that ensures safety for the terrorist placing the device. It also ensures that the device is not triggered by stray signals once placed and that the terrorist can ensure the device functions at the optimum time.
	(i). Are there indications of	Worldwide trends in the use of RCIEDs should be examined to determine if terrorists are making better progress in design

General Factor	**Detailed Factor**	**Criticality/Importance**
	technological leaps that might have been enabled by "borrowed ladders" — the technical input from other, more developed groups operating in other countries or theaters of operations?	and use of RCIEDs than could normally be expected.
8. Device Types, Projected Weapons	(a). Are these conventional ammunition items being used as designed, adapted for use in improvised launchers, or wholly improvised?	This will depend on availability of ordnance and the levels of control available to limit the supply to terrorists from other nations. Wholly improvised launchers and weapons systems are normally encountered in countries where terrorists have little choice due to the lack of readily available ordnance such as rockets, mortars, or missiles.
	(b). What are the respective effective ranges of the weapons?	Consider the ranges used and the on-target effects.
	(c). What are the effects on target and, in particular what are the effects on vehicle armor and protected structures?	Consider whether projectiles are being designed for particular purposes. Do the terrorists use different weapons depending on targets attacked?
	(d). Is there any indication of weapons development keeping pace with or attempting to outdo countermeasures development?	If armor is being modified, are the terrorists applying EOD/engineering skills to the design of their weapons to make them more effective?
	(e). What forms of initiation are being used?	Are the projectiles employing point detonating, time initiated or other means of detonation? Consider the sophistication of such initiation systems and the implications for EOD/first responders.
	(f). Are the devices launched by the use of time, victim operated or command switches?	This will depend on the target being attacked. Time may be used for static targets, while victim operated or command switches are likely employed against mobile targets.

NOTE: Information contained in this appendix was derived from a TSWG commissioned project entitled "*A Mechanism for Establishing the Potential for Transfer of Weapons Intelligence (WEPINT) Capability to Other Nations.*" August 01, 2007.

General Factor	Detailed Factor	Criticality/Importance
	(g). Are there any indications that the timing of attacks is being staggered to exploit follow-up responses (i.e. separate salvoes being used with a significant interim delay)?	This may involve the use of several salvoes to catch first responders or survivors of the first attack.
	(h). Is there a discernible program of development and operational feedback from incidents being followed by the terrorists?	This may include attempts to gain access to attack sites and gather post-operational feedback to enhance the design of future or existing systems.
	(i). Are projected weapons being used as an element in sophisticated attacks that also include the use of other IEDs?	Consider secondary devices at firing points or first responder positions.
9. Device Types, Main Charge, Explosives Used	(a). What types of explosives are being used by the terrorists?	Consider only what has been recovered from IED incident evidence or found in terrorist caches or bomb factories.
	(b). Do they have access to military or commercial explosives?	This may indicate their ability to sustain a campaign if they are only making use of recovered ammunition items. A system of collection and disposal may limit activity. If commercial explosives are being used, there may be potential for further investigation to identify and reduce sources of supply.
	(c). Are they producing their own Home Made Explosives (HME)?	Is this confirmed?
	(d). Is recovered HME being analyzed to identify constituent elements?	Have the actual chemicals used been identified following recovery of a sample from an incident?
	(e). Are there legal and procedural instruments in place to limit the availability of HME constituent elements?	It may be possible to control or even reduce the sale of such constituents to limit the capability of the terrorists. In some countries, a reduction in the ammonium nitrate content of fertilizers has had an impact on the use of HME.

General Factor	Detailed Factor	Criticality/Importance
	(f). Is detector equipment in use that is capable of detecting HME or commercial and military explosives?	Consider all aspects of this requirement, including "sniffer" systems at border controls and portable systems used by police and military patrols.
	(g). Are these detectors field deployable, and, if so, to what level are they issued?	Are there, for instance, portable testing kits issued to every police or military patrol to confirm or deny the presence of explosives in suspect materials.
	(h). What is the largest commercial or military explosive device used/encountered so far?	Consider those recovered because terrorists' claims of device size tend to be exaggerated for propaganda purposes.
	(i). What is the largest HME device encountered so far?	This will give an indication of overall capability to mount large scale attacks, especially if there was a lull in activity after such an attack.
	(j). How effective are the terrorists' own HME recipes?	Is there evidence of devices failing to propagate the main charge?
	(k). Are there any handling or safety implications in HMEs being used?	Some constituent parts of certain HME recipes are caustic or highly toxic. This will have an implication for terrorists during mixing operations and for first responders, especially EOD, WIT, and forensics teams during investigations. Some materials may also be highly sensitive when mixed and lead to significant handling hazards.
	(l). Have there been any incidents of premature explosions involving HME?	This may be linked to the storage, handling, or use of the HME.
	(m). Have the tools and equipment normally used during the manufacture of HME been identified?	Identify the commonly encountered tools and equipment used for mixing and preparation of HME. Items such as coffee grinders and cement mixers may be used to prepare and mix the constituent materials. Some items may have been heated to concentrate the chemical solutions used. This may lead to "search indicators" when planning ongoing operations to detect mixing factories.
	(n). Do terrorists have a ready supply of demolition accessories (e.g., detonators, booster charges, and	Although these items can be improvised, such activities can be hazardous, and terrorists will tend to use commercial items when possible. A limited supply will therefore have a limiting effect on any campaign.

General Factor	Detailed Factor	Criticality/Importance
	detonating cord) available to them?	
	(o). What types of initiators are being used?	
	(p). Are there procedures in place to identify and track the types and quantities of initiators being used?	The IED initiator (usually a blasting cap) is the key to the successful initiation of high explosive material. Any efforts to identify, trace, and limit their supply will have a direct impact on terrorist campaigns.
	(q). Is there any indication where these items were sourced?	This may have implications for spoiling operations and breaking terrorist supply chains.
	(r). Do the terrorists go through a phasing period with discernible lulls in activity that is likely to be linked to the availability of initiators and particular detonators?	This may be a strong indicator of robustness and limitations of terrorist supply chains used to supply these essential items.
10. Device Types, Suicide Devices	(a). Do the terrorists employ suicide bombers?	Consider evidence of such attacks, including attacks where there was no evidence of device type, but the scenario strongly indicates a particular firing system.
	(b). What have been the targets of these types of attacks?	Consider why the suicide device was used and whether it indicates a tactic devised to defeat a certain level of security and secure an attack against a high value target. This may also give indicators of device type being matched to particular targets
	(c). Are the devices effective?	Are suicide bombers being used because other means of attack have been thwarted by the use of physical security measures? Consider also whether the suicide bomber is having an effect on morale even when the actual attacks are limited in effectiveness.
	(d). What forms of switches are being used in these devices?	
	(e). Are there any indications of RCIED systems being used as the primary or backup firing switches in	Consider devices recovered and scenarios where there is a strong indication of a secondary initiation system being used after the suicide bomber has been killed or otherwise disabled.

General Factor	Detailed Factor	Criticality/Importance
	suicide devices?	
	(f). Are suicide IED attacks coordinated in a number of areas to increase effect?	Consider attacks against single targets using multiple bombers and coordinated attacks against different targets in different areas.
11. Tactical Design (Method of Employment)	(a). How do terrorists employ improvised devices?	Consider all weapon employment methods such as but not limited to: Vehicle Borne IEDs (VBIED), Water Borne IEDs (WBIED), Projected IEDs, Person Borne IEDs (PBIED), Animal Borne IEDs or Air Borne IEDs (ABIED)
	(b). What have been the targets of these types of devices?	VBIEDs and PBIEDs may be used against buildings and personnel, while WBIEDs have been effectively used against ships and other maritime infrastructure. Additionally, projected and ABIEDs may be effective when targeting areas within a secure perimeter.
	(c). Is the employment method effective?	Consider their effectiveness against the targets they are used to attack and their overall effectiveness in undermining morale. Consider also the cost of putting in place the relevant controls, checkpoints, and infrastructure protection to counter the threat.
	(d). What forms of firing switch are being used in these devices?	These could include time, victim operated, command, or a combination of these types. Command and victim operated are likely to be used for attacks on personnel, whereas time is more likely to be used against static targets or structures.
Part Two - Assessment of WTI Capability Matrix		
1. IED Scene Handling and Management	(a). What training have the police and/or military forces received in the confirmation, cordoning, clearing, and control of terrorist incidents?	Consider how effective this training is and to what level it is given. Consider if the police or military forces are regularly tested in their response to such incidents and whether their responses are modified in the light of terrorist tactics.
	(b). What processes exist for the updating of police, border control, and other investigating agencies on trends and tactics identified during terrorist incidents?	Is there a process for disseminating lessons learned to ensure first responders are kept aware of current trends, especially where they affect their likely responses to incidents?

General Factor	Detailed Factor	Criticality/Importance
2. Agencies Involved in WTI	(a). Which agency has primacy during the investigation of terrorist incidents? Are these agencies' responsibilities modified by geographic constraints?	Consider whether there is an overall agency that can have primacy over all aspects of the investigation, or whether the primacy can shift depending on factors such as the area of the attack or the target.
	(b). Which agency (police or military) is responsible for the rendering safe of terrorist IEDs?	This may be dependent on the incident location. Police may be responsible for urban areas, and military may be responsible for rural IED clearance tasks.
	(c). Who is responsible for responding to attacks against government facilities?	
	(d). Who is responsible for incidents occurring on aircraft in flight over host nation airspace?	
	(c). Who is responsible for responding to incidents on ships at sea in host nation waters?	Navy? Police? Military EOD?
3.a. WTI Forensic Investigation	(a). How is forensic evidence handled at a terrorist scene?	Do EOD teams exploit/process the scene, or is it handed over to the police following confirmation that the area is clear.
	(b). What agency gathers the evidence from such a scene?	Police? Military? Specialized post-blast search teams? Forensic scientists from the country's forensic lab(s)? Bomb data center (BDC) personnel?
	(c). Does this agency have an on-call team ready to respond immediately in the event of a terrorist incident?	How is this on-call team configured? Does it include forensic scientists? Who does it report to? Are there direct links to a BDC?
	(d). Where is gathered evidence submitted?	Is there a central forensic science lab that specializes in post-blast investigation? Are there regional forensic labs?

General Factor	Detailed Factor	Criticality/Importance
	(e). Is biometric data collected at the scene or during subsequent investigations?	Consider whether all aspects for evidence collection and handling are in place to ensure valid samples can be taken and protected from contamination.
	(f). Is there an in-country laboratory with the capability to carry out the full range of forensic studies required to investigate a terrorist incident?	This includes testing for explosive residue, categorization, and identification and matching of recovered components, firearms, and ballistics testing, as well as departments able to handle fingerprint, DNA, blood, paint, fiber, and tool matching tasks.
	(g). Is there a dedicated explosives laboratory?	Does this lab have a backlog of cases? Is there a system in place to prioritize incoming cases?
	(h). Is any part of the forensic investigation process completed out of country or can all required tests be completed in country?	This may be the case for DNA testing and some aspects of explosive testing.
	(i). What are the reaction times for these procedures?	Consider also geographical displacement and area coverage.
3.b. EOD Responses	(a). What training do the host nation EOD agencies receive?	Consider currency, levels of training, whether high or low threat, qualifications, ongoing validation, and licensing requirements.
	(b). Are they trained in gathering of forensic evidence following a terrorist attack?	Consider whether they have a role in the collection and processing of evidence. Consider also whether teams are trained in specific post-blast scene management procedures.
	(c). Do they attend training in other countries?	Consider type, duration, and currency of training. Also confirm whether all members of a unit are trained or only select individuals.
	(d). Have they been trained and are they able to operate in an environment requiring the collection DNA materials?	There are a number of conditions of dress, handling procedures, and packaging that must be applied to maintain the integrity of the source evidence.

Weapons Technical Intelligence (WTI) Capability Matrix
Potential Establishment of WTI Capabilities with Other Nations

General Factor	Detailed Factor	Criticality/Importance
	(e). Is their clothing and equipment approved for use during the forensic examination of a terrorist scene?	This includes disposable boots, gloves, clothing, and face masks.
4. Reporting	(a). What reports are submitted following a terrorist incident?	Consider existing EOD, police, and WTI reports.
	(b). How are these reports disseminated?	Are they available electronically? Are there conditions of classification that may limit their distribution?
	(c). Who produces the recognized definitive report on the incident?	Consider whether there is any form of existing WTI report produced.
	(d). Do reports cover aspects of terrorist tactical design of the incident and identify trends in terrorist tactical effectiveness?	Consider whether the report examines this aspect as well as the technical and evidential aspects of the incident.
	(e). Is there a specific WTI report produced?	By whom?
	(f). Is a photographic record made of a terrorist attack scene?	Is this solely produced by the police as an element of evidence gathering?
	(g). Who makes this record?	Law Enforcement, EOD, or other agency?
	(h). How is the resulting media handled?	Electronic or wet film? How is it processed? Is electronic media subjected to archiving using "image authentication" software? How is electronic data handled and recorded?
	(i). Is it considered as evidence and subjected to handling constraints similar to forensic material?	Does this significantly limit the options for immediate distribution and handling?
	(j). Is use made of digital capture methods?	Is the distribution of this controlled through "image authentication" software? Are any images made available for wider use outside of the evidence collection chain?
	(k). Is video used at a scene?	Who records this? How is it handled? Is it copied and sealed as evidence? Is it subject to editing?

NOTE: Information contained in this appendix was derived from a TSWG commissioned project entitled "*A Mechanism for Establishing the Potential for Transfer of Weapons Intelligence (WEPINT) Capability to Other Nations.*" August 01, 2007.

General Factor	Detailed Factor	Criticality/Importance
5. Follow-Up Analysis and Investigation	(a). How is information relating to WTI from a scene handled?	Is there a specialist agency able to identify, analyze, compare, and use WTI data? Where is this agency located?
	(b). Which agencies receive this information?	Consider transfer of information up, down, and sideways. Consider whether this information is delivered in a timely manner to effect local operations as well as strategic tracking tasks. Consider cross-agency handling and the levels of disclosure.
	(c). How is this information collated and managed?	Is it available in electronic format? Is there a system available for distribution across agencies if WTI report is to be produced?
	(d). Is it placed within a searchable database?	Consider the ability to search for data using time, geographical, type, target, effect (including casualties sustained), and components recovered. Also consider whether reports can be searched for key words and phrases. Consider whether the database is capable of generating standard or customized reports using a combination of data fields and key word search parameters. Consider the location of this database and whether it is searchable by a few key agencies, or whether it has wider distribution that allows searches to take place at any access point.
	(e). What analysis of the information takes place?	Are there dedicated WTI specialists carrying out routine tasks to identify, track, and confirm sources of WTI data? Do these specialists provide operation enabling insights on the basis of identification of WTI data?
	(f). Is the information subject to fusion with other elements of the investigation including HUMINT and SIGINT?	Consider the levels of fusion and the possibility of WTI data being an operational driver when fused with other data. This does not necessarily relate to the investigation of the actual attack but can lead to wider operational opportunities for exploitation.
	(g). Does the WTI report inform the tactical and technical countermeasures effort?	The US model is that all interested parties with a role in the provision of countermeasures have access to WTI reports to inform and, in some cases, confirm their work. Consider how this will relate to certain "no for" limitations on the vulnerabilities of equipment, especially armor and ECM.
	(h). Is there an agency carrying out countermeasure design and analysis work on behalf of the government?	Is this a government agency or a contractor? What levels of security clearance will have to be in place for them to receive timely WTI data?

General Factor	Detailed Factor	Criticality/Importance
	(i). Who provides the technical analysis of WTI?	In the UK model, EOD specialists with a Technical Intelligence background are placed at key positions in the chain of command to provide detailed technical analysis when required. These specialists may require close links with forensic gathering agencies and even assign liaison officers within the establishments to ensure early sight of new or unusual trends.
	(j). Is there a body able to provide technical assessment of the technological aspects of terrorist device design and that recognizes the implied requirements for technical, tactical, and procedural countermeasures?	This should mimic the capability of TEDAC or SCIAD (scientific advisor) in theater to provide immediate technical solutions ahead of the wider development of countermeasures. It should also ideally provide a categorization and testing facility to rapidly identify radio control devices and their operating parameters.
	(k). Would there be any resistance to using a reach back capability (to CONUS) that would enable some of this technical analysis to take place?	Consider how this form of reach back capability might work alongside existing forensic procedures and protocols. Consider timelines and how this might be expedited using existing lines of communication.
6. Existing US Involvement	(a). Are US law enforcement agencies already dealing with the subject host nation?	At what level? Consider cross-training, information sharing, and what levels of operational support are given.
	(b). Is there a program of information sharing relating to terrorist incidents?	Consider formal and informal links as well as how timely they operate.
	(c). Is there a program of technical reach back to exploit WTI material?	How often has this been used? What, if any, were the delays?
	(d). Is the host nation linked, at any level, to CONUS law enforcement information systems?	Consider one-way and two-way traffic.

NOTE: Information contained in this appendix was derived from a TSWG commissioned project entitled "*A Mechanism for Establishing the Potential for Transfer of Weapons Intelligence (WEPINT) Capability to Other Nations.*" August 01, 2007.

General Factor	**Detailed Factor**	**Criticality/Importance**
	(e). Is there an existing memorandum of understanding relating to WTI gathered from incidents involving identified US targets and interests?	Consider whether a US agency could provide a field forensic team to provide support to other nation police forces during the investigation of a large IED incident. At what level would this support be provided? Would this support require full disclosure?
	(f). Does this include attacks against US "flag carrier" commercial companies or in-country-owned enterprises deemed to represent the United States?	
7. Specific Questions	(a). If a device exploded on the grounds of the US embassy, who would investigate the scene of the attack?	
	(b). If the attack consisted of a missile fired from a launch system 100 yds away and outside the embassy grounds, who would investigate the scene?	
	(c). If technical evidence was recovered at the scene, where would this evidence get examined?	
	(d). What would be the mechanism for providing that information to agencies for action on behalf of the United States?	

General Factor	Detailed Factor	Criticality/Importance
	(e). Would the police or the military render safe a device located against the outer wall of the embassy?	
Part Three - Assessment of WTI Processes and Capabilities Needed to Support and Coordinate WTI Efforts		
1. Forensic Capability	A forensic lab capable of carrying out the examination of forensic data recovered from explosion scenes	This should be able to identify explosive residues from contacted material and match components that have been subjected to the effects of an explosion. This lab should ideally be able to isolate, classify, and identify DNA material from submitted exhibits, including the essential database to make these exhibits searchable. The lab should have a field deployable team capable of conducting specialized collection tasks at the scene of significant incidents.
2. Technical Exploitation Agency	A technical analysis agency	This should be able to identify the specific make, model, and type of any electronic circuit recovered in either a complete or damaged state. This agency should have a specific expertise relating to the use of RCIEDs and be able to provide specific data contributing to ECM spectrum management planning. This organization requires the ability to technically exploit all forms of electronic equipment recovered during WTI tasks and carry out the identification, testing, categorization, and working parameters of recovered or matched equipment. It should also have links to the forensic laboratory to enable "quick look reporting" of significant equipment during the forensic investigation process when urgent action is required. It is possible that this agency would form part of the forensic capability but is not necessarily required to do so.
3. Intelligence Structure	A developed intelligence structure	This should be able to deal with technical WTI data recovered from IED scenes. This structure must be able to exploit all aspects of WTI activity at all levels. Dedicated WTI specialists should be in place at different levels that can provide a technical overview of incidents and also work closely with other agencies to exploit WTI across agency and geographic boundaries. This WTI specialist should have access to the worldwide community of BDC and be able to liaise closely with them.

General Factor	Detailed Factor	Criticality/Importance
4. Reporting and Database System	A standardized reporting and database system	This should be able to readily adapt and incorporate the raw data provided by WTI reporting. The system should be searchable and able to provide data patterns using recognized input relating to time, geography, types of incident, types of device, recovered components, groupings involved, and incident effectiveness, among others. The reporting system should make WTI reports available at all levels to maximize exploitation of strategic and tactical intelligence.
Part Four - WTI Infrastructure Necessary to Support WTI Training		
1. WTI Policy	This should be in place prior to the training being considered. There should be a clear understanding of how WTI teams will be used. A system to assess staff for ability to fulfill a requirement, similar to the doctrine, organization, training, material, leadership and education, personnel, and facilities (DOTMILPF) system, should be used. A developed policy is clearly the first step in the formulation of a training regime.	How WTI teams are to be configured, equipped, tasked, managed, and deployed should be agreed upon prior to the start of training. This will allow the training to have a fact-based operational focus rather than an assumption-based focus.
2. Student Start States	Candidates for WTI team training should be carefully selected to ensure overall suitability for the role and efficiency of training.	Although a well-structured training regime should be able to take students with only limited experience and turn them into effective investigators, there are clearly advantages in selecting students for the role. To ensure cross-skill redundancy within a deployed team, all members of that team are given the same detailed package of training. In countries where English is not the de facto second language, then consideration should be given to trainer training, followed by mentored dedicated team training; otherwise all training should be carried out in English.

General Factor	Detailed Factor	Criticality/Importance
3. Facilities Available	(a). A suitable classroom	This should be well lit, ventilated, and accommodate classroom instruction, including the use of dedicated IT systems when teaching report writing.
	(b). A realistic training area	This should provide a number of "target" buildings and areas that can be used to run realistic training scenarios. The targets available should include stretches of roadway, buildings, simulated or real infrastructure targets, and cache or bomb factory sites. Where possible, these sites should be separated geographically from each other to ensure that teams are not working too closely together during exercises.
	(c). A demolition range	This should allow for the detonation of large simulated IEDs during training and assessment of WTI teams. The ability to accurately stage post-blast scene areas adds significant realism to the training package and helps to prepare teams for the demands of operational investigation. Depending on the start state of the students, there may also be a requirement to carry out an explosive effects demonstration. Ideally, the range should have suitably trained and qualified staff to handle, prepare, place, and initiate the explosive charges used during demonstrations and exercises.
	(d). Explosives	There is a requirement for suitable explosive components for use during demonstrations and assessment exercises and a detailed list of the explosives required to support training.
	(e). Equipment	A standardized equipment list is necessary to detail the equipment required for the basic WTI mission. This list should include some of the items issued to US WTI teams to enhance their utility at a scene. To ensure effective training, each WTI team should be allocated the same complete set of equipment as would be issued for operations.
	(f). IT	Ideally, each team should have access to a laptop computer linked to a LAN capable of mimicking the types of IT systems they are likely to use when deployed. This requirement also extends to the assessment exercise period of the course. As an example, US Military WTI teams use a system designed to give all of the functionality of the IT systems they use when deployed in Afghanistan.
	(g). Vehicles	Each team should have a vehicle capable of deploying them to remote sites of an exercise or training area. These can be military or civilian type vehicles.

General Factor	Detailed Factor	Criticality/Importance
	(h). Training Aids	A large number of simulated IEDs and other training aids are required. These may include simulated ammunition items for use as main charges in IED scenarios, if those types of charges are being encountered

Appendix E.
The CJ2E Concept

Combined Joint Intelligence Exploitation (CJ2E)

Introduction. The CJ2E is an in-theater command and control structure that is established as necessary to integrate and synchronize disparate theater-level military, intelligence, LE, multinational and HN collection, exploitation, analysis, and dissemination capabilities and processes.

The CJ2E concept was first implemented by the International Security Assistance Force (ISAF) International Joint Command (IJC) in Afghanistan in 2010 to address the operational challenges inherent in an asymmetric environment and to ensure the outputs of the exploitation enterprise were fully integrated into intelligence collection, exploitation, analysis and reporting.[1] Establishment of a CJ2E can be tailored to meet the operational needs of the regional commander and to support all operational phases (**Figure E-1**). While the CJ2E is well suited for an asymmetric environment where insurgents seek anonymity in the population, it is not suited for a task force engaged in mid- to high-intensity combat. In that circumstance, collection and exploitation support would likely be focused on helping illuminate enemy plans and intentions.

Historically, the Army has deployed an echelon above corps military intelligence battalion to serve as the theater's TECHINT organization responsible for the exploitation of captured conventional enemy weapon systems. During a conventional conflict, this TECHINT organization may be directed to serve as the core upon which a Joint Captured Material Exploitation Center (JCMEC) is established. Traditional TECHINT of state-sponsored, conventional weapon systems involves a methodical and deliberate process that, while sufficient to support a commander in a conventional conflict, is not well suited to the rapidly changing asymmetric threat environment such as that recently experienced in Iraq and Afghanistan.

These new asymmetric threat environments presented the challenge of managing and coordinating forward deployed forensic, biometric, document and media, and electronic exploitation activities at the tactical and operational levels. Captured material from an asymmetric environment was subject to numerous laboratory examinations capable of revealing enemy battlefield technical evolutions as well as to exploit DNA and fingerprints used to associate material or people with specific activities and locations. Establishment of the CJ2E proved necessary to manage the disparate service and interagency exploitation activities required in this rapidly evolving asymmetric threat environment.

[1] NOTE: CJ2E was established shortly after stand-up of ISAF Joint Command (IJC) to create a theater-level command and control structure for integrating and synchronizing exploitation capabilities and processes in the Afghanistan Theater of Operations (ATO). Two Fragmentary Orders (FRAGO): ISAF FRAGO 122-2010 (Establishment of the ISAF/IJC CJ2E) and IJC FRAGO 198-2010 (Exploitation Synchronization Working Group) formalized coordination authorities, staffing, roles, and processes for theater exploitation.

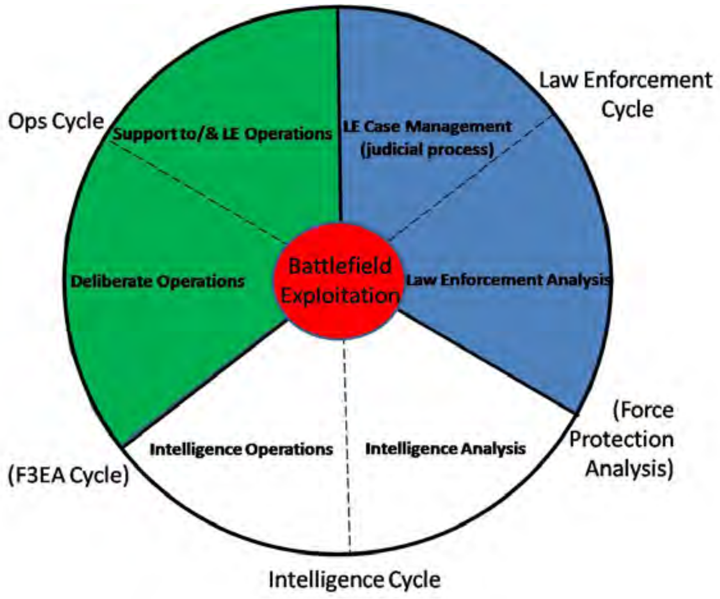


Figure E-1. Range of Exploitation's Consumers. *A commander's exploitation capability must align to support specific analytic and operational needs. Support to F3EA targeting cycle links human signatures (DNA and fingerprints) to materials and locations or force protection by identifying new and emerging threats in a timely manner. The same system of exploitation capabilities can transition to support the prolonged detention and prosecution of captured insurgents and terrorists.*

Mission. The mission of the ISAF IJC CJ2E is to:

- Coordinate and synchronize the exploitation of captured enemy materials to maintain a common operations picture over exploitation resources across the battlespace
- Advocate, manage, and maintain the exploitation architecture, systems, processes, and procedures to ensure information visibility
- Gain situational understanding of all exploited material in Afghanistan theater of operations (ATO)

Figure E-2 illustrates the wide range of exploitation activities. IJC CJ2E partners with the NATO Training Mission – Afghanistan to achieve unity of effort to develop Afghanistan National Security Forces exploitation capacities and capabilities.

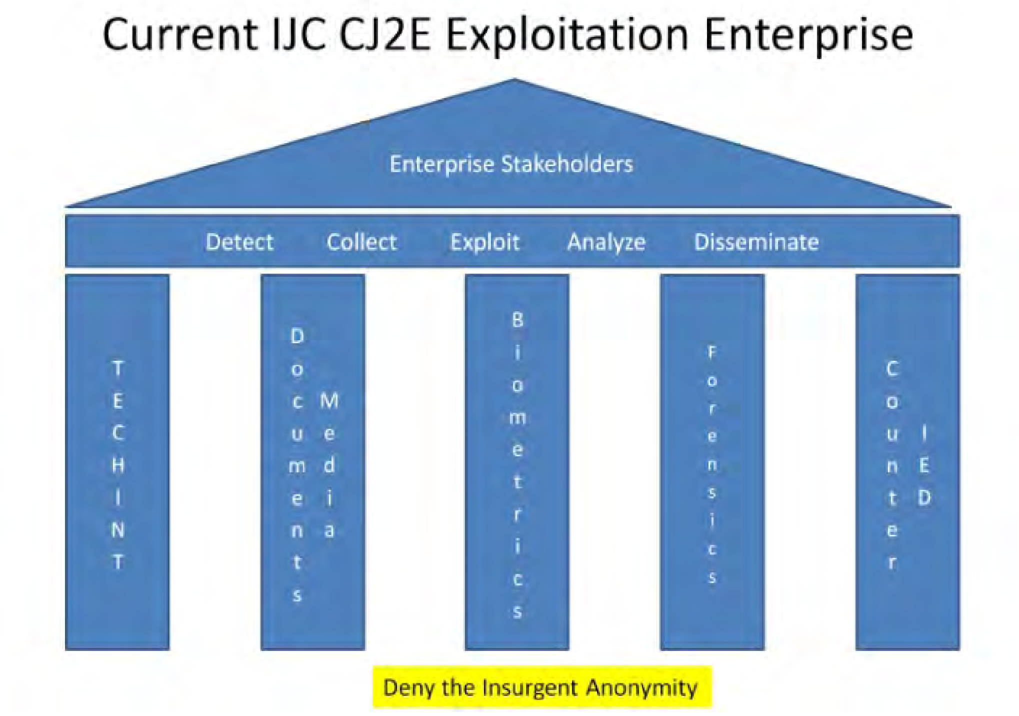


Figure E-2. Pillars of Exploitation. *The pillars represent a wide range of exploitation activities. The commander, aided by the J2E, prioritizes the pillars' introduction into an operational theater on the basis of mission requirements, type threat faced, and authorities granted to collect and exploit captured enemy material and equipment.*

Establishment. Institutionalization of a CJ2E ensures a centralized theater coordinating authority exists that is adequately manned and equipped to integrate and synchronize battlefield collection, exploitation, and analysis capabilities and processes in support of a range of stakeholders representing military, intelligence, and law enforcement communities. The CJ2E serves as the synchronizing organization to facilitate the coordination of exploitation activities with all stakeholders and partners, to include multinational and HNs to ensure unity of effort when:

- Developing priorities for collection and exploitation
- Directing and synchronizing the introduction of exploitation capability into the battlespace
- Adjusting the location and level of exploitation effort based on mission needs

Instrumental to the CJ2E is its role in policy discussions that facilitate information sharing agreements between coalition partners and host nations. The CJ2E exploitation enterprise coordinates and synchronizes the exploitation of a wide range of processes with varied outcomes that include:

- TECHINT (e.g., enemy weapons systems capabilities, employment trends, and the introduction of new capability or unique applications of existing systems)

- Document and media exploitation (DOMEX);
- Biometric enabled intelligence (BEI)/forensic enabled intelligence (FEI)
- Counter-IED (C-IED) information and material, such as the tactical characterization and technical categorization of a device, their forensic handling, electronic and mechanical engineering design, and explosive chemical attributes

Future.

Joint Staff. The CJ2E is an essential organization in the intelligence apparatus which supports the JFC during Joint Operation within the joint intelligence operations center (JIOC), as illustrated in **Figure E-3.**

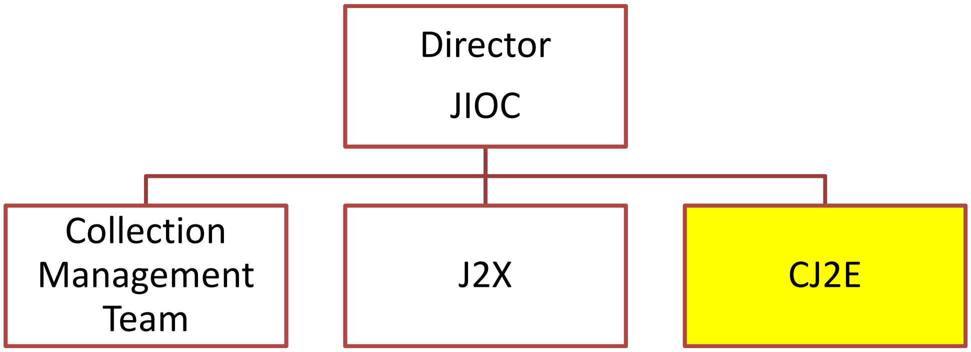


Figure E-3. *The CJ2E is organized under the JIOC Director.*

The introduction of a new exploitation capabilities in operational theaters that provide traditional forensic exploitation results (i.e., DNA, fingerprint extraction and database matching, explosive chemistry, firearms examination), as well as the ability to discover and download data from a wide range of electronic media at the tactical to the operational levels, requires management of a specialized staff to shape its contributions and to monitor efficiency. Synchronizing and directing service and command capabilities to support specific lines of operation or adjusting their outputs to dynamically adapt to new battlefield circumstances are particularly challenging. New battlefield circumstances include:

- Training host national forces to improve or build a captured material collection and exploitation system
- Transitioning from a system designed to support kinetic targeting operations and force protection material and method development to a process that producing outputs for prosecutorial purposes
- Identifying new enemy material capability and attributing it to its source

To address that challenge faced by the CJ2E requires continual engagement with subordinate operational staffs that are deployed across the battlespace, to ensure collaboration, eliminate redundancy and to effectively manage exploitation throughput. It is important to understand that operational commanders own the theater's exploitation system, not its contributors. Therefore, the

CJ2E provides governance to ensure that capabilities are continually adjusted to meet tactical and operational requirements.

Suggested Establishment. The CJ2E is typically task organized with services or components being leveraged to provide the necessary personnel and resources (recommended manning: O6 Director, O4/O5 Deputy, Biometrics SME, C-IED SME, and OPS Officer). These resources are necessary to execute the following tasks, at a minimum:

Tasks. The essential task is to coordinate and synchronize the technical and scientific exploitation of found or captured materiel and documents. Related tasks include the following:

- Evaluate and establish the commander's collection and exploitation requirements for deployed laboratory systems or material evacuation procedures based on the mission, its object and duration, threat faced, military geographic factors, and authorities granted to collect and process captured material

- Establish and maintain situational awareness of the employment and design of the enemy's primary weapons systems within the operational environment (for instance, in Iraq and Afghanistan the enemy's primary weapons systems is the IED)

- Quickly identify and characterize evolutions in the enemy's principal weapon systems technical attributes and associated signature data to maintain a common threat operating picture

- Coordinate exploitation systems, processes, procedures, and architecture to ensure there is common use of key terms to aid in data storage and retrieval, establish security classification guidelines for information sharing with host nation and coalition partner, and set the criteria for timeliness and format of exploitation reporting to meet the commanders' operational needs

- Ensure exploitation information visibility at all levels of operation to support force protection, targeting, material sourcing, and signature characterization of enemy activities (e.g., HME fabrication and IED emplacement techniques); the identification of weapon systems technical attributes that can be detected (e.g., frequency of the RF spectra used in IED components); and the provision of materials collected, transported, and accounted for with the fidelity necessary to support the prosecution of captured insurgents or terrorists

- Prepare collection plans for a subordinate task force responsible for finding, recovering, and neutralizing conventional and improvised weapons (e.g., Task Force Paladin, HME Task Force, etc.) and weapons of mass destruction

- Provide direction to forces to ensure that the initial site collection and exploitation activities are conducted to meet the commanders' requirements and address critical information and intelligence gaps

Training. Currently, there is no institutionalized staff training available for the CJ2E staff. Recent incumbents, prior to their deployment, have arranged their own situational awareness training with HQDA G38, NGIC, Joint Document Media Exploitation Center, and the DIA's Directorate for Science and Technology. A formal blueprint for training is needed as part of a strategy to mature and field the CJ2E staff. This training should cover the following:

- Benefits and limitations of the forensic science exploitation processes to provide useful results. (e.g., forensics is based on the comparison of an unknown to a known to provide a result of value; collecting and exploiting fingerprints has limited utility until a relational database to compare it against is established, which takes time)

- Impact of environmental conditions (e.g., heat, wind, blown sand, cold) on laboratory operations, their cost, and infrastructure support needs

- Match collection and exploitation capabilities against mission requirements and the threat (e.g., conventional mid- to high-intensity combat operations or having to identify insurgents as they hide in the populace)

- Familiarity with Service collection and exploitation deployable systems (e.g., what can they process, to what level of throughput, to what degree of fidelity/precision, and how quickly)

- Assess transportation network available to move captured or found materials from point of recovery to the laboratory system and the time needed to do so

- Familiarity with reach back support systems and interagency capabilities/roles to support deployed forces

- Evaluation criteria for host or supported nations' collection and exploitation processes and rule sets to determine how to integrate, complement, or support their efforts

Observations: The DoD, in a very limited time, has built and fielded a formidable range of technical and forensic exploitation capabilities that can support a range of outcomes in support of deployed forces. Commanders require a CJ2E element that can plan, manage and synchronize these exploitation capabilities. It must operate as a system of systems and be open, efficient, and adaptive. The CJ2E must be able to develop new processes as necessary to accommodate threat and mission evolutions in the operational environment, and to apply routines, rules, and SOPs to govern the activity occurring between each exploitation activity (e.g., terms, report content and format, processing times, and exploitation standards). Significant independent capabilities have been established within DoD, however the CJ2E is necessary to govern the processes and rules required to manage and shape their activity and define outcomes.

Appendix F.
Maritime Considerations and Enablers

Maritime WTI Considerations and Enablers

While the WTI processes of collecting, preserving, exploiting, analyzing, and disseminating material and/or information remain constant regardless of the environment, the potential complexities associated with conducting WTI Level 1 and 2 exploitation in a maritime environment poses unique challenges. These challenges require specialized capabilities and procedures, and may require extensive resources (manning, equipment, and support) and training to overcome.

Environmental factors such as current, depth, visibility, salinity and weather conditions can limit and/or preclude detailed collection efforts from an underwater incident site. These same factors can disperse and decompose post-blast materials if not collected in an efficient and timely manner. Preservation of materials from the water (fresh, brackish, or salt) can also be problematic as electronics and other materials can rapidly corrode or degrade if not properly preserved when recovered. Tactical (Level 1) and Operational (Level 2) technical and forensic exploitation of recovered improvised weapons, to include IEDs, and associated components from the maritime environment, will require specialized equipment, procedures, and training beyond those used in Iraq and Afghanistan. The following are some of the WTI exploitation process areas that require additional considerations and enablers when working in a maritime environment:

> Search: Localization of an incident site is key to collection success and may require the use of layered capabilities such shipboard SONAR or towed array SONARs to search large areas and/or the use of unmanned underwater vehicles (UUV), remotely operated vehicles (ROV), or diver held devices to develop detailed mapping of the debris fields to focus collection efforts. The Navy has extensive underwater search capabilities located at Mobile Diving and Salvage Units (MDSU); at EOD Mobile Units; and in the Naval Fleet with shipboard SONAR, UUV, and ROV systems.
>
> Collection: Due to the environmental factors mentioned above, underwater post-blast (UWPB) investigations will likely require large numbers of divers from MDSUs and/or EODMUs, supported by UWPB SMEs from organizations like the IHEODTD TSD or FBI Evidence Response Teams (ERT), to conduct material collection efforts in support of large scale post-blast investigations. Additionally, specialists in damage assessment may be needed to investigate the targeted vessel or maritime structure to assist with post-blast material collection and determination of the method of attack and weapon used. The structural engineering and analytical capabilities of NSWC Carderock’s Survivability and Weapons Effects Department enable the analysis of weapons effects on maritime infrastructure and vessels, which can provide tactical insight into the employment method, type and size of weapon used in a maritime attack scenario.
>
> Preservation: Material preservation in a maritime environment poses unique challenges which must be taken into consideration before recovery efforts are initiated. The method of initial preservation of materials recovered at or below the waterline may depend on the type of material recovered; the availability of follow on exploitation capability; and expected time until the material can be exploited. Procedures may range from packaging

the material in the water it was recovered from for transport to an exploitation facility, washing the material in fresh water then air drying, or just air drying the material. Preservation of recovered materials from above the waterline would be in accordance with established procures. The ultimate goal in the preservation of recovered materials is to use the best method possible to enable follow on technical and forensic exploitation.

Exploitation: The potential for larger, more complex improvised weapons, to include IEDs, in the maritime environment generates the need for greater Level 2 exploitation capabilities than those traditionally seen in the Iraq and Afghanistan. These capabilities include additional more sophisticated X-ray diagnostic capabilities and advanced nondestructive disassembly techniques to enable technical and forensic exploitation to the greatest extent possible. The TSD CEXC program in coordination with the IHEODTD's In-Country-Exploitation (ICE) teams possess organic capabilities to conduct on site high power X-ray diagnostic operations, nondestructive disassembly , and technical exploitation of improvised weapons systems, to include IEDs, from the maritime environment. In cases where increased x-ray diagnostics and or nondestructive disassembly capabilities are not available, the use of explosive stripping techniques by Naval EOD technicians would be an alternative to enable the Level 2 technical and forensics exploitation of a weapon/device. The forensic aspects of the exploitation process are conducted by the DFSC FXD and TEDAC.

Appendix G.
Weapons Technical intelligence Generic Information Requirements Handbook (WTI-GIRH)

March 2014

Weapons Technical Intelligence Generic Information Requirements Handbook (WTI-GIRH)

Foreword

The Weapons Technical Intelligence Generic Information Requirements Handbook (WTI-GIRH) consolidates frequently used priority intelligence requirements/essential elements of information (PIR/EEI) to facilitate rapid planning for contingency operations and expeditionary forces. Staffs at all levels must be prepared to provide commanders with accurate, timely, and detailed intelligence/information in support of Weapons Technical Intelligence and Counter-IED requirements. This Handbook is intended to assist staff planning and execution of operations against potential asymmetric threats.

The WTI-GIRH differs from traditional GIRHs, in that it focuses not just on the enemy and the environment, but also on the blue force capabilities, architectures and missions.

The WTI-GIRH can be used as a checklist to determine information gaps, and as a baseline support tool for intelligence personnel providing operational intelligence to forward deployed units. This manual is not inclusive of everything that will be encountered in theater. It is intended to be used in conjunction with other supporting materials such as the following:

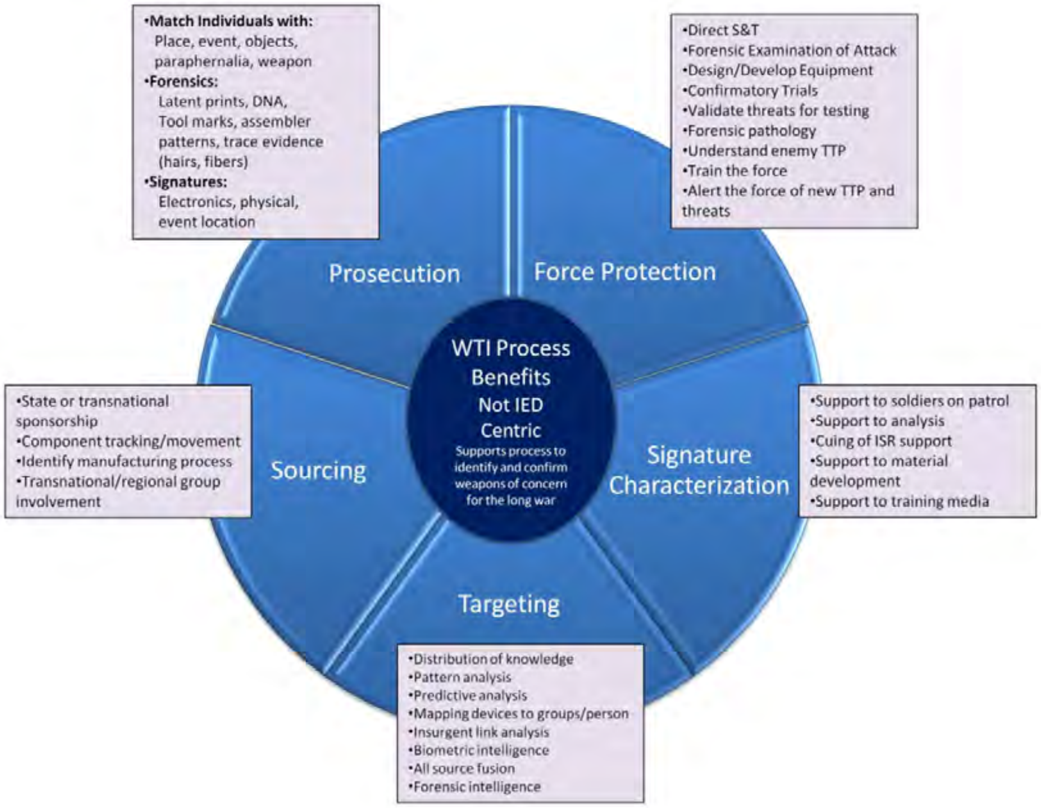
- Weapons Technical Intelligence Improvised Explosive Device Lexicon
- Weapons Technical Intelligence Homemade Explosives Lexicon
- Naval Explosive Ordnance Disposal Technology Division Explosives, HME Precursors and Blasting Caps Identification Guide
- Marine Corps Intelligence Activity General Intelligence Requirements Handbooks
- Central Intelligence Agency World Fact Book
- Jane's Books

Contents

Introduction

Weapons Technical Intelligence (WTI)

-A category of intelligence and processes derived from the technical and forensic collection and exploitation of improvised explosive devices, associated components, improvised weapons, and other weapon systems.


•Match Individuals with:
Place, event, objects, paraphernalia, weapon
•Forensics:
Latent prints, DNA, Tool marks, assembler patterns, trace evidence (hairs, fibers)
•Signatures:
Electronics, physical, event location
•Direct S&T
•Forensic Examination of Attack
•Design/Develop Equipment
•Confirmatory Trials
•Validate threats for testing
•Forensic pathology
•Understand enemy TTP
•Train the force
•Alert the force of new TTP and threats
Prosecution
Force Protection
WTI Process Benefits
Not IED Centric
Supports process to identify and confirm weapons of concern for the long war
•State or transnational sponsorship
•Component tracking/movement
•Identify manufacturing process
•Transnational/regional group involvement
Sourcing
Signature Characterization
•Support to soldiers on patrol
•Support to analysis
•Cuing of ISR support
•Support to material development
•Support to training media
Targeting
•Distribution of knowledge
•Pattern analysis
•Predictive analysis
•Mapping devices to groups/person
•Insurgent link analysis
•Biometric intelligence
•All source fusion
•Forensic intelligence

The Five Outcomes of WTI (Figure Credit: DIA/JIEDDO)

Variables That Can Impact WTI

Each Area of Operations (AO) has unique variables that can impact the ability to employ WTI exploitation in support of the unit's mission(s).

Representative variables include:

- COCOM emphasis on WTI
- Battlespace Geometry (Contiguous/Non-Contiguous)
- Location of activity (urban/rural or combination)
- Volume of enemy IED activity
- Operational Tempo
- Nature of the threat –enemy TTP
- Skill and adaptability of enemy IED designers and emplacers
- Military Geographic factors

Host Nation (HN) factors:

- Capability of indigenous EOD /Site Exploitation Teams, their SOPs/protocols for incident response, recovery, exploitation and reporting of results. (Who owns the problem)
- Where does sovereignty reside – what rules are in play?

Philippine Police investigate an IED attack (Photo Credit: DIA)

The level of COIN:

- The United States is in the lead in Combat Operations
- Combined Operations with U.S. Forces are routine, with HN Forces in the lead
- The HN Forces call on U.S. Forces for specialized capability when required

Levels of Exploitation & Analysis

The WTI process can be described as three distinct phases: tactical (Level 1), operational Level 2), and strategic (Levels 3, 4 and 5). The distinctions between these phases of activities are of time, place and customer –not of value. Tactical WTI activities occur nearest to the time and place of the incident, such as at an IED post-blast location. Actors in this phase can involve local military forces or law enforcement and will have an immediate impact on the environment. At the operational phase, activities are in direct support to the local, in-country forces, and these activities may or may not take place in the same country as the incident. Strategic phase activities may occur anywhere in the world and involve long-term effects with immediate international implications. This can include analysis of the international IED supply chain or targeting of a foreign participant outside of the immediate theater.

BIG QUESTIONS:

- What exploitation is needed at the tactical, operation and strategic levels to produce what outputs and products to serve whose needs?
- What are the results needed at that level? (Targeting, Quick, Incomplete / Prosecution, Longer, Complete)
- Outcomes needed for each level of exploitation? (Support to Targeting process, Force Protection, Component & Material Sourcing, Detainee Operations and Prosecution, and Signature Characterization).
- Are the necessary authorities and resources needed to match the exploitation requirements, at all levels, present to facilitate desired outcomes?
    - What are the logistical requirements to support the collection and exploitation?
    - Do we have primacy at the site/incident?
    - If not, do we have access to the captured materials/detainees?
    - Do we have access to the HN exploitation processes and outputs?

OBSERVATIONS: Addressing the questions provided above defines and builds the conceptual architecture for the near to mid-term range of WTI capabilities needed to support all levels of application and analysis.

Battalion and Brigade staffs must be intimately familiar with the timelines, prioritization matrices and logistical requirements associated with the exploitation process. The Staff needs to be aware of the impact that operations and the environment of the battlespace can have on this process, so as to effectively manage expectations and timeliness of the exploitation results/outcomes.

WTI and Intelligence Preparation of the Battlefield (IPB)

Weapons Technical Intelligence and Intelligence preparation of the battlespace should be used to benefit from one another in the most efficient manner. WTI helps serve the IPB by providing historical context in order to establish past responses and aid in developing future COAs. Information from the IPB goes back into the WTI process in order to remain as current as possible and continue to work hand in hand.

Intelligence preparation of the battlespace (IPB) is an analytical tool and process that is utilized to help understand the enemy, weather, terrain and other aspects of the environment, and the options and impact it presents to both friendly and threat forces. It is a systematic, continuous, and integrated process of analyzing the weather, terrain, and threat in a specific geographic area. IPB integrates threat doctrine with the weather and terrain as they relate to the mission within a specific battlefield environment. This is done to determine and evaluate threat capabilities, vulnerabilities, and probable courses of action (COAs). IPB results can be incorporated into the intelligence estimate, but more importantly, IPB products can be easily and quickly visualized and absorbed by decision-makers. The IPB process emphasizes providing intelligence in the form of graphics and images—formats that help the commander rapidly visualize, assimilate, and apply the intelligence in the decision-making process.

IPB assists in the preparation of estimates, friendly COAs, and in the analysis and selection of friendly COAs. It helps friendly planning by providing predictive intelligence designed to help commanders understand the threat's probable intent and most likely future COA. In assessing the threat's probable intent, most likely COA, and most dangerous COA, threat models are developed, based on his normal or "doctrinal" organization, equipment, tactics, techniques, and procedures. Threat models result from a detailed study of the enemy. Threat models consist of three parts: doctrinal templates, a description of preferred tactics and options, and identification of high-value targets (HVTs).[1]

Unfortunately, insurgencies and terrorists rarely publish a doctrine from which we can extract models and templates, and their irregular approach is seldom understood (even by those who have faced it) in sufficient detail to facilitate an effective IPB. Current counterinsurgency doctrine and publications provide very little, if any, assistance in providing quantifiable and specific information to help warfighters better comprehend, template, and predict insurgent enemies and their actions.[2]

If we apply these methods and doctrinal templates to the analysis of Saddam's conventional army in Desert Storm and OIF I, we see an army heavily reliant upon the massing of artillery fires in support of the defense (a page taken from U.S. General James Van Fleet's "Rolling Defense," a tactic he employed during the Korean War). This tactic required Saddam's army to maintain mammoth stockpiles of artillery ammunition, located in hundreds of Ammunition Supply Points (ASP) throughout Iraq.

After the fall of Saddam's army, and the subsequent cessation of Major Combat Operations, conventional wisdom would hold that "conventional" doctrinal templates had become obsolete. However, as the nature of the threat shifted from that of a conventional army to a guerilla force, and eventually to a complex insurgency, these doctrinal templates would be of use once again. Analysis of the insurgents' TTPs and history of attacks reveals the IED emerged as the enemy's weapon of choice. As insurgents sought resources for the IEDs being manufactured in country, artillery shells became the predominant Main Charge. The source of these shells was the oftentimes now unsecured, former regime ASPs. These ASPs had already been plotted on the map as part of the OIF-I conventional IPB process.

The Weapons Technical Intelligence (WTI) process can be applied to this situation, providing definitive associative connections between devices and components used in attacks, those found in insurgents' caches, individuals, and the original sources of these weapons and components. These associations can be mapped and plotted, helping to develop pattern and link analyses and insight into the terrorist and insurgent networks.

USMC EOD prepare captured ordnance for disposal (Photo Credit: USMC)

Chapter 1: Building the WTI Architecture

You will rely on the collection and passing of information and data to support your intelligence effort. You will need the data available from a variety of collectors –from the warfighters themselves, from intelligence units and collection systems. You will need to receive feeds from systems in your control, your subordinate units' control, higher and adjacent headquarters, theater, national, or coalition control. You will need to leverage other organizations to produce intelligence products that are beyond your organic capability –these will include Host Nation and Coalition organizations and entities. You will need to pass the products of your efforts to others with a proper clearance and a legitimate need to know. You will not succeed without leveraging every possible resource available to you, or more precisely, the resources that are available to you through the architecture you build.

> Architecture is simply the set of interconnected physical systems by which you will receive or pass information or data from one entity to another for a specified purpose. In thinking about an architecture, you will need to think about inputs, processors, communications and outputs. More specifically, you will need to think about hardware, software, communications, circuits, COMSEC materials, network classification, technicians, funding, database access, LNOs, training, and TTPs. All are necessary for an effective architecture.
>
> THE SIMPLEST VIEW: What do you want? Who has it? What will it take to talk to them?
> -MG James "Spider" Marks, US Army

Blue Force Baseline Intelligence Assessment

- ▪ What is your Mission
- ▪ What is the Commander's Intent?
- ▪ Describe your intelligence structure and how you are organized:
  - ▫ How are you manned?
  - ▫ Do your personnel have the skills and training to do what you are asking them to do?
  - ▫ What systems are you using to communicate?
    - ▫ Internally
    - ▫ Externally
  - ▫ How are these systems administered and maintained?
  - ▫ Relationships to other organizations

- ▫ Current operations
  - ▫ Support to decision-making in planning and execution -how do you:
    - ▫ Maintain real time situational awareness

        - Enable force protection
        - Support targeting
        - Guide collection

- Available Maps and Imagery
- Country Handbooks
- Priority Intelligence Requirements

WTI Exploitation Capabilities

- Anticipated outputs in support of:
    - Targeting
    - Force Protection
    - Prosecution
    - Sourcing
    - Signature Characterization
- Potential actions to be cued from Exploitation:
    - Additional Collection
    - HVI raid
    - Prosecution
    - ISR
- EOD
    - Organic?
    - Command relationship
    - Higher assets
    - Host nation assets
        - Do we have access?
    - Coalition assets
        - Do we have access?
    - Tasking procedures
    - Tasking priorities
    - Training
    - Collection capabilities
    - Reporting procedures
        - `Timelines
    - Products produced
    - Logistical requirements
    - ECM
    - CCIRs
- Weapons Intelligence Teams?
    - Organic?
    - Command relationship
    - Tasking Procedures
    - Tasking priorities
    - Collection capabilities
    - Reporting procedures

        - Timelines
    - Products produced
    - Logistical Requirements
- Site Exploitation Teams?
    - At what echelon?
        - Company
        - Battalion
        - Higher?
    - Capabilities
        - Search
        - IED material identification and collection
        - Latent print collection
        - DNA collection
        - DOMEX (Document and Media Exploitation)
        - Tactical Questioning
    - Support
        - Transportation of materials
        - QRF
        - Cordon
        - UAS
    - Host Nation
        - Evidentiary and prosecutorial requirements
        - Capabilities
    - Coalition
        - Evidentiary and prosecutorial requirements
        - Capabilities
        - Do we have access?
- Higher Echelon Forensic Exploitation (operational, strategic)
    - Anticipated outputs ISO:
        - Targeting
        - Force Protection
        - Prosecution
        - Sourcing
        - Signature Characterization
    - Forensic Exploitation Capabilities
        - Latent Fingerprints
        - DNA
        - Fibers
        - Tool marks
        - Chemical residue
        - Bulk Explosives
        - Ballistics
    - Host nation assets
        - Do we have access?
            - Materials
            - Prisoners

            - Products
            - Databases
            - Evidentiary and prosecutorial requirements
    - Coalition assets
        - Do we have access?
    - Tasking procedures
    - Tasking priorities
    - Reporting procedures
        - Timelines
    - Products produced
    - Logistical requirements
- Databases
    - Biometrics ***(fingerprints, irises, voice, face, DNA)***
        - Theater database (Size of data base – number of records by type modality: Finger print, DNA, Facial image)
        - National (FBI)
        - Host Nation (Will host Nation share biometric records, allow real time access for comparative analysis and provide match reports?)
            - National ID (Host nation provides criteria to receive, age when issued to citizen and counterfeit recognition tips.)
            - Criminal records
            - Military records
            - Current/Former Regime
            - Do we have access?
        - Size of Database
        - Systems requirements
        - Limitations
        - Collection
            - Devices
            - Procedures
        - Watch-list management
    - Host Nation Vehicle Databases
        - Do we have access?
        - VIN#s
        - Registration
        - License Plate Numbers
        - Driver’s License
- Detainee Operations
    - Detainee Collection Point/Facilities Locations
        - Transportation To/From
        - Time of travel
    - Holding Timelines
        - Company
        - Battalion

  - RCT/BCT
  - Security Agreements/Treaties
- Host Nation detainee facilities
  - Police
  - Military
  - Special
- Coalition Facilities
  - Do we have access to conduct questioning, gather intelligence and receive Host Nation reports?

Intelligence, Surveillance, Reconnaissance (ISR)

What assets are available?

- Human Intelligence (HUMINT)
  - Tactical HUMINT Teams (THT) / HUMINT Exploitation Teams (HET)
    - Organic?
    - Command relationship
    - Higher assets
    - Adjacent assets
    - Tasking procedures
    - Tasking priorities
    - Sources
  - Interrogator/Translators
    - Organic?
    - Command relationship
    - Clearances
    - Language skills
    - ROE/Detainee Guidelines/Orders
    - Timelines
  - Other available assets
    - Scout Platoon
    - Recon
    - ODA
    - NSW
    - Civil affairs
    - Information Ops
    - Tactical PsyOps
    - State Dept (PRT)
  - Host Nation assets
    - Do we have access?
      - Advisors
      - LNOs
      - Mil to Mil exchange
      - Police

      - DAO
      - Personal relationships
    - Coalition assets
      - Do we have access?
- Signals Intelligence (SIGINT)
  - SIGINT Support Teams, STG Teams, CST, Systems
    - Organic?
    - Command relationship
    - Higher assets
    - Adjacent assets
    - Host nation assets
      - Do we have access?
    - Tasking procedures
      - Timelines for requests (how far out?)
      - Dynamic re-tasking priorities
    - Tasking priorities
    - SIGINT IPB
    - Digital Network Exploitation
- Unmanned Aerial Systems (UAS) –Full Motion Video, Radar, SIGINT, Measurement and Signature Intelligence (MASINT)
  - Airspace deconfliction
  - UAS platforms
    - Organic?
    - Command relationship
    - Higher assets
    - Adjacent assets
    - Host nation assets
      - Do we have access?
    - Tasking procedures
      - Timelines for requests (how far out?)
      - Dynamic re-tasking priorities
  - Armed?
    - ROE
- Nontraditional Intelligence, Surveillance, and Reconnaissance (NTISR)
  - Fixed and Rotary aircraft with collection pods
    - Organic?
    - Command relationship
    - Higher assets
    - Adjacent assets
    - Host nation assets
      - Do we have access?
    - Coalition assets
      - Do we have access?
    - Tasking procedures
      - Timelines for requests (how far out?)

        - Dynamic re-tasking priorities
    - Tasking priorities
    - Other planning considerations
        - Refueling
        - Communication requirements
        - Time on station

Chapter 2: Operational Capabilities

Blue Force Oper*a*tional Assessment

Just as the prioritization for collection activities should be based on realistic exploitation requirements and capabilities, exploitation of materials, information and individuals needs to be prioritized in accordance with the anticipated potential actions that can be cued as a result of the exploitation.

- Mission
- Adjacent units
- Size of the Force
- Available Air assets
    - Time (Response and if on station)
    - Movement of PAX
    - Priorities
    - Close Air Support
    - Logistics
    - NTISR
    - Airspace deconfliction
- Available Ground assets
    - Time (Response and if on station)
    - Transportation
    - Armor
    - Movement of PAX
    - Logistics
- Limitations of movement
    - Host Nation concerns
    - Boundaries
    - Weather
    - Terrain
    - Road network's density and surfacing
    - Enemy activity

- Action Arm (Air/Ground)
  - Theater
    - SOF
      - Tasking procedures
      - Timelines for requests (how far out?)
      - Tasking priorities
      - Targeting Lines
  - Organic Time Sensitive Targeting Team
    - Dedicated (standing by)
      - Training
      - OPTEMP
      - Capability
      - Tasking procedures
      - Timelines for requests (how far out?)
      - Tasking priorities
    - Host Nation
      - Training
      - OPTEMP
      - Capability
      - Tasking procedures
      - Command Relationships
      - Advisors
      - LNOs
      - Comms
      - Timelines for requests (how far out?)
      - Evidentiary and prosecutorial requirements
      - Situational primacy
- Climatic and Forecasted Weather / Possible effects
  - Latitude / Regional climate
  - Seasonal?
  - Humid / wet
  - Dry / dust

Chapter 3: Improvised Weapons

Improvised weapons are a category of weapon which include IEDs and improvised weapon systems as well as conventional weapons employed in a different manner (e.g. air-to-air rocket fired from an improvised ground launcher). These weapons are fabricated or employed in an improvised manner incorporating destructive payloads and fillers designed to kill, destroy, incapacitate, harass, or distract. They may or may not incorporate military ordnance, but are normally devised from a combination of military ordnance and nonmilitary components. Improvised weapon systems may incorporate one or more weapons with all related equipment, materials, and means of delivery and have similar features as state-manufactured military weapons. Both sub-categories of improvised weapons are extremely lethal and are the preferred instrument of irregular warfare due to the deadly effect, ease of manufacturing and limited personnel exposure to employ.

IMPROVISED WEAPONS SYSTEMS

Improvised weapon systems fabricated from both military and non-military hardware incorporating similar design and functional characteristics as conventional weapons. Improvised weapons are designed by insurgents who can take ordnance designed for one specific use (e.g. air-to-ground rocket) and adapt it for a different purpose (e.g. ground-to-ground rocket). Improvised weapon systems could incorporate one or more weapons with all related equipment, materials, and means of delivery and deployment required for self-sufficiency. An examples of an improvised weapon systems is the Improvised Rocket Assisted Mortar (IRAM) employed in Iraq. This system utilizes a conventional 107mm rocket mortar attached to an improvised warhead and fuzing system. It also incorporates an improvised launch platform thus having the means of delivery. This system blends conventional ordnance products and design features with improvised fabrication methods and common materials found at local hardware and electronics shops.

The recovery and technical analysis of improvised mortar systems revealed similar components and designs as previously encountered mortars, yet continued to advance in lethality and employment and let to the development of improvised direct fire missiles incorporating shape charge warheads. Technical intelligence comparison of welds, metallurgy, circuit wiring, main charge, and flight stability design allowed intelligence analysts to assess PIRA had begun using light engineering factories for fabricating their advance improvised weapons. Analyzing insurgent manufacturing processes and the geographical areas which favor weapon production can assist tactical units focus their search efforts; making the enemy’s supply chain vulnerable to detection and interdiction.

The Iraqi insurgent used of IRAMs was a significant ‘step change’ in both their technical evolution as well as their targeting strategy. The IRAM was to give them a capability to provide concentrated indirect fires on well defended FOBs. Once aligned to engage target, it was a ‘fire and forget’ weapon system that would, using its last round, self destruct complicating post incident exploitation y EOD and WIT.

Chapter 4: Improvised Explosive Devices (IED)

The following information is taken from the *WTI IED Lexicon* – DIA/JIEDDO.

Projectiles and electric blasting caps used by insurgents to fabricate an IED(Photo Credit: Troy)

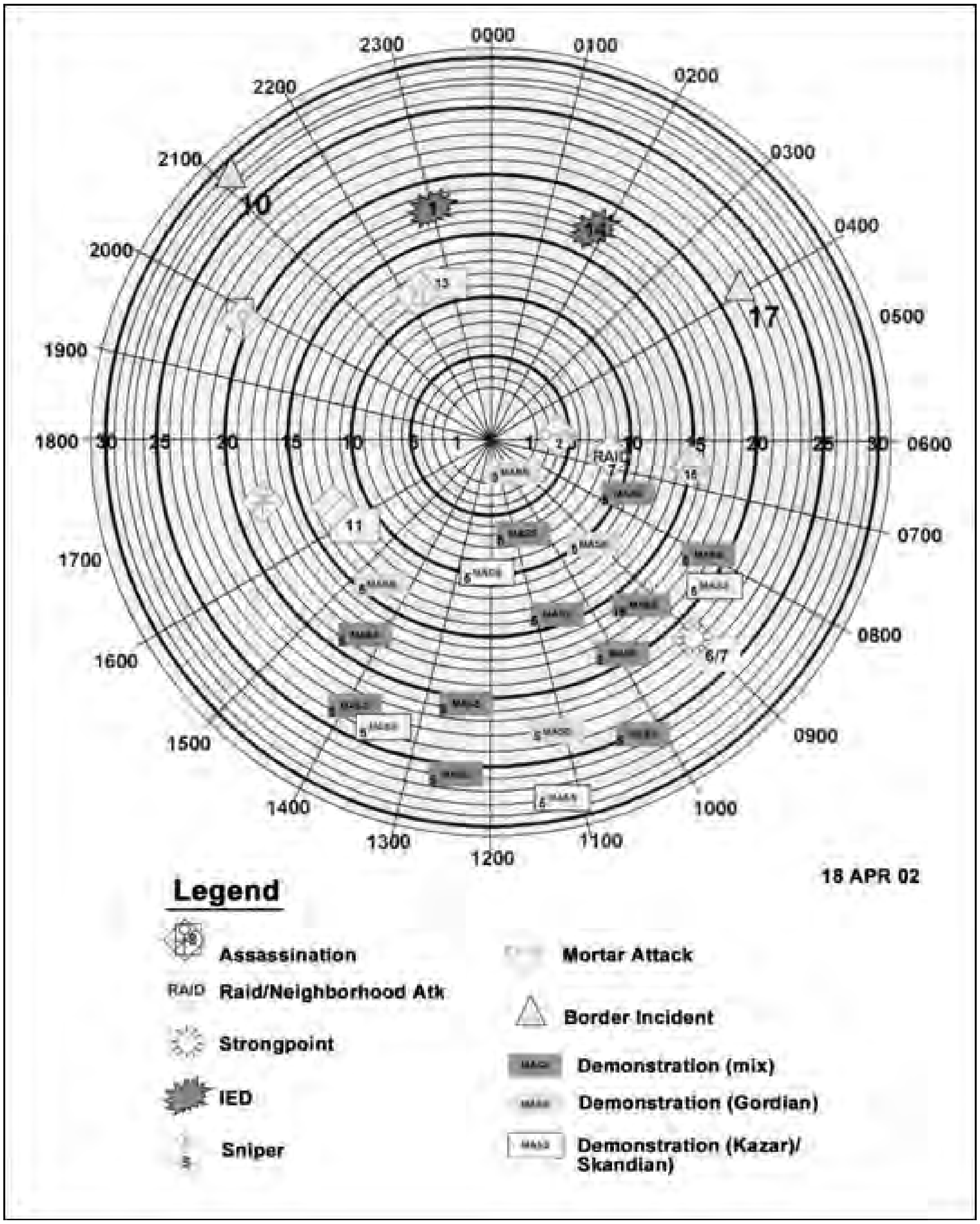
Improvised Explosive Device (IED): *A device placed or fabricated in an improvised* manner incorporating destructive, lethal, noxious, pyrotechnic, or incendiary chemicals and designed to destroy, incapacitate, harass, or distract. It may incorporate military stores, but is normally devised from nonmilitary components.

Explosion: A nuclear, chemical or physical process leading to the sudden release of energy.

Tactical Characterization: A manner in which an IED incident is planned and conducted (tactical design) and the intent (purpose of device).

Technical Categorization: A description of an IED device using a hierarchical construct to identify its key components. The components identified in this categorization are the elements from which technical and forensic information is recovered and exploited.

Pattern Analysis: Using prior actions and activities to identify trends in activities or behaviors. Once identified, these patterns can be used to predict future enemy actions, plan intelligence, surveillance, and reconnaissance (ISR) activities. This is an important aspect of IPB.



Example of a Pattern Analysis Wheel (Figure Credit: DIA)

Event Signature Development/Device Profiling: The process of analyzing the tactical and technical identifiers of an IED incident to support force protection, targeting, prosecution, and sourcing.

TTP Identification: An IED primarily intended to cause a reaction by forces in an effort to learn and understand employed tactics. This knowledge is then used by the attacker to plan new attacks incorporating the lessons learned to inflict additional casualties or to avoid countermeasures. The IED need not function to serve this purpose. A Hoax IED can have TTP identification as its intended **outcome.**[3]

Tactical Characterization

- **Tactical Design** –The specific design of an IED attack – including but not limited to: position of the IED, the type of IED, method of actuation, type of road segment used, concealment technique, use of secondary devices, the time of day, etc. Tactical design addresses the question of "why here, why now, and why in this way". Terms used to describe a specific type of device or component of a device (e.g., VBID) are often used to describe all or part of the tactical design.
  - Method of Identification (examples not all inclusive)
    - Visual Observation
    - Working Animal
    - Search and Detect Sensors
    - Human Tip
  - Method of Employment (examples not all inclusive)
    - Suicide/Proxy
      - Air Borne IED
      - Water Borne IED
      - Animal Borne
      - Vehicle-Borne
      - Person-Borne
      - Projected
  - Method of Emplacement (examples not all inclusive)
    - Subsurface
    - Surface
    - Elevated
  - Method of Attachment
    - Magnet
    - Tied
    - Mechanical
    - Adhesive
  - Sensor Defeat
    - Surgically Implanted
    - Low Metallic Content
    - Anti-X-Ray
    - Non Metallic Content
    - Masking Agents
  - Role of IED
    - Primary Device
    - Secondary Device

- Attack Geography
  - Device Placement Characteristics
    - Distance to Target
    - Blast Dimensions
    - Estimated Net Explosive Weight
    - Blast Crater material
    - Line of Site
    - Placement Relative to Target
    - Contact Point
    - Firing Point
    - Concealment
    - Aiming Marker
    - Antenna Orientation
  - Site-Specific Characteristics
    - Angle of Attack
    - Obstacles
    - Routes
- Incidental Environmental Conditions
  - Visibility
  - Time of Day
  - Weather

- **Purpose of Device –**The immediate or direct tactical effect of the IED

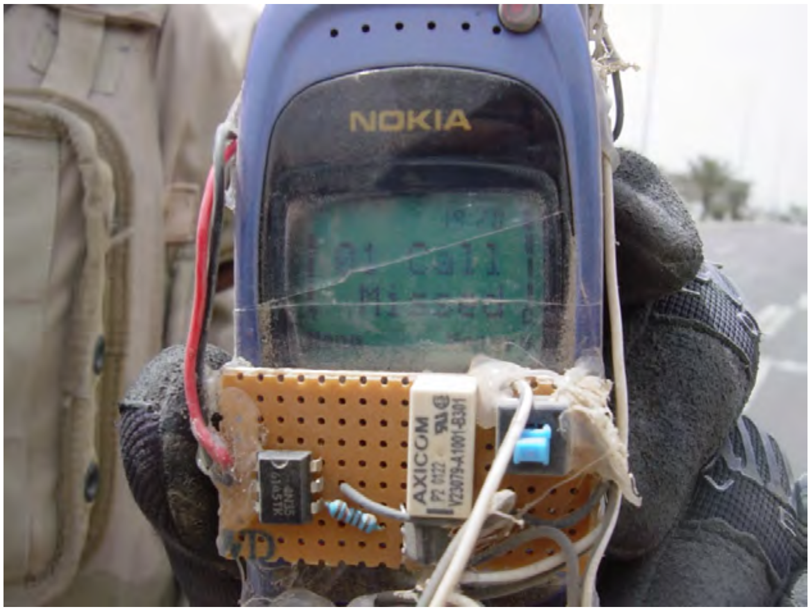
  - Anti-Armor
  - Anti-Vehicle
  - Anti-Infrastructure
  - Anti-Personnel
  - TTP Identification
  - Anti-Aircraft
  - Anti-Maritime
  - Obstacle Creation
  - TTP Identification

Technical Categorization

A description of an IED using a hierarchical construct to identify its key components. The components identified in this categorization are the elements from which technical and forensic information is recovered and exploited.

- **Switch** –*A device for making, breaking, or changing a connection in an IED*. A single switch can have multiple functions (i.e., arming and firing).
  - Firing Switch/Arming Switch
    - Command switch
      - Command Wire
      - Pull
      - Radio Controlled

  - Optical
  - Active Infrared
  - Command Projectile
- Time switch
  - Time Mechanical
  - Time Chemical
    - Time Electronic
- Victim operated switch
  - Tension
  - Tension release
  - Pressure
  - Pressure release
  - Pressure/Pressure/Pressure Release
  - Collapsing Circuit
  - Membrane Switch



Cell Phone used as an IED Switch in Iraq (Photo Credit: DIA)

- **Initiator** -*Any component that may be used to start a detonation or deflagration. An initiator will be categorized as either a detonator or an igniter*.

  - Electric
    - Commercial Initiator
      - Detonator
      - Igniter
    - Military Initiator
      - Detonator
      - Igniter

    - Improvised Initiator
      - Detonator
      - Igniter
  - Non-Electric
    - Commercial Initiator
      - Detonator
      - Igniter
    - Military Initiator
      - Detonator
      - Igniter
    - Improvised Initiator
      - Detonator
      - Igniter

- **Main Charge –** *The explosive charge which is provided to accomplish the end result in a munition. Examples for end results are: bursting a casing to provide blast and fragmentation; splitting a canister to disperse sub-munitions; or producing other effects for which it may be designed.*
  - High Explosives
    - Commercial Explosives
      - Blasting Agent
      - Cast Explosive
      - Binary Explosive
      - Det Cord
      - Liquid Explosive
      - Shaped Charge
      - Plastic Explosive
      - Dynamite
    - Military Explosives
      - Munitions
        - Mortar Munitions
        - Sub Munitions
        - Missiles
        - Projectiles
        - Grenades
        - Sea Mines
        - Rockets
        - Mines
        - Air Dropped Bombs
      - Demolition Materials
        - Platter Charge
        - Shaped Charge
        - Booster
        - Bulk Explosives
    - Improvised Explosives/HME

      - Explosive Components
      - Explosive Mixtures (FOX)
  - Low Explosives
    - Commercial Explosives
      - Propellants
      - Pyrotechnic Fireworks
      - Small Arms Ammunition/Cartridge Cases
    - Military Explosives
      - Propellants
        - Black Powder
        - Smokeless
        - Liquid
        - Triple Base
        - Cordite
      - Incendiary
        - White Phosphorous
        - Illuminate
        - Thermites
        - Napalm
        - Smoke
    - Improvised Explosives/HME
      - Explosive Mixtures
        - Propellants
        - Burning Fuses
        - Smoke
        - Incendiary
  - Main Charge Configuration
    - Directional Effect
      - Improvised Platter Charge (Misznay-Shardin Effect)
        - Improvised Claymore
        - Explosively Formed Projectile (EFP)
      - Improvised Shape Charge (Monroe Effect)
        - With Metal Liner
        - Without Metal Liner
    - Omni-Directional (Blast Effect)
      - Improvised Grenade
      - Improvised Mine
      - Improvised Mortar
      - Improvised Rocket
- **Power source** *–A device that stores or releases electrical or mechanical energy. The key elements of information about a power source are its type and source, number of batteries and their configuration (series or parallel), its voltage (if electrical) and how it is connected to close an IED switch.*

  - Electrical Energy

        - Direct current
        - Alternating current
    - Mechanical Energy

- **Container** –
    - Concealment – A vessel commonly used to prevent the discovery of an IED by visual inspection. May also be used to add fragmentation.
    - Confinement – A vessel commonly used to hold the main charge together. May also be used to add fragmentation.

- **Enhancements** – *An optional, deliberately added component as opposed to a secondary hazard which modifies the effects of the IED. The IED would be effective, yet produce a different measureable result if this material were not added. The effect can be additional physical destructing, proliferation of dangerous substances (radiation, chemicals, etc.), or other results to enhance the effect of the IED.*

    - Improvised
        - Fuel
        - Fragmentation
        - Bio-Toxin
        - Chemical
    - Commercial/Toxic Industrial Materials
        - Toxic Industrial Chemical
        - Toxic Industrial Biological
        - Toxic Industrial Radiological
    - Military/Weaponized
        - Chemical Agent
        - Biological Agent

Chapter 5: Homemade Explosives (HME)

Fertilizer recovered in Afghanistan commonly used to manufacture HME
(Photo Credit: JIEDDO)

-Homemade Explosives can be made from commonly available commercial chemicals with relatively minimal effort.

When dealing with homemade explosives, it is important to not only look for what has already been manufactured, but also for components of the manufacturing process as well as what resources are available. For example, in an area that heavily relies upon farming, there is most likely a large supply of fertilizer. If primarily Ammonium Nitrate explosives are being used in this same area, this should warrant further investigation.

Typical Homemade Explosives[4]

- Ammonium Nitrate Mixtures (commonly ANFO)
- Black Powder
- Chlorate / Perchlorate Mixtures
- Ethylene Glycol Dinitrate (EGDN/NG)
- Hexamethelylene Triperoxide Diamine (HMTD)
- Hydrogen Peroxide Mixtures
- Methyl Ethyl Ketone Peroxide (MEKP)

- Triacetone Triperoxide (TATP)
- Urea Nitrate (UN)

Chemical Components

- Oxidizers –*Substances that oxidize other substances, especially one that supports the combustion of fuel; an oxidizing agent.*

  - Ammonium Nitrate
    - *Fertilizer*
  - Hydrogen Peroxide
    - *Disinfectant*
    - *Bleaching Agent*
    - *Hair Products*
  - Nitric Acid
    - *Industrial Chemical*
  - Potassium Chlorate
    - *Match Heads*
    - *Pyrotechnics*
  - Potassium Nitrate
    - *Black Powder*
    - *Saltpeter*
    - *Stump Remover*
    - *Pyrotechnics*
  - Potassium Perchlorate
    - *Airbag Initiator Formulas*
    - *Pyrotechnics*
  - Potassium Permanganate
    - *Disinfectant*
    - *Algae Control*
  - Sodium Chlorate
    - *Herbicide*
    - *Pyrotechnics*
  - Sodium Nitrate
    - *Fertilizer*
    - *Food Preservative*

- Fuels -*Oxidizers can be blended with a variety of fuels to produce explosives*

  - Alcohols
    - *Ethanol*
    - *Methanol*
    - *Isopropanol*
  - Cellulose
    - *Sawdust*

    - *Cotton*
  - Coal
    - *Charcoal*
  - Energetic Fuels
    - *Nitromethane*
    - *Nitrobenzene*
  - Flake / Powdered Metals
    - *Aluminum*
    - *Magnesium*
    - *Iron*
  - Fuels
    - *Kerosene*
    - *Diesel*
    - *Gasoline*
  - Solvents
    - *Acetone*
    - *Methyl Ethyl Ketone*
    - *Naphtha*
  - Sugars
    - *Sucrose*
    - *Glucose*
    - *Confectioner's Sugar*

- Precursors –*Two or more precursors could produce an explosive*

  - Acetone
    - *Nail Polish Remover*
    - *Paint Remover*
  - Citric Acid
    - *Food Additive*
    - *Water Softener*
    - *Powdered Drinks*
  - Ethylene Glycol
    - *Antifreeze*
  - Hexamine
    - *Camp Stove Fuel Tablets*
  - Hydrochloric Acid
    - *Muriatic Acids*
    - *Toilet Bowl Cleaners*
  - Hydrogen Peroxide
    - *Disinfectant*
    - *Bleaching Agent*
    - *Hair Products*
  - Methyl Ethyl Ketone
    - *Paint Remover*
    - *Solvents*

- Nitric Acid
  - *Industrial Chemical*
- Sulfuric Acid
  - *Car Batteries*
  - *Drain Cleaners*
- Urea
  - *Fertilizer*

Manufacturing Equipment

The manufacturing equipment will depend on the homemade explosive. The equipment may be scientific, simplistic, or improvised to provide grinding, mixing, stirring, distilling, filtering, drying and cooling capabilities.

- Grinders
  - *Mortar and Pestle*
  - *Coffee Grinders*
  - *Ball Mill*
- Mixers and Stirrers
  - *Blenders/Mixers*
  - *Buckets/Plastic Ware*
  - *Magnetic stirrers*
- Ice Baths
- Distillers
  - *Slow Cooker*
  - *Rotovap*
  - *Coffee Pots*
  - *Hot Plate/Stovetop*
- Filters
  - *Coffee Filters*
  - *Filter Funnels*
- Drying Equipment
  - *Fans*
  - *Heat Lamps*
  - *Tarps (outdoor)*
- Safety Equipment
  - *Dust/Vapor Mask*
  - *Face Shield*
  - *Safety Goggles*
  - *Improvised Venting*

Chapter 6: IED Tactical and Technical Resources

The tactical and technical designs of IEDs are only limited by the skill and education of the bomb-maker, the available resources, and the operational environment. Conversely, the education level of the populace and the insurgents, the resources, terrain, and local infrastructure, can serve as indicators as to the whether the enemy might employ IEDs, as well as potential clues to their tactical and technical designs.

It is important to note throughout this chapter, specifically with Homemade Explosives, that certain components/resources on their own are not necessarily conclusive evidence of terrorist activity. For example, a farmer who owns a grinder does not automatically mean he is producing explosives. However, suspicions should be raised if he runs a small farm yet owns a large commercial grinder or a laser cutter.

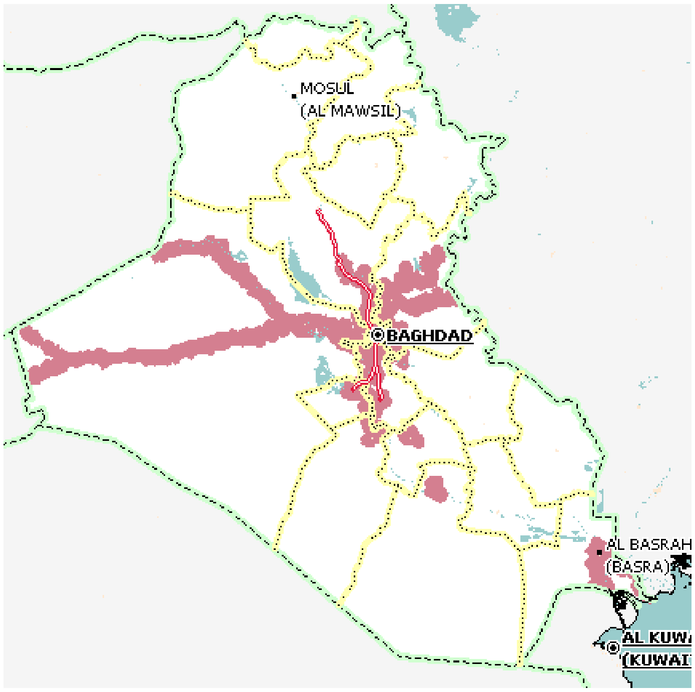
Tactical Resources; Skills, Training, Capabilities

To determine the level of skills, training, education, and targeting methodologies specific to the adversaries' employment of the IEDs, refer to Chapter 8: Irregular Warfare; Structural Organization of the Insurgent/Terrorist Group, Methods of Operation. If the adversary is associated with the country's former regime military, or that of a neighboring, hostile country; refer to Chapter 9: Indigenous Forces/Indigenous EOD Capabilities.

Technical Resources

- **Initiator** – (safety fuse/time fuse, blasting caps/detonators, squibs/igniters, etc.)
    - Domestic production
        - Precursors
        - Finished products
            - Types
            - Amounts
            - Describe markings
            - Nomenclature
            - Commercial names
            - Are there available samples
        - Manufacturing locations
        - Storage facilities
    - Importation
        - Importer
        - Source
        - Other parties involved
        - Ports of entry

- Describe domestic use (mining, military use, civil engineering, construction/blasting, etc).
    - Location of activity
    - Storage and securing of materials
    - Laws/Regulations on sale/purchase
    - Reporting on thefts, black market sales
    - Host Nation data base of explosive material reference samples for explosive chemistry comparative analysis
    - Listing of manufactures and identification of products licensed for sale



(Map showing Iraq's cell phone coverage (Figure Credit: DIA)

- **Switch Resources**
    - Command switch
        - Radio Controlled IED (RCIED)
            - Frequencies
            - Push to Talk
            - Long Range Cordless Phones
            - Dual Tone, Multi Frequency
            - Cell phone/GSM
                - Networks
                - Infrastructure (towers, facilities, etc)
                - Coverage areas
                - Blackout areas
                - History of systems

      - Consistency
      - Privacy/security
  - Internet
    - Availability
    - Consistency
    - Bandwidth
    - Networks
    - WiFi
    - Internet cafes

- **Container** *–the type of container used is limited only by the imagination and skill of the builder. A history of attacks, targets, and methods of concealment, can provide indications of the types of containers that may be employed, as well as the material resources needed to acquire or build the containers.*

- **Main Charge Resources** - *Substance capable of providing an explosion by its own energy when initiated.*

  - *Commercial Explosive*
    - Domestic production
      - Precursors
      - Finished products
        - Types
        - Amounts
        - Describe markings
        - Nomenclature
        - Commercial names
        - Are there available samples
      - Manufacturing locations
      - Storage facilities
    - Importation
      - Importer
      - Source
      - Other parties involved
      - Ports of entry
    - Describe domestic use (mining, military use, civil engineering, construction/blasting, etc).
      - Location of activity
      - Storage of materials
    - Domestic controls
    - Ease of purchase

  - Military Explosive (Munitions and Bulk Military Explosive)
    - Domestic production
      - Types

      - Amounts
      - Describe markings
      - Nomenclature
      - Manufacturing locations
      - Storage facilities
      - Condition/Age
    - Importation
      - Country of origin
      - Types
      - Amounts
      - Describe markings
      - Nomenclature
      - Condition/Age
    - Ammunition Supply Points (ASPs)
      - Current/former regime
      - Locations
      - Description of facilities
      - Types of munitions
      - Security at site
    - Military forces (those that consume and store munitions)
      - Artillery unit / Armor units/ Engineers/EOD
        - Current regime/former regime
        - Current status
        - Present locations
        - Past locations
        - Bases
        - Unit ASPs/Ammo Dumps
        - Basic load by direct and indirect fire system type

- Homemade Explosive (HME) -*Many chemical components of HME can be associated with and sourced from industries and activities to include; farming, water treatment, pharmaceutical production, plastics manufacturing, etc.*

  - Determine the farming regions and arable land
  - Fertilizer *(Urea, Ammonium Nitrate, etc.)*
    - Common types used
      - Description
      - Nomenclature
      - Available samples
    - Domestic production of fertilizer
      - Types
      - Manufacturing locations
      - Storage/distribution facilities

        - Importation
            - Country of origin
            - Types
            - Amounts
        - Domestic controls
        - Ease of purchase
    - Chemical Components
        - Domestic Chemical production
            - Types
            - Nomenclature
            - Commercial names
            - Manufacturing locations
            - Storage facilities
            - Distribution facilities
        - Importation
            - Importer
            - Source
            - Other parties involved
            - Ports of entry
        - Describe domestic use (government, industries and businesses)
        - Location of activities
        - Domestic controls
        - Ease of purchase

- **Enhancements -** *are an optional additional component that modifies the effects of the IED. Whether they are employed, and how they are chosen can be based on the target, the intended outcome, and the availability of resources. These enhancements may include; fuel and fragmentation, as well as chemical, biological, radiological, and nuclear materials.*

    - Sourcing Methods
        - Theft
        - Insider provides
        - Purchase commercially
        - Homemade

(Considerations: types, history, locations and security)

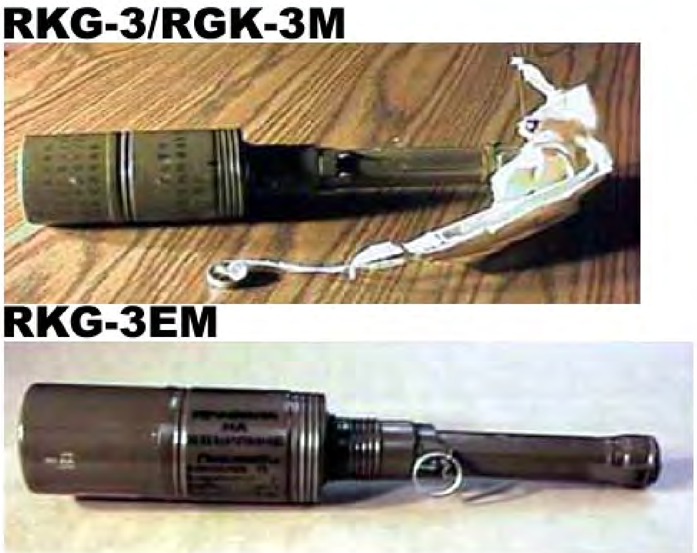
    - Chemical enhancements
        - From industrial sources
            - Pesticides
            - Water treatment plants
            - Raw chemical production
        - Weaponized (military)

- Current/former regime
- Production facilities
- Chemical Weapons units

- Biological enhancements
  - Research facilities
    - Government
    - Academic
    - Private industry
  - Weaponized (military)
    - Current/former regime
    - Production facilities
    - Bio Weapons units
  - Nature (i.e. anthrax, ricin from castor beans)
- Radiological material enhancements
  - Research facilities
    - Government
    - Academic
    - Private industry
  - Medical facilities
  - Industrial applications
  - Radiological waste
    - Storage
    - Transportation
- Nuclear enhancements
  - Weapons
    - Security
  - Research facilities
    - Government
    - Academic
    - Private industry
  - Reactors
    - Status
    - Security
    - Fissile material storage
    - Waste storage

Chapter 7: Weapons of Concern

Weapons of concern are defined as new, or advanced conventional or improvised weapons that are significant enough to challenge our national level response. They're weapons which cause considerable numbers of casualties (KIA/WIA) and can penetrate or defeat our current countermeasures thus causing the commander to continuously alter his operations and force protection measures to mitigate the effects. Additionally, weapons of concern cause a dramatic response by the S&T community to rapidly develop and acquire enhanced equipment solutions. An example of a weapon of concern is a sniper rifle newly introduced by the insurgents into the battlespace capable of penetrating US and Coalition Forces protective body armor. The addition of this weapon could possibly cause the tactical commander to adjust mounted and dismounted TTPs and make the R&D community rapidly develop a materiel solution to counter the weapons' effects.



This photograph displays the different types of RKG-3 grenades employed by insurgents in Iraq. RKG's gave insurgents a "top attack" capability against up-armored vehicles. As armor improved underneath the side areas of vehicles, insurgents moved their attacks to more vulnerable top armor (Photo Credit: Wikipedia)

Weapons of concern are typically dynamic systems that reflect new enemy acquisitions or new modifications of older weapons and can include technology advancements in night vision devices and laser target designators.

- Common Weapons of Concern:
  - Anti-material sniper rifles
  - Thermobaric weapons
  - Anti-tank guided missiles
  - Mortar and rocket warheads containing sub-munitions
  - Improvised rocket propelled grenade
  - Anti-tank grenades

- Man Portable Air Defense Systems (MANPADS)

WIT functions apply to weapons of concern the same with IEDs and improvised weapons. The technical and forensic evaluation provides useful information to determine the type of weapon used in an attack and lead to identifying the individual and enemy group responsible. For example, if insurgents employ a thermobaric weapon to attack a US or Coalition facility, laboratory analysis of samples taken from the point of detonation could identify the main compounds of the warhead filler (e.g. isopropyl nitrate and aluminum). Furthermore, if a rocket launcher were collected from the area, latent fingerprints could be used to identify the individual and link him to the threat network responsible for the attack. Furthermore, analysis of the exact markings from a weapon could potentially identify the country where the weapon was manufactured and may indicate whether the weapon was sold to a third party.

Chapter 8: Irregular Warfare

Insurgency can be defined as 'a popular movement that seeks to overthrow the status quo through subversion, political activity, insurrection, armed conflict and terrorism.' By definition, insurgent movements are grass roots uprisings that seek to overthrow established governments or societal structures. All are popular uprisings that employ the weapons of the weak (subversion, guerrilla tactics, and terrorism) against the established power of states and conventional military forces.

Conversely, Terrorism can be defined as 'politically motivated violence against civilians, conducted with the intention to coerce through fear.' Terrorism is a component in almost all insurgencies, and insurgent objectives (that is, a desire to change the status quo through subversion and violence) lie behind almost all non-state terrorism.[5]

Insurgent/terrorist forces, civil population and terrain are virtually inseparable factors in counterinsurgency/counterterrorism operations. Therefore, detailed intelligence is required on all three elements for effective targeting (both kinetic and non-kinetic), and to support the commanders' decision making ability.

Structural Organization of the Insurgent/Terrorist Group

- Determine the structural organization of the insurgent/terrorist group
  - Identification
  - Composition
  - Overall organizational characteristics
    - Strength
    - Combat efficiency
    - Status of training
    - Means of communication
      - Couriers/messengers
      - Postal service

            - Person to person
            - Dead drop
            - Phone
                - Landline
                - Mobile phones
                - Satellite phones
                - Prepaid phone card
            - Radio frequencies
            - Pagers
            - Internet
        - Communications equipment captured with insurgents/terrorists
        - OPSEC procedures
        - Morale and discipline
    - Ideology
        - Nationalist/Separatist
        - Ethnic
        - Tribal
        - Religious
        - Criminal/Gang

Location and Relationships

- Locate the insurgent/terrorist groups.
    - Insurgent/terrorist camps
    - Safe houses
    - Areas of operation / Influence
    - Lines of Communication (LOC)
- Describe the relationship between the insurgents/terrorists and the population.
- Describe the groups' relationships with any external forces.
- Identify any hostile, neutral, or friendly organizations or elements that may be assisting the insurgent/terrorist groups:
    - Identification
    - Name
    - Location
    - Organizational structure
    - Type of support (personnel, logistics, monetary)
- Do the insurgents/terrorists have a State Sponsor?
    - Method of support
    - Location
- Is the insurgent/terrorist group supported by other insurgent/terrorist groups?
    - Group name
    - Method of support
    - Location
- Does the insurgent/terrorist group have a non-state sponsor?

Methods of Operations

- Identify the insurgent/terrorist groups' methods of operations:
    - Political
    - Economic
    - Proselytizing
    - Propaganda / Information operations
    - Types of tactics employed
    - Previous attacks
- What is the profile of previous actions:
    - Frequency
    - Timing
    - Security measures
    - Geographical dispersion
    - Results
    - SALUTE Report
    - Strengths
    - Weaknesses
    - Single or multiple acts
    - Purpose
        - Intended outcomes:
            - Maximize body count
            - Maximize psychological impact
            - Demonstrate capability
            - Targeted assassination
            - Political statement
            - TTP identification
        - Identify targets
            - Targets of opportunity
            - HN security forces
            - US forces/personnel
            - Food and agriculture
            - National monuments and icons
            - Healthcare facilities
            - Nuclear reactors, facilities and waste
            - Drinking water and waste water treatment systems
            - Energy
            - Banking and finance
            - Defense industrial base
            - Information Technology/Telecommunications
            - Chemical sector
            - Postal and shipping
            - Non-supportive civilian population
            - Opposing religious leaders
            - Opposing tribal leaders
            - Opposing militia

            - Infrastructure
                - Transportation systems
                - Dams
                - Government facilities
                - Commercial facilities
                - Community
                    - Religious establishments
                    - Nightclubs
- Type of weapons:
    - Handguns
    - Assault weapons
    - Grenades
    - Rocket Propelled Grenades (RPGs)
    - Crew served weapons
    - Improvised mortars
    - Improvised landmines
    - Improvised Explosive Devices (IEDs)
    - Chemical and biological means (conventional/unconventional)
    - Ability to resupply

Chapter 9: Country Information

Friendly forces moving to or operating from an incident country are concerned about indigenous forces and their ability to affect mission planning and execution. Even in the most permissive of environments, information on the country's politics and military should be assessed.[6]

Indigenous Forces

- Describe the significant strengths and weaknesses of indigenous forces.
- Determine if indigenous forces will be an asset or a liability
- Determine outside state and non-state support.
    - Identify type and capability of support
    - Identify most likely geographic area to receive support.
    - Identify units/groups/cells whom are most likely to receive support and how.
- Identify the indigenous forces' weapons, special equipment, communications, discipline and loyalty.
- Determine if indigenous forces have received any specialized training and from what country to include provider of the training (COIN, Counterterrorism, C-IED, Civil Disturbance, etc.)
    - Which units
    - Capabilities
    - Who trained them
    - Training received
    - When and where conducted (How long ago?)
    - Any retraining?
    - Level of proficiency
- Determine if indigenous forces can either employ or mitigate the effect of CBRN weapons.
    - Type
    - Method of employment
- Identify possible reinforcements.
    - Location
    - Size
    - Weapons available
    - Time/Distance factors
    - Availability
    - Capacity
    - Probability
    - Ingress/Egress routes/capabilities
    - Communications
- Determine the response to active ECM employment, tactical and operational jamming.

- Electronic Countermeasures (Who is responsible for providing technical data for maintaining currency of the frequency load to be jammed.)
  - Types, vehicle, personnel and airborne systems
  - Condition
  - Effectiveness
  - Maintenance
  - Frequencies
  - How often is the jamming load updated
  - What branch of service is responsible for the operation of the Electronic Countermeasures

- Determine the customs processing procedures.
  - Planes
  - Boats/Ships
  - Trains
  - Automobiles
- Determine border crossing/port or place of entry procedures.
  - Searches
  - Documents
  - Security
- Determine smuggling activity (What is being smuggled; arms, explosives, drugs, commercial goods, people)
  - Points of entry
  - Groups involved
  - Routes and ratlines
- Determine Identification procedures.
  - National ID
  - Drivers' Licenses
  - Vehicle registration
  - Provincial/Municipal ID
  - Biometrics Databases
  - Military
  - Local Security Forces (Police/Militia/Neighborhood)
- Describe the judicial system.
  - Location of courts
  - Location of prisons
  - HN Constitution
  - Evidentiary requirements
  - Prosecutorial constraints/restraints
  - Regional assessment of judges and courts

Indigenous EOD Capabilities

- Police EOD
- Military EOD
- Teams Chains of Command

- Recent activities
- Primacy on incident sites:
    - Local Police
    - National Police
    - Army/military
- What other nations do they operate and/or train with?
- Areas of Operations:
    - Urban
    - Rural
    - Regional
- EOD Personnel:
    - Schools/training attended
    - OPTEMPO
    - Morale
    - Training on equipment
    - Proficiency in equipment on hand
- What missions and operations do EOD Teams perform:
    - Security/Magazine Safety
    - Range clearance
    - EOD services OPS military and civilian
    - How EOD Teams integrate into other military OPS
    - Other roles and missions EOD Teams perform
- State of readiness:
    - Effectiveness of team
    - Weaknesses/Strengths
- Incident Reporting Procedures (Report content and format, how data based, accessible to U.S. Forces and terminology/lexicon applied.)
- Equipment (EOD specific)
    - Types
    - Condition
    - Effectiveness
    - Maintenance
    - Communications and computers
    - ECM
    - Tactics, Techniques and Procedures
    - Budget allowance
- Electronic Countermeasures (Who is responsible for providing technical data for maintaining currency of the frequency load to be jammed.)
    - Types, vehicle, personnel and airborne systems
    - Condition
    - Effectiveness
    - Maintenance
    - Frequencies
    - How often is the jamming load updated
    - What branch of service is responsible for the operation of the Electronic Countermeasures

The Land and the People

- Determine the date(s) the unit or organization arrived in the operational area.
- Identify what maps are needed. Determine if there are indigenously produced edition maps available.
    - Series
    - Sheet
    - Edition
    - Scale
- Identify available imagery.
- Determine the information that can be gained from available interviewees.
- Determine the cultural and sociological makeup within the area of operations
    - Average age
    - Average educational level
    - Literacy rate
    - Type of family system
    - Languages spoken
    - Typical diet
    - Average caloric intake
    - Customs
    - Basic physical condition
    - Morale and discipline
    - Special historic information about the people
    - Race and Religion
        - Racial, Tribal and Ethnic Groups
        - Group leaders
        - Social mores of note
        - Taboos of the population (concerning sex, religion, politics, medicine, alcohol, and hospitality)
        - Differences, tensions and disputes
        - Geographic distribution (sectarian map)
    - Roles/duties of women
    - Typical daily routine
    - Political affiliations
    - Common expressions/gestures
- Determine the type of telecommunication/information systems equipment available in-country
    - Equipment nomenclature/systems
    - Quality and procedures
    - Level of Maintenance
    - Problems with systems
    - Information systems
        - Civilian and government radio/television facilities
        - Newspapers/magazines, posters, billboards, leaflets
- Determine the Lines of Communication and Transportation.

- Describe the communication and transportation networks
- Condition and use of Highways/Roads
- Conditions and use of Railways
- Condition and use of civil aviation facilities
- Condition and use of inland waterways/ports
- Areas controlled by government forces
- Area(s) controlled or influenced by other forces
- Identify vulnerable High Payoff Targets (HPT) along LOCs (i.e. bridges, overpasses, tunnels)

References

1. MAGTF Staff Training Program (MSTP) IPB pamphlet
2. FM 34-130, *Intelligence Preparation of the Battlefield.*
4. *WTI IED Lexicon* –DIA/JIEDDO October 2012
5. *Indicators and Warnings for Homemade Explosives* -TSWG
3. *Countering Global Insurgency* –David Kilcullen
6. MCIA-1540-003-03

CONTACT INFORMATION:

Defense Intelligence Agency
DTK-2
(434)-995-4100

Appendix H.
References

U.S. Defense Intelligence Agency /U.S. Joint IED Defeat Organization, *Counter Improvised Explosive Device Strategic Plan 2012-2016*. Joint IED Defeat Organization.

Actions Needed to Improve Visibility and Coordination of Counter-IED Efforts, GAO Report 10-95. Washington, DC: Government Accounting Office, 2005.

Addley, Ester. "Alexander Litvinenko Murder." *The Guardian*. December 13, 2012.

After Action Report for Operations Enduring Freedom (OEF) 12.2-13.2. After Action Report, USMC Regimental Combat Team 7, II MEF (Forward), 2013.

"Allied Joint Doctrine for Countering - Improvised Explosive Devices." *AJP-3.15 (A)*. North Atlantic Treaty Organization, March 16, 2011.

Arnold, Daniel 2LT. "The 203rd MI Battalion (Technical Intelligence) in Operation IRAQI FREEDOM." *Military Intelligence Professional Bulletin 31, no. 1*. January-March 2005.

Atkinson, Rick. "The single most effective weapon against our deployed forces." *The Washington Post*, September 30, 2007.

—. "There was a two-year learning curve...and a lot of people died in those two years." *The Washington Post*. October 1, 2007.

—. "Weapon of Choice." *Small Wars Journal*. September 30, 2007.

Attack the Network. Fusion, Analysis and Training (FAT) Report, 1 (3), Afghanistan: Paladin, Combined Joint Task Force, 2011.

Attack the Network Part II. Fusion, Analysis and Training (FAT) Report, Afghanistan: Paladin, Combined Joint Task Force, 2011.

Baker, Mark O., and James McAfee. "Using Trends to Conduct Effective Counter Improvised Explosive Device Training." *IED Bulletin VI (No. 10-50)*. Center for Army Lessons Learned (CALL), July 2010.

Barbero, LTG Michael. "JIEDDO statement to the House of Reprensentatives Committee on Appropriations Subcommittee on Defense." September 20, 2012.

Bergen, Peter. "Reevaluating Al-Qa'ida's Weapons of Mass Destruction Capabilities." *USMA CTC Sentinel, 3 (9)* (Combating Terrorism Center at West Point) 3, no. 9 (September 2010).

Black, MAJ Rick and Kelly, MAJ Rob. "3rd Infantry Division Improvised Explosive Device Defeat Cell Operations in Operation Iraqi Freedom V." *Center for Lessons Learned, 3rd Battle Command Tactics Techniquies and Proceedures,* , 2008: 12.

Bonnomo, James, and al et. "Summary to "Stealing the Sword, Limiting Terrorists Use of Advanced Conventional Weapons"." The RAND Corporation, 2007.

Bureau of Alcohol, Tobacco, Firearms and Explosives, National Explosives Task Force. http://www.atf.gov/content/explosives/explosives-enforcement/national-explosives-task-force (accessed December 4, 2013).

"Capstone Concept of Operations for DoD Weapons Technical Intelligence." Defense Intelligence Agency, December 2009.

Carroll, LTC Phillip III. "Mine and Booby Trap Warfare: Lessons Forgotten." Carlisle Barracks, PA: US Army War College, 1988.

"Challenges and Implications to the Future Joint Force." *The Joint Operating Environment 2008.* Virginia: United States Joint Forces Command, 2008.

Chivers, C. J. "Countering Qaddafi's Heat-Seeking Missiles and Tracking Them back to their Sources: At War, Notes From the Front Lines." *The New York Times.* July 26, 2011.

—. "Mao's Rockets and Modern War, Part III: At War, Notes From the Front Lines." *The New York Times.* December 19, 2011.

"Combating Weapons of Mass Destruction." *Joint Publication 3-40.* Joint Chiefs of Staff, June 10, 2009.

"Commander's Guide to EOD Operations: Observations, Insights and Lessons Learned." *Handbook 10-65.* U.S. Army Center for Army Lessons Learned, September 2010.

Connor, Tracy. "Pressure cooker bombs used around the world for years." NBC News, April 16, 2013.

"Counter-Improvised Explosive Device Operations." *Joint Publication 3-15.1.* Washington: Joint Chiefs of Staff, January 9, 2012.

"Countering Improvised Explosive Devices." The White House, June 14, 2012.

"Countering the Threat of Improvised Explosive Devices: Basic Research Opportunities, Abbreviated Version." National Academy of Science, 2007.

"Counterinsurgency." *FM 3-24.* Headquarters Department of the Army, December 12, 2006.

Cragin, Kim, and al et. "Sharing the Dragon's Teeth, Terrorist Groups and the Exchange of New Technologies." The RAND Corporation, 2007.

Crawford, Richard and Tharp, LtCol Adam. "Role of Law Enforcement Professionals in Attack the Network Strategy." *Air Land Sea Bulletin, 2012-3,* 2012: 27.

Danzig, Richard, et al. "Aum Shinrikyo: Insights into how Terrorists Develop Biological and Chemical Weapons. Second Edition." Center for a New American Security, December 2012.

"Defense Joint Operations Center (DJIOC) Support to JIEDDO DTG 230612ZMAY06." *DIA Message.* DIA Director, May 23, 2003.

"Department of Defense Ammunition and Explosive Safety Standards." *DoD Manual 6055.9-M.* DoD, February 29, 2008.

"Department of Defense Dictionary of Military and Associated Terms." *Joint Publication 1-02.* Joint Chiefs of Staff, July 15, 2012.

"Department of Defense Support to Humanitarian Mine Action." *CJCSI 3207.01C.* Chairman of the Joint Chiefs of Staff, September 28, 2013.

"Department of Energy (DoE)." *The Office of Science Laboratories.* http://science.energy.gov/laboratories/ (accessed December 5, 2013).

Department of Homeland Security, Mission. http://www.dhs.gov/our_mission.htm (accessed December 4, 2013).

Department of Homeland Security, Office of Bombing Prevention. http://www.dhs.gov/obp (accessed December 4, 2013).

"Department of Justice." *About DOJ, Our Mission.* http:www.justice.gov/about/html (accessed December 5, 2013).

"Department of Justice." *Department of Justice Agencies, ATF.* http://www.justice.gov/agencies/index-list.html#ATF (accessed December 5, 2013).

"Department of Justice." *Departments of Justice Agencies, FBI.* http://www.justice.gov/agencies/index-list.html#FBI (accessed December 5, 2013).

"Department of Justice." *Department of Justice Agencies, INTERPOL Washington.* http://www.justice.gov/interpol-washington/about.html (accessed December 5, 2013).

"Department of Justice." *Departments of Justice Agencies, DEA.* http://www.justice.gov/agencies/index-list.html#DEA (accessed December 5, 2013).

Department of Justice, About DOJ, Our Mission Statement. http://www.justice.gov/about.html (accessed December 4, 2013).

Department of State, Bureau of Counterterrorism. http://www.state.gov/j/ct/index.htm (accessed December 4, 2013).

Department of State, Mission. http://www.state.gov/s/d/rm/index.htm#mission (accessed December 4, 2013).

"DoD Information Sharing Strategy." *National Intelligence Community.* Washington, DC: Department of Defense, May 14, 2007.

Ewell LTC Julian J. and Hunt, MG Ira A. Jr. "Vietnam Studies: Sharpening the Combat Edge, The Use of Analysis to Reinforce Military Judgement." Washington, DC: Department of the Army, 1974.

"Exposure Letters." *UCLA EDU.* www.ph.ucla.edu/epi/bioter/detect/anteled_letter.a.html.

"FBI unveils sceince of anthrax investigation." *Sandia National Laboratories.* https://share.sandia.gov/news/resources/release/2008/anthrax.html.

Gallego, Pablo Esteban Para. “IEDs: A Major Threat for a Struggling Society.” *The Journal of ERW and Mine Action,* 2009.

Garaux, CPT Joseph M. “The IED Fight: Technical Shortcomings and the Value of Strategy.” *Marine Corps Gazette,* 2010: 8.

Gettig, M. MAJ. “Five Factors of an IED Attack.” *Military Intelligence Professional Bulletin,* 2011: 26-28.

“Global Trends 2025: A Transformed World.” U.S. National Intelligence Council, November 2008. 68.

“Glossary of EOD Terminology, Abbreviations and Designations.” *TM 60A-1-1-15*. Headquarters Department of the Army, January 11, 2002.

Good, Creg. “IED Reporting with the Weapons Technical Intelligence Lexicon.” *Counter-IED Bulletin X, Center for Army Lessons Learned*, 2012: 37.

Harden, Toby. *Bandit Country: The IRA & South Armagh.* London: Hodder and Stoughton, 1999.

—. *Dead Men Risen: The Welsh Guards and the Real Story of Britain’s War in Afghanistan.* London: Quercus, 2011.

Hart, GySgt Jason R. USMC. *Weapons Intelligence Team After Action Report for Counter IED Operations in Support of Regimental Combat Teams 2 and 8 from December 2010 to May 2011.* Afghanistan: Combined Joint task Force Paladin Southwest, 2011.

Hay, LTG John. “Vietnam Studies, Tactical and Material Innovations,.” *CMH-Publication 90-21*. Department of the Army, 1974. 131.

Huddleston, Samual and et al. “The Warfighter’s Guide to Counter-IED Analysis.” *Joint IED Defeat Organization*, 2010.

“INSCOM Roles with Regard to BEI and Analysis Tools Supporting the DOD Biometrics Executive Agent.” *Memo through DA-G2 for CG INSCOM.* DA Deputy Chief of Staff (G3/5/7), May 2, 2007.

“Intelligence.” *FM 2-0.* Headquarters Department of the Army, September 2010.

“Intelligence Community Information Sharing Strategy.” National Intelligence Community, February 2008.

Jackson, Brian A. “Appitude for Destruction: Organizational Learning in Terrorist Groups and its Implications for Combating Terrorism.” The RAND Corporation, 2005.

Jackson, Brian A, and David Frelinger. “Stealing the Sword, Rifling Through the Terrorist’s Arsenal.” The RAND Corporation, October 2007.

Jackson, Brian et al. *What Do We Need to Know and How Do We Learn It.* Project Memorandum 1929-OSD, Arlington, VA: RAND Corporation, 2005.

Jackson, Brian, et al. “Intelligence Support to Counter IED Operations.” The RAND Corporation, October 2005.

“Joint and National Intelligence Support to Military Operations.” *Joint Publication 2-01.* Joint Chiefs of Staff, January 5, 2012.

“Joint Improvised Explosive Device Defeat Organization (JIEDDO).” *Department of Defense Directive 2000.19E.* Department of Defense, February 14, 2006.

“Joint Intelligence.” *Joint Publication 2-0.* Joint Chiefs of Staff, June 22, 2007.

“Joint Operations Accross the Range of Military Operations.” *Joint Publication 3-0.* Joint Chiefs of Staff, August 11, 2011.

Joint Prosecution and Exploitation Center (JPEC) Operations and the Use of Forensics in Iraq (Revision 1). Quantico, VA: Marine Corps Center for Lessons Learned, 2009.

Kagan, Kimberly. “Iraq Report, Iran’s Proxy War against the United States and the Iraqi Gorvernment.” The Institute for the Study of War, May 2006 - August 20, 2007.

Knights, Michael. “Deadly Developments: Explosively Formed Projectiles in Iraq.” *Jane’s Intelligence Review*, 2007: 8.

Langford, Ian. “Understanding and Defeating a Complex Adaptive System.” *Australian Army Jornal, Volume IX, no. 3,* 2012: 108.

Larry, Dick A. “Evolution of EOD in the Combined Arms Fight.” *Air Land Sea Bulletin 2009-2*, 2009: 21-22.

Larson, Krista. “French, Mali troops recover explosives in Gao.” *USA Today.* Associated Press, February 13, 2013.

Lee, Henry, and al et. *Henry Lee’s Crime Scene Handbook.* London: Elsevier, 2001.

Liebmann, David et al. “COIN and Company Fusion Cell Operations.” *Infantry Magazine*, 2010: 30.

Magner, Jeffery L. and Maxey, George J. *A Study of Factors Affecting Mine and Boobytrap Detection.* Alexandria, VA: Human Resources Research Organization, 1973.

“MAGTF Counter-Improvised Explosive Device Operations.” Department of the Navy, Headquarters United States Marine Corps, 2011.

“Management Guidance (Assigned Analytic Subtopics).” *Defense Intelligence Analysis Program.* DoD FM/A, August 2011.

Maxwell, David. *email to Dr. Russell W. Glenn; Subj: Re: IED experiences.* email. July 26, 2012.

McCrystal, Stanley. *My Share of the Task.* London: Portfolio Publishing, 2013.

Merriam-Webster Online. http://www.merriam-webster.com/dictionary/sensor (accessed December 2013).

Moulton, John. “Rethinking IED Strategies: From Iraq to Afghanistan.” *Military Review*, 2009: 31.

Muhl, Gerald M. “Defeating Improvised Explosive Devices (IED): Asymetric Threats and Capability Gaps.” *U.S. Army War College student paper.* March 23, 2011.

Muller, Richard A. “The Dirty Bomb Distraction, The biggest danger from radiological weapons is the misplaced panic that they would cause.” *MIT Technology Review.* MIT, June 23, 2004.

National Counter Terrorism Center (NCTC), What We Do. http://www.nctc.gov/about_us/what_we_do (accessed December 4, 2013).

“National Strategy for Information Sharing and Safeguarding.” *Executive Summary.* Office of the President of the United States, December 2012.

Obama, Barack. “Countering Improvised Explosive Devices.” The White House, February 26, 2013.

Odierno, Raymond T. et al. “ISR Evolution in the Iraqi Theater.” *Joint Forces Quarterly no. 50*, 2008: 54.

Office of the Director of National Intelligence, Mission, Vision and Goals. http://www.odni.gov/index.php/about/mission (accessed December 4, 2013).

“Operational Terms and Graphics.” *FM 1-02.* Headquarters Department of the Army, September 2004.

“Operations in Chemical, Biological, Radiological and Nuclear (CBRN) Environments.” *Joint Publication 3-11.* Joint Chiefs of Staff, August 26, 2008.

Oppenheimer, A. R. *IRA, The Bombs and the Bullets.* Dublin: Irish Academic Press, 2008.

Perry, Walter L. and Gordon, John IV. “Analytic Support to Intelligence in Counterinsurgencies.” *RAND Corporation*, 2008: 39.

Pita, Rene, and Gunaratna. “Revisiting Al-Qaida’s Anthrax Program.” *USMA CTC Sentinel.* Vol. 2. no. 5. USMA, May 2009.

“Requirements for AFG Theater Biometrics and Forensic Support Operations.” USFOR-A CJ3 BMO MEMO, March 26, 2006.

Rhone, MAJ Percy, interview by Ms Jenna Fike. *Operational Leadership Experiences, Combat Studies Institute* (December 1, 2010).

Richardson, John B. IV. “Be the Hunter, Not the Hunted, Defeating the RKG-3 Ambush.” *Armor*, 2009: 5.

Robinson, Linda. “The Future of U.S. Special Operations Forces.” *Council on Foreign Rleations Report No. 66.* Council on Foreign Relations, April 2013.

STRATFOR Global Intelligence, Security Weekly. “Nigeria’s Broko Haram Militants Remain a Regional Threat.” January 26, 2012.

"Suicide Attacks in Afghanistan (2001-2007)." *UN's Assistance Mission in Afghanistan.* UN Assistance Mission in Afghanistan (UNAMA), September 9, 2007.

"Technical Intelligence." *ATP 2-22.4.* Washington, DC: Headquarters, Department of the Army, 2013. 2-7.

"Terrorism and WMD in the Contemporary Operational Environment." *TRADOC G2 Handbook No. 1.04.* Traning and Doctrine Command (TRADOC), August 20, 2007.

"Updated Information Regarding Likely Components used in Boston Marathon Devices." *FBI-DHS Joint Intelligence Bulletin.* April 23, 2013.

"US Army Research and Development and Engineering Command, Intelligence and Information Warfare Directorate, Mission." http://www.cerdec.army.mil/directorates/i2wd.asp (accessed December 5, 2013).

"USMC, Role of Law Enforcement professionals Program." Marine Corps Center for Lessons Learned (MCCLL), 2009.

"Weapons Technical Intelligence (WTI) Improvised Explosive Device (IED) Lexicon." Defense Intelligence Agency / Joint IED Defeat Organization, October 2012.