Asymmetric Warfare Group Advisor takes cover with Soldiers while man-portable line charge system is detonated during training exercise near Forward Operating Base Zangabad, Afghanistan (U.S. Army/Alex Flynn)

Understanding the Enemy

The Enduring Value of Technical and Forensic Exploitation

By Thomas B. Smith and Marc Tranchemontagne

The escalation of improvised explosive device (IED) incidents and related casualties during Operations *Iraqi Freedom* and *Enduring Freedom* led to a new intelligence field related to technical intelligence (TECHINT) called *weapons technical intelligence* (WTI), which combined technical and forensic IED exploitation techniques to link persons, places, things, and events. WTI operationalizes technical and forensic activities by fusing the technical, forensic, and biometric disciplines to produce actionable intelligence for countering threat networks. It is an especially powerful tool against terrorist organizations that rely on IEDs as a primary weapon in their arsenals. Given the enduring nature of the IED problem, careful consideration is required to ensure that we have the necessary counter-IED capability and capacity to meet future threats across the range of military operations. Across this range and at each level of war from tactical to strategic, TECHINT and WTI make critical contributions to joint warfare and military decisionmaking.

WTI development has been incremental and idiosyncratic and has led

Captain Thomas B. Smith, USN, is Commanding Officer of the Naval Surface Warfare Center Indian Head, Explosive Ordnance Disposal Technology Division. Commander Marc Tranchemontagne, USN (Ret.), was an Explosive Ordnance Disposal Officer. He is currently an Associate with R3 Strategic Support Group.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2014		**00-00-2014 to 00-00-2014**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Understanding the Enemy: The Enduring Value of Technical and Forensic Exploitation	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **National Defense University,Joint Force Quarterly,260 Fifth Avenue, S.W. (Building 64, Room 2504) Fort Lesley J. McNair,Washinggton,DC,20319**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

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

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**7**	

to the fielding of a number of new capabilities including Counter-IED Task Forces, Counter-IED Operations/Intelligence Centers, Combined Explosives Exploitation Cells (CEXCs), Expeditionary Forensic Labs (EFLs—formerly Joint Expeditionary Forensic Facilities), and Weapons Intelligence Teams, all of which contribute to WTI. A few capabilities have been written into doctrine or have become programs of record, such as the CEXC platoons, which deploy small footprint expeditionary laboratories for the technical exploitation of IEDs and other ordnance, and the Army EFLs, which perform expeditionary forensic exploitation of IEDs as their name implies.[1] The relationships among these organizations, however, remain largely ad hoc; in the maritime domain, they are untested. These exploitation capabilities—technical and forensic, with the related discipline of biometrics—should be tested with multi-Service concepts of operation, exercised jointly, integrated into joint operational planning, and codified in joint doctrine that addresses the exploitation enterprise holistically.

The need for improved planning and interagency cooperation in counter-IED operations is well documented. A recent Government Accountability Office report found that Department of Defense (DOD) strategic planning does not adequately document the milestones and metrics required to achieve desired goals.[2] Additionally, Presidential policy directs interagency efforts toward effectively exploiting IED materials, advancing our information analysis, and maintaining our deployable counter-IED resources, among other activities.[3] For the foreseeable future, terrorist use of IEDs is expected to "pose a fundamental, significant and enduring threat."[4]

Discussion

Across the range of military operations, traditional TECHINT takes primacy in conventional conflict, and WTI takes primacy in irregular warfare.[5] Traditional TECHINT products are used to "prevent technological surprise, neutralize an adversary's technological advantages, enhance force protection . . . [and] support the development and employment of effective countermeasures," as well as inform acquisition priorities and shape strategic decisionmaking.[6] The Army, for example, maintains antiarmor and antiair task forces that analyze battle damage to identify enemy capabilities, friendly technological gaps, countervailing tactics, techniques, and procedures (TTPs), and areas for product improvement. Although a single weapons system is seldom decisive on its own, new or enhanced technologies can be disruptive. U.S. military superiority serves as a strategic deterrent to war, and U.S. technological superiority underpins that military advantage.[7]

WTI allows operational commanders to interrupt an enemy's decision cycle and interdict IED tactical employment in real time. Simply put, it can mitigate the costs of technical surprise in terms of personnel, equipment, and dollars by placing better information in the hands of warfighters when prioritizing and planning operations. Its five outcomes—force protection, targeting, component and material sourcing, support to prosecution, and signal characterization—contribute to operational success in irregular warfare. WTI supports counterinsurgency and counterterrorism in current contingencies, but could also contribute to peace enforcement, counterpiracy, maritime security, promoting the rule of law, and countering other irregular challenges. At the operational and tactical levels of war, WTI contributes directly to the doctrinal counter-IED lines of operation: attack the network, defeat the device, and train the force.[8] In some cases, due to lack of either international agreement or deployed capacity, valuable information is lost when captured material is disposed of where it is found rather than being routed to a forward WTI facility for analysis.

Terrorist and insurgent groups have used IEDs so effectively in Iraq and Afghanistan that they have been called "weapons of strategic influence."[9] Terrorists have been proficient at synchronizing IED attacks with information operations to weaken public confidence in the government, demonstrate terrorist effectiveness, and damage coalition morale. On March 11, 2004, for example, terrorists simultaneously detonated bombs on four trains near Madrid 3 days before Spain's general election. The incumbent president had a small lead in opinion polls going into the election and was favored to win in spite of his unpopular decision to contribute Spanish troops to the U.S.-led coalition in Iraq. The attacks killed 191 people, wounded 1,800, and changed the outcome of the election, which led to Spain withdrawing its forces from Iraq. Strategically, terrorists have also used IED attacks to influence U.S. public opinion and undermine the Nation's political resolve.

In October 2011, the Department of Justice unsealed an indictment describing the illegal export of electronic devices to Iran. Four men from Singapore 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 recovered 16 of the RF modules from IEDs in Iraq. By locally 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.[10] This success is an 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 connections to the broader Intelligence Community.

At the operational level of war, TECHINT and WTI inform military decisionmaking by supporting intelligence preparation of the operational environment and helping to protect friendly critical requirements, identify enemy critical vulnerabilities, and attack the enemy center of gravity. Insurgent reliance on IEDs in Iraq created an opportunity for coalition forces. For the insurgents, IEDs were a critical requirement—the most lethal, effective, and fearsome weapons they possessed—that also proved to be a critical vulnerability. Initially regarded primarily as a force protection issue, the

IED came to be viewed more properly as an intelligence opportunity that could yield key information about the network of bomb designers, builders, emplacers, triggermen, financiers, component suppliers, trainers, planners, and operational leaders who made up the web of actors who execute IED attacks.[11]

WTI contributes to defeating the enemy center of gravity because it provides insight into the network—how it is led and sustained and how it operates—that is critical to defeating it. Attack-the-network operations fit neatly within the find, fix, finish, exploit, analyze, disseminate (F3EAD) architecture developed by the special operations community during counterterrorism operations in Iraq and Afghanistan. When synchronized with biometric enrollment and detention operations, WTI creates synergy that deepens the operational commander's knowledge of the adversary. Forensic information correlated to biometric databases allows coalition forces to associate a specific IED to a discrete individual, link clusters of devices to a specific bombmaker or IED cell, recognize patterns of insurgent operations, and identify named areas of interest against which commanders can plan operations. Technical exploitation of IED components can indicate where a bombmaker learned his technique and whether IED components were obtained locally or imported.

For democracies such as the United States, political will and public support tend to be critical vulnerabilities—possibly even the friendly center of gravity at the strategic level. IEDs are used by the enemy in part to sow fear, create a perception of host nation weakness, undermine troop morale, split coalitions, provoke overreaction by security forces, alienate local populations, and erode political will. WTI has been used extensively to support rule of law initiatives that demonstrate the effectiveness of the host nation's judicial system and reinforce public confidence in the legitimacy of the government. Identifying the perpetrators of attacks on civilians can help to isolate insurgents from the populace and undermine their propaganda.

In terms of joint functions, TECHINT and WTI support command and control (now replaced by *mission orders* in Army doctrine), fires, movement and maneuver, intelligence, sustainment, and protection.[12] In counterinsurgency, understanding the enemy network allows commanders to develop actionable intelligence and exercise "disciplined initiative" consistent with commander's intent.[13] Understanding how the enemy perceives the operational environment can inform a commander's decisions on such matters as arranging forces, designating operational areas, achieving effective span of control, and synchronizing operations. The fusing of technical, forensic, and biometric information into actionable intelligence permits precise fires to shape the operational environment, including supply chain interdiction, counterthreat finance operations, information operations, cache destruction, and the capture of high-value individuals. Landmines, IEDs, and naval mines are antiaccess and area-denial weapons that serve as impediments to both movement (for example, the reception, staging, and onward integration of coalition forces) and maneuver. Moreover, mines and IEDs are often used to prevent sustainment and resupply of friendly forces. At the strategic level of war, naval mines can be used to blockade critical ports and target commercial shipping in a strangulation strategy. Technical exploitation of these weapons informs strategic and operational planning and facilitates the development of countermeasures and countervailing TTPs.

Operational analysis demonstrates that WTI yields measurable effects on the battlefield and can be used by commanders to set operational priorities. Recent analysis in Afghanistan, for example, showed that removing bombmakers from the battlefield led to statistically significant reductions in IED attacks in a given area for a quantifiable period of time. Other generally accepted metrics such as cache destruction and route clearance showed no statistically significant effect.[14] Compelling statistical evidence that detaining even relatively low-level insurgent bombmakers produces measurable effects won over skeptical commanders and resulted in a marked increase in evidence-based targeting.[15] Bombmaking requires special skills and training that are not easily replaced.

Technical exploitation is critical to ensuring that the U.S. Armed Forces maintain a technological advantage against any adversary. Across all phases of operations from peacetime-shaping through stability operations and enabling civil authority, technical exploitation and foreign material acquisition functions provide critical TECHINT on an enemy's ordnance order of battle. An understanding of adversary strengths and weaknesses gained from exploitation of enemy ordnance may influence operational planning and force protection.[16] During World War II, for instance, Germany developed bomb fuzes with antihandling mechanisms to target British bomb disposal personnel during the blitz. Exploitation of recovered fuzes led to countermeasures that allowed clearance operations to continue. It also led to tighter operational security regarding bomb disposal procedures. Recovering captured enemy equipment—including enemy ordnance—is both a combatant command and national requirement and is doctrinally performed at the operational level by a Joint Captured Material Exploitation Center with reachback and collaboration across the interagency.[17]

The forensic aspect of exploitation, which links persons, places, things, and events, supports theater strategic goals of reestablishing the rule of law by supporting criminal prosecutions. While getting bombers off the street or battlefield is a positive end in itself, demonstrating the effectiveness of the host nation's judicial system reinforces public confidence in the legitimacy of the host nation government. Identifying the perpetrators of attacks on civilians helps cut insurgents off from the populace and undermines their propaganda. The public's faith in its government and civic institutions' ability to deliver positive social goods is essential to winning in counterinsurgency, where the goal is less to defeat the insurgent than to make him irrelevant.

Exploitation can also provide a powerful metric for evaluating policy. In Iraq, fingerprint matches from recovered IEDs have demonstrated that the recidivism rate among released detainees was higher than believed and that Iraq's amnesty program had returned many bad actors to the street. In Afghanistan, evaluation of recovered homemade explosives (HME) provides insight into the effectiveness of programs to ban the importation of certain fertilizers used in HME production. While the in-country exploitation of IEDs is considered operational, it provides the crucial linkage to strategic, national, and special exploitation capabilities, such as the Federal Bureau of Investigation's (FBI's) Terrorist Device Analytical Center, National Ground Intelligence Center, U.S. Army Criminal Investigation Laboratory, and other national resources.

One way exploitation can influence strategic decisionmaking is by providing early indication of third-country participation in a conflict or state sponsorship of a terrorist organization. For example, the technical exploitation of explosively formed penetrators (EFPs) during Operation *Iraqi Freedom*, corroborated by other intelligence, provided an early indication that EFPs were not being manufactured in Iraq but were imported from a third country. Metallurgy helped confirm that the high-purity copper EFP liners were not produced in Iraq. Differences in the liners indicated the kind of press that was required to fabricate them—a heavy press not commonly seen in Iraq—as well as an indication of the number of different presses that were being used.[18] Similarly, identifying third-country conventional ordnance in a war zone might belie that country's claims of neutrality. In an insurgency, foreign ordnance might indicate external support, arms smuggling, or the presence of foreign fighters. Such evidence can shape strategic decisionmaking.

Technical exploitation can provide evidence of violations of international law and treaties. In countering the proliferation of chemical, biological, radiological, nuclear, and high-yield explosive weapons of mass destruction (WMD), identifying the country of origin of recovered, seized, or contraband weapons would be a necessary precursor to diplomatic or other action under the Proliferation Security Initiative. Moreover, characterizing the extent of the threat posed by WMD requires an understanding of the level of sophistication of such weapons. In peace enforcement operations, the recovery and exploitation of banned weapons might provide evidence of cease-fire violations. Likewise, the exploitation of recovered drifting mines can provide evidence of violations of international norms and treaties—in this example, the Hague Convention of 1907.

The presence of naval mines in the northern Arabian Gulf was one factor that prevented an amphibious landing at Ash Shuaybah, Kuwait, during Operation *Desert Storm*. Later technical exploitation of these mines showed that many were neither active nor laid effectively. In fact, many lacked batteries and sensors.[19] Had this technical information been available earlier, it might have influenced operational and, perhaps, theater-strategic planning.

At the tactical level of war, WTI outcomes help to predict, prevent, detect, neutralize, and mitigate IED attacks. They have been essential in the development of electronic countermeasures for radio-controlled IEDs and have created new opportunities for commanders to gain tactical advantages in novel ways. WTI outcomes are used to target insurgents, develop force protection measures, formulate counter-IED TTP, design countermeasures, provide indications and warnings of IED attacks, interdict supplies and precursors, and support prosecution by the host nation. The exploitation of an IED incident also yields important information about incident geometry that can help friendly forces understand where an insurgent is likely to emplace an IED or how he might trigger it.[20] Not only do WTI products help friendly forces develop TTP to avoid IED ambushes, but they also enable commanders to target the insurgents who employ the devices. WTI allows tactical forces to seize the initiative and become the hunter rather than the hunted.

The Way Ahead

Lessons learned from technical and forensic exploitation in Iraq and Afghanistan have created new capabilities, interdisciplinary methodologies, and operational units for the technical and forensic exploitation of explosives, explosive hazards, and foreign ordnance. The institutionalization of these capabilities—directed by the Joint Requirements Oversight Council—has been incremental, and no joint operating concept for their employment exists. Nor is there an operating concept or doctrine for organizing and employing the various technical and forensic organizations, disciplines, functions, and processes resident in DOD and the Interagency.

Many stakeholders exist across DOD and the other Federal agencies. The Defense Intelligence Agency has primary responsibility for intelligence activities and programs related to forensics.[21] The Navy is the DOD Single Manager for explosive ordnance disposal (EOD) technology, which includes technical exploitation of recovered explosives, explosive devices, and other explosive hazards. The Navy executes this responsibility through the Indian Head EOD Technology Division.[22] The Army is the DOD Executive Agent (EA) for forensic disciplines relating to DNA, serology, firearms and tool marks, latent prints, questioned documents, drug chemistry, and trace materials, as well as forensic medicine disciplines.[23] It is also the EA for biometrics, a separate but related and complementary field that uses measurable biological and behavioral characteristics to uniquely identify people.[24] The Air Force is the EA for Digital and Multimedia Forensics relating to computer and electronic device forensics, audio forensics, image analysis, and video analysis.[25] Counter-IED operations in Operations *Iraqi Freedom* and *Enduring Freedom* have also relied on coalition partners, particularly the British, who have a lot of experience with WTI.

The Services have developed a variety of modular, scalable, deployable laboratories for overseas contingencies, including those used by the Navy CEXC

Afghan and coalition security force uncovers Taliban weapons cache containing materials for constructing IEDs, including ammonium nitrate, homemade explosives, and detonation triggers, during operation in Helmand Province (DOD/Justin Young)

platoons and Army EFLs. The Army also maintains heavy and light mobile laboratories to conduct field confirmatory chemical, biological, and explosive analysis and near-real-time chemical air monitoring. Experience in Operations *Iraqi Freedom* and *Enduring Freedom* demonstrates that an in-country exploitation capability provides a degree of responsiveness due to physical and psychological proximity to the warfighter that a U.S.-based capability cannot match while providing a comparable level of exploitation. Laboratory exploitation in recent operations has taken place in large bases as well as austere forward operating bases. Extension of these operations continues in U.S. Naval Forces Central in support of Combined Task Force 56, for example, moving a comprehensive capability outside Iraq and Afghanistan for the first time to assist in partnering efforts. Moving a scaled-down laboratory element forward for a major operation could improve timely intelligence delivery to the warfighter even further. Scaling these laboratories for ground transport on heavy vehicles, intertheater lift, and seabasing has recently been exercised and is already supporting combatant command exercise and engagement plans.

Technical and forensic exploitation operations have not been exercised in a maritime context. Maritime operations might include operating from a seabase, supporting maritime security operations, supporting a Marine Air-Ground Task Force ashore, and conducting WTI operations for underwater threats. The Navy has only a minimal capability to collect forensic evidence in the aftermath of an underwater explosive incident such as the terrorist IED attack against the destroyer USS *Cole* or the sinking of the South Korean corvette ROKS *Cheonan* by a North Korean submarine. It lacks appropriate doctrine, procedures, training, and equipment to conduct site exploitation and postblast investigation underwater to support WTI—a task that only Navy EOD technicians can execute due to the diving requirement. The FBI runs an underwater postblast investigation course, but it does not provide unit-level training.

The 2010 Quadrennial Defense Review (QDR) identified several key initiatives to ensure that DOD is prepared to provide appropriate support to civil authorities. Regarding counter-IED operations, it states, "to better prepare the Department to support civil authorities seeking to counter potential threats from domestic IEDs, DOD will assist civil authorities with counter-IED TTPs and capabilities developed in recent operations."[26] This contingency has not been exercised and the authorities have not been worked out, but it would seem that

DOD's expertise in counter-IED technical and forensic exploitation operations would be an important asset for defense support of civil authorities. Immediate military support to civilian authorities by EOD forces is allowed by U.S. law but is also ad hoc. As recently demonstrated, the Army's 387th Ordnance Company responded to 64 "call outs" during the Boston Marathon bombing.[27] Mindful of the Posse Comitatus Act, we should provide a seamless system that credentials and integrates military EOD operations in support of civil authorities nationally.[28]

The proliferation of IED knowledge suggests that these devices will continue to be used by terrorists, insurgents, and criminal elements at home and abroad. The Army's EFLs and the Navy's Technical Support Detachment with its subordinate CEXC platoons would be well suited to fulfill the QDR priority of enhancing domestic counter-IED capabilities. The Armed Forces have a large body of combat-tested military EOD technicians experienced in the IED fight who could quickly mobilize to support civilian efforts in the aftermath of an event similar to the Boston and Oklahoma City detonations, or worse, a sustained terrorist bombing campaign. Formal training and credentialing to facilitate their employment in support of civilian authorities in the event of a significant disaster are among the easier options.

Summary

The exploitation of enemy ordnance has important strategic implications for preventing technological surprise and informing strategic decisionmaking. At the strategic level of war, scientific and technical intelligence and WTI can help to:

- ensure U.S. technological advantage and its implicit deterrent effect
- prevent a future enemy from benefiting from disruptive new technologies or counter those technologies once fielded
- support operational and theater-strategic planning
- indicate third-country involvement in hostilities
- indicate state sponsorship of terrorist organizations
- provide evidence of violation of international norms and treaties
- provide metrics for evaluating theater-strategic and national policies
- support development of formal international partnerships
- enable combatant command theater security cooperation plans.

At the operational level of war, TECHINT and WTI contribute to:

- the three counter-IED lines of operation and F3EAD: attack the network, defeat the device, and train the force
- operational planning (Joint Operation Planning Process, Military Decision Making Process, network planning process)
- intelligence preparation of the operational environment
- host nation rule of law
- enabling formal data and information exchanges.

At the tactical level of war, TECHINT and WTI provide information used to:

- target insurgents
- develop force protection measures
- develop friendly TTPs
- develop countermeasures
- provide indications and warnings of IED activity
- interdict supplies and precursors
- support prosecution by the host nation.

Conclusion

An operating concept for conducting expeditionary technical and forensic exploitation would provide commanders with a framework for organizing and employing joint force technical and forensic exploitation capabilities. It would provide a holistic, synchronized approach to integrate multiple organizations, disciplines, functions, and processes that support technical and forensic exploitation. It would provide a joint task force commander a framework for planning, organizing, and executing technical and forensic exploitation operations including those in a maritime environment. Using lessons learned from Iraq and Afghanistan, a concept of operations would identify best scientific, technical, and operational practices for experimentation and future Service and Joint doctrine. While a number of new organizations and capabilities have emerged to confront IEDs, no complete doctrine, organization, training, materiel, leadership and education, personnel, and facilities solution exists for planning and executing technical and forensic exploitation operations across the range of military operations. Given the proven value of technical and forensic exploitation operations across this range and at every level of war, with the related discipline of biometrics, these exploitation capabilities should be tested with multi-Service concepts of operation, exercised jointly, and codified in joint doctrine that addresses the entire exploitation enterprise. **JFQ**

Notes

[1] In 2008, the Joint Requirements Oversight Council (JROC) directed the institutionalization of CEXC and the Joint Expeditionary Forensic Facilities (now EFL) through a doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF) Change Request, JROCM 128-08. Joint Staff Memorandum, JROCM 128-08, *Joint Improvised Explosive Device (IED) Defeat DOTMLPF Change Recommendation*, June 20, 2008.

[2] U.S. Government Accountability Office (GAO), *Defense Forensics: Additional Planning and Oversight Needed to Establish an Enduring Expeditionary Forensic Capability: Report to Congressional Requesters* (Washington, DC: GAO, June 2013), 9, available at <www.gao.gov/assets/660/655546.pdf>.

[3] The White House, "Countering Improvised Explosive Devices," Policy Statement, February 26, 2013, 3, available at <www.whitehouse.gov/sites/default/files/docs/cied_1.pdf>.

[4] Presidential Policy Directive 17, *Countering Improvised Explosive Devices* (Washington, DC: The White House, June 15, 2012), 2.

[5] Defense Intelligence Agency (DIA) and Joint Improvised Explosive Device Defeat Organization, *Weapons Technical Intelligence Handbook*, Version 1.1 (Washington, DC: DIA, October 2010), 9.

[6] Joint Publication (JP) 2-0, *Joint Intelligence* (Washington, DC: The Joint Staff, June 22, 2007), B-6.

[7] At the strategic level, TECHINT is called scientific and technical intelligence (S&TI); JP 2-0, B-6.

[8] The term *attack the network* is gradually being replaced by *countering threat networks.* For additional information on counter-IED lines of operations, see JP 3-15.1, *Counter-Improvised Explosive Device Operations* (Washington, DC: The Joint Staff, January 9, 2012), III-5.

[9] Joint Improvised Explosive Device Defeat Organization (JIEDDO), "Official Website of the Joint IED Defeat Organization," available at <www.jieddo.dod.mil/index.aspx>. According to the mission statement, "JIEDDO leads DOD [Department of Defense] actions to rapidly provide Counter Improvised Explosive Device (C-IED) capabilities in support of the Combatant Commanders and to enable the defeat of the IED as a weapon of strategic influence."

[10] Peter Finn, "U.S. Parts Illegally Used for Iraq Bombs: Trigger Modules Were Smuggled to Iran, Indictment Charges," *The Washington Post*, October 26, 2011, A9, available at <http://articles.washingtonpost.com/2011-10-25/world/35277242_1_hossein-larijani-hia-soo-gan-benson-iranian-procurement-networks>.

[11] For a discussion of critical factors (capabilities, requirements, and vulnerabilities) and center of gravity, see JP 5-0, *Joint Operation Planning*, and Naval Warfare Publication 5-01, *Naval Planning.* JP 5-0 defines *critical vulnerability* as "an aspect of a critical requirement which is deficient or vulnerable to direct or indirect attack that will create decisive or significant effects." JP 5-0, *Joint Operation Planning* (Washington, DC: The Joint Staff, August 11, 2011), III-23–25.

[12] "Joint functions are related capabilities and activities grouped together to help JFCs integrate, synchronize, and direct joint operations. Functions that are common to joint operations at all levels of war fall into six basic groups—C2, intelligence, fires, movement and maneuver, protection, and sustainment." JP 3-0, *Joint Operations* (Washington, DC: The Joint Staff, August 11, 2011), chapter III.

[13] Field Manual (FM) 3-0, *Operations*, Change 1 (Washington, DC: Headquarters Department of the Army, February 22, 2011), 5-2.

[14] Colonel Leo Bradley, USA, commander, Combined Joint Task Force Paladin, "Personal Observations," lecture, Defense Strategies Institute, EOD/IED and Countermine Symposium, July 24, 2013.

[15] Lieutenant Sarah Turse, USN (former officer-in-charge, CEXC Afghanistan), interview by Marc Tranchemontagne, August 27, 2012.

[16] JP 2-01, *Joint and National Intelligence Support to Military Operations* (Washington, DC: The Joint Staff, October 7, 2004), III-32.

[17] Ibid. The Joint Captured Material Exploitation Center is one of three doctrinal Joint Exploitation Centers, along with the Joint Document Exploitation Center and Joint Interrogation and Debriefing Center.

[18] Commander Scott Kraft, USN (former officer-in-charge, CEXC Iraq, Baghdad), interview by Marc Tranchemontagne, October 18, 2011.

[19] DOD, *Conduct of the Persian Gulf War: Final Report to Congress,* April 1992, 286, available at <www.dod.mil/pubs/foi/operation_and_plans/PersianGulfWar/404.pdf>. "Many deployed mines lacked sensors or batteries which prevented their proper operation. During MCM operations, 95 percent of the UDM-type acoustic influence mines were evaluated as inoperable. Several moored contact mines were recovered on the bottom and apparently 13 percent of the moored mines broke away from their moorings. However, even the poorly planned and improperly deployed minefields caused damage to two combatants and were one of several reasons the amphibious invasion was not conducted."

[20] DIA, 23–29.

[21] DOD, *DOD Forensic Enterprise (DFE)*, DOD Directive 5205.15E (Washington, DC: DOD, April 26, 2011), 2, available at <www.dtic.mil/whs/directives/corres/pdf/520515e.pdf>.

[22] In 1947, the Bureau of Naval Weapons established the first unit for research, development, test, and evaluation (RDT&E) of explosive ordnance disposal EOD equipment at the U.S. Naval Powder Factory within the EOD School. It eventually became the EOD Technology Center and, presently as NSWC Indian Head EOD Technology Division, has had joint service responsibility for EOD RTD&E since 1951, as directed in DODD 5160.62, *Single Manager Responsibility for Explosive Ordnance Disposal Technology and Training (EODT&T).*

[23] DOD, *DOD Forensic Enterprise*, 1, available at <www.dtic.mil/whs/directives/corres/pdf/520515e.pdf>.

[24] DOD, *DOD Biometrics*, DOD Directive 8521.01E (Washington, DC: DOD, February 21, 2008), 1, available at <www.dtic.mil/whs/directives/corres/pdf/852101p.pdf>.

[25] DOD, *DOD Forensic Enterprise.*

[26] DOD, *Quadrennial Defense Review Report* (Washington, DC: DOD, February 2010), 20, available at <www.defense.gov/qdr/qdr%20as%20of%2029jan10%201600.PDF>.

[27] Rick Crawford, "Testimony," House Armed Services Committee, EOD Priorities for FY2012 NDAA, 112th Cong., 1st sess., 2012, available at <http://docs.house.gov/meetings/AS/AS00/20130508/100806/HHRG-113-AS00-Wstate-C001087-20130508.pdf>.

[28] The Posse Comitatus Act of 1878, 18 U.S.C. §1385, as amended, limits the power of the Federal Government to enforce laws using Federal military personnel.