JFQ | Joint Force Quarterly

Issue 80, 1st Quarter 2016

Global Health Engagement

Inside U.S. Cyber Command

American Wolf Packs

Explosive ordnance disposal technician, 11th Civil Engineer Squadron, prepares to dispose of IED as part of Operation *Llama Fury*, August 25, 2015 (U.S. Air Force/Brittain Crolley)

The Enduring IED Problem

Why We Need Doctrine

By Marc Tranchemontagne

I sometimes hear people express the hope that the IED threat will diminish as Western forces pull out of Afghanistan. Unfortunately, nothing could be further from the truth—the IED has now entered the standard repertoire of irregular forces in urban areas across the planet, and there are no signs this threat is shrinking; on the contrary, it seems to be growing.

—David Kilcullen, *Out of the Mountains*

Commander Marc Tranchemontagne, USN (Ret.), is an Associate with R3 Strategic Support Group. He served more than 21 years as a Special Operations Officer and Master Explosive Ordnance Disposal Technician.

As the Services and joint force update their doctrine after nearly a decade and a half of counter–improvised explosive device (IED) operations in the Middle East, Africa, and Asia, now is a good time to consider what we have learned about operating in IED-rich environments. At the start of Operation *Enduring Freedom* in 2001, we lacked counter-IED doc-

trine—as well as counterinsurgency and counterterrorism doctrine—and had to figure things out on the fly. It was a steep learning curve with a high cost in lives lost and equipment destroyed, and the United States spent billions to counter a weapon that costs only a few dollars to make.

In addition to counter-IED doctrine and assorted handbooks, manuals, and lexicons, we created rapid acquisition authorities, notably the Joint IED Defeat Organization, now a combat support agency; new countermeasures such as counter-radio-controlled IED electronic warfare (CREW) systems; a new intelligence process (weapons technical intelligence [WTI]); counter-IED task forces and other ad hoc units such as the Joint CREW Composite Squadron, Task Force ODIN, weapons intelligence teams, and deployable counter-IED laboratories; law enforcement, interagency, and international partnerships; universal counter-IED training and specialized courses in homemade explosives (HME), post-blast investigation, and IED electronics; counter-IED working groups and other new staff elements; new families of armored vehicles; and many innovative tools to meet the IED threat.[1] Some initiatives have been incorporated into doctrine or have become programs of record, some have been shelved, and others remain ad hoc. As a joint force, it is important to institutionalize what we have learned from hard experience in IED-rich environments.

IEDs affect how we fight, that is, how we plan for and execute joint operations. Operating in an IED-rich environment creates additional challenges for U.S. forces, just as operating in a chemical warfare environment would. Operation *Iraqi Freedom* may represent the worst case for an IED-rich environment, with numerous experienced, technology-savvy, externally supported violent extremist organizations (VEO) with overlapping and competing sectarian, nationalist, and international agendas in a developed theater. Future operating environments, however, may match its complexity and lethality. Today's bomb makers will take their experience and expertise to other battlefields. Even in a conventional war, our adversaries are likely to turn to unconventional warfare tactics, using a mix of special forces, paramilitary units, militias, and surrogates to counter our military superiority. IEDs will figure in their order of battle.

Although IEDs are more closely associated with irregular warfare, they have been used in every modern conflict, often on a large scale as a matter of policy and doctrine. Explosive booby traps were used extensively in World War I by both sides, but that story is eclipsed by the overwhelming carnage caused by artillery, machine guns, and gas in that war. British, Australian, and New Zealand troops, for example, covered their withdrawal from Gallipoli by booby-trapping their trenches and abandoned stores to obstruct pursuit by Turkish forces.[2] During the Korean War, North Korean troops, following Chinese and Soviet doctrine of the era, saturated areas that they abandoned with mines and booby traps.[3] IEDs, mines, and booby traps were such problems in World War II, Korea, and Vietnam that the Services issued numerous field manuals and handbooks to prepare deploying forces to deal with them. One of the earliest counter-IED pamphlets, *German Ruses*, was published in 1917. Its warnings remain valid today.[4]

What Are IEDs?

The term *improvised explosive device*—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—covers a wide range of explosive hazards, including roadside bombs and explosive booby traps.[5] At a minimum, an IED is made up of an explosive charge and a means of setting it off. Typically, however, IEDs have five components: a container, a main charge, an initiator, a switch, and a power source. Some include enhancements such as additional fragmentation or pyrophoric, chemical, biological, and radiological materials, which increase the bomb's lethality or its explosive, incendiary, or psychological effect. Explosively formed penetrators and shaped charges incorporate special liners that focus the explosive's energy, allowing it to penetrate armor. Many IEDs incorporate military munitions or commercial components.

The IED is frequently referred to as the *weapon of choice* of threat networks globally. However, this expression does not bear scrutiny. The *weapon of choice* construction has two implications: first, that the user has a choice of weapons and that among those choices the IED is preferred, and second, that the user can choose to use or not use IEDs, as in "Afghanistan is a *war of necessity* but Iraq is a *war of choice*." The first implication is simply untrue, and the second does little to further our understanding of the IED problem. Like *weapon of influence*, *weapon of concern*, *weapon of interest*, *war of necessity*, and dozens of other inelegant constructions using *of*, *weapon of choice* is an uninspired kluge whose meaning is too ambiguous to help us understand the IED problem. The term ought to be retired, especially in policy, doctrine, and other thoughtful writing. Not only is the syntax poor and the meaning imprecise, but it also has become a cliché and a poor substitute for critical thinking. The words we use matter because they frame how we think about and solve operational problems.

When terrorists have a choice of weapons, the IED is not always preferred. Conversely, when terrorists have limited alternatives, the IED is often merely the best choice available. Threat networks might choose other weapons for a variety of practical, social, or cultural reasons: al Qaeda used airplanes in the September 11 attacks, al Shabaab gunmen used small arms to attack the Westgate shopping mall in Nairobi, Kenya, in September 2013, and Hutu militants used mostly machetes to kill nearly 1 million Tutsis during the Rwandan genocide in 1994. In the United States, it is much easier to buy guns than it is to purchase explosives or many of the precursor chemicals needed for making them. Many groups would certainly choose other weapons—for example, man-portable anti-aircraft

missiles and anti-armor rockets, chemical and biological weapons, mortars and other indirect-fire weapons, or computer viruses—if they were available. Suicide IEDs were pioneered by the secular Tamil Tigers in Sri Lanka in the 1980s, and today are used by many radical Islamic groups. In spite of their effectiveness, however, their appeal is far from universal.[6] There are many reasons for threat networks to rely on IEDs, including avoiding the potential constraints imposed by a state sponsor, achieving rough parity with better-equipped government forces, inspiring fear, and attracting media attention. These factors, however, do not make IEDs *necessarily* the weapon of choice. In contemplating future contingencies, we ought to consider the circumstances in which using IEDs would be an attractive option for our adversaries.

The phrase *weapon of strategic influence* also should be scrapped. A weapon is a weapon, and it is how a weapon is used that gives it its strategic influence. Other weapons have just as much strategic utility. Shoulder-fired Stinger missiles helped hasten the Soviet withdrawal from Afghanistan during the Soviet-Afghan War from 1979–1989, and an assassin wielding a pistol murdered Archduke Franz Ferdinand of Austria in June 1914, triggering World War I. It is not the IED itself that is strategic but the terrorist act for which it is used. Terrorism is always a political act—usually aimed at coercing governments or populations—and therefore of a strategic nature. It is terror that is strategic; IEDs are merely another means of terrorizing.

Why IEDs?

Like any other weapon, IEDs can be used for various strategic, operational, and tactical purposes. IEDs are different from conventional weapons, however, in important ways that make them appealing to a range of adversaries. These differences include the following:

- ease and low cost of fabrication using commercially available materials, which makes them cost effective and allows nonstate actors to operate without state sponsorship
- lethality, which compensates for a lack of more powerful conventional weapons
- variability in design, which makes developing countermeasures and countervailing tactics difficult
- adaptability to the operating environment, which makes IEDs more versatile and difficult to detect
- scalability, which allows terrorists to modulate their level of violence
- deniability, which appeals to actors who wish to avoid attribution
- low risk to the bomber relative to other means of attack, such as ambushes and raids
- operational effects on movement and maneuver and force protection
- strategic and psychological effects generated by the high publicity that IED attacks garner.

At the strategic level of war, IED attacks support our adversary's propaganda, portraying the host nation as impotent and undermining U.S. national will. At the operational level, our adversaries use IEDs to shape how we fight—tempting us to hunker down in heavily defended outposts and venture out only in armored convoys, thereby distancing us from the people we need to engage. At the tactical level, our adversaries use IEDs to constrain our freedom of action, counter our superiority of arms, and attrit our forces.

Strategic. Insurgent groups in Iraq and Afghanistan proved proficient at synchronizing IED attacks with information operations to weaken public confidence in the government, demonstrate their effectiveness, and undermine coalition resolve. Spectacular IED attacks gain media coverage and demonstrate a group's effectiveness, which furthers its recruiting and attracts funding, especially when competing for resources against other VEOs. The presence of multiple VEOs in an operating environment, as witnessed in Iraq and now Syria, is often accompanied by higher levels of violence and makes the IED problem more complex.

IEDs help the insurgent raise the cost of the conflict to an unacceptable level in terms of casualties suffered, resources depleted, and time expended, and foster the sense that the conflict cannot be won. IEDs can be used to harm a nation's economy by restricting the flow of goods and services over internal lines of communication and creating a climate of insecurity that discourages foreign investment, trade, and tourism. IED attacks on Iraqi oil pipelines, for example, denied the government much-needed revenue for reconstruction during *Iraqi Freedom*.

IEDs are often regarded as an asymmetric means to counter U.S. military strength, but military power is only one factor. U.S. strength in the other elements of national power—diplomatic, informational, and economic—serves to isolate adversary groups from the state sponsorship that could provide them with the sophisticated conventional weapons they would need to match U.S. and host-nation forces. U.S. hard power and soft power deter other nations from sponsoring terrorists or limit such support to methods that are deniable, such as the explosively formed penetrators that Iran provided to Shiite groups in Iraq.[7] IEDs provide terrorists a means to attack U.S. forces while avoiding the constraints that a sponsor might impose on them.

Operational. Our enemies use IEDs to shape the operating environment to their advantage by impeding friendly force movement and maneuver, defeating force protection measures, and complicating logistics. IEDs constrain our mobility and hinder our freedom of action, which isolates our troops from the population they need to influence and protect. Suicide bombers give the enemy a means, in terms of space and time, to attack in our operational depth, including in our rear areas, such as an insider attack on a command center.

Operating in an IED-rich environment forces commanders to allocate limited resources to force protection and sustainment and slows the tempo of operations. To avoid IEDs, we rely on helicopters and cargo planes for intertheater lift, which increases cost and slows sustainment. During Operation *Iraqi Freedom*, multinational forces devoted considerable resources to keeping main

supply routes open. Lesser roads were often impassible, which further constrained our mobility. The IED provides a means for qualitatively and quantitatively inferior groups to operate over a larger area and strike at a time and place of their choosing. This, in turn, reduces their vulnerability as they attrit U.S. forces. IEDs serve as force multipliers that allow insurgents to create larger effects on the battlefield without massing forces.

Tactical. IEDs give our enemies tactical advantages in ways that other weapons do not. IEDs compensate for a lack of conventional weapons by providing greater lethality, standoff, and survivability than small arms. They also provide a countermobility capability against mounted and dismounted units, and a means to attack hardened targets such as armored vehicles and fortifications. Like landmines, IEDs alter the terrain to channelize movement into prepared ambushes. In addition, IEDs provide standoff that reduces the bomber's vulnerability by keeping him out of the range of our weapons and sensors. The IED's indiscriminate nature and anonymity make it even more fearsome and effective as a psychological weapon, heightening the combat stress of friendly forces.

In conventional warfare, when the enemy is forced to withdraw, he typically mines and booby-traps any facilities or stores he leaves behind. The presence of booby traps prevents soldiers from taking shelter in captured buildings and bunkers, leaving them exposed to the elements and vulnerable to attack by aircraft and artillery.[8] During the Korean War, the North Koreans even booby-trapped timber, knowing that United Nations forces would be scavenging for firewood to stay warm.[9]

Countering IEDs Across the Phases of Operation

IEDs have different implications for each phase of operation. During the "shaping" and "deter" phases, they are largely a force protection problem. Routine peacetime presence and multilateral exercises place U.S. forces within reach of adversaries who might employ IEDs.

During the "seize the initiative" and "dominate" phases, in which the focus of operations is on capturing and occupying the enemy's territory, IEDs are primarily an impediment to movement and maneuver that will be breached or bypassed like other explosive obstacles. Timing and tempo typically are more highly valued in phase two and phase three operations in order to bring about the enemy's collapse or culmination.

In the "stability" and "transfer to civil authority" phases, the IED becomes a means for former regime elements and other antagonists to continue the fight. In these phases of operation, the exploitation of IEDs provides U.S. forces a means to gain insight into the networks hostile to the occupying force, as it does in counterinsurgency and counterterrorism operations. Exploitation allows us to attribute IEDs to specific individuals who can then be targeted.

The competing demands of mobility and intelligence are important considerations when operating in an IED-rich environment. This language from the Marine Corps's *MAGTF C-IED Operations* captures the distinction nicely:

> *To effectively manage threats in an IED-rich environment, commanders must provide guidance on appropriate actions when an IED is encountered. Essentially, the on-scene commander facing an IED has to decide whether to mark and bypass or isolate the area for follow-on EOD* [explosive ordnance disposal] *neutralization and exploitation. Tactical considerations and leadership guidelines will dictate which action is taken. Finally, law of war considerations must factor into the on-scene commander's decision whether to destroy an IED. The principles of necessity, distinction, proportionality, and unnecessary suffering must be weighed in making this decision.*[10]

Guidance would likely change across the phases of an operation, with assured mobility taking priority in the "seize the initiative" and "dominate" phases and the intelligence value of IEDs taking priority in the "shape," "deter," "stabilize," and "enable civil authority" phases. Assured mobility is emphasized in engineering doctrine, while the intelligence value of IEDs is emphasized in EOD and WTI publications. Joint doctrine should give commanders an understanding of how to reconcile the competing requirements of mobility, force protection, and IED exploitation.

It is also important in phases two and three to preempt the IED problem by disposing of unexploded ordnance (UXO) and captured munitions—something we failed to do in Iraq. Unsecured Iraqi munition stockpiles were quickly looted and became a major source of enemy supply early in the insurgency. Similarly, in Vietnam, Viet Cong guerrillas used unexploded U.S. ordnance in booby traps and locally manufactured munitions.[11] Separatists from the National Organization of Cypriot Fighters in Cyprus in the 1950s went as far as salvaging munitions from sunken warships, which they then steamed out in order to obtain material for explosives.[12] Captured munitions and ammunition supply points must be guarded or destroyed. UXO should be cleared from the battlefield as units move forward. These tasks must be planned for and have forces allocated to them. Phase zero shaping activities should also include clearing explosive remnants of war to prevent munitions from past conflicts from becoming IEDs in future conflicts.

Counterinsurgency

Counterinsurgency provides the context for our recent experience in IED-rich environments. The IED fight is in part a contest for control over the environment and the population. We interdict the bomber's access to explosives by clearing unexploded ordnance, destroying enemy ammunition supply points and arms caches, and regulating HME precursors, such as ammonium nitrate fertilizers. We restrict the bomber's access to the electromagnetic spectrum with electronic warfare systems such as CREW and Wolfhound, and we likewise restrict his access to resources through counter-threat finance and supply chain interdiction. We restrict the bomber's access to terrain with barriers, entry controls, route clearance, and surveil-

Explosive ordnance disposal technician, 3rd EOD, 9th Engineer Support Battalion, performs sweep with metal detector during post-blast analysis training scenario at Emerson Lake training area, September 19, 2015, Twentynine Palms, California (U.S. Marine Corps/Levi Schultz)

lance, and to the population through counterinsurgency activities like census taking and biometric enrollment, which enable network targeting. Many counterinsurgency best practices are essential to countering IEDs, and many counter-IED practices are good counterinsurgency. A handwritten sign posted at a Marine combat outpost aptly illustrated this relationship, stating that the "best counter to IEDs = #1 the Afghan people, #2 ANSF partners and then metal detectors, dogs, GBOSS [ground-based operational surveillance system], airplanes, etc. 80% of our IED finds have been the direct result of tips from local nationals because of the respect that you show to the people—and because they've watched you ruthlessly close with and destroy the enemy."[13]

The Environment

IEDs have been encountered in every domain, but have seen use primarily in land-based attacks. Most IEDs used at sea or in the air have been little different from those used on land. The time bomb that brought down Pan Am Flight 103 over Lockerbie, Scotland, in December 1988 was an IED concealed in a suitcase, while the time bomb that sank *SuperFerry 14* in Manila Bay in the Philippines in February 2004 was concealed in a television set.

The nature of the target or the environment, however, may significantly affect design and tactical employment. In World War I, for example, French forces at Salonika brought down a German aircraft by loading the basket of an observation balloon with several hundred pounds of explosives and command-detonating it via a telegraph cable as the pilot tried to strafe the balloon. The aircraft was destroyed and the pilot, who had previously shot down several other observation balloons, was killed.[14] During the Second World War, the British Special Operations Executive developed an altimeter switch for destroying an aircraft in flight.[15] The aircraft at greatest risk, however, are helicopters, especially medevac helicopters called upon to extract personnel wounded in an IED ambush. Special care must be taken to ensure their landing zones are clear of secondary IEDs. During the Vietnam War, Viet Cong guerrillas developed many ingenious anti-helicopter devices that were designed to be triggered by the aircraft's rotor wash.[16] The growing commercial unmaned aerial vehical market may provide new opportunities for adversaries to use IEDs in the air.

The maritime environment has seen some high-profile IED attacks, most notably the October 2000 suicide boat bombing of the USS *Cole* in Aden, Yemen, and the similar October 2002 attack on the French tanker MV *Limburg*. Overall, however, IED attacks in the maritime domain have been much less common than on land. Operating at sea requires skills in navigation, coastal piloting, ship handling, and combat swimming that are not easily acquired. It is also harder to blend into the population at sea, and weapons testing and rehearsals are more difficult. Media coverage of an attack—vital to modern terrorists—is less reliable and less spectacular far from shore.[17] However, a few groups, notably the Tamil Tigers, have been very effective in the maritime domain. Viet Cong sappers also conducted

Mine clearing line explosive charge launches from Company A, 4th Brigade Special Troops Battalion, 4th Brigade Combat Team, 101st Airborne Division vehicle on Route Dodge, Paktika Province, Afghanistan (U.S. Army/Zachary Burke)

some limpet mine and IED attacks against U.S. ships during the Vietnam War, including the sinking of the USNS *Card*, a utility aircraft carrier.[18] Sea ports are important logistics hubs for the movement of personnel, equipment, and supplies into theater and thus make desirable targets. The geography of rivers, deltas, canals, inland waterways, archipelagic waters, and narrow and inland seas make them suitable for interdiction with IEDs, including improvised sea mines, to give irregular adversaries a limited sea-denial capability.

Weapons Technical Intelligence

One of the most important innovations for countering IEDs has been the development of weapons technical intelligence. In August 2003, coalition forces in Iraq identified an operational need for an IED exploitation capability "to provide immediate in-theater analysis, technical intelligence and advice to EOD personnel and provide advice on changes to force protection measures."[19] The technical exploitation of IEDs—WTI—eventually became its own subset of technical intelligence (TECHINT) and comprises 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 weapons systems.[20] Traditional TECHINT and WTI differ in several important ways related to their purpose, execution, and outcomes.

While TECHINT applies to the full range of foreign war materiel, including aircraft, armor, sensors, communications, and munitions, WTI applies only to improvised weapons, particularly IEDs, and their components. For this reason, TECHINT has broader application, especially in conventional warfare where technical analysis can yield the scientific and technical intelligence needed to ensure the survivability of U.S. systems and to design countermeasures to enemy capabilities. WTI finds its greatest utility in irregular warfare in which a typically lightly armed, irregularly equipped enemy improvises his own weapons and explosives. These improvised weapons bear the unique signatures—technical, forensic, behavioral—of their builders, which makes exploiting them useful for attributing attacks to specific individuals, groups, and networks.

Attribution is an import distinction between TECHINT and WTI. While TECHINT may be used to target a nation's capacity to produce particular weapons and systems, WTI is used to target individual bomb makers and the terror network to which they belong. IED design is exceptionally variable and minor differences in construction can tell investigators much about the bomber, his training, and his sources of supply. Biometrics are rarely relevant to TECHINT but are essential to WTI, which fuses technical and forensic information to produce biometrically enabled

intelligence. While both TECHINT and WTI support countermeasure development and force protection, WTI's five outcomes—force protection, component material sourcing, targeting, support to prosecution, and signature characterization—are more relevant to defeating adversary networks and supporting host-nation rule of law.[21]

A single conventional munition may yield ample technical intelligence about the munition in question. Representative samples are sufficient because mass-produced munitions are identical and attribution is not a factor. With IEDs, however, every device must be exploited for the unique signatures of individual bomb makers that can be correlated through pattern analysis and mapped geospatially. Two people given identical components and instructions will produce IEDs that are surprisingly different in appearance, with unique biometric markers such as latent fingerprints and DNA and different behavioral markers such as the placement of components or skill in soldering. As an example, consider how easy it is to pick out your child's artwork from all the other nearly identical masterpieces displayed in his or her classroom at back-to-school night. The implication is that the volume of collected material that must be processed for WTI is unlimited (theoretically 100 percent), which makes WTI much more labor intensive, at least for field collection, triage, and chain of custody management.

TECHINT is conducted in both peacetime and wartime and is generally a more deliberate, methodical discipline. It strives for a complete understanding of a weapons system that can serve as the foundation of development and acquisition programs for new weapons, countermeasures, and equipment. IED use, by contrast, is almost always an act of violence related to criminality, terrorism, or war, which drives a heightened sense of urgency to exploit devices quickly and derive actionable information from them. WTI is often more urgent because obtaining combat information is a higher priority than waiting for fully developed intelligence.[22] Not only does WTI seek to characterize the IED technically (how it was constructed) but tactically (how it was employed and for what purpose). Much of the most useful WTI analysis occurs in theater at expeditionary labs.

Like TECHINT, WTI benefits from an interagency effort and its reports are used across government. In 2013, for example, the Federal Bureau of Investigation (FBI) arrested two Iraqi refugees in a sting operation in Kentucky after their fingerprints were found to match latent prints collected from an unexploded IED in Iraq.[23] Federal law enforcement personnel provided key forensic capabilities and added rigor to the evidence management processes of the counter-IED task forces in Iraq and Afghanistan. The FBI's Terrorist Explosive Device Analytical Center continues to fully analyze and exploit IEDs recovered overseas.

The Enduring Threat

As a result of the proliferation of IED knowledge available on the Internet, in extremist publications, and at terrorist training camps as well as the exploitation of readily available off-the-shelf technologies, VEOs are able to develop and employ IEDs with a relatively small investment. The example of tactical—and perhaps operational and strategic—success associated with IED attacks in Iraq and Afghanistan may inspire other violent actors to employ IEDs to counter U.S. military strength and achieve their objectives. Various VEOs, including al Qaeda, have stated their intent to obtain and use chemical, biological, radiological, and nuclear weapons. New threat actors operating in different environments will use IEDs in novel and unpredictable ways. Not everything that is possible is probable, but the limitless variability of the IED will continue to be confounding for planners and strategists.

Knowledge of IED construction is more readily available than ever, yet the requisite skills remain difficult to acquire. Working with sensitive homemade explosives and complex electronics is risky, and even experienced bomb makers are killed by their own devices through error or miscalculation. The limited availability of IED expertise has several implications for friendly forces.

Operational experience in IED-rich environments such as Northern Ireland, Iraq, and Afghanistan has shown that there are often hierarchies of bomb makers, including experienced "master bomb makers" who pass on their techniques to others in the organization. For example, Yehya Ayash, nicknamed "the Engineer," served as the chief bomb maker for Hamas and is credited with greatly improving the technical sophistication of its IEDs in the early 1990s.[24] Master bomb makers may have learned their skills in terrorist training camps or through legitimate occupations such as quarrying, chemistry, or electronics and then honed them over the course of many years. A bomb maker's special skills are not easily replaced, so removing the bomb maker from the environment usually has a direct measurable effect on the rate of IED incidents. Experienced bomb makers are a critical adversary capability that can be targeted, and the relationship between master and apprentice is a node that can be exploited.

Successful countermeasures and countervailing tactics force the bomb makers to alter their designs and techniques, thereby increasing the chance for error. Fielding unproven and perhaps less reliable IED designs carries increased risk of failure and may require new tactics for employment. Effective IED countermeasures often have the desirable secondary effect of stressing the bomb-making network and forcing lethal errors on the bomb maker.

IEDs have been the signature weapon in the wars of attrition our enemies have waged against us in Iraq, Afghanistan, and other regions, and have featured in every major conflict in the modern era. They have resulted in a high cost in casualties and materiel, and have impaired our ability to achieve our objectives. Recognizing that the IED has been and will continue to be a threat to U.S. forces and mission accomplishment—throughout the range of military operations and across all the phases of operation, in both traditional and irregular conflict—the joint force needs to capture

authoritatively and comprehensively the fundamental principles and best practices of operating in IED-rich environments before they are forgotten.

As our force levels in Afghanistan fall and our operational tempo decreases, now is a good time to consider what we have learned about IEDs and invest the intellectual energy into ensuring our doctrine is relevant to future conflicts. While the IED is not the only threat we face, its effectiveness suggests it is not going away any time soon. JFQ

Joint Publications (JPs) Under Revision (to be signed within 6 months)

JP 1-04, *Amphibious Embarkation and Debarkation*

JP 1-06, *Financial Management Support in Joint Operations*

JP 2-01.2, *Counterintelligence/Human Intelligence*

JP 3-13.3, *Operations Security*

JP 3-14, *Space Operations*

JP 3-34, *Engineer Operations*

JP 3-68, *Noncombatant Evacuation Operations*

JP 4-01.2, *Sealift Support to Joint Operations*

JP 4-01.5, *Joint Terminal Operations*

JP 4-01.6, *Joint Logistics Over-the-Shore*

JP 4-03, *Joint Bulk Petroleum and Water*

JPs Revised (signed within last 6 months)

JP 1-0, *Joint Personnel Support*

JP 3-05.1, *Unconventional Warfare*

JP 3-50, *Personnel Recovery*

JP 3-61, *Public Affairs*

JP 6-0, *Joint Communications System*

Notes

[1] JCCS-1 (Joint CREW Composite Squadron-1) was a Navy-run electronic warfare unit in Iraq that managed CREW systems and developed CREW-related tactics, techniques, and procedures. Task Force ODIN (observe, detect, identify, and neutralize) was an Army aviation battalion in Iraq that flew the MQ-1B Warrior-Alpha unmanned aerial vehicle to provide reconnaissance, surveillance, and target acquisition (RSTA) against insurgents using improvised explosive devices (IEDs). The range of materiel solutions that the Joint Improvised Explosive Device Defeat Organization (JIEDDO) fielded is extraordinary—aerostats, explosives detectors, electronic countermeasures, patrol dogs, ground-penetrating radar, robots, personnel protective equipment, optics, mine rollers—and reflects the variability and unpredictability of the IED threat.

[2] Ian Jones, *Malice Aforethought: A History of Booby Traps from World War One to Vietnam* (London: Greenhill Books, 2004), 33.

[3] Ibid., 226.

[4] General Staff (Intelligence) General Headquarters (GHQ), *German Ruses* (1st Printing Co., R.E., GHQ, April 8, 1917), available at <http://museumvictoria.com.au/collections/items/1955526/document-german-ruses-13th-australian-field-ambulance-world-war-i-1914-1918>.

[5] Joint Publication (JP) 1-02, *Department of Defense Dictionary of Military and Associated Terms* (Washington, DC: The Joint Staff, November 8, 2010, as amended through March 15, 2015), s.v. "improvised explosive device."

[6] Walter Laqueur, *The New Terrorism: Fanaticism and the Arms of Mass Destruction* (New York: Oxford University Press, 2000), 192.

[7] Stanley A. McChrystal, *My Share of the Task: A Memoir* (New York: Penguin Group, 2013), 252.

[8] Jones, 45.

[9] Ibid., 227.

[10] MCIP 3-17.02, *MAGTF* [Marine Air-Ground Task Force] *Counter-Improvised Explosive Device Operations* (Washington, DC: Department of the Navy, Headquarters U.S. Marine Corps, November 14, 2012), 4–5.

[11] Fleet Marine Force Reference Publication (FMFRP) 12-43, *Professional Knowledge Gained from Operational Experience in Vietnam, 1969, Special Issue, Mines and Boobytraps*, (Washington, DC: Headquarters U.S. Marine Corps, July 20, 1989), 3.

[12] Jones, 229.

[13] MCIP 3-17.02, figure 1-1.

[14] Jones, 47.

[15] Ibid., 167.

[16] FMFRP 12-43, 66.

[17] James Pelkofski, "Before the Storm: al Qaeda's Coming Maritime Campaign," U.S. Naval Institute *Proceedings* 131, no. 12 (December 2005), 20–24.

[18] Paul Huard, "Viet Cong Commandos Sank an American Aircraft Carrier," *Medium.com*, available at <https://medium.com/war-is-boring/viet-cong-commandos-sank-an-american-aircraft-carrier-7f243ede06b3>.

[19] Brigadier General Barbara Fast, C2, CJTF7, for Defense Intelligence Agency, through Commander JCMEC, memorandum, *Iraqi Theater of Operations (ITO) Combined Explosives Exploitation Cell*, October 23, 2003.

[20] JP 1-02, s.v. "weapons technical intelligence."

[21] Defense Intelligence Agency (DIA) and Joint Improvised Explosive Device Defeat Organization (JIEDDO), *Weapons Technical Intelligence Handbook*, Version 2.0 (Washington, DC: DIA and JIEDDO, March 2014), 4.

[22] *Combat information* is "unevaluated data, gathered by or provided directly to the tactical commander which, due to its highly perishable nature or the criticality of the situation, cannot be processed into tactical intelligence in time to satisfy the user's tactical intelligence requirements." JP 1-02, s.v. "combat information."

[23] U.S. Department of Justice, "Former Iraqi Terrorists Living in Kentucky Sentenced for Terrorist Activities," available at <www.fbi.gov/louisville/press-releases/2013/former-iraqi-terrorists-living-in-kentucky-sentenced-for-terrorist-activities>. In another recent incident, a London taxi driver's fingerprints linked him to an IED that killed a U.S. Soldier in Iraq. Laura Perez Maestro and Don Melvin, "British Man Found Guilty in U.S. Soldier's Death in Iraq," *CNN.com*, available at <www.cnn.com/2015/05/21/world/briton-guilty-u-s-soldier-death/index.html>.

[24] Laqueur, 139.