

## Improvised Explosive Devices: Ready for the Future?

by

Colonel Stephen F. Elder  
United States Army

Under the Direction of:  
Professor Albert F. Lord



United States Army War College  
Class of 2017

### DISTRIBUTION STATEMENT: A

Approved for Public Release  
Distribution is Unlimited

The views expressed herein are those of the author(s) and do not necessarily reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

REPORT DOCUMENTATION PAGE			Form Approved--OMB No. 0704-0188		
The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.					
1. REPORT DATE (DD-MM-YYYY) 01-04-2017		2. REPORT TYPE STRATEGY RESEARCH PROJECT		3. DATES COVERED (From - To)	
4. TITLE AND SUBTITLE Improvised Explosive Devices: Ready for the Future?			5a. CONTRACT NUMBER		
			5b. GRANT NUMBER		
			5c. PROGRAM ELEMENT NUMBER		
6. AUTHOR(S) Colonel Stephen F. Elder United States Army			5d. PROJECT NUMBER		
			5e. TASK NUMBER		
			5f. WORK UNIT NUMBER		
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Professor Albert F. Lord			8. PERFORMING ORGANIZATION REPORT NUMBER		
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) U.S. Army War College, 122 Forbes Avenue, Carlisle, PA 17013			10. SPONSOR/MONITOR'S ACRONYM(S)		
			11. SPONSOR/MONITOR'S REPORT NUMBER(S)		
12. DISTRIBUTION / AVAILABILITY STATEMENT    Distribution A: Approved for Public Release. Distribution is Unlimited. To the best of my knowledge this SRP accurately depicts USG and/or DoD policy & contains no classified information or aggregation of information that poses an operations security risk. <b>Author:</b> <input checked="" type="checkbox"/> <b>PA:</b> <input checked="" type="checkbox"/>					
13. SUPPLEMENTARY NOTES Word Count: 8403					
14. ABSTRACT The United States has invested a great deal of money and effort to defeat Improvised Explosive Devices (IEDs) and attack IED networks over the last decade. This paper aims to identify the strategic impacts and subsequent reactions realized as a result of the IED threat in order to capitalize on lessons learned. It will specifically review organizational structure, policy/doctrine and technology development related to the strategic implications. It will also explore potential emerging threats to be considered as the U.S. and coalition forces prepare a continued defense against the IED threat. Finally, the paper will suggest necessary related improvements to maintain Counter IED (CIED) capability.					
15. SUBJECT TERMS EOD, Exploitation, IED, JIEDDO, CIED, Threat, WTI					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES 38	19a. NAME OF RESPONSIBLE PERSON
a. REPORT UU	b. ABSTRACT UU	c. THIS PAGE UU			19b. TELEPHONE NUMBER (w/ area code)

## Improvised Explosive Devices: Ready for the Future?

(8403 words)

### Abstract

The United States has invested a great deal of money and effort to defeat Improvised Explosive Devices (IEDs) and attack IED networks over the last decade. This paper aims to identify the strategic impacts and subsequent reactions realized as a result of the IED threat in order to capitalize on lessons learned. It will specifically review organizational structure, policy/doctrine and technology development related to the strategic implications. It will also explore potential emerging threats to be considered as the U.S. and coalition forces prepare a continued defense against the IED threat. Finally, the paper will suggest necessary related improvements to maintain Counter IED (CIED) capability.

## **Improvised Explosive Devices: Ready for the Future?**

Our capabilities to counter IEDs have evolved and grown. We must not become complacent, but must continue to challenge ourselves and each other to be more effective against these threats.

—Barack Obama<sup>1</sup>

Prior to United States involvement in Afghanistan and Iraq, the term “Improvised Explosive Device” or IED was known only to those professional Explosive Ordnance Disposal (EOD) operators tasked with neutralizing explosive hazards – today it is a common term. An adversary’s effective use of the IED has become more than just familiar in name, as it has cost the United States dearly in both national blood and treasure; it has influenced policy, shaped and spawned formations/organizations, and forced rapid procurement and fielding of Counter IED (CIED) technology. Future solutions to a problem as complex as the IED must address strategic implications related to the IED weapon system over the last decade, analyze the potential future IED threat environment, and consider recommendations in an effort to ensure the hard earned lessons endure and remain relevant well into the future.

Having experienced over a decade of the IED threat evolution in both Afghanistan and Iraq and witnessing the United States and coalition responses from the tactical to strategic level, the U.S. is currently at a decision point with respect to developing a strategy to retain battlefield lessons learned. The impact of the IED threat to U.S. Joint Forces drove substantial investments, such as technology development, force structure, and policy/doctrine updates.

### **Background**

Understand the threat in low intensity conflict will use mine/booby trap operations much like those 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.<sup>2</sup>

Improvised Explosive Devices have been around for centuries but most recently came back into the spotlight during the Afghanistan and Iraq wars due to their extreme effectiveness. The Joint Improvised Threat Defeat Agency (JIDA) estimates half to two-thirds of U.S. service men and women killed or wounded in Iraq and Afghanistan were a result of IEDs. There were over 3,100 killed and 33,000 wounded U.S. military personnel because of IEDs.<sup>3</sup> In fact, the IED threat grew to such an extent that in 2003, then U.S. Army Deputy Chief of Staff for Operations LTG Richard A. Cody stated, "The IED problem is getting out of control ... We have to stop the bleeding."<sup>4</sup> While the casualty numbers alone related to both Afghanistan and Iraq are cause for alarm and action, IEDs are obviously not limited to the operational environments of those two conflicts and remain an enduring and persistent threat. Over the period between 2011 and 2015, the Non-Governmental Agency, Action on Armed Violence reported 105,071 (86,395 civilians and 18,676 armed actors) were recorded killed or wounded by IEDs.<sup>5</sup> This data is important as it both sets the background and highlights the span and impact of the global IED threat - beyond OPERATION IRAQI FREEDOM (OIF) and OPERATION ENDURING FREEDOM (OEF).

Casualty data related to IEDs is telling and fits well into the equation and background when researching the question of why was there such a profound proliferation of the IED? Besides their effectiveness, history and experience points to three main explanations that can be attributed to the propagation of IEDs. Although some have posited various 'complex' ideas in regard to the strategic and operational advantages that insurgents gain from IEDs, within the scope of this background, the

following are considered and will later be tied to impacts and strategic reactions: (1) low cost / easy access to material for construction and employment, (2) standoff preventing 'direct engagement', and (3) anonymity.<sup>6</sup>

Early in both the Iraq and Afghanistan conflicts, various insurgent/terrorist or criminal groups had very easy access to mines, artillery shells and other high explosive ordnance (main charges) that littered the battlefield. Instead of employing said ordnance as conventionally designed, they quickly learned to 'improvise' simply by inserting an initiator (blasting cap) into the main charge, then conceal the device and wait for an opportune circumstance to use it against vehicular or foot traffic. As the supply of conventional ordnance in unsecured Iraqi Army weapons storage facilities was depleted, the insurgents adapted their approach and began to substitute with homemade and commercial explosives placed in specially fabricated containers. An example was the explosively formed projectile (EFP) that had devastating effects and first appeared in Southern Iraq in late 2004. Commercial explosives such as blasting caps, detonation cord, and liquid/bulk explosives typically used for construction, road building and quarrying are common and often obtained via the black market or theft represent another source for the fabrication of IEDs.<sup>7</sup> More recently and away from the war zones, one can also gain a perspective regarding the ease with which knowledge transfer occurs and low cost materials facilitate IED construction as evidenced in Boston by the Tsarnaev brothers learning to make pressure cookers and pipe bombs from *Inspire* magazine, an open source al-Qaida publication.<sup>8</sup> While the aforementioned highlights low cost and easy access being a key factor associated with the enemy

attraction to the IED, another element to consider is that of standoff from their intended target and expected security force responses.

Throughout the early days of coalition force operations (2003 timeframe), enemy forces initiated their attempts to attack coalition forces, gain power and apply their will using the weapons they had knowledge of and access to – primarily machine guns, rocket propelled grenades and small mortars.<sup>9</sup> Enemy forces quickly learned that in order to achieve effects with these weapons, they would have to be relatively close engaging coalition forces in a more conventional manner which typically did not work in their favor. To counter overwhelming coalition force numbers, technology and weapons systems, the insurgents turned to the IED. The insurgents required only basic explosive functioning knowledge and could place IEDs to achieve effects while minimalizing their risk of detection. These early, basic IEDs afforded the enemy sufficient standoff to avoid direct fire retaliation. Standoff also allowed the insurgents to protect their most valuable resource and the last background reference point – anonymity.

Coalition forces were suffering casualties from IEDs with little opportunity to kill or capture the enemy. The emplacer simply could disappear into an urban maze or hide in plain sight in the inevitable crowd of onlookers after an attack, maintaining anonymity.<sup>10</sup> The lack of intelligence related to individuals or networks enjoying their anonymity caused a complex problem for a force accustomed to fighting a 'conventional' adversary who would seek contact with and engage in sustained combat with friendly forces. As a result, friendly forces had to begin the process of developing the capabilities needed to; identify networks, characterize their activity, locate their members, fix their location, and develop targeting strategies to eliminate them. The enemy proved to be fluid and

adaptive, evidencing the characteristics of a complex adaptive system, which was very adept in responding to and countering friendly efforts to eliminate them.<sup>11</sup>

Given the proven effectiveness of the IED in nearly any environment, the ease and low cost of its manufacture, ability for the enemy to effectively employ it in a standoff configuration against their targets while retaining their anonymity, it is easy to understand why the IED has been and will likely remain a weapon of choice and great effectiveness well into the future. Because of these enduring positive attributes for the IED, it is important to address the strategic impacts and associated U.S. reactions in order to continue to capitalize on the hard lessons learned as the United States moves into an uncertain future and a resource-constrained environment. Mr. Russell McIntyre, formerly of the Defense Intelligence Agency, accurately compared its employment with criminal activity in a city, "We will never completely eliminate the IED threat...the best we can responsibly do is provide a balanced solution to mitigate the impacts suppressing the networks that employ them. However, like criminal activity it cannot be completely eliminated."<sup>12</sup> To fully appreciate the significant national efforts and investment placed against the IED problem set (strategic impact/reaction), one should evaluate the over a decade of evolution and in some cases creation of organizations, policy/doctrine, and material development.

### Strategic Impacts

U.S. Forces in Vietnam experienced the anti-personnel effectiveness and sheer lethality of improvised explosive weapons early in the war. By 1967, the number of, then called booby traps and now called IEDs were producing significant battlefield casualties in South Vietnam, "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."<sup>13</sup> As highlighted above, the pre 9/11 history of IEDs was significant (just forgotten) in U.S. military history, the post 9/11 period proved revolutionary for IED defeat doctrine, organization, training, technology, material development, and related spending. During that period the Department of Defense (DOD) spent over \$75 billion to counter IEDs on the battlefield.<sup>14</sup> Included in this figure is an estimated \$40 billion related to efforts in protecting the force with fielding Mine Resistant Ambush Protected (MRAP) vehicles.<sup>15</sup> As evidenced by the dollar amount the U.S. invested in counter IED (CIED) efforts over the last decade, it is easy to comprehend the impact of IEDs' influence from the tactical to strategic level. Trying to reconstruct what the nearly \$75 billion investment has actually procured is difficult, but a brief look at the strategic areas including organization, policy/doctrine/best practices technology, and material development is worth consideration. The IED threat caught the U.S. Armed Forces by surprise. While in 2002 the U.S. had EOD units trained and equipped to handle crude IED threats, greater emphasis was placed on reducing other explosive hazards such as conventional ordnance. The U.S. military lacked an organization capable of responding to such an IED threat beyond the immediate tactical level.

### Organization

Subsequent to General Cody's call for action to "...stop the bleeding..." and commander's call for support, the Army responded first by establishing an IED Task Force that later formed the base for the Joint IED Defeat Organization (JIEDDO). JIEDDO was established by the Department of Defense in 2006.<sup>16</sup> JIEDDO quickly

became the main effort in synchronizing IED defeat efforts within the DOD and grew from a 10-person Army task force formed in October 2003 to 3000 personnel in 2006 with an annual budget of \$3.7 billion.<sup>17</sup> In 2015, JIEDDO was re-designated as the Joint Improvised-Threat Defeat Agency (JIDA) and reduced to 1000 personnel with a \$500 million dollar budget.<sup>18</sup> In the 2016 National Defense Authorization Act, Congress directed JIDA, "...merge its primary funds to a successor's pot of money, eliminate its standalone IED intelligence center and subsume its research, development and acquisition activities in a larger military or defense agency..." forcing reorganization under the Defense Threat Reduction Agency (DTRA).<sup>19</sup>

Today, JIDA has changed from a combat support agency to an office within the DTRA, known now as the Joint Improvised-Threat Defeat Organization (JIDO).<sup>20</sup> JIDO Director, LTG Michael Shields stated in a September 2016 news release, "The threat to our deployed warfighters from improvised threats continues to grow and as such, Congress and the Department of Defense have determined that our organization (JIDO) must be enduring...we will continue to execute our quick reaction capability mission as part of DTRA and as such, we will continue to help the warfighter adapt to the current and emerging threats on the battlefield by rapidly delivering capability at the speed of war. The only change the warfighter will experience is the change of our name."<sup>21</sup> Regarding organizations and strategic reaction to the IED threat, in addition to DOD's initial creation of JIEDDO, the services responded as well.

The services responded with organizational innovations that included but were not limited to: The Combined Explosive Exploitation Cell (CEXC) in Camp Victory, Baghdad, Theater Explosive Exploitation (TEX) in Bagram, Afghanistan, fielded

Weapons Intelligence Teams, established CIED Task Forces' TROY in Iraq, PALADIN in Afghanistan and most recently TF ATLAS in support of OPERATION INHERENT RESOLVE, Kuwait/Iraq.<sup>22</sup> In addition to the DOD efforts to establish organizations in order to address the IED threat, there are currently 21 non-DOD federal programs supporting IED defeat national policy within the interagency.<sup>23</sup> Furthermore, under a 2006 force design update, the Army nearly doubled the active duty EOD capability in both sheer numbers and organization. Because of the reduction in deployed forces, nearly all of the aforementioned have been either stood down or are at risk as the U.S. moved away from sustained combat operations in Afghanistan and Iraq.

These very organizations or formations were created and/or expanded to help mitigate the previously highlighted reasons that the IED is favored as the enemies' weapons of choice. Despite the persistent threat posed as an immediate threat to our allies in Iraq and Afghanistan and a future one for our forces, these organizations have been either eliminated or are in danger of being eliminated. The EOD force structure reductions mentioned earlier are especially unfortunate for two reasons. First, a significant number of combat experienced EOD operators have left the force and secondly, organizations like the CIED task forces were very dependent on using existing EOD units to provide the skilled manpower needed to operate effectively. Naturally, the task forces stood up have an expected shelf life proportional to the reason for their creation – so they are not enduring by design. However, the EOD units created to handle the IED threat for the next conflict were cut by a third due to the Budget Control Act of 2011. Already mentioned was the JIEDDO to JIDA to JIDO transition moving it from an annual \$3.7 billion budget in 2006 to an office within the DTRA

(transferring remaining funds/capability with it). Both Congress and the Department of see the IED threat to Joint Forces going away. An alternate conclusion might include consolidating efforts were designed to save money and improve organizational efficiencies. Regardless, the reduction decisions were made without a comprehensive threat assessment coupled with a mission area analysis that would provide the underlying logic to guide this reduction in capabilities and funding, but the threat is not going away. Trends are that the U.S. should learn from the past and not cast aside capability in an effort to save money and resources; it will simply end up costing more in the end.

#### Policy/Doctrine

Just as the U.S. was caught flat-footed regarding organizational structure to effectively respond to the IED threat, it was equally constrained by lack of policy and doctrine pre 9/11 to guide training, force structure for EOD operational capability, material development or joint operational responses in the theater of operations. However, post 9/11, doctrine and policy evolved from a basic EOD Field Manual to a Presidential Policy Directive (PPD-17) in 2013 to a Joint EOD Publication in 2016 - all because of the Improvised Explosive Device threat. While PPD-17 (Countering Improvised Explosive Devices), directs the “building and maintaining of capabilities and technologies to continue to counter the IED threat in the homeland,” documents such as Joint Publication’s 3-42, 3-15.1, *Joint EOD Operations and CIED Operations*, respectively and the Weapons Technical Intelligence (WTI) CIED Lexicon continue to be invaluable complimentary assets.

A clear example of doctrine developed by JIEDDO in collaboration with the Defense Intelligence Agency (DIA), the services, the interagency, and our coalition

partners include the WTI Lexicon published in 2007 with subsequent revised editions.<sup>24</sup> Prior to its publication, there existed no common language to populate reporting and intelligence on IED incidents and collection. Without this common language promulgated by the lexicon and populated into proper intelligence channels and databases, enemy anonymity would have certainly continued to frustrate targeting efforts. Similar direction and emphasis regarding the CIED threat can be seen in the recent publication of both Joint EOD and CIED doctrine, a credit to a lot of hard work within DOD.

Joint Publication 3-15.1 (JP 3-15.1) *CIED Joint Operations* provides joint doctrine for planning and executing CIED operations and outlines responsibilities, provides command and control considerations, discusses organizational options, details the CIED process and attack the network methodology, and introduces models for coordinating with CIED supporting organizations.<sup>25</sup> Captured within JP 3-15.1, are critical lines of effort (LOE) that were realized and developed by both TF TROY / PALADIN, the following LOEs form the basis for the conduct of all CIED planning and operations: “attack the network” (AtN) “defeat the device,” (DtD) and “train the force” (TtF).<sup>26</sup> The purpose of highlighting related joint publications is to demonstrate how the IED as a weapon system provided the catalyst taking us from zero CIED doctrine to that mentioned above, which provides detailed guidance to the joint force with reference to CIED operations.

Additionally, CIED and associated violent extremist/terrorist related strategic direction can be seen in a number of national-level documents: including the National Security Strategy, the Defense Strategic Guidance, the National Military Strategy, the

Unified Command Plan, and the White House Policy Statement on Countering Improvised Explosive Devices to name a few. While most of the aforementioned doctrine and policy represent DOD actions, as referenced in several other Homeland Security documents, the threat is not limited to or a sole responsibility of DOD and the military. Protecting the homeland, defending interests abroad, and sustaining strategic flexibility require a proactive approach that counters threat networks and anticipates evolving IED designs, tactics, and technology. In February 2007, the Homeland Security Presidential Directive 19 (HSPD-19), *Combating Terrorist Use of Explosives in the United States*, was signed.<sup>27</sup> This document and subsequent implementing instructions direct a whole-of-government approach that envisions seamless federal, state, and local government efforts to “deter, prevent, detect, protect against, and respond to explosive attacks.”<sup>28</sup>

Clearly, as shown with examples of doctrine and policy (as noted above as the HSPD-19 and the PPD-17), the IED threat generated a strategic response, which resulted in much needed policy and direction. While the U.S., coalition forces and global CIED community capitalized on the direction policy and doctrine such as the WTI Lexicon, JP 3-15.1, and Homeland Security Directives provided over the last decade, they also profited from an explosion in several areas of CIED technology development.

#### Countermeasures and Technology

Since the enemy quickly learned that for under \$200, he could defeat coalition armor and kill or wound entire crews with the IED, it is understandable why it became a weapon of choice and why friendly forces responded – usually as a reactive vs. proactive stance. As an example, insurgents began burying large IEDs in roads, the reaction included development of ground penetrating radar for detection of buried IEDs.

The coalition's response to the IED threat largely evolved over time and was usually not the result of a deliberate strategy. Capability was often provided in response to Joint Urgent Operational Needs Statements (JUONs) emanating from combat operations.<sup>29</sup> Battlefield IED employment caused strategic impacts for force protection, CIED defeat equipment, data and exploitation countermeasures and technology. Perhaps the most important aspect involved with IED countermeasures and defeat technology rests in the intelligence and exploitation realm. Proper characterization of the threat is necessary in order to responsibly counter it.

Exploitation of IEDs and associated components in Afghanistan in 2004 consisted of Army EOD taking pictures of the devices, sometimes putting pictures and a few details in a local database and bagging the components for storage in a locker with no follow-on purpose. As IEDs became proliferated throughout Afghanistan, the threat changed and coalition forces quickly realized the requirement for exploitation. A JUONS from theater highlighted a capability gap in exploitation and subsequently derived intelligence needed to counter the IED device and defeat the associated networks, and the U.S. reacted.

There already existed a blend of disparate IED collection and exploitation capability in both Iraq and Afghanistan, which included contributions from the services and different branches that included EOD, Military Police fielded forensic laboratories and Weapons Intelligence Teams. None of the aforementioned capability had functioned previously together as a coherent, synchronized system and therefore lacked common reporting language, information content for their reports or format complemented by an associated WTI database to store and share the collected

information.<sup>30</sup> The Combined Information Data Network Exchange (CIDNE) quickly became the theater reporting backbone which leveraged reporting (including IED reports) to support research and analysis, significant activity trends, casualty reports and so on. CIDNE became the first real organizing theater level database that enabled interoperability, information sharing and data discovery within the exploitation community. While a common database is essential, equally important is the information (exploitation) being fed into the 'system.'

A number of various exploitation capabilities and forensic laboratories deployed forward in support of the overall CIED effort. With few exceptions related to higher level targeting and intelligence, the labs served under either TF TROY or PALADIN in a range of functions in order to: provide and inform a range of outcomes to support the commander from support to targeting, inform force protection material and TTP development, and to provide evidence for legal proceedings.<sup>31</sup> Forensic technology is the one thing that most labs had in common which provided invaluable information, taking away that factor of 'anonymity' by linking a forensically derived identity (by recovering fingerprints or DNA) to a device or location as previously discussed. Many might take something as simple as fingerprinting and biometrics for granted; however, it is important to note that capability like this and many others took time to mature in theater to become useful.

With the bulk of U.S. and coalition forces withdrawn from active theaters of operation, forensic lab capability and associated intelligence are no longer seen as 'required' and have subsequently been disbanded or put in storage configuration, with the exception of a forward deployed capability in Kuwait supporting OIR. While CIDNE

was identified as the single reporting tool and data repository within the Central Command area of operation, it was not and is not DOD owned and never became a program of record. The gravity of this issue was realized by the author in March 2016 while trying to retrieve data in support of OIR CIED operations. CIDNE servers containing the tens of millions of entries related to OIF, were withdrawn along with U.S. troops from Iraq. In order to get the servers and database back in operation and to capitalize on previous inputs, contracts were required, which proved to be a very cumbersome process given current budget constraints. Impacts were felt throughout the theater as coalition forces were constrained when attempting to advise and assist the Iraqi Army related to CIED exploitation and defeat operations. As an example, the millions of reports that documented enemy TTPS, tactical employment and characterization of IEDs stored was largely unavailable early in support of OIR.

Exploitation through hard work and technology informed force protection measures to keep personnel as safe as possible. Outputs for mitigation were often derived directly from exploitation, such as, enabling the building of surrogate devices replicating enemy systems to support field trials of proposed up armoring efforts. According to a *USA Today* article printed in 2013, "The IED has given rise to a multibillion-dollar industry in vehicle and body armor, robots, ground-penetrating radar, surveillance, electrical jamming, counterintelligence...the Government Accountability Office says it's impossible to estimate the total U.S. cost...but the Pentagon has spent at least \$75 billion on armored vehicles and tools for defeating the weapons."<sup>32</sup> There is no doubt these measures and the herculean efforts regarding force protection and IED detection mitigated the devastating impacts on both equipment and personnel. While

force protection measures improved along with the threat, so did the technology for the EOD technician whose job it is to 'defeat the device.'

The ability to disarm IEDs, recover them intact, instead of just blowing them up remotely is a very important aspect that directly feeds into the WTI cycle to inform targeting, prosecution, research, force protection, etc. Again, an initial capability gap existed as in 2004, EOD technicians were primarily provided conventional ordnance tools that were bulky and offered little to offset the risks associated with disarming devices. Multiple JUON's later, both theaters' EOD techs now had capability like advanced lightweight X-Ray systems and detection tools, more capable robots, effective electronic countermeasures, and standoff tools and charges. The results were felt from the tactical to strategic levels as real exploitation and subsequent intelligence started coming in from the operators and at a greatly reduced risk to them.

Whether organizational structure, doctrine and policy, or CIED countermeasures and technology; each has clearly had strategic implications. There are countless more examples (such as training) that could serve to showcase over ten years of strategic legacy associated with countering the IED as a weapon system; however, highlighting the aforementioned serves to make the point. Former JIEDDO Director, LTG (USA) Barbero stated, "As we continue to address the improvised explosive device threats of today, we must simultaneously prepare for tomorrow's counter-IED and counter-threat network effort by institutionalizing the knowledge, capabilities, and experience we have amassed during the last decade."<sup>33</sup> While this section of the paper has emphasized a few of the very capabilities and knowledge LTG Barbero spoke of, analyzing the

anticipated future threat of IEDs will help to shape associated capabilities moving into the future.

### Threat

Diverse enemies will employ traditional, unconventional, and hybrid strategies to threaten U.S. security and vital interests. Threats may emanate from nation states or nonstate actors such as transnational terrorists, insurgents, and criminal organizations. Enemies will continue to apply advanced as well as simple and dual-use technologies (such as improvised explosive devices).<sup>34</sup>

As historian Sir Michael Howard once observed, “No matter how clearly one thinks, it is impossible to anticipate precisely the character of future conflict. The key is to not be so far off the mark that it becomes impossible to adjust once that character is revealed.”<sup>35</sup> The IED will remain the weapon of choice for groups along the threat continuum from the disenfranchised to the terrorist and will remain an enduring global threat due to the accessibility of materials and the potential strategic impact resulting from their use.<sup>36</sup> Moreover, highlighted in TRADOC Pam 525-3-1, *The Army Operating Concept: Win in a Complex World*, “Demographic trends such as urbanization, youth bulges, and migration are creating overpopulated megacities in which a growing pool of youth is willing to engage in violence to achieve their goals. Globalization and ready access to information will increase the perception of inequity between individuals, groups, and nations, creating informed classes of haves and have-nots. Likewise, the decreasing cost of technology and increasing threat of WMD and improvised explosive devices (IED) will give weaker groups and individuals the ability to threaten otherwise stronger forces.”<sup>37</sup>

Conflict waged because of these drivers is not easily categorized and just like the use of the Improvised Explosive Device, the domains will evolve over time and involve a

range of threats that will be difficult to characterize, let alone define.<sup>38</sup> Within the future operating environment, the three most emerging future threats related to IED defeat include the 'mega-city,' air and maritime environments.

### Operational Environment

Over the last decade the threat environment faced by U.S. and coalition forces was relatively stable, bound by two operational areas (Afghanistan and Iraq) and characterized by a variety of IEDs as the principal material and casualty producer.<sup>39</sup> The potential range of future environments, including land, air and maritime will likely contain a more complex and diverse range of threat capability – IEDs and improvised weapons system will be part of this equation. To a much greater degree than in the past, these threats will be adaptive and will likely present a blended application based on strategic desires and outcomes, Weapons of Mass Destruction (WMD) included.

### Land / Megacity

There will likely be a shift from the mountains, desert rural areas and even cities like Mosul and Baghdad our forces were accustomed to operating in, to developed megacities. In The U.S. Army Chief of Staff's June 2014 Strategic Studies Group (SSG) study on the megacity environment the authors concluded, "It is inevitable that at some point the United States Army will be asked to operate in a megacity and currently the Army is ill-prepared to do so."<sup>40</sup> This author believes that not only the Army, but the entire DOD CIED community is ill-prepared to effectively mitigate IEDs incorporated as a weapon within the megacity environment. CIED forces will face numerous and new complex military geographic challenges while operating in cities with populations exceeding 10 million people (defined as megacities). Although research indicates divergent views on the validity of the megacity threat (as highlighted in the

aforementioned SSG study), with the exception of sheer force requirements based on the size of the city, the technical aspect of CIED operations would be generally unchanged.

There are a few specific facets of this operational environment that will directly affect CIED forces and represent an emerging obstacle for CIED defeat that should be considered. Competition among a cluttered electromagnetic (EM) environment between public, governmental and commercial users who will undoubtedly insist on their access to airwaves will require both unique jamming capability, and detailed characterization/deconfliction of spectra.<sup>41</sup> Within such an EM environment, operating radio-controlled tools, such as robots or firing devices for IED detection and neutralization will prove difficult if not properly analyzed and deconflicted. Equally important and perhaps more difficult to manage in the urban environment include the ability to effectively jam potential nefarious signals used to initiate IEDs on command.

While a key tenant, as previously mentioned regarding effective CIED defeat, includes exploitation based on disarming IEDs vs. blowing them up; this factor is compounded in an urban environment. The local populace and its government would likely not tolerate collateral damage caused by U.S. and coalition forces within a densely populated area.<sup>42</sup> Another challenge posed by the urban environment and collateral damage includes both the ability to track and ultimately engage targets such as the Suicide Vehicle Borne IED (SVBIED) from the air. While Mosul may not currently fall into the megacity realm, the U.S. has experienced recent related targeting challenges of SVBIEDs; "...the dense urban sprawl of Mosul, have created a nightmare scenario for Iraqi troops entering the city. Suicide vehicles spring from back alleys and

cut in and out of side streets before striking Iraqi vehicles. The speed of the car bombers and an urban environment packed with civilians have made airstrikes against them almost impossible. Col. John Dorrian, spokesman for the U.S.-led campaign against the Islamic State, confirmed the problem, saying that the deeper into the city the Iraqis get, the harder it is for U.S. air power to stop the suicide vehicles.”<sup>43</sup>

The final factor to consider within the scope of megacity threat considerations to future CIED defeat efforts includes the subterranean environment. Again, operations in Iraq provide a mere glimpse of the difficulties subterranean environments present, Iraqi Commanders operating in the Mosul area “...knew urban warfare among civilians and human shields in Mosul would be difficult, but the tunnels are making it worse. The officers described the battlefield as more of a sphere than a plane – with threats coming from side to side above and below.”<sup>44</sup> Additionally, The Iraqi Special Forces and Peshmerga units are reporting that the tunnels-their entrances/exits - are frequently booby-trapped. Presenting yet another unique threat environment for EOD operators who will be needed to support the clearing and exploitation of material found in the tunnels.<sup>45</sup> Imagine the complications of IED detection and neutralization capability for the sub surface challenge posed by the enemy in a megacity using tunnel systems including those already in place for sewer, water power lines, transit etc. to hide, conceal arms, explosives and move undetected. This environment is one that the U.S. EOD community is not equipped to effectively operate in.

#### Air / Unmanned Aerial Systems

Highlighted in the 2016 *Joint Operational Environment 2035: The Joint Force in a Contested and Disordered World* includes the threat posed by UAS when used as weapons systems by criminal and terrorist organizations.<sup>46</sup> Today, at least 90 nations

and non-state groups are known to operate drones, including 10 countries with armed drones and an additional 20 countries have armed drone programs in development.<sup>47</sup> As this technology continues to proliferate, simple weaponized drones will be increasingly within the reach of virtually any state and many non-state actors. Already, non-state actors such as Hamas, Hezbollah, the Islamic State of Iraq and Syria (ISIS), and Libyan rebel groups have used drones to conduct tactical surveillance. Regarding ISIS' capability, a senior naval analyst with the Middle East Security Project at the Washington, D.C.-based Institute for the Study of War reported, "They don't have reusable attack drones, but I think it is just a matter of time before they jury-rig surveillance drones into flying IEDs. Basically, they could turn them into little kamikaze drones."<sup>48</sup>

The analyst was correct in his assessment made in 2015. On October 2, 2016 in Erbil, Iraq, a drone flown by ISIS injured two French Paratroopers and killed two Peshmerga soldiers.<sup>49</sup> The attack is possibly the first where a drone fitted with an improvised explosive device has inflicted casualties on troops from a Western nation. Clearly, the UAS, which originally appeared as a hobbyist toy, is emerging as a multi-functional terrorist tool capable of delivering explosive charges as well as conducting surveillance. Highlighted in *A World of Proliferated Drones: A Technology Primer*, "UAS are also widely accessible to potentially disruptive actors and because drones, assembled from component parts generally do not have identifiable markings, could increase the difficulty of attribution if used in an attack. In addition, due to their size, construction material, and flight altitude, hobbyist drones are difficult to defend against if their presence in a particular area is unknown or unexpected."<sup>50</sup> While the UAS threat

will continue to complicate CIED defeat efforts, another threat consideration includes the maritime environment.

### Maritime

In 2012, then Deputy Secretary of Defense Ash Carter charged the Senior Integration Group within DOD to come up with ways to counter water-borne explosive devices, maritime suicide missions, and other associated threats.<sup>51</sup> While most associate the IED threat with operations in support of OEF and OIF (land operations), there is a very real threat posed by the use of IEDs in the maritime environment. The underwater improvised explosive device represents an increasingly pernicious threat within the maritime domain. An attack on the nation's ports and harbors using an underwater IED would have a crippling impact on the economic health and security of the nation. Delivery of maritime IEDs might include the use of small crafts, man-piloted IEDs, submersibles, unmanned underwater vehicles that can home in on a tanker or combat vessel and initiate an attack.<sup>52</sup>

There are numerous examples overseas of the use of small vessels as a waterborne improvised explosive device (WBIED) to attack maritime targets. These tactics could be applied against the United States and its interests to attack vessels, infrastructure, and industry (such as refineries and chemical plants) in the maritime domain.<sup>53</sup> From the unfortunate October 2000 attack on the USS COLE to a 2005 arrest of a senior al-Qaeda operative who had intended to place a one ton bomb on a yacht and ram a cruise ship carrying vacationing Israeli soldiers in Turkey; each represent a small range of high-profile tactics and targets that could be replicated in the United States.<sup>54</sup> Similar to the UAS profile, as technology developments increase capability (payload and remote operation), the maritime IED threat scenario can be anticipated to

increase. As opportunities decrease for terrorist organizations related to combat operations and the U.S. becomes generally 'complacent,' this author believes we will see a spectacular maritime attack – IEDs will be the method of destruction.

Just as the IED as a weapon system evolved from a simple low impact explosive device alongside the road to lethal EFPs responsible for penetrating armor and many subsequent casualties, the U.S. should anticipate and be prepared for the future IED threat. The megacity, UAS and maritime IED threats should be studied in detail and solutions applied as the environment shifts. The U.S. should not lose focus of the threats faced to date with respect to lessons learned in OEF and OIF, DOD must rather, begin to think about future threats, apply lessons learned instead of boxing up all of the gained capability and pretending like the IED threat will not exist beyond the current conflicts – it will not go away. In fact, the IED threat that continues to proliferate overseas could soon be seen in a “theater near you” – domestically.

### Domestic

While domestically, the U.S. Homeland has not experienced the IED threat to the same degree as seen by the Armed Forces fighting overseas, there remains a very credible threat to the homeland. Although there are many “benign” IED incidents reported within the homeland annually, as seen in the most recent high profile attack in 2013, the Tsarnaev brothers detonated IEDs at the Boston Marathon that caused both loss of life and an economic impact worth noting. The explosions killed three individuals and wounded 264 nearby racers and spectators. Sixteen of the wounded persons experienced traumatic amputations. The unexpected attack closed the city of Boston for four days while over 1,000 first responders searched for the suspects.<sup>55</sup> The homemade explosive devices used were constructed from pressure cookers, firecrackers, ball

bearings, Christmas lights, and remote control car parts assembled by plans accessed from the internet via extremist literature.<sup>56</sup> It is estimated the economic loss to the greater Boston area due to the shut down during the ensuing man-hunt exceeded \$333 million.<sup>57</sup> Clearly, the U.S. homeland is not immune from the IED threat. As aforementioned, only two individuals with as little as \$500 and an IED “cook book” inflicted loss of life, serious injuries and over \$330 million in damages. Similar to combat operations, domestically, the IED offers a low cost and effective way to accomplish an end and should be anticipated as a weapon of choice to inflict harm and create economic disruption within the homeland. While military formations deployed overseas have dealt with and adapted to the IED threat, one must consider is the homeland is postured to react accordingly – beyond an isolated event. Suppose future domestic IED threats include roadside bombs on major interstates, what would the U.S. ready to respond?

The ability to stop the “lone wolf” or the insurgent network bomb-maker before an explosion is difficult, therefore security professionals project IEDs will remain a threat for the foreseeable future.<sup>58</sup> As bombs continue to be a criminal and terrorist weapon of choice, the need to defeat these devices requires an integrated and seamless coordination of government resources. In the U.S. there are approximately 18,000 police departments; however, there are only 465 public safety bomb squads equipped to handle explosive threats.<sup>59</sup> The lack of civilian agencies trained and equipped to respond to explosive threats as well as their reliance on the military for assistance when their capabilities are overwhelmed highlights the need for increased interoperability between the Department of Defense and civilian agencies.

## Insights / Recommendations

It is a myth that military organizations tend to do badly in each new war because they have studied too closely the last one; nothing could be farther from the truth. The fact is that military organizations, for the most part, study what makes them feel comfortable about themselves, not the uncongenial lessons of past conflicts. The result is that more often than not, militaries have to relearn in combat—and usually at a heavy cost—lessons that were readily apparent at the end of the last conflict.<sup>60</sup>

Even as the U.S. presence in Iraq and Afghanistan remains diminished, U.S. forces and respective partner nations will continue to confront the dangers and challenges posed by improvised explosive devices and the networks that employ them globally. During the past fourteen years, the U.S. has 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.<sup>61</sup> Despite the cessation of major land warfare and a congressional mandate for fiscal constraint, the U.S. and coalition partners need to remain focused on staying ahead of technical evolutions regarding the IED threat. Both Weapons Technical Intelligence and force structure (organizations) are two strategic areas that must be addressed to increase CIED capability now and into the future.

### Exploitation / Weapons Technical Intelligence

Previously asserted in this paper, low cost, anonymity and standoff are three reasons the IED is a favorite (and effective) weapon system used by the enemy. Weapons technical intelligence, that is, linking collection, exploitation, reporting and action as system is critical to mitigating these variables to a negligible risk level. Many of the capabilities that enabled forensic science combined with the ability to conduct multi-media exploitation need to be forward deployed (expeditionary) in order to effectively

identify/target IED networks through denying them anonymity (biometrics), and increasing attribution (forensics) were supplementally funded; therefore, their enduring nature is in doubt.<sup>62</sup> Without institutionalization, expeditionary forensics will likely begin in future conflicts just as it started – ad hoc. Two additional related elements within WTI and exploitation worthy of emphasis and directly related to CIED efforts include intelligence sharing /information discovery, dissemination, and a codified requirement for an expeditionary database to retain associated intelligence of value.

As highlighted earlier in this paper, CEXC and TEX are examples of initial assets created for forward exploitation capability in Iraq and Afghanistan. In both cases, these assets matured in theater and very quickly became invaluable (beyond even CIED purposes) as they incorporated forensic technology that ensured a high degree of accuracy in the processing result and consequent confidence by the submitting units in the results provided. Particularly important in when reaching targeting decisions that could result in a kill/capture order. The ability to exploit as far forward as possible cannot be undervalued. With very few exceptions, as an EOD BN S3 and later IJC-CJ2E in Afghanistan, the respective formations were able to gain adequate intelligence via in-theater exploitation for immediate action versus waiting indefinitely for CONUS-bound results and reports. Not to be overlooked, efforts should continue to be considered regarding forensic equipment/capability operations in truly austere or maritime environments that may require an adaptation including: reduction in its size, environmental hardening, and downsizing of instrumentation. USSOCOM sees a requirement for future forensic science capabilities to be “mobile, light, handheld, on-site, palletable, and droppable.”<sup>63</sup>

The Terrorist Explosive Device Analytical Center (TEDAC, part of Department of Justice), whose mission is to help eradicate the IED threat by conducting strategic-level forensic and technical exploitation, served as the final stop for all IED materials (after prioritized forward exploitation).<sup>64</sup> By no fault of TEDAC, geographical separation from the forward deployed troops led to frustration for forward commanders eager to execute operations based on exploitation of material their forces sent back to the lab. Another factor related to TEDAC and device processing is that they treat all material as potential evidence (slower law enforcement nexus) and as such, this approach adds a time penalty for the tactical commander.<sup>65</sup> Because of this and the previously discussed issues of sheer responsiveness, the U.S. should maintain scalable expeditionary forensic capability in order to capitalize on the invaluable production of this capability. Since there is an established requirement for expeditionary forensic capability, the U.S. must have a proper database and information dissemination/sharing method that benefits all.

Similar to the labs, databases and subsequent reporting of significant activities, reports and exploitation fed into them was ad-hoc at the beginning of OEF/OIF. Each discipline seemed to have their own 'internal' reporting and password protected data base that did not allow efficient discovery and dissemination of information – CIED and subsequent exploitation reporting was no different. Eventually, as previously mentioned, CIDNE came to the fore as the sole reporting database designated within CENTCOM. All other 'stand-alone' systems were required to feed into CIDNE.<sup>66</sup> It is worth mention that many analysts, particularly at the strategic level, noted that they spent far too much time searching through multiple sources of poorly accessible and discoverable data,

and not enough time analyzing that data. A CIDNE-like theater wide information-sharing environment is required in order to aggregate data from multiple sources, across multiple intelligence disciplines and across multiple security classification domains.<sup>67</sup> Because of familiarity, confidence and proven reliability gained throughout OEF/OIF, CIDNE seems like a logical solution to institutionalize so that at a minimum, we have a 'warm start' in the future.

### Force Structure / Organization

Most agree the IED as a weapon system has proven so effective it will likely remain an enemy weapon of choice well into the future. Unfortunately, the same cannot be said for some of the very organizations whose responsibility it is to defeat the threat, including both U.S. Army EOD, and formerly JIEDDO. As already mentioned, because of the Budget Control Act of 2011, Army EOD was cut by a third and JIDA has changed from a Combat Support Agency to an organization within the Defense Threat Reduction Agency, now JIDO.<sup>68</sup> In the case of similar overseas contingencies where the threat of IEDs exist, this now leaves the Geographic Combatant Commands with less trained and equipped forces available to neutralize explosive hazards, similar to what was experienced from 2002-2005. Similarly, some of the capabilities relied upon (2006-2013) within what used to be the JIEDDO have either been consolidated, transferred or completely disappeared.

The encouraging news is that Congress and the Department of Defense determined that JIDO remain an enduring capability. The DOD must continue to leverage JIDO within the CIED community and adjust expectations gained during a time of what seemed like nearly an endless amount of resources and funding they previously provided. Now is the time to reflect on the areas that have proven to be true

requirements versus 'nice-to-have' and anticipate how to best leverage support for future operations. As an example, while the JIDO focus is not strictly on the CIED threat and environment anymore, it does offer a more 'focused' strategy towards improvised threats (think UAS) – not specific to CIED operations necessarily, but could easily be configured to.

Identified in the 2016 JIDO CONOP, "JIDO will maintain an embedded presence with deployed U.S. joint forces. In coordination with the Military Service components, this allows JIDO to assist Joint Force Commanders to identify and understand their risks and vulnerabilities, and enables: a rapid and early understanding of capability gaps, the timely validation of requirements, and informed investments in counter-threat technologies and non-material solutions within the CCDRs' latest time of need. With Joint IED Defeat Fund's (JIEDDF) flexibility and authorities, JIDO initiates, accelerates, develops, and delivers urgent (0-2 years) counter-improvised threat solutions addressing validated CCMD capability requirements."<sup>69</sup> Frankly, the EOD community in general has been spoiled by the vast resources previously offered that created an expectation of, "we ask, we get..." JIDO has consolidated and CIED organizations must adapt as well and seriously analyze what actual requirements are involved with successful CIED mission accomplishment in the future.

While Joint Force EOD resourcing has generally reduced since the drawdowns in Iraq and Afghanistan, Army EOD has experienced the greatest impact to date. For example, in 2005, the Army Vice Chief of Staff directed the Army EOD force to double in size due to extreme high Operational Tempo (OPTEMPO) and demand from commanders in both Iraq and Afghanistan. This made sense and subsequently, with a

near 1:1 ratio of EOD companies to Brigade Combat Teams (BCTs), EOD OPTEMPO decreased while responsiveness in support of maneuver formations increased, as there was enough depth to imbed EOD technicians directly with maneuver forces.

Unfortunately, the 2005 growth in capacity is now being reversed.

General Dunford, the Chairman of the Joint Chiefs of Staff reported to the Senate Armed Services Committee on March 17, 2016, "...We continue to operate systems in several critical mission areas and deploy personnel with specific specialty skills at high rates, resulting in minimal to no surge capacity in those areas...this negatively impacts the Joint Force's responsiveness...High Demand/Low Density capability shortfalls that pose significant military risk include:...explosive ordnance disposal assets."<sup>70</sup> Despite this, Army EOD forces were reduced by a third and it is abundantly clear that Defense management of Army EOD forces must be updated.

Army EOD forces account for merely 3% of Ordnance Soldiers.<sup>71</sup> Although there is no true linkage among the remaining 97% of Ordnance Soldiers (ammunition and maintenance) to EOD, EOD forces are managed by and remain under the sustainment proponent. EOD's force protection core competencies such as rendering safe IEDs, conducting route clearance, and integrating into BCTs are an Operational Support function. However, they are still trained, manned and equipped under the sustainment proponent. Because of this, the management of EOD equities and oversight by the Combined Arms Support Command (CASCOM) has been marginal. While it is generally accepted that the EOD force should downsize, given the Army requirement to reduce overall, the Army EOD force was cut disproportionately to pay manpower bills assigned to the Ordnance Corps. If Army EOD were established as a stand-alone branch and

modeled in Total Army Analysis (TAA) separate from the sustainment warfighting function, Army EOD capacity required for the next “surge” would be better postured to respond to the associated requirements in order to counter the inevitable IED threat.

### Conclusion

The Improvised Explosive Device threat is enduring and will continue to present global challenges for those countering it well into the future. Although the IED is not new, U.S. and coalition forces in support of OEF and OIF were not prepared for the threat presented by insurgents’ use of it – there are lessons to be learned. Whether spending over \$70 billion, standing up task forces, updating/creating policy and doctrine or developing technology to counter the IED threat, advantage must be taken regarding what has been learned/developed and seriously evaluated in order to posture for the future IED threat. It would be deadly and reckless to neglect the advantages that have been gained over the last decade because of the drawdown in major operations. Williamson Murray reminded us in his *Thinking About Innovation* article, “...The result is that more often than not, militaries have to relearn in combat—and usually at a heavy cost—lessons that were readily apparent at the end of the last conflict.” Let us not forget.

### Endnotes

<sup>1</sup> Barack Obama, *Presidential Policy Directive on Countering Improvised Explosive Devices* (Washington, DC: The White House, February 26, 2013), 1, [https://www.whitehouse.gov/sites/default/files/docs/cied\\_1.pdf](https://www.whitehouse.gov/sites/default/files/docs/cied_1.pdf) (accessed December 10, 2016).

<sup>2</sup> Phillip W. Carroll III USA, *Mine and Booby Trap Warfare: Lessons Forgotten*, Study Project (Carlisle Barracks, PA: U.S. Army War College, February, 29, 1988), 14, <http://handle.dtic.mil/100.2/ADA194094> (accessed December 12, 2016).

<sup>3</sup> Greg Zoroya, “Homemade Bombs Caused Death and Agony for Troops and Prompted Changes in Military Equipment,” *USA Today Online*, December 19, 2013, <http://www.usatoday.com/story/news/nation/2013/12/18/ied-10-years-blast-wounds-amputations/3803017/> (accessed December 14, 2016).

<sup>4</sup> Rick Atkinson, "The IED Problem is getting out of Control. We've got to Stop the Bleeding," *Washington Post Online*, September 30, 2007, [http://www.washingtonpost.com/wp-dyn/content/article/2007/09/29/AR2007092900751\\_5.html?sid=ST2007092900754](http://www.washingtonpost.com/wp-dyn/content/article/2007/09/29/AR2007092900751_5.html?sid=ST2007092900754) (accessed December 14, 2016).

<sup>5</sup> Iain Overton, "Improvised Explosive Devices – A 5 Year Overview," *Action on Armed Violence*, November 24, 2016, <https://aoav.org.uk/2016/improvised-explosive-devices-5-year-overview/> (accessed December 12, 2016).

<sup>6</sup> John Moulton, "Rethinking IED Strategies, From Iraq to Afghanistan," *Military Review*, July–August 2009, 26.

<sup>7</sup> Russell L. McIntyre, interview by author, Charlottesville, VA, November 26, 2016.

<sup>8</sup> State of Massachusetts, *After Action Report for the Response to the 2013 Boston Marathon Bombings* (Boston, MA: State of Massachusetts, December 2014), linked from *State of Massachusetts Home Page*, <http://www.mass.gov/eopss/docs/mema/after-action-report-for-the-response-to-the-2013-boston-marathon-bombings.pdf> (accessed November 12, 2016).

<sup>9</sup> Thomas E. Ricks, *Fiasco* (New York: Penguin Books, 2006), 202.

<sup>10</sup> McIntyre, interview by author.

<sup>11</sup> Ibid.

<sup>12</sup> Ibid.

<sup>13</sup> Jeffery L. Maxey and George J. Magner, *A Study of Factors Affecting Mine and Booby-trap Detection: Subject Variables and Operational Consideration* (Alexandria, VA: Human Resources Research Organization, 1973), 3, <http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=AD0769635> (accessed December 12, 2016).

<sup>14</sup> Zoroya, "Homemade Bombs caused Death and Agony for Troops."

<sup>15</sup> U.S. Government Accountability Office, *Counter-Improvised Explosive Devices: Multiple DOD Organizations Are Developing Numerous Initiatives: Report to Congressional Committees* (Washington, DC: U.S. Government Accountability Office, August 1, 2012), 1, <http://www.gao.gov/assets/600/593242.pdf> (accessed December 17, 2016).

<sup>16</sup> U.S. Department of the Army, *Joint Improvised Device Defeat Organization*, DoDD 2000.19E (Washington, DC: U.S. Department of the Army, February 14, 2006), 3.

<sup>17</sup> JIEDDO, *JIEDDO Annual Report: Report to Congressional Committees* (Washington, DC: Joint Improvised Defeat Organization, December 2010), 2, [https://www.jieddo.mil/content/docs/JIEDDO\\_2010\\_Annual\\_Report\\_U.pdf](https://www.jieddo.mil/content/docs/JIEDDO_2010_Annual_Report_U.pdf) (accessed December 17, 2016).

<sup>18</sup> Jen Judson, "As JIEDDO Becomes JIDA, IED Threat Builds in Theater," *Defense News*, November 19, 2015, <http://www.defensenews.com/story/defense/land/2015/11/19/as-jieddo-becomes-jida-ied-threat-builds-in-theater/76050828/> (accessed December 17, 2016).

<sup>19</sup> Daniel Goure, "FY2016 NDAA Is Undermining Real Acquisition Reform," *Real Clear Defense*, November 3, 2015, [http://www.realcleardefense.com/articles/2015/11/03/fy2016\\_ndaa\\_is\\_undermining\\_real\\_acquisition\\_reform\\_108639.html](http://www.realcleardefense.com/articles/2015/11/03/fy2016_ndaa_is_undermining_real_acquisition_reform_108639.html) (accessed February 15, 2017).

<sup>20</sup> Jen Judson, "JIDA to Become JIDO under Defense Threat Reduction Agency," *Defense News*, February 2, 2016, <http://www.defensenews.com/story/defense/land/2016/02/02/jida-become-jido-under-defense-threat-reduction-agency/79707958/> (accessed April 13, 2017).

<sup>21</sup> Defense Threat Reduction Agency, "Joint Improvise-Threat Defeat Agency Joins DTRA/SCC-WMD as the Joint Improvised-Threat Defeat Organization," September 30, 2016, 2, <http://www.dtra.mil/Portals/61/Documents/Press%20Releases/2016-009%20DTRA%20inc%20JIDO.pdf?ver=2016-10-03-083803-157> (accessed February 13, 2017).

<sup>22</sup> Russell McIntyre, "Counter-IED Collection and Exploitation: A Capability in Need of a System of Systems Approach," [https://issuu.com/deltabusinessmedialimited/docs/counter-ied\\_report\\_spring-summer\\_20\\_f723f74921fc7b?e=6269486/35939260](https://issuu.com/deltabusinessmedialimited/docs/counter-ied_report_spring-summer_20_f723f74921fc7b?e=6269486/35939260) (accessed December 18, 2016).

<sup>23</sup> Stephen Darnell, "National Strategic Plan for U.S. Bomb Squads National Bomb Squad Commanders Advisory Board," January 8, 2015, [http://nbscab.org/NBSCAB/nbscab\\_new.php](http://nbscab.org/NBSCAB/nbscab_new.php) (accessed February 10, 2017).

<sup>24</sup> McIntyre, "Counter IED Collection and Exploitation," 56.

<sup>25</sup> U.S. Joint Chief of Staff, *Counter Improvised Explosive Device Operations*, Joint Publication 3-15.1 (Washington, DC: U.S. Joint Chiefs of Staff, January 9, 2012), i.

<sup>26</sup> *Ibid.*, x.

<sup>27</sup> Michael D. Barbero, *Counter-IED Strategic Plan 2012 – 2016* (Washington, DC: JIEDDO, January 1, 2012), 5, <https://www.scribd.com/document/123346581/JIEDDO-C-IED-Strategic-Plan> (accessed December 22, 2016).

<sup>28</sup> *Ibid.*

<sup>29</sup> McIntyre, "Counter IED Collection and Exploitation," 57.

<sup>30</sup> *Ibid.*

<sup>31</sup> *Ibid.*, 58.

<sup>32</sup> Zoroya, "Homemade Bombs Caused Death and Agony for Troops," 7.

<sup>33</sup> Barbero, *Counter-IED Strategic Plan*, iii.

<sup>34</sup> U.S. Army Training and Doctrine Command, *The U.S. Army Operating Concept: Win in a Complex World*, TRADOC Pamphlet 525-3-1 (Fort Eustis, VA: Headquarters, U.S. Army Training and Doctrine Command, October 31, 2014), 10, <http://www.tradoc.army.mil/tpubs/pams/tp525-3-1.pdf> (accessed December 29, 2016).

<sup>35</sup> Ibid., iv.

<sup>36</sup> Barbero, *Counter-IED Strategic Plan*, 3.

<sup>37</sup> U.S. Training and Doctrine Command, *The U.S. Army Operating Concept*, 9.

<sup>38</sup> Ibid.

<sup>39</sup> McIntyre, interview by author.

<sup>40</sup> Marc Harris, Robert Diao and Nicholas Melin, *Megacities and the United States Army: Preparing for a Complex and Uncertain Future* (Washington, DC: United States Army Strategic Studies Group, 2014), 3.

<sup>41</sup> McIntyre, interview by author.

<sup>42</sup> Ibid.

<sup>43</sup> Thomas Gibbons Neff, "ISIS Video Shows how the Group has Turned Car Bombs into its Version of Airstrikes," *Washington Post Online*, November 15, 2016, [https://www.washingtonpost.com/news/checkpoint/wp/2016/11/15/isis-video-shows-how-the-group-has-turned-car-bombs-into-its-version-of-airstrikes/?utm\\_campaign=Early%20Bird%20Brief%2011.16.2016&utm\\_medium=email&utm\\_source=Sailthru](https://www.washingtonpost.com/news/checkpoint/wp/2016/11/15/isis-video-shows-how-the-group-has-turned-car-bombs-into-its-version-of-airstrikes/?utm_campaign=Early%20Bird%20Brief%2011.16.2016&utm_medium=email&utm_source=Sailthru) (accessed December 30, 2016).

<sup>44</sup> William Booth and Aaso Ameen Shwan, "ISIS Tunnels Complicate Fight for Control of Mosul," *The Washington Post Online*, November 6, 2016, <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=0ahUKEwjz9q7vsfSAhVFbSYKHxOjAbMQFggdMAE&url=https%3A%2F%2Fwww.pressreader.com%2Fusa%2Fthe-washington-post-sunday%2F20161106%2F281719794148358&usq=AFQjCNGYze3hgNC3oXqMo5mtl4QNRylxIQ&sig2=p8ITN9ojP9hv7wMyenMwPq&bvm=bv.148747831,bs.1,d.eWE> (accessed December 30, 2016).

<sup>45</sup> Ibid.

<sup>46</sup> U.S. Joint Chief of Staff, *Joint Operational Environment – 2035 The Joint Force in a Contested and Disordered World* (Washington, DC: U.S. Joint Chiefs of Staff, July 14, 2016), 14, <https://fas.org/man/eprint/joe2035.pdf> (accessed December 30, 2016).

<sup>47</sup> Horowitz and Fuhrmann, "Droning on: Explaining the Proliferation of Unmanned Aerial Vehicles," [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2514339](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2514339) (accessed December 31, 2016).

<sup>48</sup> Nancy Youssef, "Is ISIS Building a Drone Army," *The Daily Beast*, March 18, 2015, <http://www.thedailybeast.com/articles/2015/03/18/is-isis-building-a-drone-army.html> (accessed December 31, 2016).

<sup>49</sup> Kelsey D. Atherton, "IED Drone Kills Kurdish Soldiers, French Commandos," *Popular Science*, October 11, 2016, <http://www.popsci.com/booby-trapped-isis-drone-kills-kurdish-soldiers-french-commandos> (accessed December 30, 2016).

<sup>50</sup> Kelly Sayer, *A World of Proliferated Drones: A Technology Primer* (Washington, DC: Center for New American Security, 2015), 29, [http://drones.cnas.org/wp-content/uploads/2016/03/CNAS-World-of-Drones\\_052115.pdf](http://drones.cnas.org/wp-content/uploads/2016/03/CNAS-World-of-Drones_052115.pdf) (accessed December 31, 2016).

<sup>51</sup> Gordon Lubold, "Waterborne IEDs," *Foreign Policy*, October 15, 2012, 2, <http://foreignpolicy.com/2012/10/15/the-pivot-to-asia-and-the-urgent-fight-against-waterborne-ieds/> (accessed January 2, 2017).

<sup>52</sup> *Ibid.*, 3.

<sup>53</sup> U.S. Department of Homeland Security, *Small Vessel Security Strategy* (Washington, DC: U.S. Department of Homeland Security, April, 2008), 11, <https://www.dhs.gov/xlibrary/assets/small-vessel-security-strategy.pdf> (accessed January 2, 2017).

<sup>54</sup> *Ibid.*

<sup>55</sup> State of Massachusetts, *After Action Report for the Response to the 2013 Boston Marathon Bombings*.

<sup>56</sup> Silvia Wingfield, "Boston Marathon Bombers used 'Sophisticated' Bombs made of Parts from Christmas Lights, Model Cars: Prosecutors," *New York Daily News*, May 24, 2014, <http://www.nydailynews.com/news/crime/boston-marathon-bombers-sophisticated-bombs-prosecutors-article-1.1801484> (accessed February 6, 2017).

<sup>57</sup> Bill Dedman and John Schonen, "Adding up the Financial Costs of the Boston Bombings," *NBC News*, April 30, 2013, <http://usnews.nbcnews.com/news/2013/04/30/17975443-adding-up-the-financial-costs-of-the-boston-bombings> (accessed February 6, 2017).

<sup>58</sup> Anna Mulrine, "Pentagon Warns that US Faces IED Threat at Home," *The Christian Science Monitor*, July 17, 2012, <http://www.csmonitor.com/USA/Military/2012/0717/Pentagon-warns-that-US-faces-IED-threat-at-home> (accessed January 27, 2017).

<sup>59</sup> U.S. State and Local Law Enforcement Agencies, *A BJS Report, Alaska Justice Forum, University of Alaska Anchorage* (Anchorage, AK: U.S. State and Local Law Enforcement Agencies, Fall 2011), [http://justice.uaa.alaska.edu/forum/28/2-3summerfall2011/f\\_lawenf\\_census.html](http://justice.uaa.alaska.edu/forum/28/2-3summerfall2011/f_lawenf_census.html) (accessed February 7, 2017).

<sup>60</sup> Williamson Murray, "Thinking about Innovation," *Naval College Review* 54, no. 2 (Spring 2001): 122-123, <https://www.usnwc.edu/.../Thinking-about-Innovation---Murray,-Williamson.aspx> (accessed January 2, 2017).

<sup>61</sup> Defense Intelligence Agency, Joint IED Defeat Organization, *Weapons Technical Intelligence (WTI) Improvised Explosive Device (IED) Lexicon* (Washington, DC: U.S. Defense Intelligence Agency, March 2014, Version 2.0), i.

<sup>62</sup> Christine A. Hughes et al., *Best Practices for Expeditionary Forensics* (Washington, DC: CNA's Center for Naval Analyses Study, June 2015), iii.

<sup>63</sup> *Ibid.*, 42.

<sup>64</sup> Ibid., 9.

<sup>65</sup> McIntyre, interview by author.

<sup>66</sup> William J. Fallon, U.S. Central Command Commander, “Fragmentary Order 09-1290 to Operation Order 09” (Implementation of CIDNE as the USCENTCOM AOR Event Reporting Tool), MacDill Air Force Base, FL, U.S. Central Command, September 1, 2007.

<sup>67</sup> Ibid., 35.

<sup>68</sup> Judson, “JIDA to Become JIDO Under Defense Threat Reduction Agency.”

<sup>69</sup> Michael Shields, “JIDO CONOP,” October 1, 2016, <https://www.jida.mil/content/docs/CONOP.pdf> (accessed January 4, 2017).

<sup>70</sup> General Joseph Dunford Jr., USMC 19th Chairman of the Joint Chiefs of Staff, Posture Statement presented to the Senate Armed Service Committee, 114th Cong., 2nd sess. (Washington, DC: U.S. Marine Corps, March 17, 2016), [http://www.armed-services.senate.gov/imo/media/doc/Dunford\\_03-1716%20.pdf](http://www.armed-services.senate.gov/imo/media/doc/Dunford_03-1716%20.pdf) (accessed January 13, 2017).

<sup>71</sup> *The United States Army Ordnance Corps & School Home Page*, <http://www.goordnance.army.mil/eod/eod.html> (accessed January 4, 2017).