



Statement By

Lieutenant General Michael D. Barbero

Director

Joint Improvised Explosive Device Defeat Organization

United States Department of Defense

Before the

United States House of Representatives

Committee on Appropriations

Subcommittee on Defense

September 20, 2012

NOT FOR PUBLICATION UNTIL RELEASED BY THE HOUSE COMMITTEE ON
APPROPRIATIONS, SUBCOMMITTEE ON DEFENSE

Chairman Young, Ranking Member Dicks, and distinguished members of the Subcommittee; it is my privilege to update you on the Department of Defense's (DOD) efforts to mitigate the effects of improvised explosive devices (IED). Let me begin by thanking you for recognizing the importance of the counter-IED (C-IED) mission. The funding support you provide enables DOD to rapidly field critical C-IED capabilities our warfighters require to complete their mission.

Mission

In February 2006, the DOD officially established the Joint Improvised Explosive Device Defeat Organization (JIEDDO) to focus on the IED threat in Iraq and Afghanistan. JIEDDO's mission, as defined by DOD Directive 2000.19E, "is to focus (lead, advocate, coordinate) all DOD actions in support of the Combatant Commanders' and their respective Joint Task Forces' efforts to defeat IEDs as weapons of strategic influence."¹ JIEDDO is singularly focused on the IED threat and exists to rapidly field capabilities to reduce the effectiveness of this asymmetric weapon.

Resourcing the Counter-IED Mission

A large contributor to JIEDDO's support to the warfighter was the establishment of the Joint IED Defeat Fund by Congress in 2007. The flexibility of the three-year, colorless appropriation ensures JIEDDO is able to rapidly respond to urgent warfighter C-IED needs. I want to thank the committee for recognizing the importance of this rapid response capability and providing the requisite funding support needed throughout the years.

The JIEDDO budget requests represent a mixture of deliberate, planned programs as well as estimates for urgent C-IED needs of Combatant Commanders. Three-year funding allows JIEDDO to rapidly apply resources to critical areas of the C-IED fight and the flexibility to provide the warfighter the best C-IED capabilities to meet operational requirements.

¹ *Joint Improvised Explosive Device Defeat Organization*, DOD Directive 2000.19E (14 February 2006), para 4.

From fiscal years (FY) 2006-2008, JIEDDO supported operations in two theaters of conflict requiring budgets ranging from \$3.7 billion to \$4.5 billion. In 2009, JIEDDO supported the Afghan surge and other requirements with a budget of \$3.1 billion. While the Afghanistan area of operation presented evolving challenges, JIEDDO's FY 2011 budget of \$2.8 billion reflected the requirements of a single theater of support.

As support to theater and unanticipated needs from the warfighter continue, JIEDDO is predicting to commit more than \$2.7 billion during FY 2012, which includes FY 2010 and FY 2011 carryover funds. However, JIEDDO's projected FY 2012 carryover has decreased significantly due to additional urgent requirements to support dismantled operations this year. As a result, the FY 2013 request of \$1.9 billion is critical to JIEDDO's ability to meet the urgent C-IED needs of our warfighters.

Lines of Operation

To provide the requisite support to the Combatant Commands, JIEDDO focuses efforts along three lines of operation: Attack the Network, Defeat the Device and Train the Force. To enable a successful C-IED program, these lines of operation must work in harmony. Underpinning these three lines of operation is the organizational requirements of staff and infrastructure.

The first line of operation, Attack the Network, is the decisive endeavor. It encompasses all the material and non-material C-IED enablers to attack threat networks by first identifying, and then exploiting, critical threat network vulnerabilities. Attacking the network is the most complex line of operation, but it is how we achieve decisive results.

From the support provided to U.S. joint and coalition conventional and special operations forces, JIEDDO has built a deep knowledge base on threat networks. JIEDDO's Counter-IED Operations/Intelligence Integration Center (COIC) effectively and rapidly fuses more than 200 data sources and has developed or modified more than 60 software tools to allow analysts embedded with units and through integrated reach-back support to increase force protection and maneuverability of the supported

operational commander. Since 2007, JIEDDO has delivered more than 14,500 intelligence products to U.S. and coalition conventional and special operations customers in response to their requests; trained more than 25,000 civilian, military, interagency and intelligence community personnel; and deployed more than 1,100 personnel in support of operations in Iraq, Afghanistan and other Combatant Commands.

Six intelligence agencies and organizations (Central Intelligence Agency, Defense Intelligence Agency, National Geospatial-Intelligence Agency, National Security Agency, National Reconnaissance Office and the National Ground Intelligence Center) are embedded within the COIC to synchronize intelligence-related responses to our customers. Great Britain, Canada and Australia also have embedded officers within COIC to strengthen communications and information sharing among coalition partners.

Additionally, JIEDDO is embedded at each of the five theater special operations commands, the Combatant Commands and at four interagency organizations (the Counter-Terrorism Center, the Department of Treasury, the Federal Bureau of Investigation/Counter-Terrorism and the Drug Enforcement Agency/Special Operations Division) to facilitate a whole-of-government approach to disrupt the activities of global threat networks.

Since the establishment of the COIC in 2007, JIEDDO has developed an unmatched intelligence fusion, training integration and information technology capability that provides immediate C-IED analysis and decisive tactical edge to our warfighter and Combatant Commands.

The second line of operation, Defeat the Device, is the immediate and most obvious approach to protecting our service members from IEDs. As hard as we try, it is impossible to prevent every IED from being employed. However, once the IED finds its way to the battlefield, we have fielded a wide spectrum of initiatives to detect the components, neutralize the triggering devices and mitigate the effects of an IED blast. JIEDDO developed and rapidly deployed a comprehensive portfolio of capabilities, such as mine rollers, electronic countermeasures (jammers), robotics, handheld detectors,

pelvic protection garments and aerial and ground surveillance systems, to name a few. We do not rely on just one capability. Because the threat varies from region to region within Afghanistan and we face a very agile threat, our warfighters are provided an arsenal of capabilities to customize and apply to the unique IED threat and terrain they face.

JIEDDO's ethos is to rapidly deliver high-valued capabilities to the warfighter. For example, within six months, we funded and delivered several types of handheld devices, such as the Beachcomber and Minehound, to detect buried IEDs during dismounted operations. Since delivering the first device in October 2009, we have fielded more than 8,000 handheld detectors with an additional 2,084 scheduled for delivery in the next 10 months.

In April 2011, during my visit to Afghanistan, warfighters requested a small, lightweight reconnaissance robot they could easily carry during dismounted operations to throw over walls and into buildings to detect IEDs. JIEDDO invested \$24 million to rapidly developed and field 1,157 ultra-lightweight reconnaissance robots within 10 months of receiving this requirement.

The continually evolving, adaptive enemy mandates a responsive, agile acquisition and fielding capability. Our warfighters deserve to have the best capabilities as quickly as possible.

The third line of operation, Train the Force, is essential to preparing deploying warfighters on the optimal use of the full range of available C-IED tools and to build expertise in the latest tactics, techniques and procedures. In 2011, JIEDDO provided \$24 million to field C-IED training equipment for services' pre-deployment training centers. Based on the positive feedback received from commanders and warfighters on the critical requirement to train on this equipment prior to deployment, JIEDDO funded an additional \$36 million for training equipment in 2012. To date, JIEDDO has fielded 249 THOR III Surrogate dismounted jammers; 2,196 handheld detectors; 1,372 Holley Sticks; 75 Hook and Line; 835 search kits; and 276 training aids for pre-deployment training.

Preparing our best C-IED tool — a well-trained warfighter — requires a comprehensive and adaptive pre-deployment training approach to ensure our force has adequate time to understand the integration of all aspects of the C-IED fight before deploying to theater.

Current Threat — Afghanistan

It is clear the IED is the primary weapon of choice for threat networks globally and is one of the enduring operational for the foreseeable future. In Afghanistan, these devices are the greatest source of casualties. In the past two years, IED events have increased 42 percent, from 9,300 in 2009 to 16,000 in 2011, and 2012 is on track to meet or exceed the historic number of IED events we saw in 2011.

While the overall number of IED events is high, our ability to find IEDs and neutralize them before detonation has improved significantly. The rate at which coalition mounted patrols find and clear IEDs improved from 49 percent in June through August, 2010, when we first surged forces in Afghanistan, to 65 percent in June through August, 2012. For coalition dismounted patrols, the IED found-and-cleared rate improved from 62 percent to 78 percent for the same periods. Many factors have increased the IED found-and-cleared rates in Afghanistan including applying lessons learned from Iraq, shifting C-IED systems from Iraq to Afghanistan, fielding increased numbers of C-IED capabilities, improving C-IED training and continuing the refinement of tactics, techniques and procedures tailored to the Afghan threat.

Homemade Explosives Challenge

Fertilizer-based explosives still remain our greatest threat in Afghanistan. Today, 87 percent of IEDs employed against coalition forces are homemade explosives (HME), and of those, 74 percent are made with ammonium nitrate derived from calcium ammonium nitrate — a common agricultural fertilizer. We have also seen these ammonium nitrate-based IEDs used globally.

In the early 1980s, the Provisional Irish Republican Army used ammonium nitrate-based IEDs in multiple attacks in London. The U.S. witnessed firsthand just how deadly

ammonium nitrate can be in the 1995 Oklahoma City bombing that claimed the lives of 168 people. In November 2003, a series of ammonium nitrate-based truck bombs killed more than 50 and injured 700 at multiple locations across Istanbul, Turkey. Just last year, we saw the devastating effects of ammonium nitrate-based HME attacks in Mumbai, India, and Oslo, Norway. This fertilizer and other cheap and easily procured dual-use components present a distinct advantage to our enemies and a security challenge to all of us

The complex nature of the global HME threat requires the support of unique and non-traditional partners. JIEDDO has engaged the International Fertilizer Association and fertilizer community to urge their commitment in countering the illicit use of fertilizer as an explosive. JIEDDO has asked this community to develop a whole-of-industry approach to: implement a universal dye program; explore non-detonable substitutes for ammonium nitrate; institute effective industry-wide standards, regulations and safeguards regarding the production and distribution of nitrogen-based fertilizer; and produce a global education and awareness campaign. Expanding our community of action to include unique and non-traditional partners is critical to addressing this HME challenge.

Global and Enduring Threat

While the IED has been a focal point of combat operations in Afghanistan and Iraq during the last decade, it is not exclusive to those countries or the region. The global spread of threat networks and the proliferation of IEDs and associated technology are pervasive and continue to threaten U.S. interests at home and abroad. Since 2007, IED incidents outside of Iraq and Afghanistan have increased to more than 500 events per month. Since January 2011, there have been more than 10,000 global IED events occurring in 112 countries, executed by more than 40 regional and transnational threat networks².

The extremist networks that employ IEDs have proven to be resilient, adaptive, interconnected and extremely violent. Globalization, the Internet and social media have

²Worldwide IED Database, Institute for Defense Analysis, June 2012

extended the reach of these organizations, providing platforms for recruiting, technical exchanges, training, planning, funding and social interaction. We see IED tactics and techniques used by insurgents increasing in sophistication and proliferating globally.

While we adhere to Napoleon's dictum to "march to the sound of the guns," these threat networks march to the signs of insecurity, and take the IED with them. We see this in Colombia, Pakistan, Syria, Nigeria and Somalia among others. Wherever we see turmoil or insecurity we see the spread of these networks and the spread of IEDs.

Today's IEDs are relatively simple, low-tech devices, which routinely use command wire, pressure plates or radio-controlled triggers. Many readily available components such as cell phones, agricultural fertilizers and simple electronic transmitters and receivers have legitimate commercial uses, but are easily and increasingly adapted for illicit purposes in manufacturing IEDs. The dual-use nature of IED components poses unique challenges in our ability to regulate and limit terrorist access to IED precursors and trigger components.

In the future, bomb makers will likely incorporate such enhancements as ultra-thin and flexible electronics; advanced communications mechanisms such as blue-tooth, Wi-Fi, and broadband; optical initiators; and highly energetic metals. In addition to more sophisticated technology, threat networks will develop enhanced IED concealment techniques and may even combine IED use with concurrent cyber attacks. The ubiquitous nature of IED materials, their low cost, threat networks ability to share tactics and recipes and potential for significant impact guarantee the IED will remain a threat and main casualty-producing weapon for decades to come.

Enduring Capabilities

Today and in the future, U.S. forces will operate in an IED environment. While IEDs cannot stop our units or deter our commanders from taking the fight to the enemy, these devices are the greatest source of combat casualties this decade. The IED and the threat networks that employ this asymmetric weapon are a reality of 21st century warfare and we must plan accordingly. The department is in the process of reviewing the

number of proven capabilities created during the course of the last 10 years to determine which should endure. JIEDDO has recommended five C-IED capabilities we believe should be institutionalized.

First, we must maintain the ability to rapidly provide C-IED materiel and non-materiel solutions in response to the changes in the IED threat. The constantly changing threat environment requires DOD to maintain a higher level of institutional agility.

For example, as dismounted operations increased in Afghanistan so did severe pelvic injuries to our troops. By leveraging an existing United Kingdom capability, JIEDDO was able to rapidly fund and begin delivering more than 200,000 protective outer and undergarments within 12-weeks from funding release to initial delivery. A study performed by the Army Office of the Surgeon General concluded soldiers not wearing pelvic protection systems are approximately three times more likely to suffer from major genitourinary injury following an IED incident than those wearing pelvic protection. By tapping into an already developed and proven technology and applying our rapid acquisition authorities, JIEDDO was able to rapidly respond to an urgent need within weeks, not years. The traditional DOD acquisition process could not have responded as quickly to this critical requirement.

Ensuring our commanders have freedom of maneuver now and in the future is critical. To preserve our ability to respond to changes in the IED threat, we must institutionalize a rapid acquisition capability and continue to invest in the development and fielding of new technologies. Moving forward, DOD must deliver capabilities in months — not years.

The second enduring capability is the ability to fuse operational information and intelligence, from all sources, to produce actionable intelligence — analytical products that meet the needs of both our operational commanders and domestic security partners. This is accomplished through a robust and powerful network of partners with whom analytical tools, methodologies and most importantly, information and intelligence, can be shared to identify, and then exploit, the vulnerabilities of threat networks. JIEDDO applies a suite of innovative tools to enable analysts to organize

intelligence from more than 200 data sources, resolve identities, correlate events, research patterns of life and geospatially render this information on a map to produce a blended intelligence picture that directly supports operations.

For example, JIEDDO has applied this layered analysis approach to support the interdiction of HME in the U.S. Central Command area of responsibility. Since January 1, 2012, JIEDDO has facilitated coalition force operations against HME production and cache sites, resulting in the interdiction of more than 1,000 pounds of HME and associated precursor materials every 13 days.

Sorting through the explosion of data and proliferation of isolated, independent data feeds, such as full-motion video, imagery, biometrics, intelligence community reporting, open source reporting and raw sensor feeds is a constant struggle for our warfighters and analysts. It is critical we sustain our current capabilities to continue to seamlessly share and fuse this data across the attack-the-network enterprise. We must continue to build upon current techniques to enhance data processing upon intake. The better we can sort or mine data, the faster our analysts can manipulate this information to produce actionable intelligence for our leaders and actionable evidence for our interagency law enforcement partners.

We must produce advanced analytics supporting the rapid identification of threat networks activities and our ability to push relevant analysis quickly to expeditionary forces. The speed at which these threat networks operate mandates the requirement for us to produce faster analytical assessments of emerging operational environments to support rapid exploitation. Threat networks are not going away and they will continue to employ IEDs as their weapon of choice. This requires the U.S. C-IED community to think differently and fully develop an information sharing and fusion capability for DOD, law enforcement and intelligence community information. In addition, we must ensure expedient methods are in place to share this same information with international partners when appropriate. We are all confronted by the same global set of networked enemies requiring us to remain networked in our efforts to defeat them in the future.

Third, we must maintain our ability to train our forces for these enduring threats. Today and in the future, U.S. forces will be operating in an IED environment, which is why C-IED and attack-the-network training must endure and be permanently integrated into our individual Service training institutions and centers. As we have learned in Iraq and Afghanistan, we can provide the best C-IED capabilities to the warfighter, but without the timely and relevant training component, the full capacity of equipment and tactics will never be realized.

During the Cold War we trained to conduct operations in a nuclear, biological and chemical environment. Moving forward, we must train to conduct operations in an IED environment, which includes an agile networked enemy. Individual, leader and collective C-IED and counter-network training must be institutionalized.

The fourth enduring capability is our ability to conduct relevant and timely collection, analysis and technical and forensic exploitation of current and emerging IED technologies through weapons technical intelligence (WTI). During the past eight years, JIEDDO, in conjunction with the military services, U.S. interagency and our multinational partners developed the highly effective WTI process to target extremist networks and defeat the IED.

Outside of combat zones, the WTI process is synonymous with the interagency efforts to detect and disrupt explosive threats by providing subject matter experts to both law enforcement and the intelligence community. The interagency has embraced the WTI lexicon as a means to speak the same language and begin the process of sharing data currently stove-piped in multiple agency systems. The WTI process is also captured as an essential element of the revised U.S. C-IED national strategy.

WTI has evolved from traditional technical intelligence³ and leverages law enforcement techniques as well as forensic and biometric technology to collect, exploit and analyze

³ "Intelligence derived from the collection, processing, analysis, and exploitation of data and information pertaining to foreign equipment and materiel for the purposes of preventing technological surprise, assessing foreign scientific and technical capabilities, and developing countermeasures designed to neutralize an adversary's technological advantages. Also called TECHINT." Joint Publication 1-02, 15 January, 2012.

IED-related materials and other weapons systems.⁴ This process coordinates and integrates various DOD and federal organizations and programs to facilitate everything from the onsite collection of IED material to the analysis of IED components in national laboratories. This analysis is then delivered to our military commanders to support targeting, track IED materials to their source, aid in host nation criminal prosecution and enhance force protection for our nation's warfighters.

Emerging technologies such as standoff biometric collection, rapid DNA processing and real-time latent fingerprint matching hold enormous potential to advance the WTI process into the next generation of protection. These capabilities will allow security personnel to identify threats before they reach checkpoints and to instantaneously attribute criminal and illicit activities to the perpetrators.

The benefit of the WTI process has unlimited potential and applicability to defeat improvised weapon systems that provide our enemies an asymmetric advantage. Our commanders increasingly focus operations to collect biometric data and several have referred to it as a "game-changer." Biometric, forensic and technical exploitation remove a violent extremist's greatest defense — anonymity — and makes them vulnerable to attribution, which is why the WTI capability must endure.

Fifth, and finally, the enduring global IED threat requires a whole-of-governments approach. As we move forward, the C-IED community must continue to synchronize counter-threat network capabilities and actions among domestic, international and other security stakeholders.

Today, JIEDDO is working with an expanded community of action for C-IED that did not exist previously. We have established an interagency forum consisting of U.S. intelligence and interagency partners, federal law enforcement, the Five Eyes (United States, United Kingdom, Canada, Australia, and New Zealand) community and forward-

⁴ WTI is "a category of intelligence and process derived from the forensic and technical exploitation of improvised explosive devices (IEDs), associated components, improvised weapons, and other weapons systems." WTI IED Lexicon, Edition 3.1, July, 2011.

deployed forces to achieve a more transparent and holistic effort to disrupt threat networks employing IEDs against U.S. and coalition forces globally.

We recognize no single government department or international partner has the ability to fully limit access to IED precursors, so we are integrating our efforts to go after the threat networks distributing these materials. Our U.S. government partners bring expertise in defeating and prosecuting criminal networks; applying financial pressures by going after the assets of IED network members, financiers, and distributors; enacting export controls and treaty compliance efforts that lead to the interdiction of IED components; advancing C-IED objectives through public diplomacy and policy and regulatory changes; advising on legitimate agricultural requirements; and coordinating and executing national C-IED policy efforts outside of declared combat zones through the interagency Joint Program Office for Countering IEDs. This is by no means a comprehensive list of the actions our interagency partners are applying to the C-IED fight, but it should give an idea of the collaboration occurring on all levels.

For example, the U.S. Department of Commerce added 152 persons to the Entity List because of IED-related matters. This designation stops U.S. companies from trading with these entities — companies, organizations, persons — who violated U.S. export laws. As of September 2012, the U.S. Department of Homeland Security, U.S. Immigration and Customs Enforcement, Homeland Security Investigations' Global Shield Program has produced 40 enforcement actions and 44 seizures totaling 138.70 metric tons of explosive precursor chemicals. Through coordinated efforts and strong partnership across the U.S. government and with our international partners, the C-IED community is going after these nefarious actors and effectively countering the networks that use IEDs. Maintaining this momentum against an adaptive threat requires the continued focus of the intelligence community to build a common intelligence picture. We cannot go back to a stove-piped approach to intelligence.

Moving forward, we will continue to face an ever-present threat from the overlapping consortium of threat networks employing IEDs as their weapon of choice. We have to continue to pursue a whole-of-governments approach, knitting together all the tools we

have at our disposal as we work collectively and seamlessly to understand these threat networks and mitigate the effects of IEDs. These adaptive and constantly evolving threat networks require an agile and responsive counter-threat network to defeat them. The multinational, interagency coordination we have established during the last decade must not attrite.

These five recommended enduring capabilities — rapid acquisition and fielding; operations-intelligence-information fusion, C-IED training, WTI, and a whole-of-governments approach — are synergistic and provide a comprehensive response to an enduring, complex, asymmetric and dynamic threat.

Closing

It is imperative we capture and institutionalize the lessons of a decade of combat operations. In the coming decades, the IED and the networks that employ these asymmetric weapons will continue to be a fixture of the battlefield and a threat here at home. It is our responsibility to learn and adapt institutions accordingly. There is no “silver bullet” to defeat the IED threat; our best defense is a warfighter with the right intelligence, training and equipment before they deploy into harm’s way.

Chairman Young, Ranking Member Dicks, members of the Subcommittee, again, thank you for the opportunity to appear before you today. I look forward to your questions.