



**Remarks by**

**Lieutenant General Michael D. Barbero  
Director, Joint IED Defeat Organization**

**Delivered at**

**Office of Naval Research  
Sciences Addressing Asymmetric Explosive Threats  
Program Technical Review**

**August 14, 2012**

Good morning. Thank you Mr. [George] Solhan for the kind introduction. I would like to thank you along with Dr. Kassner and Dr. Prono for your leadership. And to Rear Admiral Klunder for hosting this event.

Ladies and gentlemen, I am truly grateful for the opportunity to speak to you today. I am Lieutenant General Michael Barbero, director of the Joint Improvised Explosive Device Defeat Organization. JIEDDO, as it is commonly known, was established in 2006 to focus on the improvised explosive device problem in Iraq and Afghanistan. As you know, we are singularly focused on this threat and we exist to rapidly field capabilities to reduce the effectiveness of the IED.

I am very pleased that this conference is tackling the asymmetric explosives threat because it is clear the IED, and the networks that use these weapons, will remain a threat —to our forces and to our homelands — for decades. This threat is global — and growing. To adequately prepare our military for the future, I believe we need to look at what we have learned over the last decade, apply those lessons to our planning, and continue to be innovative and aggressive in supporting the entire domain of our research and technology development — including basic through applied science and technology as well as through technology maturation and systems acquisitions. We must recognize the significant effect IEDs have had during the last decade of combat operations.

Also, we need to examine not only the characteristics of the IED itself but also the networks that employ this device. As General John Allen, commander of ISAF stated bluntly, this is a “very tough mission against an intelligent, resourceful and resilient enemy with patience and little regard for human life.” We have seen the insurgency relying increasingly on IEDs as the weapon

of choice. In Afghanistan, these devices are the greatest source of casualties — with more than 1,500 IED events per month.

But the IED threat continues to expand well beyond Afghanistan and is truly a global threat with more than 500 IED attacks occurring outside of Iraq and Afghanistan on a monthly basis. Since January 2011, there have been nearly 10,000 global IED events occurring in 112 countries, executed by more than 40 regional and transnational threat networks.

Today's transnational extremist networks that employ IEDs have proven to be resilient, adaptive, interconnected, and violent. Globalization, the internet, and social media have extended the reach of these organizations — providing platforms for recruiting, technical exchanges, training, planning, funding, and social interaction. Their ability to seamlessly communicate and share explosive device recipes; tactics, techniques and procedures; and migrate back and forth — it's really a huge strategic advantage for these threat networks and something that will continue in the future.

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 — now and in the future.

We've also seen IED tactics and techniques used by insurgents increase in sophistication and proliferate globally. Take, for example, the explosively formed projectile that we saw in Iraq has made its way to the Gaza Strip, and recently in Somalia — all tracking back to Iran and Iran-supported organizations. Vehicle-borne IEDs that we've seen in the Middle East, we're now seeing in Mexico. And the use of female suicide bombers — pioneered by the Tamil Tigers in Sri

**Lanka — spread throughout the Middle East, worked its way to Southeast Europe, and most recently have been employed in Somalia and Nigeria. Also, ammonium nitrate-based IEDs — one of our greatest challenges in Afghanistan — are now being employed more frequently in Syria.**

**These threat networks are going to use whatever is cheapest and most available. Today's IEDs are relatively simple, low-tech devices, which routinely use command wire, pressure plates, or radio-controlled triggers. As you know, many readily available components such as circuit boards, cell phones, and simple electronic transmitters and receivers have legitimate commercial uses, but are easily and increasingly adapted into IEDs. If these networks can get their hands on commercial explosives, that's what they are going to use. But I tell you, we face a growing commercial off-the-shelf problem — radio-controlled IEDs, cell phones, circuit boards, commercial fertilizers, propane tanks, and pressure cookers are all being used.**

**In Afghanistan, we've started to see improvised blasting caps made from light bulbs. And, fertilizer-based explosives still remain our greatest threat there. 86 percent of IEDs employed in Afghanistan are homemade explosives, and of those, 83 percent are made with ammonium nitrate derived from calcium ammonium nitrate — a common agricultural fertilizer. This fertilizer and other easily procured, dual-use, ubiquitous, hard to detect components present a strategic advantage to our enemies, and a security challenge to all of us. It is clear to me that every new IED attack — on our forces or at home — builds a sense of urgency across our government to act.**

**The U.S. government and our allies are implementing efforts to identify those who are knowingly providing terrorists and insurgents access to these HME precursors and we will leverage all available tools and authorities of our governments — freezing assets, opening criminal cases, adding people and business to the denied entities list — to combat the HME threat.**

**There is no single solution to defeat this threat. We need to integrate a range of efforts — supported by a collaborative whole-of-governments approach to detect and neutralize threat networks and devices.**

**In the future, devices will likely adopt more sophisticated technology — limited only by one’s imagination. Future bomb makers will 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 materials. 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 likelihood of new and developing technology being applied to IEDs is certain — and troubling. The ubiquitous nature of IED materials, their low cost and the potential for catastrophic results guarantees the IED will remain a threat and main casualty-producing weapon for decades to come. Because of this, it is important that the science and technology community continues to be aggressive in your research, laying the foundation of innovative science and understanding that will become the basis for new and improved technologies.**

**The IED and the threat networks that employ this weapon are a reality of 21<sup>st</sup> century warfare and we must plan accordingly. So, as we look to the future we must ask ourselves, is the IED going to be here for the next decade?**

**The answer is absolutely. The IED is too cheap, too readily available, and too easy to construct. Plus, we have an entire generation of experienced, savvy, smart bomb-makers who know how to adapt and will continue to take advantage of all available off-the-shelf technology —**

**making devices more lethal and harder to detect and defeat. So the answer is yes — the IED is going to be here.**

**The next question that should be asked is — will these threat networks try and attack our forces and our homelands in the future? Again, I believe the answer is yes —terrorists will likely target us and other highly urban, industrialized, and infrastructure dominated societies.**

**So, as we look to the future, the science and technology community must remain focused on the enduring IED threat as the asymmetric weapon of choice. The research you perform today serves as the base for tomorrow’s military capabilities and is critical to maintaining military superiority and societal stability.**

**Now, I would like to discuss a few gaps in our capabilities that I believe this community can help us close.**

**First, and the number one priority of General Mattis, is pre-detonation. Providing our warfighter’s with the ability to cause IEDs to trigger at the time and place of their choosing will greatly improve freedom of maneuver and significantly reduce effective attack rates.**

**The power and cooling requirements for on-the-move pre-detonation have resulted in systems that are too large and heavy for use on tactical vehicles. We are seeking more rugged and efficient high energy systems that permit a significant reduction in size, weight, and power requirements for pre-detonation payloads.**

**Second, we need improved detection. Pressure-plate IEDs have been used frequently and effectively against both dismounted and mounted coalition forces. In order to counter current coalition force counter-IED tactics, techniques, and procedures, insurgents are utilizing low-metal**

**content carbon rod pressure plate IEDs. The devices are made of wood and utilize carbon rods — generally pulled from the cores of D-cell batteries — for contacts instead of metal. This significantly decreases the metallic signature of the devices.**

**Insurgents are also employing complex attacks against our patrolling forces and first responders — using multiple IEDs to obtain mass effect. Because most detect capabilities have short stand-off and high false alarm rates, low metal pressure-plate IEDs significantly restrict the freedom of maneuver of our forces.**

**So, we are seeking single and multi-sensor capabilities that improve the rate-of-advance for IED clearance operations and permit situational detection in tactical operations. Focus areas for development include automated target recognition, false alarm reduction and extending stand-off range.**

**Some of the largest, most catastrophic attacks against coalition forces are with high explosive weight IEDs emplaced in culverts beneath thoroughfares. We have fielded culvert access denial screens, but water flow and manpower-intensive installation requirements make these systems difficult to proliferate in all operation areas. We are seeking an interim solution that can be rapidly deployed to detect culvert tampering. Potential solutions may include unattended ground sensors or airborne capabilities, but they must provide timely, low false alarm rate detection of culvert emplacement activities or culvert IEDs to nearby coalition forces in tactical vehicles or on Forward Operating Bases.**

**Third, as I mentioned earlier, homemade explosives pose the greatest challenge to coalition forces in Afghanistan thus requiring improved ability to locate, avoid, and neutralize these non-standard IEDs. The insurgency has become very skilled at emplacing IEDs and the proliferation**

of homemade explosives has provided them with the opportunity to produce IEDs with larger explosive content.

Although we have laboratory and other stationary detect capabilities, we need eye safe, effective HME and HME precursor detection capabilities for wide area scanning by both mounted and dismounted units in counter-HME operations.

Forth, and finally, we need to counter threat networks by enhancing our 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 our domestic security partners. This is only accomplished through a robust and powerful network of partners with whom analytical tools, methodologies, and most importantly, information and intelligence is shared to identify, and then exploit, the vulnerabilities of threat networks.

Today, our warfighters, especially brigade, battalion, and tactical level, and analysts struggle to sort 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. It seems each new system requires another stand-alone. We need to develop better techniques to seamlessly share and fuse this data across the attack-the-network enterprise. The key enabler for achieving seamless sharing of information begins with applying new techniques to enhance data processing upon intake. The better we can harvest, sort, and fuse data, the faster our analyst can manipulate this information to produce actionable intelligence for our leaders and actionable evidence for our interagency partners.

Networks are supported by human-infrastructure that behaves like a supply-chain process. Threat networks raise money to fund their activities, procure supplies to build IEDs, transport the

**raw and finished materials, and distribute these materials across borders. To counter the threat network activities, we need to affectively identify, and then attack, the various parts of this chain of events. I believe central to the survival of these threat networks that employ IEDs, and the most vulnerable part of the supply chain, is money. Now, and in the future, mapping the financial networks of our adversaries is what will allow us to take action. Follow the money — money trails don't lie. This makes financial intelligence a uniquely effective source to attack on threat networks and a skill we must grow in the future.**

**We must improve 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 our ability to produce faster analytical assessments of emerging operational environments to support rapid exploitation.**

**Moving forward, many of our current research and development interests will remain of interest in the future. My challenge to you is to consider and understand our long-term capability requirements, which all emphasize the future, adaptive and universal IED threat, and use this to stimulate your research objectives. I encourage you to look for the yet to be discovered and find the keys to the phenomena that will enable us to detect and neutralize this weapon of strategic significance.**

**In closing, if you leave here today with only one take-away — it's that the IED threat is global, growing and it is enduring. Peter Singer of the Brookings Institute caged it correctly when he said, and I quote, "when it comes to how we think about IEDs, we need to face facts — threats evolve — even improvised ones."**

**We are operating in an IED environment and that is not going to change anytime soon. Ensuring our commanders have freedom of maneuver now, and in the future, is critical. Maintaining a robust science and technology program is critical to defeating the adaptive and evolving IED employed by threat networks globally.**

**While no one can predict for certain what the future threat environment will look like — I can confidently say the IED will be a factor in any future operation and a threat to our security at home. Let's prepare now for this enduring threat.**

**Again, I appreciate the Office of Naval Research and its investigators for focusing on the IED threat. The work you do here is extremely important — it's the foundation for future capabilities that will give our forces the strategic and operational advantage they require to combat this evolving asymmetric threat. JIEDDO will continue to strengthen its partnerships with the S&T community through flagship programs such as SAAET. Your work is key to our success at the very basic level. Thank you for all you do and for your time and attention this morning. With the remaining time I am happy to entertain any questions you may have.**