Remarks by

Lieutenant General Michael D. Barbero, U.S. Army
Director
Joint IED Defeat Organization

Current C-IED Operations and Future Priorities

Delivered at
International Armoured Vehicles Conference
Farnborough, United Kingdom

20 February 2012

Good morning. Thank you, Dr. Storr for the kind introduction. Ladies and Gentlemen. I appreciate the opportunity to be here today to share my thoughts, and learn from the other presentations. I am Lieutenant General Michael Barbero, the Director of the Joint Improvised Explosive Device Defeat Organization. JIEDDO, as it is commonly known, was established in 2006 to lead the Department of Defense's counter-IED activities. Our organization is singularly focused on the IED problem and we exist to rapidly field capabilities to reduce the effectiveness of the IED.

As such, this morning I would like to:

- **First, update you on the current fight against IEDs and the threat networks that employ them;**
- **Second, discuss the global and enduring nature of this threat and those counter-IED capabilities that must endure;**
- **And third, describe the gaps in our capabilities and the areas for your industries, Nations, and organizations to contribute.**

Let me say up front, I believe the IED, and the networks that employ them, will confront us all as threats, to our security forces and in our homelands, long after our forces transition their current mission in Afghanistan. IEDs are the weapon of choice for threat networks because these weapons are cheap, readily available — largely "off the shelf" — easy to construct, lethal and accurate.

Now, let me first set the stage by discussing today's IED fight and present some trends we are seeing in Afghanistan. IED events have continued to rise. In 2011, there were nearly 16,000 attempted IED attacks compared to 15,000 in 2010 and just 9,300 in 2009, an increase of 42 percent in just two years.

This spike in IED events is, I believe, a result of the surge in troops pushing into the most contentious regions of the country. The surge eliminated the enemy's safe havens and reduced their freedom of maneuver. In response, the enemy has employed IEDs as their primary means to fight.

While the number of IED events are high, our ability to find IEDs and neutralize them <u>before</u> detonation has increased 56 percent since last year and the overall number of effective attacks — those that produce casualties — has dropped by 2 percent over the last 12 months. The devices we see in Afghanistan are:

- **Relatively simple, inexpensive and homemade;**
- **Contain low or no metal content;**
- **Are increasing in net explosive weight;**
- **Detonated by a variety of means: pressure plates, command-wire, radio-controlled, suicide, and vehicle-borne triggers; and**
- **Employed in arrays,**

Of particular concern is the growth in the use of homemade explosives , also referred to as HME, that are often composed of ubiquitous and easily transported fertilizers. More than 80 percent of the IEDs used against Coalition forces are calcium ammonium nitrate-based HME. This legally produced fertilizer and other dual-use components present a true off-the-shelf advantage to our enemies and a security challenge to all of us.

For example, one bag of calcium ammonium nitrate costs around $30 U.S. dollars and produces six to eight IEDs. We have also seen these ammonium nitrate-based IEDs used globally as a weapon in our homelands — Pakistan, New York, Oslo, and Mumbai — with increasing regularity.

We have invested billions of dollars to combat a weapon — this HME-based IED — that costs the enemy only hundreds of dollars to make. The cost differential is astounding, and one we cannot sustain. Their business model in terms of cost, speed, agility is crushing ours.

As General John Allen, Commander of International Security Assistance Force stated bluntly, this is a "very tough mission against an intelligent, resourceful and resilient enemy with patience and little regard for human life."

So what are we doing about it?

Within six months, we funded and delivered several types of handheld devices, such as the Beachcomber and Goldie, to detect buried IEDs during dismounted operations. To date, we have fielded 7,382 handhelds with another 3,971 scheduled for delivery over the next 10 months.

Since July 2011, we have invested $58 million dollars to field training sets to pre-deployment training centers and units' home stations. We all know our best counter-IED weapon is a well-trained soldier, so it is critical we spend the money to ensure our operational forces are up to speed on the full-range of available counter-IED tools and the latest training before they deploy.

Early detection saves lives. JIEDDO is in the process of fielding eight additional airborne sensors to detect a specific IED triggering capability, and to detect HME precursors, and we currently have three airborne and ground-based hyper-spectral imaging systems with an additional four scheduled for delivery in the near future.

Additionally, we have fielded new modified mine rollers and culvert denial systems, and are operationally testing lightweight reconnaissance robots, man-portable line charges, and other pre-detonation systems for future rapid deployment.

But before I move on to my next topic, let me leave you some take-aways from the current fight.

- **HME/CAN is a significant threat to the safety and security of our deployed forces and to our homelands. We must address this threat;**
- **We need lighter, more integrated capabilities — sensors, jammers, pre-detonation systems — that are integrated at birth and not lashed together as an afterthought;**
- **We must understand how new technology can be exploited by the enemy and develop countermeasures up front;**
- **And, finally, of particular interest to this assembly, we can't armor our way out of this fight. By increasing the size and weight of our vehicles limits their operational effectiveness and insurgents are simply increasing the net explosive weight of devices. We must return to a balance of lethality, survivability, and off-road mobility in future vehicle families.**

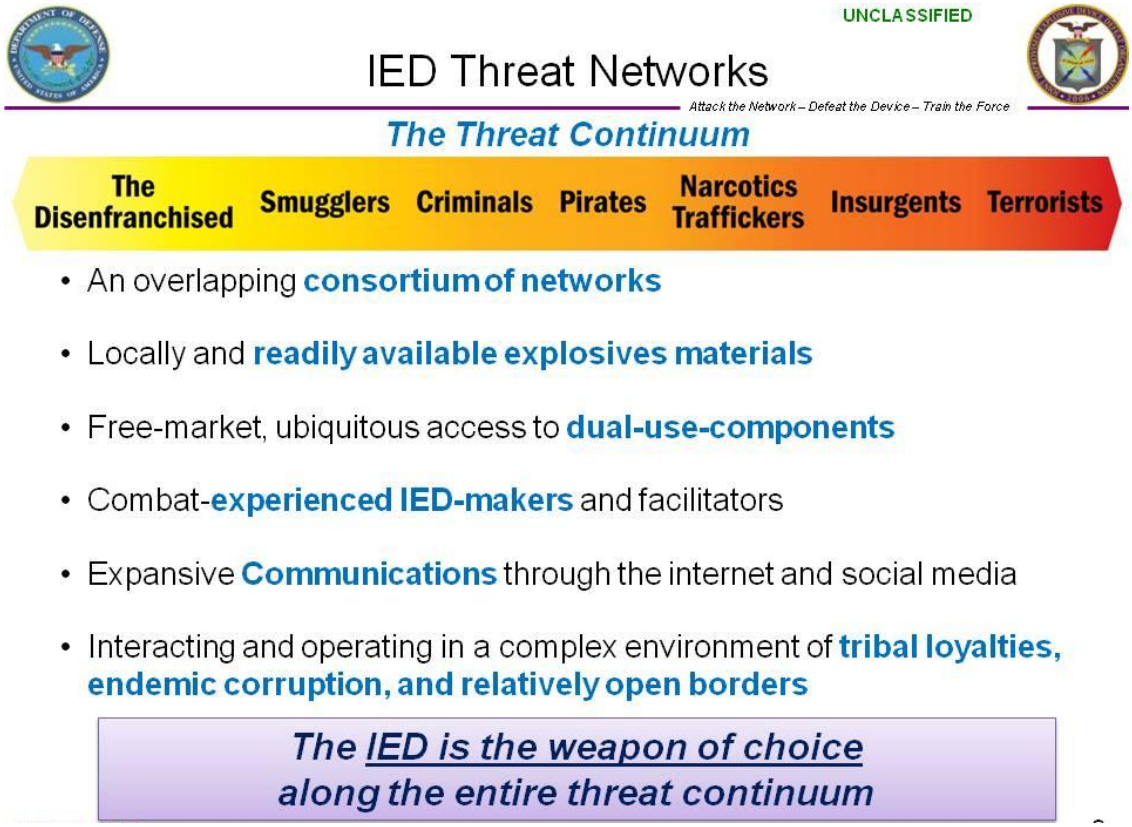
Now let me move on to the bigger picture and the threat we will undoubtedly encounter for decades to come — the global and enduring IED threat. As you probably know, IEDs have been employed with devastating effects around the world with more than 600 IED attacks occurring <u>outside</u> of Afghanistan on a monthly basis.

From January 2011 to January 2012, [outside of Iraq and Afghanistan] there were 7,492 global IED events occurring in 112 countries, executed by more than 40 regional and transnational threat networks.

IED's have been used as a strategic weapon in a variety of situations including:

- **<u>Conflict and post-conflict environments</u>;**
- **<u>Illicit drug operations</u>;**
- **<u>Insurgencies</u>;**
- **<u>Political violence</u>;**
- **<u>Religious crises</u>;**
- **<u>Ethnic conflicts</u>;**
- **<u>And other acts of terrorism</u>**

— All aimed at causing casualties, creating the perception of insecurity, and influencing the will of our nations.



The IED <u>is the weapon of choice</u> for the overlapping consortium of networks that operate along what I call the threat continuum — criminal, insurgent and terrorist alike.

Though usually addressed in a regional context, the threat is much more complex and transnational in nature, representing layers of interdependent, interconnected global networks and support systems.

As a window into the future in which we will confront a convergence of transnational threats, we should study what we see in the Afghanistan-Pakistan region. In the networks that support, supply, and employ IEDs in Afghanistan we see the following characteristics:

- **The nexus of narcotic, criminal, insurgent, and terrorist networks;**
- **Supported by the easy flow of dual-use components;**
- **Passed through legitimate businesses;**
- **Composed of locally and readily available explosive materials;**

- **Executed by a generation of combat experienced IED makers and facilitators — all interacting and operating in a complex environment of tribal loyalties, endemic corruption, and unsecure borders.**

We see similar situations in Colombia, Nigeria, and Somalia. Investigators in Thailand believe they have found a link between blasts in Bangkok and New Delhi that occurred last week. As Peter Singer of the Brookings Institute recently wrote, and I quote, "We need to stop visualizing the weapon as a tool only for insurgents or groups affiliated with al-Qaida or the Taliban."

We will continue to be confronted by these interdependent, interconnected global networks in the future. These threat organizations are seamless, overlapping and <u>not</u> confined by geographical or jurisdictional boundaries. These threat networks are viruses that breed and flourish in a climate of instability.

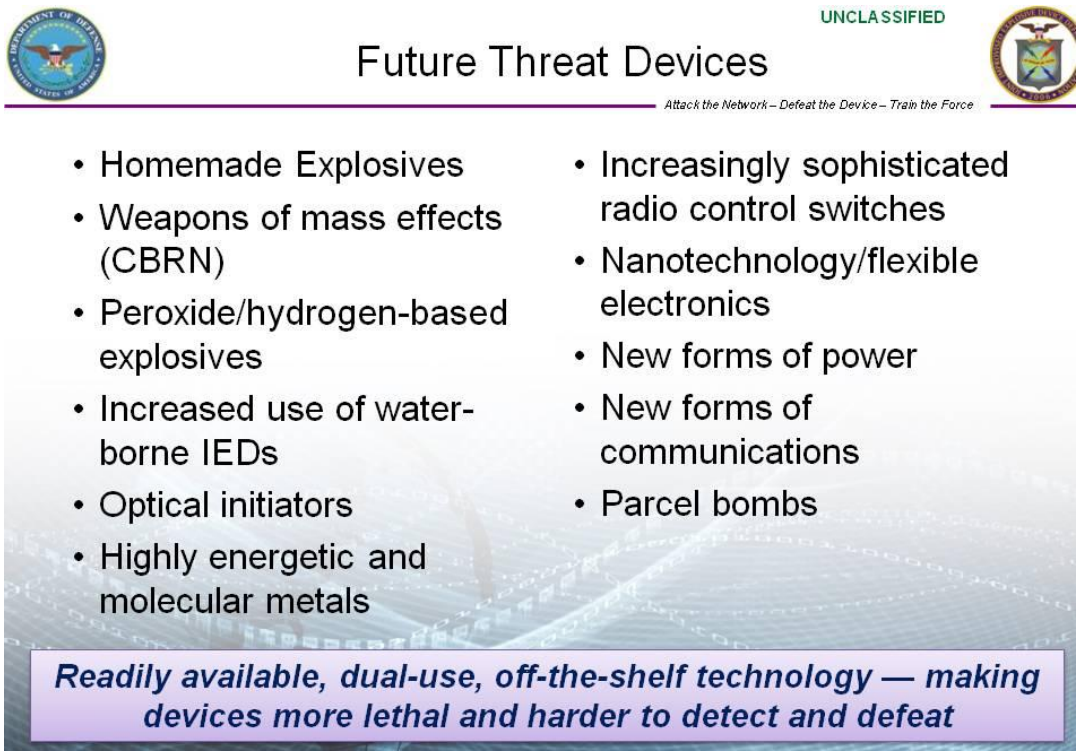
Globalization, the internet, and social media have extended the transnational reach of these organizations, allowing threat networks to easily spread IED technology.

We have seen the tactics and techniques used by insurgents in one area of the world increase in sophistication and proliferate throughout that region and into other regions. For example:

- **Explosively formed projectiles technology and bomb-making skills transferred from Al Qaida in Iraq to Al Qaida in the Arab Peninsula to Al Shabaab in Somalia;**
- **Mexican Drug Trafficking Organizations are employing vehicle-borne IEDs — a TTP that was used in the Middle East;**
- **Homemade sticky bombs we saw in Iraq to attack Iraqi government and Security Force Leaders are being in high profile attacks and assassinations recently in the news — Tehran, Georgia, and Bangkok;**
- **And, the use of female suicide bombers was pioneered by the Tamil Tigers in Sri Lanka, was picked up by various groups in the Middle East, has worked its way to Europe — the Balkans and Chechnya — and have been used most recently in Somalia and Nigeria.**

The interaction of these fully networked organizations is enabled by the latest information technologies including the internet, social media websites, web-based video conferencing and other virtual applications that provide a platform for recruiting, technical exchanges, training, planning, funding and social interaction. While <u>we</u> build our command posts, operational centers and training venues with brick and mortar and millions of dollars, <u>their</u> "centers of excellence" are all virtual, flat and unencumbered.

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.



In the future, devices will 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, WiFi, and broadband; optical initiators; and highly energetic and molecular 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 in the future <u>is certain</u> — and troubling. Threat networks will take advantage of all available "off the shelf" technology — making devices more lethal and harder to detect and defeat. <u>We must be ready to meet this challenge!</u>

As new counter-IED techniques and tactics are employed by our security forces, the enemy is adapting and evolving <u>their</u> tactics, techniques, and procedures. Make no mistake, <u>this is an arms race</u>, but instead of years it takes only weeks to months for our adversaries to adjust and field new capabilities.

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 neutralize threat networks and devices.

As the great British Soldier J.F.C. Fuller said, I quote, "no new weapon can be introduced without changing conditions, and every change in conditions will demand a modification in the application of the principles of war." The strategic effect of the IED has changed the battlefield, and domestic security — it is our responsibility to adapt to mitigate these effects — to change our business model — now and in the future.

I believe this conference, and other like venues, are important to remind us that as we execute the drawdown in Afghanistan, we must ensure that neither budget pressures nor "war fatigue" cause us to lose our focus on the enduring and global IED threat and the networks that employ them. But, we must be smarter, more agile and efficient in our approach.

While introducing the Smart Defence concept in February, NATO Secretary General Rasmussen said it best I quote, "In an age of austerity, we cannot spend more, but neither should we spend less. So the answer is to spend better…" While Smart Defence is a NATO initiative, the concept of seeking multinational solutions is beneficial to all international partners. The enduring and evolving nature of the global IED threat requires not just continuous and adequate resourcing over time, but greater collaboration and smarter resourcing.

To defeat the threat, we must continually identify likely capability gaps, their potential solutions, and develop common and interoperable responses to address these future challenges.

Enduring Capabilities

Attack the Network – Defeat the Device – Train the Force

- **Rapid Acquisition and Fielding** to respond to changes in the IED threat
- **Operations-Intelligence-Information Fusion and Analysis** to support operational commanders to Defeat-the-Networks
- **Training** to standardize for Counter-IED and Defeat-the-Network
- **Weapons Technical Intelligence** to analyze and exploit emerging devices and networks
- **Whole-of-Government(s) Approach** to maintain a coalition of counter-IED partners

An enduring threat requires enduring capabilities

As we look to the future, and the requirement to sustain counter-IED efforts, I believe there are five overarching capabilities that need to endure for my nation.

First, we must maintain the ability to rapidly provide counter-IED materiel and non-materiel solutions in response to changes in the IED threat. We must maintain a higher level of institutional agility and leverage the capabilities of our allies.

To aid in rapid response, we should look to you, our international partners and industry, for already demonstrated technologies. We must maintain this rapid acquisition capability in the future and share new capabilities and emerging technologies with our partners and across the security community.

The second capability that needs to endure is our ability to fuse operational information and intelligence, from all sources, in order to produce actionable intelligence — analytical products that meet the needs of our operational commanders and ensures security at home. 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.

Since IEDs are a global and enduring threat, that not only impact areas of operations but also affect us within our own borders, we must think differently and expand our community of action to empower all domestic and international partners with the ability to share and fuse information. We are all confronted by the same global set of networked enemies. So, we need to remain networked in our efforts to defeat them in the future.

Third, we must maintain our ability to train our forces. Counter-IED and Defeat-the-Network training must endure and be permanently integrated into our individual Service training institutions and centers. We can provide the best counter-IED capabilities to the warfigher, but without the timely and relevant training component, the full capacity of equipment and tactics will never be realized. We need you, industry, to develop training simulations that prepare our forces for this IED environment. We need training enablers from you that incorporate and reflect this new reality — the IED battlefield.

The fourth enduring capability we must maintain 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, often referred to as WTI. This capability provides U.S. and allied forces a powerful, multilevel, systematic process to collect information and materials from sites, exploit it and produce analytical outputs which mitigate the threat and get at the crux of the problem — the enemy network.

WTI builds knowledge of the networks through DNA, finger prints, and device technical signatures. For example, finger prints are collected as part of IED evidence are enrolled in a Defense Department database. In February, an overseas military base was running a volunteer background check on an applicant and submitted his finger prints for screening. The applicant's

prints matched those collected as part of IED-related evidence and he was detained. This highlights the importance of biometrics collections — it removes their greatest defense — anonymity.

<u>Fifth, and finally</u>, as I mentioned earlier, the enduring global IED threat requires a whole-of-governments approach. We must synchronize counter-threat network capabilities and actions among national, international and other counter-IED stakeholders.

Recognizing the significant threat HME poses to coalition forces in Afghanistan; JIEDDO established an HME Task Force to synchronize intelligence, operations and policy development across the multinational, U.S. interagency spectrum. Understanding that no single U.S. department or international partner has the ability to limit access to the precursors flowing into Afghanistan — the solution requires integrated efforts and leveraging the combined authorities, policies and capabilities of many agencies of our government and international partners.

For example, the U.S. Department of Commerce's Export Administration Regulations establishes a process which stops U.S. companies from trading with entities — companies, organizations, persons — that violate U.S. export laws. Commerce can start criminal proceedings against these entities by working through the U.S. Department of Justice.

In October 2011, 15 parties, located in China, Hong Kong, Iran and Singapore, were added to the Entity List for sending IED components to Iraq and Iran. Additionally, the U.S. Department of Justice indicted five people and four companies for fraud conspiracy involving the export of U.S.-origin components to Iran that were later found in IEDs in Iraq. This is a perfect example of how we are applying the various authorities of our interagency partners to the fight against IEDs.

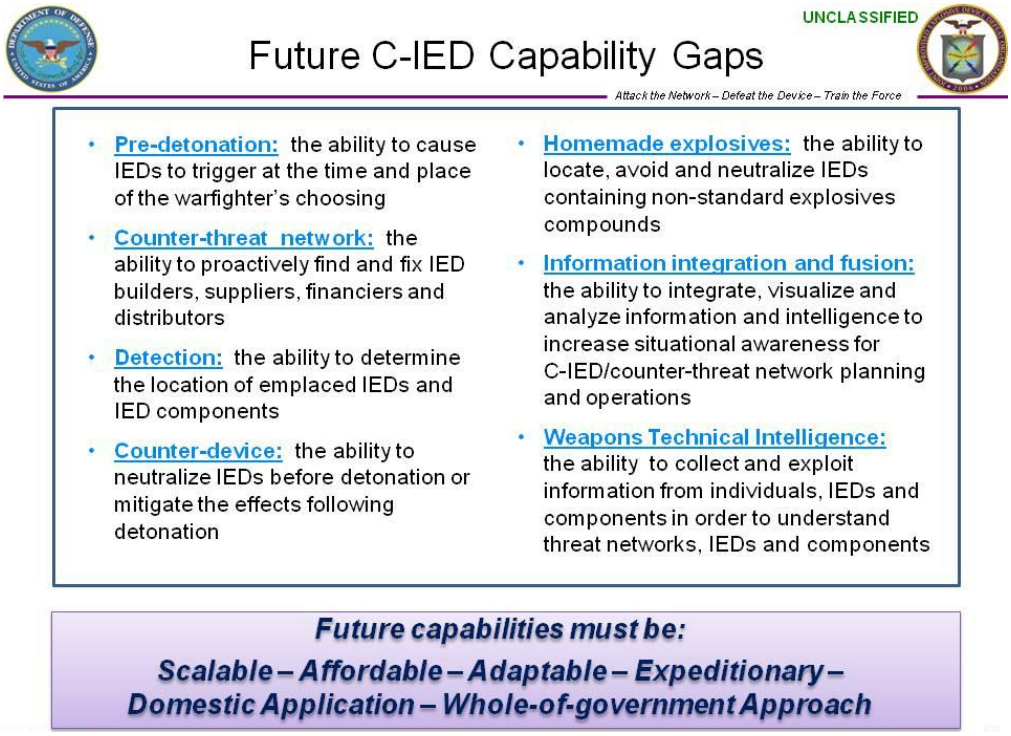
While breaking down the bureaucratic barriers has been challenging, processes and networks such as our interagency task force are essential to a successful whole-of-government

approach. We must think differently about this threat and establish interagency, multinational networks to defeat these threat networks.

These five essential enduring capabilities —

- **Rapid acquisition and fielding;**
- **Operations-intelligence-information fusion;**
- **Counter-IED training;**
- **Weapons technical intelligence;**
- **And, a whole-of-government(s) approach**

— are synergistic and provide a comprehensive response to a complex and dynamic threat. It takes a network to defeat a network.



Still looking toward the future and of interest to this audience of international business and research and development leaders, I would like to briefly mention some future capability <u>gaps</u> we have identified. We are harnessing the potential of this community and our industry partners to close these gaps.

Many of our current R&D interests will remain of interest in the future —

- **Pre-detonation;**
- **Detection;**
- **Homemade explosives mitigation;**
- **Information integration and fusion;**
- **Weapons technical intelligence; and**
- **Counter-network and counter-device capabilities.**

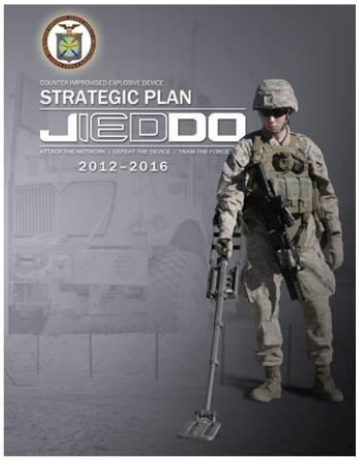
We are casting a net to harness and accelerate the most promising counter-IED solutions to combat the ever-evolving threat. I challenge you to review the specific details of these R&D gaps and apply your considerable resources to finding relevant solutions that can be applied to current capabilities as well as new innovations.

Moving forward, we will work diligently to close these future capability gaps by engaging the public and private R&D sectors to refine capabilities and develop new systems, technologies, and tactics. .

I want to make it clear to industry — the U.S. is at a strategic turning point after a decade of war. We are confronting very large budget challenges and adjustments. Our challenge is to meet future threats, and at the same time meet our responsibility to fiscal discipline. While we will continue to invest in research and development, all future capabilities must be scalable, <u>affordable</u>, expeditionary, and have domestic applicability.

Counter-IED Strategic Plan

Extends focus beyond current operations and establishes an azimuth for future and enduring C-IED capabilities



The strategy can be found at www.jieddo.dod.mil

My organization has recently released a Counter-IED Strategic Plan that extends our focus beyond current operations and establishes an azimuth for the development of future and enduring counter-IED capabilities. I have made copies of the executive summary on the table in the back of the room, but you can obtain the entire strategy on the JIEDDO website [www.jieddo.dod.mil].

<u>In closing</u>, the very wise Sir B.H. Liddell-Hart said, and I quote, "History shows us that no entirely new weapon has radically affected the course of any war; that the decisive weapon in a war has always been known, if but in a crude and undeveloped form, in the previous war."

If you leave here today with only one take-away — it is that the IED threat is global and it is enduring. We can't take our eye off of this threat as we draw down in Afghanistan. We must continue to coordinate our efforts and maintain the hard-earned counter-IED experience we have acquired during these last 10 difficult years.

We cannot allow hard-won counter-IED capabilities to attrite in this environment constrained by diminishing resources. While no one can predict for certain what the future threat

environment will look like — I can confidently say that the IED will be a focal point in any future operations.

In the 20th century, artillery was the main casualty producer on the battlefield. I believe "The IED is the artillery of the 21st century." I appreciate your time and attention this morning. Thank you.