Notes:
1. Below are informal notes taken by a JHU/APL staff member at the Seminar.
2. LTG Barbero used very detailed viewgraphs which can be downloaded from the Video Archives along with video and audio versions of the Seminar.

Introduction
LTG Barbero noted that he is often considered General Buzzkill since the questions he is asked to cover have such negative answers. The nature of the IED threat is a daunting challenge. He also mentioned that this talk would be his last official function since he would be retiring at the end of the week.

What is an IED?
- Weapon of choice for threat networks everywhere
- Involves a device placed or fabricated in an improvised way
  - Incorporating destructive and lethal chemicals
  - Designed to destroy people and infrastructure
- Used for many purposes by insurgents
  - Tactically: to maim or kill people
  - Operationally: to disrupt freedom of movement / create perception of insecurity in the population
  - Strategically: influence the will of nations
- Have great potential for creating atmosphere of fear / uncertainty as seen after
  - Boston Marathon bombings most recently
  - Madrid railroad bombing in 2004 that lead to a government’s fall and early withdrawal of Spanish troops from Iraq
- NCO in Afghanistan: “The IED is not on the battlefield; it is the battlefield.”
- Components of an IED
  - Explosive filler – military/homemade (fertilizer)/commercial (fireworks)
    - 80% Afghanistan IEDs use homemade explosives, mostly fertilizer
  - Switch – arming switch, command, plunger, pressure plate, radio control
  - Initiator – blasting cap, etc.
  - Power source – usually battery (buried underneath components making it hard to detect)
- Container – pipe, pressure cooker, non-metallic (increasingly in Afghanistan using ubiquitous plastic oil jugs as the container of choice)
- Enhancements – nails, scrap metal, toxic materials, chem-bio agents

**History of the IED – Perception vs. Reality**

- Often seen as modern concept because of prevalence in Iraq/Afghanistan
- Terminology is new – concept is not
  - Militaries have always found ingenious ways to use explosives
  - Blurry line between historic IEDs and military use of mines
- Booby traps and military demolitions designed/used by the military against intended targets are not considered IEDs
  - Similarities are obvious
  - Development of capabilities have been in parallel
- World wars spur technological advancements
  - Explosives – more powerful (TNT); new types (plastics such as C-4)
  - Advances in battery power / radio controlled initiators (key fob car starters)
- 21st century brought larger, more varied attacks designed for strategic impact
  - Waterborne – USS COLE
  - Suicide IEDs – September 11th
  - Ammonium nitrate – Oklahoma City
  - Madrid train bombing
- Tactical difference between past and current use of IEDs
  - Past: IEDs were secondary/complementary weapons designed to channelize an enemy into a kill zone – making other weapons more effective
  - Today: IED is weapon of choice, causing the majority of casualties, where opponents use direct fire to lure US troops toward IEDs

**The Current Fight**

- Another reminder of IED lethality: death of three more troops in Afghanistan today
- Chart in the slide below brings out the current status of the fight
  - Red columns show the monthly total of IED events in Afghanistan
  - June 2012 was the worst month but rates have been falling since then
  - 2011 overall had the most IED events (>16,800) with 2012 not far behind
  - White line shows causalities
- Some say that as the number of boots on the ground decrease so will the IED threat
  - But statistics do not sustain that argument – no proportional changes seen
    - 7% decline in IED events vs. 32% drop in troops on the ground
- Good news caused by many background factors:
  - Ability to identify/neutralize IEDs before explosions increased for 15 months
  - Causalities over the last 2 years have dropped by 50%
- 60% of causalities still come from IEDs making them the artillery of the 21st century – the greatest causality producers
- Attacks on Afghan Security Forces are increasing because they are in the lead in the fight but they are vulnerable
Homemade explosives are used in 80% of IED events
- 56% based on calcium ammonium nitrate (fertilizer produced in Pakistan)
- Potassium chlorate coming from Pakistan is used in an increasing percentage

Bottom line: IEDs have been and continue to be the weapon of choice because they are relatively cheap, easy to assemble with easy to get parts, and they work

Things known (see purple boxes in above chart)
- Tough fight –started a little late this year because of the poppy harvest
- Smart, determined enemy even if not well educated, tactically savvy, agile
- Must fight this weapon of choice during transitions:
  - US forces moving to an advising / assisting role
  - Afghan security forces moving toward taking the lead

Things unknown
- How will current budget pressures play out for funding continued improvements and efforts in Afghanistan?
- What will be the drawdown plan? How fast? Residual number of troops?
- How will Afghan security forces continue to develop their capabilities?
Must remember: Enemy gets a vote on how they will respond to US moves

Global Threat
- IEDs aren’t only used in Iraq and Afghanistan
- It is not just the IEDs that are the threat but also the networks that employ them
- More than 700 IED events happen outside Afghanistan every month
- More than 17,000 IED events since January, 2011
  - In 123 countries by more than 40 regional/transnational threat networks
  - Variations:
    - Delivery methods (roadside/car/suicide bombs)
    - Targets (infrastructure/security forces/civilians)
    - Actors (lone wolves to extremist groups)
- Top five countries outside Afghanistan on average over the last 6 months:
  - Columbia – 917
  - Pakistan – 635 (growing threat from insurgencies and IEDs)
  - India – 312
  - Somalia – 200
  - USA – 172 (reporting is better)

Domestic IED threat is quite real
- Can see from headlines of any given week’s newspapers
  - Reports of pipe/chemical/soda bottle bombs, high school students work
- Time-delay is the most common type of switch used
- Threat networks go after high profile targets – infrastructure, government activities, civilian populations
  - To influence public perception and create atmosphere of fear/uncertainty
- US will usually see more activity by lone wolves but others, too (Oklahoma City, first World Trade Center attack using a vehicle bomb, etc.)
  - Heritage Foundation: 53 publically known terror attacks foiled since 9/11
    - 43 could be called homegrown
  - It is considered an IED event every time a bomb squad is called to a scene,

Global Threat Networks
- Viewgraph below describes the types of networks and their attributes
  - Networks include proselytizing and recruiting through the internet and social media
  - Centrality of money (very important point) including front companies, etc.
  - Components include safe havens and training camps
  - Command & control that is flatter than anything the US has
  - They are learning organizations – more agile, adaptive, and flat than the US is
- IED is weapon of choice
  - Along Afghan/Pakistan border, Somalia, Nigeria, Syria, other global hotspots
  - Convergence of overlapping networks of criminals, smugglers, terrorists
  - Centers of excellence are all virtual, flat, unencumbered (not like US brick and mortar centers involving millions of dollars)
Converges of convenience with criminal organizations
Networks are capable of delivering their threats to the US homeland
Supported by homemade, readily available local materials
  - Example: Carbon rods from D-cell batteries put under pressure plates (just enough metal to complete circuit but not enough to be detected)

- Financing done through licit and illicit companies
- Expansive comms using the internet and social media for C4ISR
- Acting within complex tribal loyalties with an overlay of endemic corruption
- Because so agile, can easily take advantage of opportunities like the Arab Spring
- Bottom line: Their business model is working better than that of the US
  - For $100 in Afghanistan you can buy a bag of fertilizer (calcium ammonium nitrate), pot, water, propane to boil it down/decant it
  - Put that liquid ammonium nitrate out on a tarp for 48 hours to dry it out
  - Crush it and add accelerant to make it more detonable than TNT
  - Result: enough explosive material to make 4-5 deadly IEDs
Bottom line: The US must do better by raising the financial and human costs to the IED threat networks

**Strategic Advantage of Threat Networks**
- Can act virtually and seamlessly while sharing recipes, expertise, tactics, procedures, etc.
- Can use web-based/social media applications provide platforms for video-conferencing, planning, funding, recruiting, etc.
- Internet is their C4ISR
- Problem: How does the US dominate/attack that system?
- Examples of the problem: Hezbollah, (operating in 40 countries on 5 continents) and Al-Qaeda are moving into African hotspots
- US follows Napoleon’s dictum and marches to the sound of guns while these threat networks march toward signs of insecurity and take IEDs with them
  - Can take their centers of excellence with them
  - US tied to its brick and mortar centers costing millions of dollars

**Strategic Challenge and the Flow of the Transnational Threat**
- How does the US counter this transnational threat with its IEDs?
  - How to sort through social media? In different languages? Unobtrusively?
  - How to merge open, proprietary, and classified information?
- Problem: US sees differences between domestic and international issues, but threat networks do not
The slide below provides possible scenarios for IED migration

- Red stars indicate where conflicts are on-going
- Yellow stars indicate regions where conditions are ripe for conflicts
- Combat-experienced IED makers from Iraq and Afghanistan are exporting their skills worldwide
  - Al-Qaeda has become a franchise – into Syria and North Africa
  - IED instructions published on the internet
- Dual-use IED electronics and other components flow freely (blue arrows)
- Easy access to ubiquitous explosive precursors is global (e.g., fertilizer)
- Example: Al-Qaeda in the Islamic Maghreb, al-Shabaab, others share funds, expertise...
  - Al-Qaeda in Iraq is franchising its fighters throughout the region
  - Overall increase in cooperation among the networks in all fields
- Solid red arrows: most likely scenarios for IED spread with confluence of bomb makers, electronics, IED components, etc.
- Dotted red arrows: most dangerous scenarios – could lead to attacks on the US or spillover from Mexican drug violence especially by vehicle borne IEDs (VBIEDs)
- All of this activity is supported by global funding
What the US Is Doing about the Threat

Slide above depicts the many organizations that are working together to defend against the threat:

- Need a *whole of governments* approach – US is working closely with international partners, especially the UK and Australia
- Also must have strong relations among the national labs, agencies, industry, to synchronize counter-threat network efforts including:
  - Identifying networks and key players
  - Locating the licit to illicit cross-over
  - Leveraging all available parts of governments to
    - Freeze assets
    - Open criminal cases
    - Putting people and businesses on denied entities list
- Some of the results of this cooperation are shown on the right side of the slide:
  - When people are put on the UN denied list, the US can go to local governments and ask what they are doing about it
  - When companies are added to Commerce Dept denied entity list, they become radioactive to US businesses
Won’t even get updates for their Microsoft products or GE equipment

- **Bumper sticker:** Collaboration, coordination, and teamwork are needed because “It takes a network to defeat a network ... today and in the future.”
- **Concern:** Today we have troops in harm’s way in Afghanistan, but after 2014 it is unclear whether the necessary level of support will continue
- **Challenge:** How to turn intelligence into evidence for law enforcement purposes
  - Example: Using financial activity as the base for investigations

**Operational Threat Finance**
- Uses traditional and non-traditional data sets
- Results can lead to non-kinetic targeting in direct support of the combat commander
- Not necessarily about going after the money but producing targets that can be handled by non-kinetic means of disruption
- A wide range of material is used to develop the picture including:
  - Open Source
  - Bulk Data
  - Social Media
  - Specialized Access Sources
  - Public Financial Data
  - Targeted Data
  - Encrypted Sources
  - Compartmented Programs
  - Forensic Accounting
  - Auditing / Data Mining
  - Domestic and International Legal Support

- Start with building a common threat enterprise picture then take it apart and identify its vulnerabilities
- This is a good start but more needs to be done

**Centrality of Money**
- The consortium of networks involved in the threat continuum requires financing to organize, recruit, train, equip, etc.
- Disrupting access to financial resources has an impact on all aspects of operations
- Challenges:
  - Everyone does a little, no one does enough or brings it all together
  - Focused on the high-end groups such as Al-Qaeda, not the operational level and their problems
  - Face opaque situations such as the use of Hawala for money transfers
  - US government has no clearly assigned responsibilities nor even clear definitions
  - Overcome the lack of a single database
- If challenges are not met, then US will continue to face gaps, redundancies, and ineffectiveness

Would rather have a forensic financial analyst than any other kind of analyst

**Looking to the Future – Post Afghanistan**
Center for Naval Analyses has done a study on the topic
- Main takeaway: The IED threat will continue both operationally and domestically
• Expect reliance on familiar tactics and devices rather than any major new technical innovation
  o Some advances are expected but none would substantially change the threat
• Bottom line: Wherever the US goes, the IED will follow

Lessons Learned – from both Iraq and Afghanistan
• Must focus on the lessons learned and institutionalize lessons
• Threat networks are:
  o Learning organizations – more agile, flatter than US organizations
  o Operate seamlessly, virtually using the internet and social media for everything from recruiting to fund-raising to planning
  o Challenge: How does the US dominate them?
• Enemy is master of off-the-shelf technologies
  o Uses what is at hand including fertilizer, discarded batteries, scraps, etc.
  o Challenge: How does the US counter this operationally and at home?
  o US must resist returning to pre-2003 methods and develop a true rapid response acquisition process
    ▪ Will need to ask some tough questions about the system
    ▪ What are the authorities? Is funding fungible to allow quick movement into areas that show promise?
• “We are in an arms race”
  o But don’t have years to develop a new ICBM or a radar
  o Have only days or months to make the next move
• Not just a military problem
  o Success against bureaucratically unencumbered enemies requires seamless whole-of-government approach integrating all partners
    ▪ Especially after 2014
• Money is the lifeblood of these networks so need to hit them where they hurt most – in their bank accounts
  o Current efforts are too disjointed and insufficient
  o Need more focus on financial considerations so can apply pressure along the whole threat supply chain
• Lesson re-learned: Training is valuable and must accompany innovation
  o Troopers who don’t see new equipment until it/they arrive in country don’t have time to learn how to use it there
  o Best counter-IED weapon is always a well-trained soldier
• Must continue to invest in capabilities through R&D to counter evolving IED threats

Tactical Game-changers
• Constant surveillance from an unblinking eye from blimps, towers, UAVs
• Forensic bio-metric techniques on the battlefield have been found to be very useful
  o Can remove violent extremists’ greatest asset – anonymity
  o Makes them vulnerable to US retribution
Next Game-changers?

- No silver bullet
- Can't drone strike or armor your way out of the IED threat
- Requires organizations and initiatives working harmoniously to defeat threat networks
  - Complex threats need a comprehensive approach

**Summarizing the problem:** The enemy sees no difference between military operations abroad and in the homeland. So the US must not get tied down with self-inflicted statutory, regulatory, and bureaucratic challenges when going against an unencumbered, agile enemy intent on bringing the fight to the US homeland.

**Question and Answer Session**

**Re: Funding for JIEDDO**

- JIEDDO is funded as part of the war supplemental
  - Considered a temporary organization that will go away in 2014
  - But the threat will remain
- Currently well-resourced with unique authorities
  - Director can sign off on expenditures of up to $25M
  - Programs costing up to hundreds of millions can be handled by a quick staffing process leading to a sign-off by the Deputy SecDef within 10 days
- JIEDDO can reprogram its funding
  - About $280M has been reprogramed this year alone
  - Can move funds from programs no longer needed to areas needing more
  - Organized to and have special processes to do this
  - Important to have this capability in the future
    - Discussions underway to make that happen
- Big question: Does the US keep a coherent capability to stay abreast of the threat at the DoD level in the future?
  - Threat faced by all combatant commanders
  - Alternatively, capability could be broken apart to be funded by the services
  - IDA did a FOUO study showing that the future of many core resources does not look good
  - JIEDDO's primary model has been to find/develop a capability and then hand it off to the appropriate services in 24 months
    - Services pay for it either as part of the supplemental or within their base budgets
    - Has worked well until this year – a couple of the services said they can no longer support $41M worth of programs they had agreed to handle
  - Program of major concern: biometrics on the battlefield (huge database of fingerprints / DNA / iris scans)
    - Considered a major tactical advance
    - Commanders say it is so valuable that they are doing major campaigns just to collect the data
- Program transitioned to the Army but no money has been budgeted
- At a decision point: Budget has been coming down (as appropriate) but also need capability to scale back up rapidly for next 2003 event
- Requirements for the future enduring counter-IED capability:
  - Above all, a rapid acquisition and fielding system
    - Five-year plans, programs of record no longer do the job
    - Must be able to field new equipment in months, not years
    - Concept is to get new innovations to the warrior quickly
  - New innovations must also come with training (biggest gap originally)
  - Weapons technical intelligence – broad umbrella of biometrics
  - Whole-of-governments approach to face off against the enemy’s agile network structure
  - Financial intelligence (more of a cultural capability) to follow the money

Re: Drone Striking / Armoring Out of the Problem
- Drone strikes are like crack – feels good at the time but won’t stop the networks
  - Taking out key leadership does have an effect
  - But there are still networks of suppliers left untouched
- Can’t armor our way out either since 3 lbs. of explosives can do so much damage
  - Laws of physics have limits
- Consider this much like going after a crime network
  - Al Capone was taken down for tax evasion
  - So if could find the licit companies which are knowingly or unknowingly involved can put pressure on them with government/public efforts
    - FBI and the Treasury Department are the closest partners here
  - Won’t be decisive but need to go after the network at every point

Re: Tactical Approach
- Start by focusing on the device
  - Reduce casualties
  - Gives commanders more room for action
  - Improve ways to find the devices
- Must train the force in the field and get lessons learned out to them quickly
- Attack the network even though it is hard and complex but it is decisive
- Domestically, much the same
  - Must respect US laws about collection on the American population
  - Laws are not roadblocks but guardrails so should not stop efforts
- DoD needs to work harder at being able to turn intel into evidence
  - Have been trying to do so in Afghanistan but have hard time getting to releasable products which then are often of questionable value
  - Need more training and better working methods with interagency partners
    - Huge databases need to be worked
    - Now includes social media, too
- Law enforcement partners cannot be so insular
  - Redefine what a crime scene is (to include Facebook pages of bombers?)
• Must be able to get there quickly before too many others come in and corrupt that virtual crime scene
  o Need to be less protective with more sharing
  o Mostly a cultural challenge along with technical issues such as how to combine data bases
• How do we go about working with non-traditional partners especially financial institutions
  o They are willing to help with tracking the networks through money
  o Must have a focal point in government and someone in charge of the effort
  o Can be done

Re: Terrorist and Chem/Bio Weapons
• Terrorist networks currently rely on explosives rather than threats people can’t see because what they are doing works for them
• Terrorist networks are known to want chem/bio weapons especially if they could combine them with an IED
  o Just a matter of time before they do get some such capability

Re: JIEDDO's Future
• Would recommend that JIEDDO stays together to coordinate all the work going on
• DoD will make the final decision and that is being investigated at the moment
• Two possible courses of action:
  o Scale it down with ability to ramp up when necessary since it will already have maintained the data to know what to target
  o Disaggregate it and let the services handle different parts of the problem
    ▪ LtGen Barbero believes this to be the less desirable choice

Re: What Other Authorities Should the Next Director, JIEDDO Have?
• Primarily related to domestic issues
• JIEDDO already can support combatant commanders quite well
• JIEDDO cannot do the same for homeland law enforcement or other federal agencies but maybe it should
  o Especially given that the enemy sees no real difference between attacking abroad or in the US homeland
  o If troops in Afghanistan have handheld devices to detect ammonium nitrate, why shouldn’t cops on the beat at home?
• Need to break down the barriers between DoD and homeland agencies
  o JIEDDO already has liaisons with FBI and helps run part of their forensic lab
  o Improved relations could be worked through Northern Command
    ▪ It is their responsibility to translate DoD capabilities into something useful to domestic security
Re: Leadership
- Combatant commanders understand the problems but they have many other competing requirements
  - Not a cynical effort – they just weigh their requirements differently
- It is not a finished process – still institutionalizing efforts
- JIEDDO has adapted – just not fast enough

Re: Cyber, Other Innovations and IEDs
- Expect the enemy to try all options
- CNA study showed that enemy networks are interested in CBR / other innovations
  - Devices: WiFi and laser triggering, ways to defeat jammers, etc.
  - Delivery methods: micro UAVs, ground robots, etc.
  - Need to find things that are cheap and work for them
  - US needs to raise the enemy’s costs of doing business (financial / physical)
- Terrorists have not yet employed these means because they really don’t need to
  - They use what they have and what works for them
- Can expect a combination of cyber and IEDs at some point

Re: JIEDDO and Armor
- There has been a significant effort to develop armor against IEDs but it has been part of the program to understand and target the networks
- Big effort at pushing as much down to tactical commanders as possible
- Using persistent surveillance to understand patterns of life so can distinguish between farmers and terrorist laying IEDs
- Armoring/improvements to vehicles was part of the comprehensive approach
  - Laws of physics limit what can be done

Re: Psychological and Public Information Efforts
- JIEDDO does not do anything in these fields
- State Department has some public information efforts
- Pakistan has recently asked JIEDDO for US government help with a public information campaign

Re: Relations with State Department and USAID
- JIEDDO takes its lead from the combatant commanders to identify what is important
- JIEDDO should be given authority to use some of its funding for other agencies work
  - Mostly for domestic efforts
  - 2013 Budget provided $15M for any interagency effort to impede the flow of IED materials from Afghanistan and Pakistan
    - Could include training of border guards, public information programs supported by the State Department
    - Have five proposals to consider this year
- There should be more efforts since it takes a network to take down a network
  - Changes need to be made financially but most work needs to be a change in cultural issues