Attack the Network – Defeat the Device – Train the Force

The Global and Enduring IED Challenge
John Hopkins Rethinking Seminar

LTG Michael D. Barbero
Director, Joint IED Defeat Organization

May 14, 2013
IEDs Are the Weapon of Choice

**What is an improvised explosive device?**

- A device *placed or fabricated* in an improvised manner
- Destructive, lethal, noxious, *pyrotechnic or incendiary*
- Destroy, incapacitate, harass or distract
- May incorporate military or commercially available explosives, or consist of homemade explosives, such as fertilizer

**IEDs are used for multiple effects:**

- **Tactically** to maim and kill
- **Operationally** to disrupt freedom of movement and create the perception of insecurity
- **Strategically** to influence the will of our nation

“...The IED is the battlefield!”
IEDs: Perception vs. Reality

- IEDs are perceived as a modern phenomena associated with conflict in Iraq and Afghanistan
- Terminology is new — concept is NOT
- Huge technological strides during and between World Wars
  - More powerful explosives (TNT)
  - Plastic explosives (C-4)
  - Battery improvements
  - Radio-controlled explosive initiators
- Increasingly devastating and larger-scale attacks in 21st Century
  - Designed for strategic effects
  - Conducted by a wide range of organizations and individuals

Train Bombing
Madrid, Spain, 2004

Suicide IEDs
World Trade Center, 2001

Water-borne IED
USS Cole, 2000

Ammonium nitrate IED
Oklahoma City, 1995

Wall Street Bombing, 1920

Lockerbie Bombing
Pan Am Flight 103, 1988
Current Fight — Afghanistan

15 April 2012 to 15 April 2013

IED TRENDS
• IEDs = most significant threat
• Only 7% decline in IED events despite 32% decrease in boots on the ground
• Found & cleared rates have improved for 15 months

CASUALTIES
• Casualty-causing IED attacks continue to decrease, but still account for 62% of all U.S. casualties
• Attacks on Afghan National Security Forces are climbing (up 45%) as they take lead in operations

HOMEMADE EXPLOSIVES
• 80% of IEDs use HME as the main charge
  • 59% ammonium nitrate
  • 36% potassium chlorate
• HME seized increased 62%, 114 tons total

What we know:
• Tough fight ahead
• Smart and determined enemy
• Whole generation of bomb makers
• IED weapon of choice
• Two critical transitions

What we don’t know:
• Effect of budget pressures
• Deployed troop strength & drawdown timeline
• Development of ANSF capabilities
• Evolution of the threat
The IED is a Global Threat

More than 700 IED events occur each month outside Afghanistan
Domestic Threat is Real

Apr. 29, 2013, EDISON, N.J. – Police seize powerful bombs, shotgun shells from Edison High School student

Apr. 30, 2013, SATELLITE BEACH, Fla. – Florida man sleeping in car at closed park found with bomb, bomb-making materials in his car

May 2, 2013, MYRTLE BEACH, S.C. – Suspected bomb materials found in Myrtle Beach home

May 2, 2013, NEWPORT, Vt. – Soda bottle explosives found at Vt. home

May 2, 2013, YELLVILLE, Ark. – Sheriff: 13 Homemade Explosives Found at Felon’s Home During Scuffle

Apr. 29, 2013, NAMPA, Idaho – Nampa Police warn public about homemade chemical bombs

Apr. 30, 2013, MARIETTA, Ga. – Police help clear dead man’s house by removing explosive device

May 1, 2013, AUSTIN, Texas – Explosive device found in alleyway

May 1, 2013, GERMANTOWN, Wis. – Bomb squad removes explosives from home after Germantown man arrested

May 2, 2013, SUN VALLEY, Idaho – BREAKING: More Explosives Found in Blaine County

May 3, 2013, BOSTON, Ma. – Official: Boston bomb ploy had been set for July 4th

The United States remains one of the top five countries for IED activity — with more than 170 IED events during the past six months
Global Threat Networks

- Transnational, overlapping consortium of networks
- Locally and readily available explosives materials
- Free-market, ubiquitous access to dual-use-components
- Combat-experienced IED-makers and facilitators
- Financing to organize, recruit, train and equip
- Expansive communications for training and recruiting through the internet and social media
- Interacting and operating in a complex environment of tribal loyalties, endemic corruption and relatively open borders
- Planning future operations but takes full advantage of emerging opportunities: Arab Spring, Benghazi, Mali, Syria, Algeria and Nigeria…

The IED is THE weapon of choice for global threat networks
Threat Networks Strategic Advantage

- **PLANNING**
  - Rehearse operations in 3D virtual apps
  - Communicate, conduct business, pass guidance
  - Transfer funds internationally

- **RECRUITING**

- **TRAINING/BOMB MAKING**

- **FUNDRAISING**

- **ATTACKING**
  - FLASH MOBS (Arab Spring)

Their “centers of excellence” are virtual, flat and unencumbered
Transnational IED Threat

Share TTPs on Internet

Financing to organize, recruit, train, etc.

Generation of bomb makers

Ubiquitous chemical precursors

Free flow of dual-use components

Confluence of bomb maker expertise, dual-use components, readily available homemade explosives materials will likely result in intensified IED activity
The global and enduring IED threat must be met with a whole-of-governments approach. This Threat Requires a New Approach

Results

- **United Nations**: UN1988 Designations of 3 individuals
- **US Dept of Commerce**: Added 152 persons to the Entity List because of IED-related matters
- **US Dept of Treasury**: Imposed sanctions on 51 AF-PAK-based terrorist/supporters, 2 specifically for IED-related matters
- **US Dept of Homeland Security**: Global Shield produced 42 Law Enforcement actions and 51 seizures resulting in 140.67 metric tons of precursor chemicals
- **US Dept of State**: U.S.-PAK Working Group; Outreach campaign in PAK
- **US Dept of Justice**: Coordinates domestic C-IED efforts
- **US Intelligence Community**: 6 coordinated assessments; briefings at all level of IA engagement
- **Combatant Commands**: coordinating across regions to track/capture known IED facilitators

**Collaboration — Coordination — Teamwork**

It takes a network to defeat a network … today and in the future
Operational Threat Finance

The Concept:

- Leverage traditional and non-traditional data sets to illuminate disruptive opportunities
- Convert intelligence into evidence
- Fuse threat finance intelligence with larger traditional intelligence methodologies to better illuminate threat networks
  - Open Source
  - Bulk Data
  - Social Media
  - Specialized Access Sources
  - Public Financial Data
  - Targeted Data
  - Encrypted Sources
  - Compartmented Programs
  - Forensic Accounting
  - Auditing/Data Mining
  - Domestic/International Legal Support

The Effects:

- Builds common threat enterprise picture
- Enables non-kinetic action against IED facilitation networks by nontraditional partners
- Prioritizes key IED-related procurement, facilitators, accounts/nodes, and financial institutions
- Enable whole-of-governments pressure on the entire threat network
The Challenge of Financial Intelligence

Today:
• Everyone does a little
• No one does enough
• No one brings it all together

If no change:
• Gaps
• Redundancy
• Ineffective

A difficult challenge — identify the junction point and nexus between money, geography, IED materials, social networks, legitimate entities, government…
Independent Study: The Post-Afghanistan IED Threat

**Overall**
- The IED threat to deployed forces & the homeland will persist.
- The analysis suggests that this threat will largely depend on familiar technology and tactics, rather than innovation and emergent threats.

**Deployed Forces**
- The IED threat to deployed forces will persist.
- Combatant commands are concerned the lessons of OIF and OEF will be exported elsewhere.

**Homeland**
- Likely lines of operation include criminal, isolated terrorist and campaign.

**Technical innovations**
- Technical innovations that could improve IED effectiveness exist, but none appear likely to dramatically alter the IED threat.

**Emergent threats**
- The characteristics of the emergent threats are, in many ways, similar to the characteristics of OIF and OEF IEDs.
Lessons Learned

- Threat networks are agile, flat, learning organizations
  - Operate seamlessly and virtually through social media and the Internet
  - Master of off-the-shelf and dual-use components
- Must resist the inertia to return to pre-2003 processes — need to develop a truly rapid and responsive acquisition process
- The IED is not just a military problem — success requires whole-of-governments approach
- Money is the lifeblood of threat networks, so we must attack them where it hurts most — their bank accounts
- A lesson re-learned is the value of training — innovation requires training
- We must identify and continue to invest in capabilities
- You cannot drone-strike or armor your way out of the IED threat — there is no silver bullet
- Threat networks do not see a difference in overseas military operations and the homeland

These hard-earned lessons learned must be institutionalized and shared with our domestic security partners