Attack the Network – Defeat the Device – Train the Force

Attacking the IED Network

NDIA Global EOD Conference

CAPT Frederick Gaghan, USN

05 May 2011

This briefing is UNCLASSIFIED

Era of Persistent Conflict

Attack the Network – Defeat the Device – Train the Force

- Enemy will focus on irregular warfare using asymmetric means to attack and influence advanced nations
- Conventional, unconventional, lethal, non-lethal, state supported, non-state, hybrid organizations, extremism… produce a very complex environment

The world will be in persistent conflict for generations and the IED will be the weapon of choice for decades

Global IED Incidents: MAR 2009 – MAR 2011

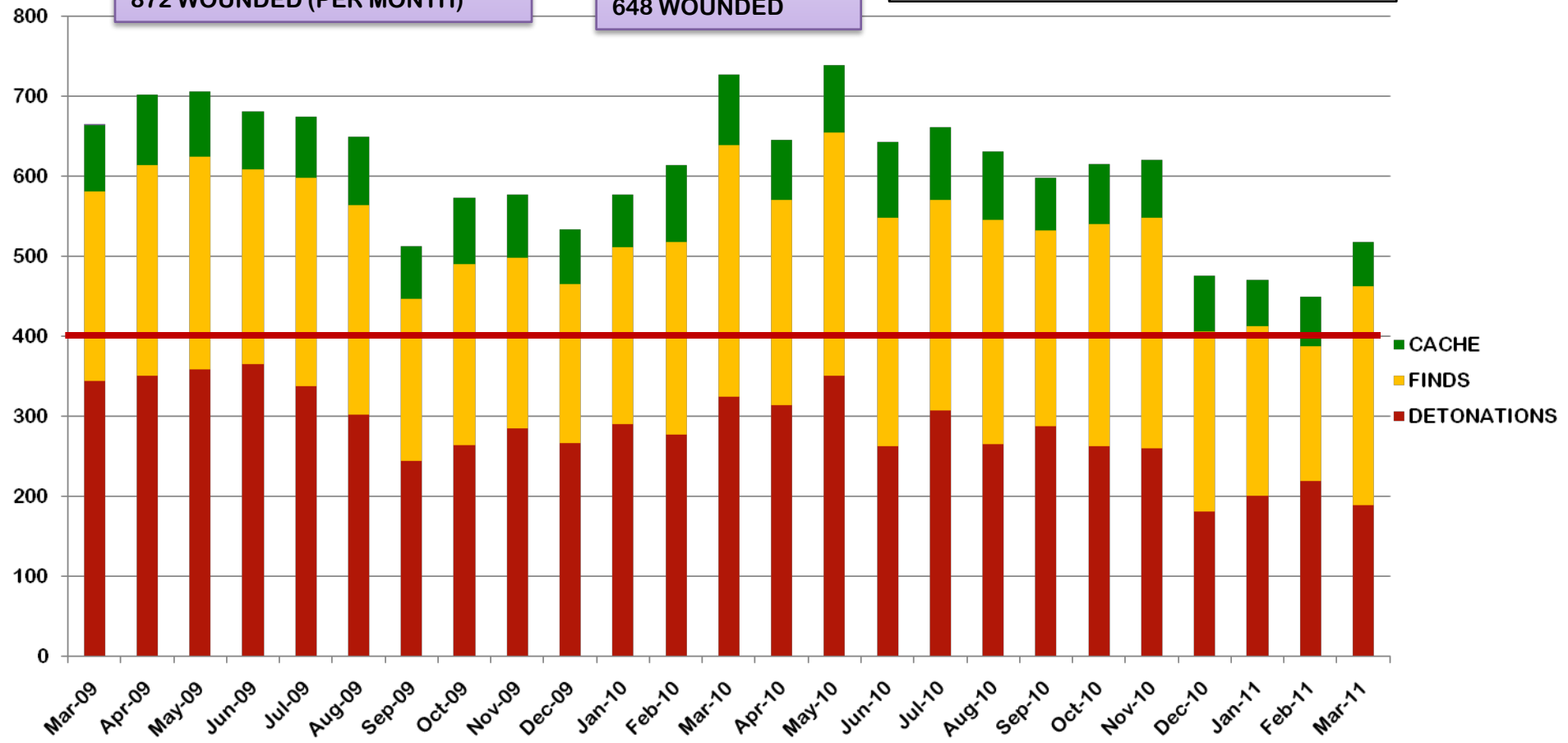
Attack the Network – Defeat the Device – Train the Force

24 Month Average
296 DETONATIONS (PER MONTH)
260 FINDS (PER MONTH)
80 CACHES (PER MONTH)
299 DEATHS (PER MONTH)
872 WOUNDED (PER MONTH)

March 2011
188 DETONATIONS
274 FINDS
55 CACHES
188 DEATHS
648 WOUNDED

LEXICON NOTE

INCIDENTS = DETONATIONS + FINDS
CACHE = FOUND, NON-COMPLETED IEDs, I.E. PRECURSOR MATERIALS (NOT COUNTED IN IED INCIDENT TOTALS)



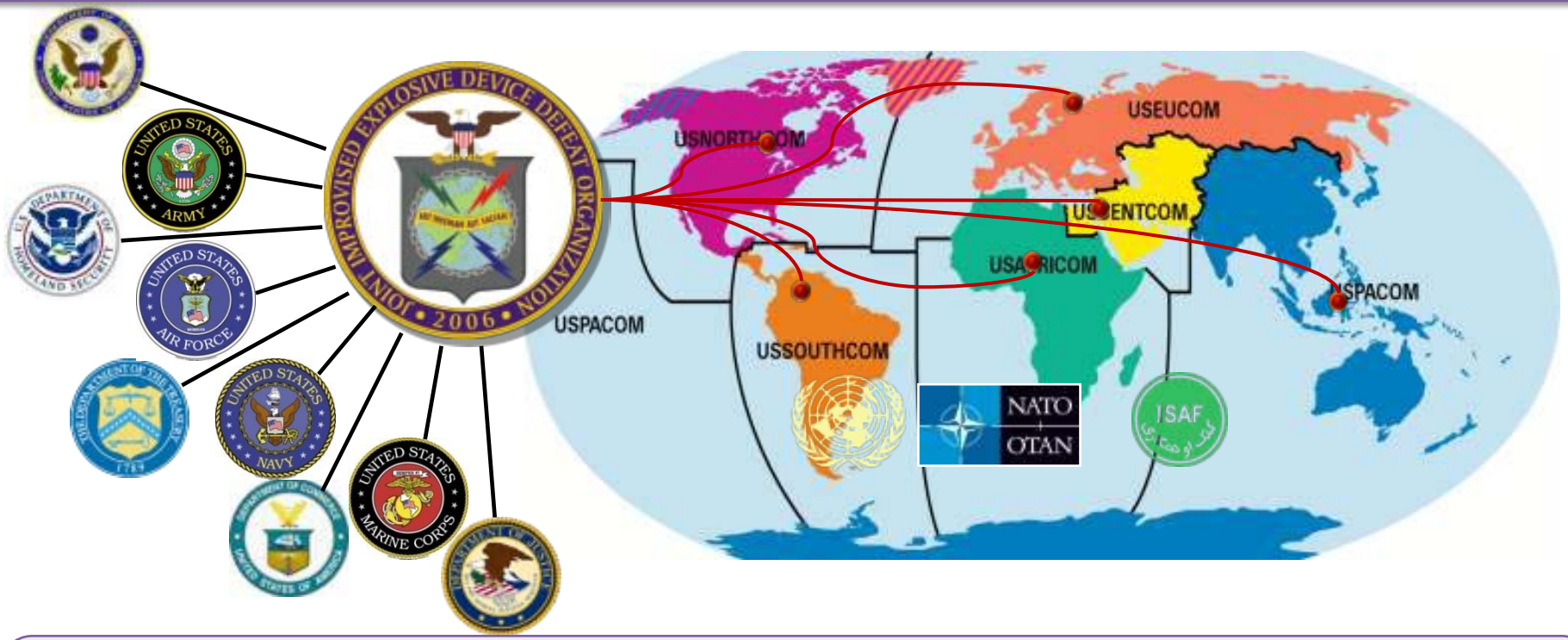
Source: Global IED Relational Database

** IED incidents occurring in Afghanistan and Iraq are not included in this database**

Why JIEDDO?

Attack the Network – Defeat the Device – Train the Force

Counter-Improvised Explosive Device (C-IED) operations is the organization, integration and synchronization of capabilities that enable offensive, defensive, stability, and support operations across all phases of campaigns in order to defeat IEDs as operational and strategic weapons of influence.



Mission Statement: JIEDDO leads DoD actions to rapidly provide Counter Improvised Explosive Device capabilities in support of the Combatant Commanders and to enable the defeat of the IED as a weapon of strategic influence

Lines of Operation (LOOs)

Attack the Network – Defeat the Device – Train the Force

LOO1 - Attack the Network: Lethal and non-lethal actions and operations against networks conducted continuously and simultaneously at multiple levels (tactical, operational, and strategic) that:

- capitalize on or create key vulnerabilities
- disrupts activities
- eliminates the enemy's ability to function

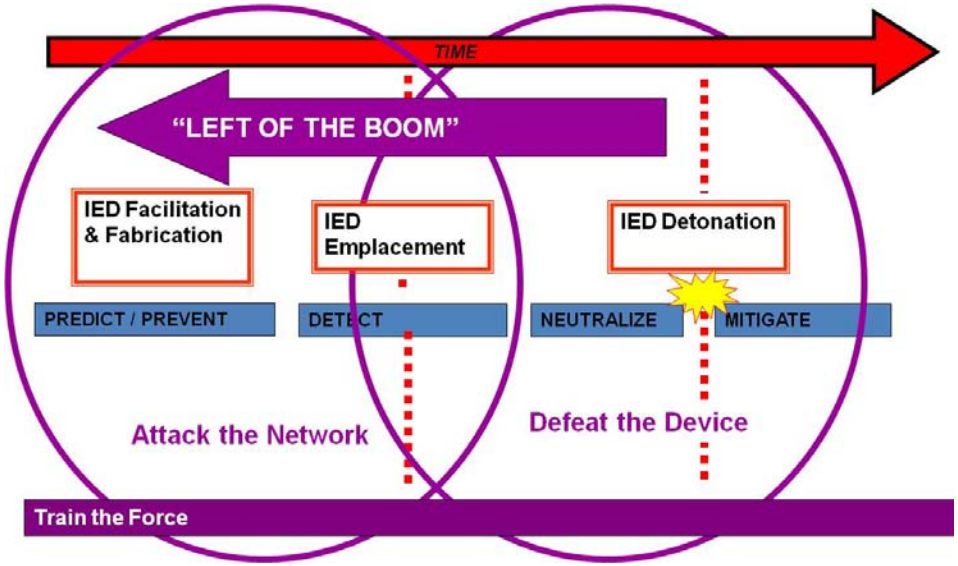
- Social and Dynamic Network Analysis
- Tagging, Tracking, & Locating
- Detect/Prevent Pre-Emplacement Activity
- Persistent Surveillance Technologies
- Sensor Enhancement and Data Exploitation

LOO2 - Defeat the Device: Detection, mitigation, and neutralization of IEDs once it has been emplaced through:

- route clearance
- device neutralization
- explosive detection
- disposal of unexploded and captured ordnance
- vehicle and personnel protection

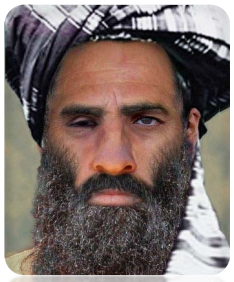
LOO3 - Train the Force: Actions and activities designed to enable Attack the Network and Defeat the Device through:

- graduate level Combat Training Center events
- C-IED training at Home Stations and the Centers of Excellence
- focused individual C-IED pre-deployment training
- training in-theater to stay ahead of adaptive enemy



Threat Overview

Attack the Network – Defeat the Device – Train the Force



Taliban

- Nationwide organization but strongest in South: Kandahar, Helmand, Zabul, Oruzgan
- Headquarters: Quetta, PAK

Hizbi Islami (Gulbuddin) (HIG)

- Operates in eastern Afghanistan and adjacent areas of Pakistan's tribal areas but has fighters integrated with Taliban throughout country
- Headquarters: Peshawar, PAK

Haqqanis

- Operate in Paktia, Paktika, Khost, Logar, and Ghazni Provinces and in Kabul City
- Headquarters: Miram Shah, PAK

Pakistan is home to several terrorist organizations, and the Headquarters for several insurgent groups operating in Afghanistan.

Attack the Network (AtN) Definition

Attack the Network (AtN) Operations are lethal and non-lethal actions and operations against networks conducted continuously and simultaneously at multiple levels (tactical, operational and strategic) that capitalize on, or create, *key vulnerabilities* and disrupt activities to eliminate the enemy's ability to function in order to enable success of the operation or campaign.

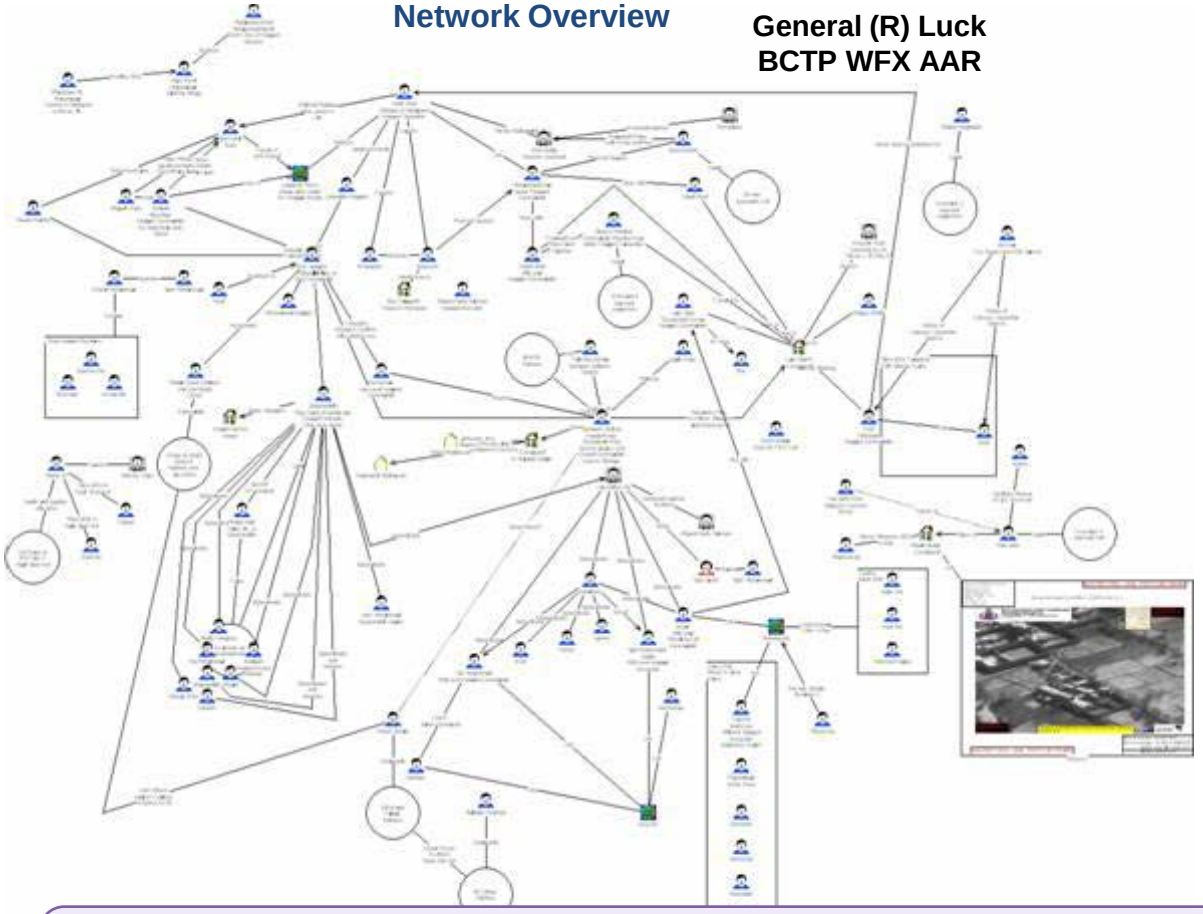
Effective AtN requires the military to understand where IED networks divert legal, dual use chemical precursors and electronics from the marketplace into the IED network

Common Operational Picture

Attack the Network – Defeat the Device – Train the Force

Network Overview

General (R) Luck
BCTP WFX AAR



- **HVI C/KOpns**
- **KLE**
  Key Leader Engagements
- **CMO**
  Civil Military Operations
- **IO**
- **CERP**
  Commanders Emergency Response Program
- **PRT**
  Provincial Reconstruction Team
- **Medical**
- **Governance**
- **Drug Eradication**

Achieving a Broader perspective

- Develop knowledge of network
- Define desired effects
- ID and integrate actions (lethal and non lethal)
- Assess tasks and effects

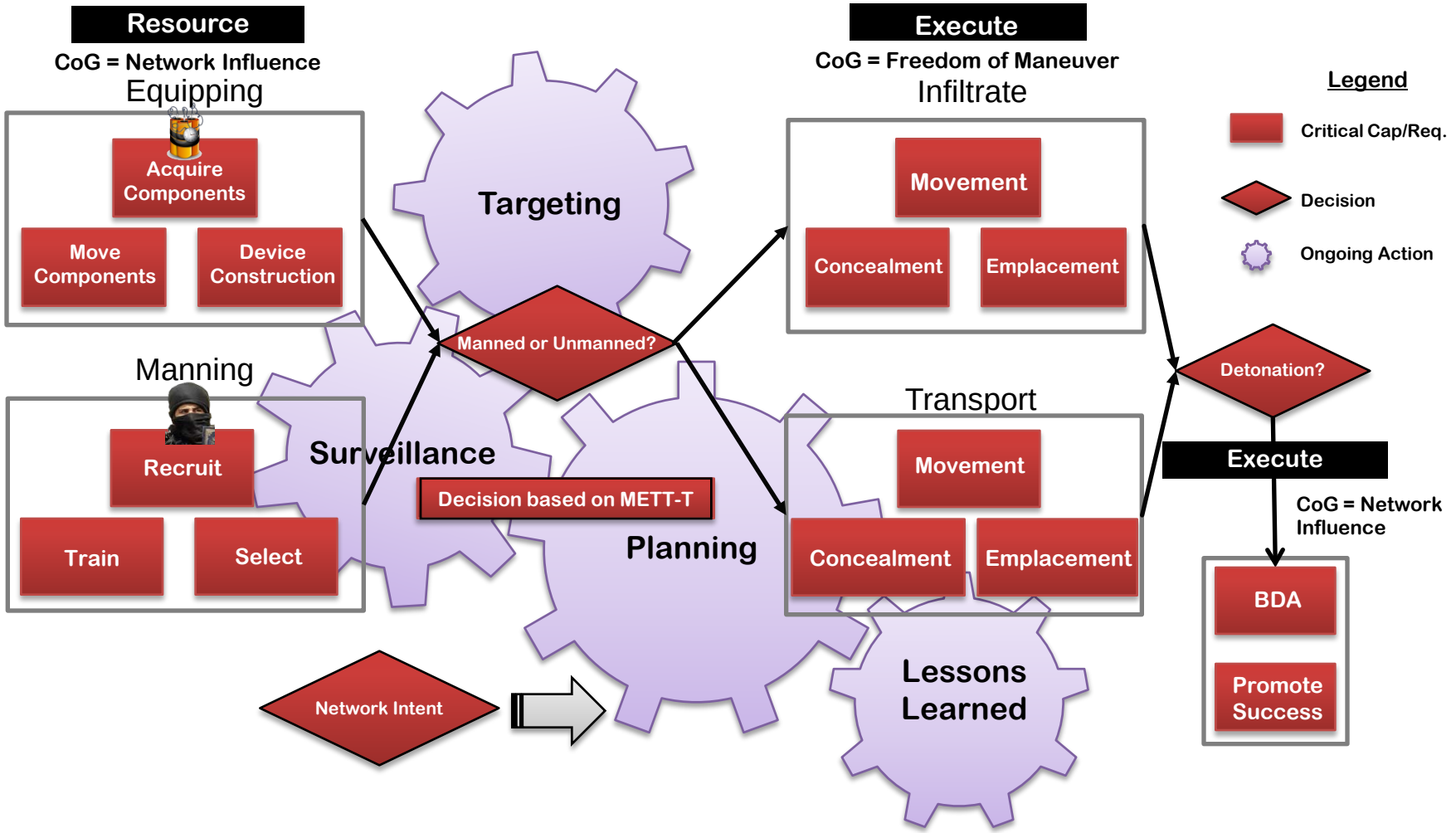
Critical Factors Analysis (CFA)

- **Attack the Network focuses on direct and indirect offensive operations against vulnerabilities**
- **Different agencies have different capabilities that will effect specific parts of the enemy network**
- **CFA helps the inter agency and "whole of government" allocate and prioritize resources against enemy network vulnerabilities**

CFA aims to build on the Common Intelligence Picture and Common Operating Picture by ensuring we use the right agency against a specific enemy vulnerability to achieve the greatest effect

Enemy Operational Architecture

Attack the Network – Defeat the Device – Train the Force



Enemy Mission: When feasible, utilize IED attacks IOT demoralize CF forces and destabilize GIROA

Enemy Intent: **Purpose:** Discredit CF forces and delegitimize GIROA
Method: Exploit CF and ANP/ANSF CVs through IED attack
End State: Eliminate legitimate influences and accelerate withdrawal of occupying forces

F3EAD for C-IED Operations

Find, Fix, Finish, Exploit, Analyze, Disseminate

Attack the Network – Defeat the Device – Train the Force

IED Incident

Site Security & Exploitation

Device Exploitation

Develop Device Profiles

Capture or Kill
Bomb makers, Financiers, Suppliers
Take down the Network

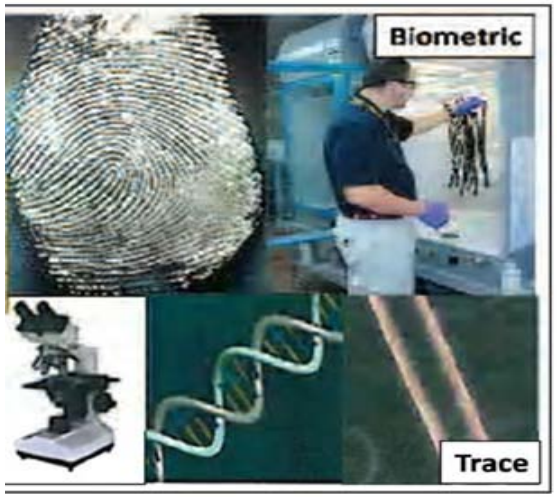
Identify the Cells & Networks

Actionable Intelligence Support Judicial Process

C-IED TTPs & Training

Site Exploitation

- **Site exploitation involves a systematic process of collecting materiel from a site for immediate and future exploitation—feeding and updating the Common Intelligence Picture**
- **It is critical that tactical units understand the value of preserving evidence and moving it from the field to the laboratory**



Common C-IED Forensic Functions

Five Forensic Modalities; each with a different authoritative database (Photography, Biometrics, Tool Marks, Trace Analysis, and Document/Media Exploitation)

Weapons Technical Intelligence (WTI) Handbook Version 1.0 Sep 2009

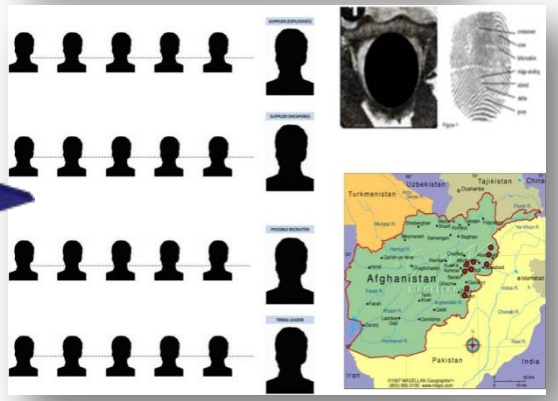
A Three-Pronged Attack

Attack the Network – Defeat the Device – Train the Force

Defeat the Device (DtD)

EOD trained for Exploitation

Attack the Network (AtN)



Train the Force (TtF)

One cannot Attack the Network without Defeat the Device and Train the Force

Online Resources: JKnIFE

Attack the Network – Defeat the Device – Train the Force

SIPR

https://jknife.jieddo.dod.smil.mil

CENTRIXS-ISAF

http://www.jknife.usa.isaf.cmil.mil

NATO Secret WAN

http://knife.act.nato.int/portal

NIPR

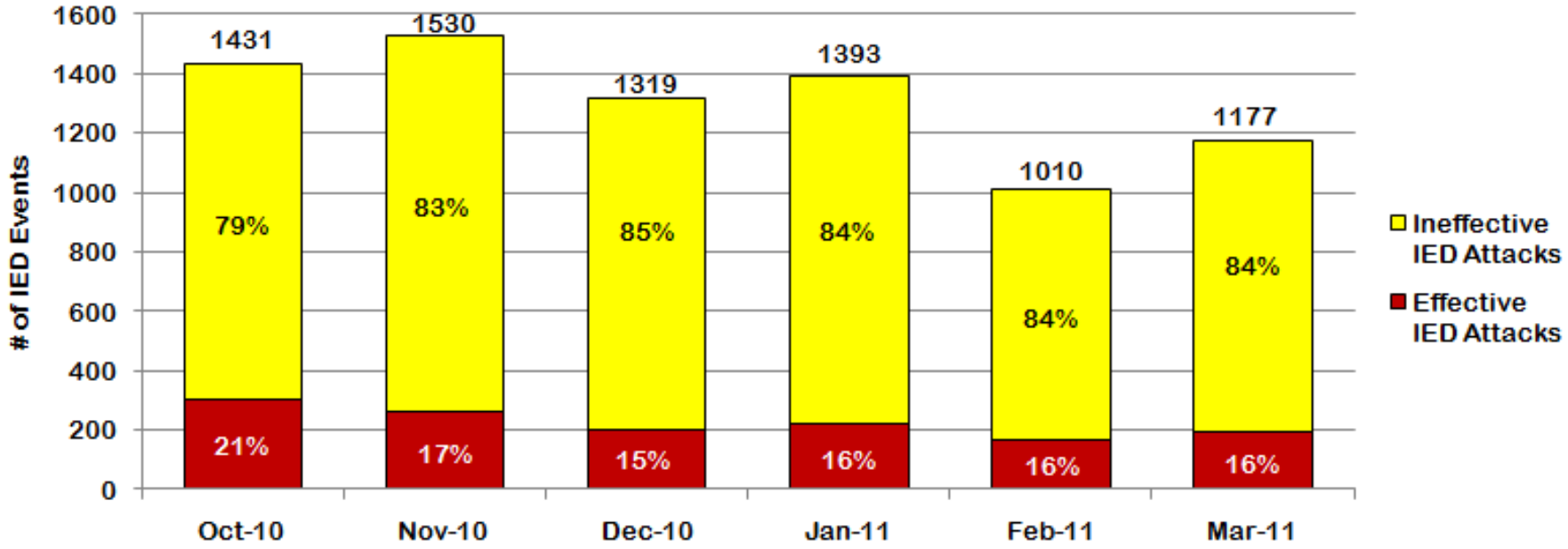
https://jknife.jieddo.dod.mil

NATO Transnet

http://transnet.act.nato.int/WISE/CounterIED/KnIFE0

Afghanistan IED Trends

Attack the Network – Defeat the Device – Train the Force



IED efficacy has <u>decreased</u> despite an increased OPTEMPO

Reasons for success:
- Effective COIN strategy
- Effective C-IED enablers w/trained forces
- Effective host nation security force
- Political reconciliation
- Lethal targeting of irreconcilables

JIEDDO Today: Areas of Strategic Focus

Attack the Network – Defeat the Device – Train the Force

- Reduce the flow of homemade explosives into Afghanistan
- Mitigate threat to dismounted troops
- Support our forces in Iraq as the mission transitions
- Provide support to coalition partners and allies
- Foster whole-of-government approach to the IED threat

Summary

- The IED is not a weapon on the battlefield – it IS the battlefield
- We must contain the spread of IEDs as a global weapon of choice for violent extremists
- We must continue to strive to make IEDs too costly to produce and too risky to employ by:
  - Attacking networks that emplace IEDs
  - Training our forces to protect themselves
- IEDs are not just a tactical problem
- Effective AtN begins with tactical and sensitive site exploitation conducted by maneuver and EOD units

www.jieddo.dod.mil www.jieddo.dod.smil.mil www.coic.smil.mil