

Joint Improvised-Threat Defeat Agency

Overview Brief

2 August 2016
Ms. Lisa Swan



HELPING WARFIGHTERS ADAPT

JIDA
JOINT IMPROVISED-THREAT DEFEAT AGENCY

The overall classification of this briefing is **UNCLASSIFIED**

APPROVED FOR PUBLIC RELEASE

An Enduring Global Threat



Share TTPs on Internet



Financing to organize, recruit, train, etc.



Generation of bomb makers








Ubiquitous chemical precursors



Free flow of dual-use components

More than 20,000 IED incidents globally causing more than 55,000 casualties

-  = Conflicts on-going
-  = Conditions set for IED activity
-  = Knowledge/people
-  = Material
-  = Most dangerous scenario

Strategic Approach



Leveraging External stakeholders in a Holistic approach to rapid, innovative solutions



LINES OF EFFORT

Anticipate and Mitigate the effect of Improvised Threats

Providing both materiel and non-materiel solutions to the warfighter



Enable freedom of maneuver

Working upstream from the immediate threat while supporting the warfighter with Operations and intelligence fusion



Cannot focus on one approach — all three must work together

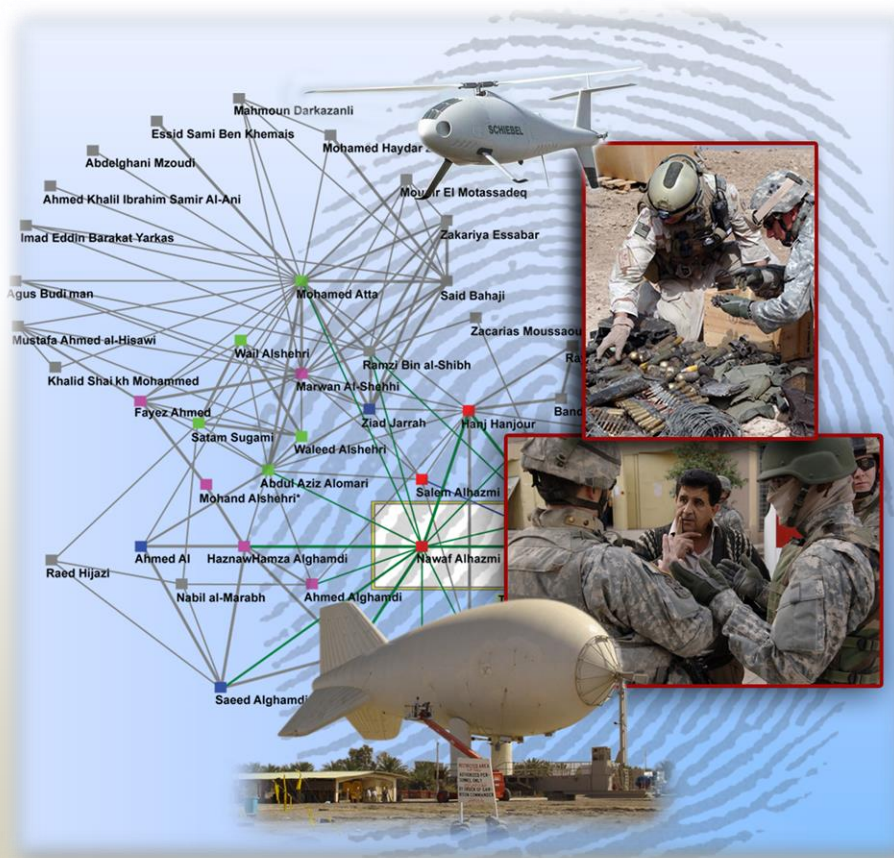
Core Functions



- **Assist Situational Understanding (of threat network activities)**
 - Operationally connected, planning assistance, identifies technology gaps, enable upstream threat facilitation network effects
- **Enable Rapid Capability Delivery to Implement DoD Accelerated and Urgent Acquisition Models**
 - Proactive, threat-based acquisition, urgent-emergent, counter-threat technologies and non-material investments
 - 0-2 years/urgent, 2-5 years/emergent, 5+ years/bring technology closer
- **Enable DoD Responses to Improvised Weapons**
 - Communities of action solution approach - leverage others' authorities, access, and capabilities – USG and coalition

Attacking Threat Networks

- Common intelligence & operational pictures
- Lethal and non-lethal targeting
- Counter-bomber targeting
- Integration of commercial & government off-the-shelf tools
- Analytical methods – trends, social networks, pattern, etc.
- Financial intelligence
- Data fusion
- Persistent surveillance
- Technical, biometrics and forensic exploitation



Prevent the use of Improvised Threats by attacking enemy vulnerabilities at multiple points in the complex network of financiers, IED makers, trainers and supporting infrastructure

Protecting the Force



- *Apply Advanced Technologies*
- *Rapidly Develop, Procure, Deliver Solutions*
- *Provide Training Support (kit and threat) throughout the deployment cycle*
- *Assess and Improve, sense and adjust via warfighter feedback*

A Well-Trained and Equipped Warfighter is our Best Tool

Enabling a Community of Action



Leveraging the access, tools and authorities of all partners to counter improvised threats



- U.S. Government
- Intelligence Community
- International Partners
- Academia
- Think Tanks
- Private Sector
- Industry

Access — Authorities — Collaborate — Coordinate — Leverage
“It takes a network to defeat a network.”

Parting Thoughts



- Threat networks are agile, flat, learning organizations
- To be forward leaning, we cannot only focus on the device itself
- Being embedded at the tactical edge is key to rapid and responsive solutions
- The improvised threat is not just a military problem — success requires a community effort and holistic solutions
- Innovation is not automatic
- To be anticipatory, we must identify gaps and invest in capabilities
- Rapid response requires a risk-tolerant posture
- JIDA defines success by iterative solutions delivered at the speed of war

