

COUNTER-IMPROVISED EXPLOSIVE DEVICE

STRATEGIC PLAN EXECUTIVE SUMMARY



JIEDDO

ATTACK THE NETWORK | DEFEAT THE DEVICE | TRAIN THE FORCE

2012-2016

As we continue to address the improvised explosive device threats of today, we must simultaneously prepare for tomorrow's counter-IED and counter-threat network effort by institutionalizing the knowledge, capabilities, and experience we have amassed during the last decade. Building upon hard-earned lessons learned, this Counter-IED Strategic Plan extends the focus beyond current operations and establishes an azimuth for the development of future and enduring counter-IED capabilities.

The IED is the weapon of choice for the overlapping consortium of networks operating along the entire threat continuum – criminal, insurgent, and terrorist alike. Threat networks use IEDs because they are cheap, readily available, easy to construct, lethal, and effective. The IED is a weapon used strategically to cause casualties, create the perception of insecurity, and influence national will. This threat is complex and transnational in nature, representing layers of interdependent, inter-connected global threat networks, and support systems.

MICHAEL D. BARBERO
Lieutenant General, U.S. Army
Director



Strategic Vision

Reduce the effectiveness and lethality of IEDs to allow freedom of maneuver for joint forces, federal agencies, and partner nations in current and future operating environments

The Enduring Threat

The future IED threat consists of an overlapping consortium of networks spanning the entire threat continuum — from criminal gangs to insurgencies to terrorists with global reach — for which the IED is the common weapon of choice. These threat networks operate in an environment characterized by the easy flow of dual-use components through legitimate businesses and one with access to local, readily available explosive materials. A generation of combat-experienced IED makers with skills for hire, who operate where weak and corrupt governance and desperate socioeconomic conditions prevail, can easily create political and economic instability. These networks and devices will be an enduring threat to our operational forces and to our domestic security.

Threat Networks

The threat is much more complex and transnational in nature, representing layers of interdependent, interconnected global networks and support systems. These networks adapt rapidly, communicate quickly, and are unconstrained by political borders. In geographic areas where IED use is more likely, most of the populace share similar social, economic, and religious identities. Weak governance and the absence of rule of law, corruption, mass migration, poverty, illiteracy, high unemployment, large populations of disaffected youth, and competition for water, food, and natural resources are factors that serve to unite and motivate a disaffected population.

Today's threat networks have proven to be resilient, adaptive, interconnected, and agile. They have learned to operate flexibly, aggregating and disaggregating quickly in response to countermeasures, extending their reach in physical and virtual dimensions. They adapt technology in short cycles and rapidly evolve tactics, techniques, and procedures. They operate unbounded by the law of war, rules of engagement,

central policy, moral constraints, or other limitations from a central authority. The IED is the common weapon of choice for elements along the threat continuum.

Device Technology

Today's IEDs, relatively simple “low-tech” devices, routinely use command-wire, victim-operated, or radio-controlled triggers. Many components are readily available, have legitimate commercial uses, and are easily adaptable as parts of bombs, e.g., circuit boards, cell phones, and simple electronic transmitters and receivers. Homemade explosives, often composed of ubiquitous fertilizers, easily transportable and convertible to greater-than-TNT explosive power, are predominant in IEDs and have been routinely employed against troops and domestic targets. IEDs are highly effective because of the innovative ways the adversary employs them. They are assembled with no or low amounts of metal components and can be concealed in plastic jugs, walls, wood, or debris. The rudimentary nature of basic IED technology simplifies design and construction techniques, which can be easily communicated via the Internet.

Methods of Delivery

Today, threat networks employ a variety of means to deliver IEDs to their targets. These explosives are commonly buried in or alongside roads or in culverts, transported by vehicles to a detonation site, or used by suicide bombers. The current threat also includes a variety of waterborne techniques — surface, submersible, and semi-submersible.

Domestic Challenge

Protecting the homeland, defending interests abroad, and sustaining strategic flexibility require a proactive approach that counters threat networks and anticipates evolving IED designs, tactics, and technology. The Defense Department's demonstrated C-IED capabilities, experience abroad, and international working relationships can have significant impact upon the domestic C-IED effort. Strong partnerships with our allies and all U.S. government agencies to synchronize our counter-threat network capabilities and actions are required. The domestic threat evolves and adapts quickly and continuously. U.S. domestic capabilities must evolve more rapidly — it takes a network to defeat a network.

The Disenfranchised Smugglers Criminals Pirates Narcotics Traffickers Insurgents Terrorists

Threat Continuum

Meeting the IED Challenge

IEDs have emerged as the threat weapon of choice and are one of the greatest operational and domestic challenges of the 21st century. There is no single solution to defeat the IED because there is no single enemy IED network. A range of efforts — supported by a whole-of-government approach — to neutralize threat networks and devices is required.

To defeat the threat, we must continually identify likely capability gaps and focus our supporting communities of interest to develop solutions. Leveraging the research and development (R&D) community in this endeavor ensures innovation that addresses these future challenges and provides a venue to discover and develop C-IED-related research and technology related to the C-IED mission.

Enduring Capabilities

To counter this enduring threat, we must integrate the five enduring capabilities described below. These enduring capabilities must be scalable, affordable, adaptable, expeditionary, appropriate for domestic application, and support a whole-of-government approach.

- **Rapid acquisition and fielding**
Employ authorities, flexible resources, streamlined processes, and effective oversight to drive the research and development community to rapidly field C-IED solutions
- **Operations-intelligence-information fusion**
Enable analytic capability to understand and counter threat-network activities globally
- **Training**
Establish standards and provide training and build partner C-IED and counter-network capacity
- **Weapons technical intelligence**
Exploit IED technologies and biometrics to inform intelligence, enable targeting, and counter threat networks
- **Whole-of-government approach**
Synchronize actions among joint, interagency, inter-governmental, international, and other federal agencies' C-IED stakeholders

These essential enduring capabilities are synergistic and provide a comprehensive response to a complex and dynamic threat.



Lines of Operation

The five enduring capabilities are employed through three mutually supporting lines of operation — Attack the Network, Defeat the Device, and Train the Force. The lines of operation provide the organizing construct and focus of effort for this strategic plan. They serve to integrate the C-IED enduring capabilities, synchronize internal operations, and increase agility. The three lines of operation are defined as:

- **Attack the Network.** Enables offensive operations against complex networks of financiers, IED makers, trainers, and their supporting infrastructure.
- **Defeat the Device.** Provides technologies to detect IED components, neutralize the triggering devices, and mitigate the effects of an IED blast to ensure freedom of maneuver and effective operations for commanders.
- **Train the Force.** Enables deploying forces to combat IED employment by attacking the network, integrating equipment and systems for the individual and battle staffs, and enhancing their knowledge and proficiency of C-IED tactics, techniques, and procedures.

Future C-IED Research and Development Requirements

Harnessing the innovative potential of the research and development community to meet a dynamic, complex, and adaptive threat is especially important. DoD will “cast a net into the future” to accelerate the most promising C-IED solutions to combat the ever-evolving threat. Our goal is to promote an informed and agile research and acquisitions process that stays ahead of the threat, and develops timely and effective C-IED systems solutions.

FUTURE R&D CAPABILITY GAPS 2012

- Pre-detonation
- Counter Threat Network/Attack the Network
- Detection
- Counter-device
- Homemade Explosives
- Information Integration and Visualization/
Information Fusion
- Weapons Technical Intelligence

C-IED Strategic Plan Goals

Goal 1: Rapidly identify, validate, and prioritize immediate and future C-IED requirements to enable Combatant Commanders to effectively attack complex IED production and support networks; detect and neutralize IEDs; and employ a trained force capable of addressing the IED threat.

Goal 2: Provide operations and intelligence fusion, analysis, training, and sensitive activity support to the Combatant Commanders, federal agencies, and coalition partners to enable freedom of maneuver from IEDs and to enhance a collective ability to counter threat networks and supporting activities.

Goal 3: Rapidly seek, develop, and acquire C-IED solutions to fulfill validated requirements that ensure a Combatant Commander’s ability to effectively attack complex IED

production and support networks; detect and neutralize IEDs; and employ a trained force capable of addressing the IED threat.

Goal 4: Lead DoD C-IED training and training capability development that support the Joint Staff’s, the Services’, and Combatant Commanders’ efforts to prepare joint forces to successfully attack the network and defeat the device in contemporary and future operating environments.

Goal 5: Build a joint, interagency, intergovernmental, and international C-IED community of action through collaborative planning, information sharing, and cooperative capability development for discrete IED problem sets (e.g., homemade explosives, domestic threat, partner C-IED capability development).

Way Ahead

The mission to disrupt the transnational threat networks employing IEDs, and to defeat the IED itself, requires a comprehensive and seamless effort supported across all levels of our government. This threat must be met with a whole-of-government approach that integrates efforts and leverages the combined authorities and capabilities of all interagency partners. While we are never going to stop all IEDs, a holistic, decisive, whole-of-government approach will significantly impact the effect the IED has in future operations and to our domestic security.

The IED threat and the networks that employ them will endure — they are here to stay. This compelling threat requires us to maintain constant vigilance, an enduring counter-threat network, and counter-IED capabilities.

The global IED threat must be met with a coherent and focused approach that collaboratively and continually seeks effective solutions. This strategy sets the path for the C-IED effort in collaboration with partner nations, the interagency, and intergovernmental organizations to enable the defeat of the IED as a weapon of strategic influence.