COUNTER-IMPROVISED EXPLOSIVE DEVICE

STRATEGIC PLAN

JIEDDO

ATTACK THE NETWORK | DEFEAT THE DEVICE | TRAIN THE FORCE

2012–2016

Cover image: A U.S. Marine with 1st Platoon, India Company, 3rd Battalion, 4th Marine Regiment, (3/4) uses a compact metal detector during a training exercise at Mojave Viper at Marine Corps Air Ground Combat Center, 29 Palms, Calif. (Photo by Lance Cpl. Christopher M. Burke)

Foreword

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.

When discussing future threats, it is important we consider both the networks that employ IEDs as well as the device itself. 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.

In the networks that support, supply, and employ IEDs, we see the nexus of narcotic, criminal, insurgent, and terrorist networks supported by the easy flow of dual-use components through legitimate businesses, using local readily available explosive materials, and a generation of combat-experienced IED makers — all interacting and operating in current or emerging conflict areas. They are largely seamless, overlapping, and not confined by geographical or jurisdictional boundaries. These threat networks are like a virus that breeds and flourishes in a climate of instability.

Globalization, the Internet, and social media have extended the transnational reach of these organizations, allowing threat networks to easily spread IED technology. Of great concern is the growth in the use of homemade explosives. These IEDs, comprised of fertilizers and other legally produced materials, have been used with devastating effects worldwide — from the battlefields of Iraq and Afghanistan to domestic targets such as Oklahoma City and Oslo, Norway. The ubiquitous nature of IED materials, their low cost, and the potential for strategic impact guarantee the IED will remain a threat and main casualty-producing weapon for decades to come.

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.

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

Table of Contents

Strategic Vision 1

Mission 1

Assumptions 1

Strategic Environment — the Current and Enduring Threat 2

Meeting the IED Challenge 6

Goals and Objectives 10

Future C-IED Research and Development Requirements 12

Conclusion 13

Acronyms 15

The following annexes will be available upon completion:

- **Annex A: Action Plan**
- **Annex B: Process Integration**
- **Annex C: References**

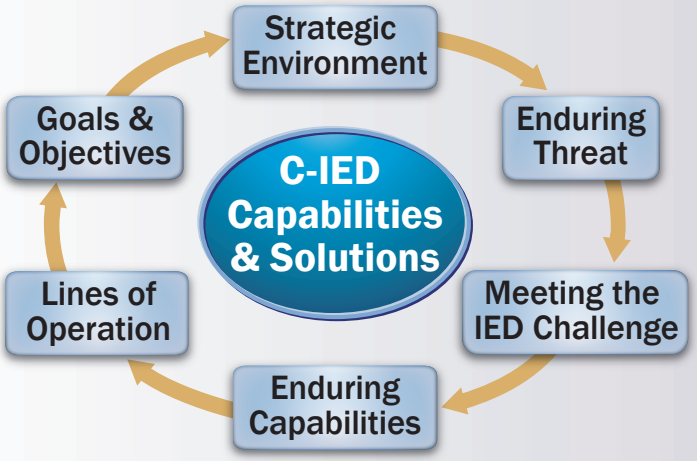
> "In the 20th century, artillery was the greatest producer of troop casualties. The IED is the artillery of the 21st century."
>
> *Lieutenant General Michael Barbero*
> *Director, Joint IED Defeat Organization*

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

We will use a synchronized and integrated approach to coordinate the Department of Defense's counter-IED efforts and rapidly provide capabilities to counter the IED threat in support of operational commanders. Critical to these efforts are forces trained in the latest C-IED techniques and provided with tailored and fused intelligence support. As authorized, we will provide support to other federal agencies as they analyze, pursue, disrupt, protect, and respond to the terrorist use of explosives in the United States. We will aggressively seek to maintain the research and development advantages needed to neutralize the IED threat.

Above all, we must remain agile and responsive to the needs of our commanders and warfighters, proactive in our approach, and tireless in our pursuit of comprehensive and timely solutions to the IED threat.



Mission

Lead DoD actions to rapidly provide C-IED capabilities and solutions in support of Combatant Commanders, the Services, and as authorized, other federal agencies to enable the defeat of the IED as a weapon of strategic influence.

Assumptions

- An enduring global IED threat will drive Combatant Commander requirements for C-IED capabilities.
- Homemade explosives will continue to be widely available and employed in IEDs.
- Fiscal constraints will likely result in a call for shared responsibilities and resources with other federal agencies.
- Future C-IED operations will include allies or coalition partners, requiring U.S. forces to contribute to multinational solutions in concert with our allies and partners.
- Deployed units will continue to require a rapid response to C-IED issues and threats.
- U.S. forces will continue to transition security responsibilities in Afghanistan; however future operations will require C-IED capabilities.
- In the event of an IED-related domestic incident, the lead federal agency will require DoD support.
- A networked and adaptive adversary aided by the latest information technology will continue to evolve and interact with other violent extremist organizations to constantly modify the design of IEDs and their methods of employment.

Strategic Environment — the Current and Enduring Threat

The Problem

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.

Background

The IED threat is enduring and not new. In 1605, a radical group attempted to blow up the British Parliament and assassinate King James I. Though averted, the attack was one of the first large-scale attempts to use explosives as a weapon of strategic influence — in this case, to change a government. In 1919, extremists conducted simultaneous attacks in eight U.S. cities, targeting U.S. government officials including members of Congress. The next year, anarchists exploded a bomb on Wall Street that killed 38. Throughout World War II, guerrillas and partisans used explosives to conduct sabotage. During the Vietnam War, the Viet Cong made extensive use of mines and IEDs against U.S. forces, both on land and in rivers, causing 33 percent of all U.S. casualties.

A GLOBAL THREAT

From January to November 2011, outside of Iraq and Afghanistan:

- **6,832 IED events globally, averaging 621 per month**
- **12,286 casualties**
- **111 countries**
- **Conducted by individuals supported by 40 regional and transnational threat networks**
- **Of those totals, 490 events and 28 casualties were in the United States**

The Provisional IRA employed sophisticated improvised mortars and remote-controlled IEDs during the conflict in Northern Ireland, and Hezbollah made extensive use of explosives against Israeli forces in Lebanon. In March 2004, there was a bombing of a commuter train in Madrid. This had a major strategic effect — as it was timed before a national election, and influenced Spain's support to Operation Iraqi Freedom.

There also was the failed Times Square attempt in May of 2010. In 2011, significant IED-related events occurred in Pakistan, India, Yemen, Somalia, Nigeria, Colombia, Norway, and bomb-making materials were found at home — in San Jose, California.

Threat Networks

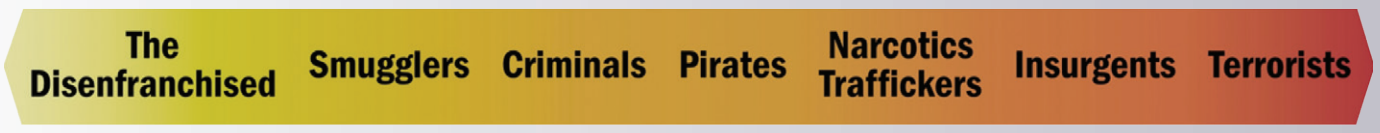
Though best understood in a regional context, the threat is much more complex and transnational in nature, representing layers of interdependent, interconnected global networks and support systems. These networks adapt rapidly, communicate quickly, and are unconstrained by political borders. In geographic 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. These factors, fueled by opportunistic leadership, can lead to the emergence of insurgencies and violent extremist organizations. These extremists often find common cause with existing criminal elements who are apt to use the circumstances to gain power and strengthen their illicit activities. The interaction of these networked organizations is enabled by the latest information technologies that provide recruiting opportunities, technical expertise, training resources, planning support, funding, and social interaction. Especially noteworthy is the essential nature of financial resources that

THE IED IS THE WEAPON OF CHOICE FOR ADVERSARIES OPERATING ALONG THE THREAT CONTINUUM.

facilitate these illicit networks. Disparate groups of differing origins easily interact and leverage each others' ability to finance their causes, launder money, and transfer funds around the globe. Criminal networks have long been able to effortlessly use and manipulate otherwise legitimate networks to move money, resources and information.

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 (TTPs). Finally, today's networks 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.

Social trends and communications technologies envision more diffuse network hierarchies with amorphous leadership structures in the future. The users of IEDs will adapt the most recent and successful TTPs gained from experiences in Iraq, Afghanistan, and elsewhere, and use them for political, ideological, or criminal purposes worldwide. They will seek to build the capability for more complex attacks, as seen in the July 2011 coordinated bombings in Mumbai, India. Their fundraising and financial transaction techniques will become more sophisticated, they will link with pirates and other criminal enterprises to enable their operations, and they will seek covert support from sympathetic state and non-state actors.



Threat Continuum

Device Technology

The IED will remain the weapon of choice for groups along the threat continuum and will remain an enduring global threat due to the accessibility of materials and the potential strategic impact resulting from their use. Today's IEDs are relatively simple "low-tech" devices which 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. In current combat theaters, more sophisticated devices, particularly explosively formed projectiles and advanced triggers, have caused disproportionate levels of casualties relative to the numbers employed.

ADVERSARIES WILL CONTINUE TO EVOLVE IED LETHALITY AND TACTICAL EMPLOYMENT — FUTURE DEVICES WILL BE OF LARGELY OFF-THE-SHELF TECHNOLOGY.

In the future, devices will adopt ever more sophisticated technology, limited only by the terrorists' imaginations. Most fearsome would be weapons of mass effect — chemical, biological, radiological, or nuclear — for which commercial control measures are not yet developed or in place. Future bomb makers will seek to incorporate such enhancements as peroxide- and hydrogen-based explosives; nanotechnology and flexible electronics; new forms of power, e.g., microbial fuel cells, non-metallic and solar; advanced communications (Bluetooth, 4G, Wi-Fi, broadband); optical initiators (using laser or telemetry more than infrared); and highly energetic and molecular materials. Indicators have shown that terrorist networks which innovate with these new technologies are also developing enhanced IED concealment techniques and may even combine IED use with concurrent cyber attacks. Bomb makers will take advantage of available technology and innovate in response to countermeasures — weapons will be more lethal and harder to detect and defeat.

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. In some areas, postal bombs are common. IED users have resorted to specialized delivery techniques to circumvent C-IED measures, such as embedding IEDs in shoes, underwear, toner cartridges, and cameras. There are efforts to

Upper right: Afghan National Security and International Security Assistance Forces conducted a clearing operation in Ormuz district, Helmand province. The operation lead to the discovery of 616 pounds of wet opium, 88 pounds of concentrated fertilizer, narcotics paraphernalia, and a pressure plate. (Photo courtesy ISAF)

Middle right: U.S. Air Force Master Sgt. Kevin Bullivant, an explosive ordinance disposal technician with the 466A Explosive Ordnance Disposal Team, sweeps off the explosive charge of an improvised explosive device found in a wadi in Jamal, Afghanistan. (Photo by Staff Sgt. Andrew Guffey)

Bottom right: The Newseum expanded its FBI exhibit with a section focusing on the FBI's role in fighting terrorism before and after Sept. 11, 2001. Sixty new artifacts include Richard Reid's shoes he tried to ignite while on a commercial flight. (Photo by Jeff Malet, maletphoto)

achieve low-detectable methods and greater precision using smaller-sized devices. Examples include shipping containers at varied transportation nodes; remotely piloted delivery in all domains — land, sea, air, and space; and even surgically implanted devices on humans and animals.

Domestic Nexus

The threat of IED use within the United States is real. A free and open society with guaranteed civil liberties is vulnerable — elements of the same overseas IED threat continuum and networks seek to strike within the borders of the homeland. While the use of explosives by organized crime and other groups within the United States is not new, the nature of today's threat has unique elements.

First, the threat is largely from non-state actors who wish to take the fight to the U.S. homeland is a relatively recent development. An organized, sophisticated, and tactically adept network of terrorist-affiliated individuals with access to offshore resources is an ever-present danger. Al-Qaida, its associated groups, and the Tehrik-e-Taliban in Pakistan have made attempts within the past year to attack the homeland, often recruiting Americans or Westerners who can pass heightened security measures. Second, the availability of a range of bomb-making technology and components allows motivated and empowered individuals to act alone or with only a few accomplices. Third, and particularly worrisome, is the threat of domestic radicalization and homegrown extremism —individuals who have lived primarily in the United States but are energized by ideology promoted by foreign terrorist organizations.

THE DOMESTIC THREAT

On May 25, 2011, the FBI Joint Terrorism Task Force arrested two al-Qaida in Iraq-affiliated, Kentucky-based Iraqi refugees, *Waad Ramadan Alwan* and *Mohanad Shareef Hammadi*.

- ***Alwan* was arrested for conspiracy to murder a U.S. national while outside the United States, conspiracy to use a weapon of mass destruction, and attempting to provide materiel support or resources to terrorists.**
- ***Hammadi* was also arrested for attempting to provide materiel support or resources to terrorists, as well as knowingly transferring, possessing, or exporting a device designed or intended to launch or guide a rocket or missile.**

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. In 2007, the Homeland Security Presidential Directive 19, *Combating Terrorist Use of Explosives in the United States*, was signed. This document and subsequent implementing instructions direct a whole-of-government approach that envisions seamless federal, state, and local government efforts to "deter, prevent, detect, protect against, and respond to explosive attacks."

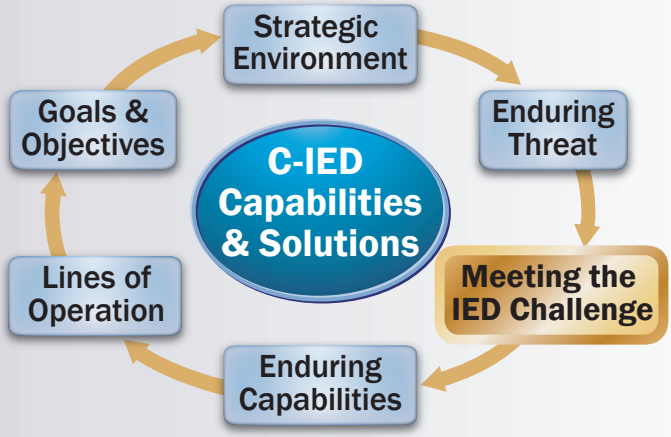
The Defense Department's demonstrated C-IED capabilities, experience abroad, and international working relationships can have significant impact upon the domestic C-IED effort. Strong partnerships with our allies and all U.S. government agencies to synchronize our counter-threat network capabilities 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.

EFFECTIVE SOLUTIONS TO THE DOMESTIC EXPLOSIVES THREAT REQUIRE A SEAMLESS WHOLE-OF-GOVERNMENT APPROACH.

Meeting the IED Challenge

IEDs have emerged as the threat weapon of choice and are one of the greatest challenges facing coalition forces in the current theaters of operation. The ubiquitous nature and lethal effect of IEDs used by insurgents directly threaten deployed forces' freedom of maneuver and the ability of indigenous governments to provide for the safety and security of their populations. 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.

Defeating the device is an unceasing effort, making use of the latest technological advances, to counter the adaptive adversary's adjustments to friendly C-IED capabilities. To have a decisive and lasting impact on the adversary's use of IEDs, friendly actions must focus on defeating the adversary's network. This requires the fusion of information, analysis, and partner support. It also requires a focused approach that is agile, adaptive, innovative, persistent, and relentless.



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.

This strategic plan's vision and mission describe the "ends" of this strategy — the requisite C-IED capabilities and solutions in the hands of the warfighters, supporting Combatant Commanders, the Services, and as authorized, other federal agencies to enable the defeat of the IED as a weapon of strategic influence. The "ways" are a set of enduring capabilities employed via three lines of operation, which in an interagency and multinational context, may be considered as lines of effort. The third leg of the strategy, the "means" are the resource allocation processes used to ensure capability to rapidly respond to emerging IED threats.

U.S. Marine Corps Lance Cpl. Christopher Smith, left, a combat engineer with 2nd Platoon, Lima Company, 3rd Battalion, 5th Marine Regiment, looks for a potential improvised explosive device during a census patrol in Sangin, Helmand province, Afghanistan. (Photo by Lance Cpl. Dexter S. Saulisbury)

Enduring Capabilities

An effective C-IED effort requires specific and focused capabilities to address both the threat networks and their devices. Joint forces must be enabled to counter an adversary's use of increasingly sophisticated and ever-evolving IEDs. With assistance from the R&D community, the materiel response must rapidly harness the latest technologies and concepts to enable engineering, procurement, and fielding of effective and timely C-IED systems. Joint force freedom of maneuver requires well-trained forces with unique skill sets who are able to develop situational understanding, be proactive, and employ advanced technology. The exploitation of threat networks and devices by leveraging all available all-source information and intelligence is essential.

The U.S. military is not the only group affected by IEDs. Allies and partner nations are also vulnerable, and the U.S. homeland continues to be an attractive target. A comprehensive, long-lasting solution to the IED and the adversary networks requires cultivating a culture of cooperation, collaboration, information exchange, and when necessary, mutual support and assistance on the part of international and interagency national security and public safety partners.

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

ENDURING CAPABILITIES

- Rapid Acquisition and Fielding
- Operations-Intelligence-Information Fusion and Analysis
- Training
- Weapons Technical Intelligence
- Whole-of-government Approach

- **Rapid acquisition and fielding** is the scalable ability to employ authorities, flexible resources, streamlined processes, and effective oversight to drive the R&D community to rapidly anticipate, identify, develop, and integrate emerging technologies and concepts into effective fielded C-IED solutions.
- **Operations-intelligence-information fusion and analysis** is an expeditionary and scalable network and analytical capability enabling DoD, other federal agencies, and coalition partners to understand threat-network activities globally. This fused, analytic capability leverages all available, all-source information and intelligence, to provide the most accurate, effective, time-sensitive information and counter-network support to Combatant Commanders and, as authorized, other federal agencies.
- **Training** is the ability to develop, define, and set C-IED and attack-the-network training standards for joint forces in response to Combatant Commanders' requirements and integrate those standards into appropriate joint and DoD concepts and doctrine in support of Combatant Commander requirements, to provide training and to build partner C-IED and counter-network capacity.
- **Weapons technical intelligence** (WTI) is the ability to conduct relevant and timely collection, analysis, and technical and forensic exploitation of current and emerging IED technologies to swiftly enable force protection, component and materiel sourcing, targeting, countering of threat networks, and expeditious support to prosecution.
- **Whole-of-government approach** is the ability to rapidly synchronize counter-threat network capabilities and actions among joint, interagency, intergovernmental, international, and other federal agencies' C-IED stakeholders. This is done through collaborative planning, information sharing, and cooperative capability development to reduce the impact of IEDs on operational forces and the threat to the homeland.

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 (LOOs) are the "ways" that 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 LOOs are defined as:

- **Attack the Network** enables offensive operations against complex networks of financiers, IED makers, trainers, and their supporting infrastructure. Attack the Network is focused on information fusion, extensive partner collaboration, and expanding analytical support to combatant commands. Key to DoD's Attack the Network effort is the C-IED Operations/Intelligence Integration Center (COIC), which harnesses, masses, and fuses information, analysis, technology, interagency collaboration, and training support. COIC support enables more precise attacks to defeat violent extremist networks. Personnel with unique skill sets can be forward deployed to provide timely analysis, accurate information, and responsive support to forces in theater. COIC's extensive reachback capability supports commanders' with all-source information fusion and analysis.

- **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. A unique process of accelerated requirements determination and acquisition gives DoD the ability to rapidly research, develop, produce, integrate, assess, and field proven materiel and non-materiel C-IED initiatives to counter known, newly deployed, and emerging IED threats. The goal is to provide fielded solutions to the warfighter between four and 24 months from requirements identification.

Cpl. Sean Connell launches a Raven unmanned aerial vehicle, providing a demonstration of the system to then-Chief of Staff of the Army Gen. George W. Casey Jr. at the National Training Center in Ft. Irwin, Calif. (Photo by D. Myles Cullen)

The arm of a Talon robot grasps a mortar tail during an operations check on the robot at Forward Operating Base, Azizullah, Afghanistan. The robot is used to interrogate IEDs when explosive ordnance disposal personnel need to investigate an IED from a safe distance. (Photo by Staff Sgt. Stephen Schester)

- **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 TTPs. Focused C-IED training provides the most up-to-date tactics and technologies to troops at the individual and unit level. Commanders and staffs are educated and trained to integrate Attack the Network and Defeat the Device tools and enabling resources. To be successful, joint forces must understand threat networks and how to attack and defeat them.

Goals and Objectives

Our overarching goal is to mitigate the effects of IEDs on the commander's freedom of maneuver and to enable the defeat of these devices as weapons of strategic influence. JIEDDO's role, as an integral part of the whole-of-government approach — to lead, advocate, and coordinate all DoD C-IED actions in support of the Combatant Commander — provides for unifying goals today and in the future. These goals embrace a larger C-IED community of action while continually seeking innovative solutions to the C-IED problem set.

This strategy has five principal goals with supporting objectives that institutionalize C-IED within DoD and, as authorized, provide support and assistance to other federal agencies to meet the evolving IED threat. These goals directly support and are tied to the JIEDDO LOOs of Attack the Network, Defeat the Device, and Train the Force. This provides for clear, consistent, effective, and efficient resource provision that builds C-IED capability. We synchronize operations and intelligence fusion, requirements identification and validation, rapid acquisition of desired capabilities, and training to enhance proficiency, while partnering with other DoD organizations, the interagency and multinational entities. These goals and objectives will be validated annually and can be changed or modified as required.

We will track and assess the accomplishment of these goals through action plans based on published goals and objectives that are reviewed on a quarterly basis to assess progress.

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.*

- **Objective 1.1:** Support the validation of current and emerging Combatant Commanders' requirements to ensure priority capability gaps are being addressed.
- **Objective 1.2:** Determine both current and future required capabilities by identifying threat-focused operational needs and capability gaps to rapidly respond to dynamic C-IED needs.
- **Objective 1.3:** Prioritize acquisition decisions to support C-IED requirements to ensure investments are made with the greatest impact for the warfighter.

- **Objective 1.4:** Ensure resources are justified and applied to ensure congressional approval of resource allocation to rapidly develop and field C-IED capabilities.
- **Objective 1.5:** Conduct assessments that enable transition, transfer, terminate, or continue decisions within 24 months from initiatives origination to institutionalize C-IED capabilities and ensure the JIEDDO investment is leveraged for the future.
- **Objective 1.6:** Direct, monitor, and modify, as necessary, activities regarding the WTI process as they pertain to the collection, technical and forensic exploitation, and analysis of IED components to swiftly enable force protection, targeting, component and materiel sourcing, and expeditious support to prosecution. Establish the standards, processes, and procedures required for application of forensics to WTI collection, analysis, and exploitation.

Goal 2: *Provide operations and intelligence fusion, analysis, training, and sensitive activity support to 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.*

- **Objective 2.1:** Staff, train, and equip a scalable, deployable, highly qualified workforce to sustain Combatant Commander integration support and global contingency operations.
- **Objective 2.2:** Provide operationally relevant and timely operations-intelligence fusion, analytical support, and training integration to enable Combatant Commanders to attack threat networks.

- **Objective 2.3:** Innovate and improve information technology infrastructure and analytical methods to enhance global collaboration in fully established or austere environments.
- **Objective 2.4:** Build partnerships to enable global threat information sharing, analysis, and collaboration to leverage and focus a whole-of-government effort.
- **Objective 2.5:** Maintain a global knowledge base of current and future IED threats to provide solutions to counter friendly vulnerabilities.
- **Objective 2.6:** Provide sensitive activities support to enable Combatant Commanders' and, as authorized, other federal agencies' counter-threat network operations.

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.*

- **Objective 3.1:** Develop, procure, implement, evaluate and deploy C-IED solutions to enable offensive operations against networks; ensure freedom of maneuver and effective operations for commanders; and enable deploying forces to mitigate the impact of IED employment.
- **Objective 3.2:** Aggressively seek innovative C-IED solutions requiring research and technology maturation and prioritize within DoD to advance capabilities required for the future.
- **Objective 3.3:** Conduct continuous evaluation of C-IED capabilities based on identified requirements, goals, and objectives to determine effectiveness.
- **Objective 3.4:** Underwrite risk by understanding the future threat, rapidly applying resources, and synchronizing DoD efforts.
- **Objective 3.5:** Provide effective management and oversight of JIEDDO contracts.

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.*

- **Objective 4.1:** Develop and execute a synchronized C-IED training plan supporting Joint Staff, Service, Combatant Command, and, as directed, partner nation and interagency C-IED training requirements.
- **Objective 4.2:** Develop C-IED training programs and capabilities, and transition those that are enduring to the Services.
- **Objective 4.3:** Collect and incorporate C-IED after action reviews, lessons learned, and TTPs into C-IED training.

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).*

- **Objective 5.1:** Assist Combatant Commanders to develop international and interagency partner C-IED capability and capacity building to mitigate the effects of IEDs.
- **Objective 5.2:** Seek opportunities to expand the role of international and interagency partners to synchronize C-IED capabilities and to share information, intelligence, and technology.
- **Objective 5.3:** As authorized, assist the C-IED efforts of other federal agencies — as part of the whole-of-government approach — to provide for defense support of civil authorities and to support interagency organizations when directed, to augment and enhance C-IED capabilities to protect U.S. citizens and national infrastructure.

GOALS AND OBJECTIVES ENABLE US TO TRANSFORM STRATEGIC GUIDANCE INTO SPECIFIC, EFFECTIVE, AND MEASURABLE ACTIONS.

Future C-IED Research and Development Requirements

Harnessing the innovative potential of the R&D 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. We can find capability gaps by considering Combatant Commanders' requirements over time, extrapolating the technical and tactical threat trends, and conducting a comparative analysis of the most fruitful possibilities given existing systems and promising new technologies. DoD will close these future capability gaps by engaging the public and private R&D sectors to refine capabilities and develop new systems, technologies, and tactics.

These sectors consist of a wide variety of organizations and represent the Services, government agencies, commercial firms, the defense industry, research laboratories, and academia. These multifaceted entities can be selectively engaged to address issues across the IED spectrum. An effective DoD C-IED R&D strategy can play to each of their strengths and develop a true synergy across the community of interest. The elements of this strategy will include research funding, collaborative development, policy direction, developmental contracts, information sharing, and venture capital investment. The end result of these efforts is the first, but most important, step in future capabilities development to combat an adaptive threat — understanding the most promising short-, medium-, and long-term opportunities for R&D investments. The 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 solutions to safeguard our troops, our citizenry, and our international partners.

FUTURE R&D CAPABILITY GAPS 2012

- Pre-detonation
- Counter-threat Network

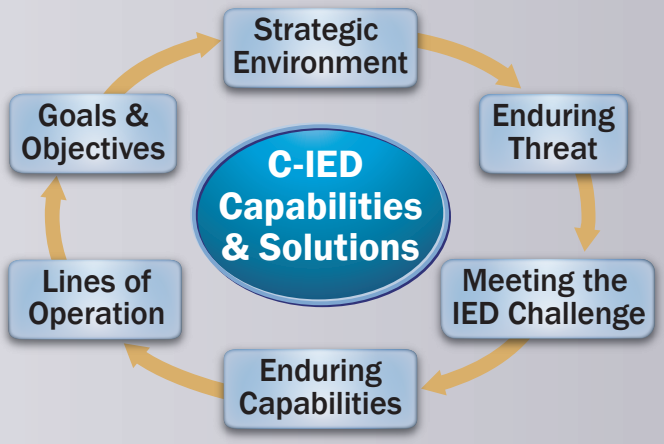
- Detection
- Counter-device
- Homemade Explosives
- Information Integration and Fusion
- Weapons Technical Intelligence

U.S. Army Spc. John "Rocky" Montoya scans his sector while on a combat patrol to sweep for roadside bomb triggermen in the Alingar district in Afghanistan's Laghman province. Montoya is a M2 gunner assigned to the Laghman Provincial Reconstruction Team. (Photo by Staff Sgt. Ryan Crane)

Conclusion

The armed forces of the United States and partner nations will continue to be engaged throughout the world. In future operations, joint forces will encounter improvised explosive devices employed by determined adversaries. These cost-effective, adaptive weapons and the violent extremist organizations that use them are sure to evolve over time. The IED threat will not be limited to overseas operations; intelligence trends indicate the potential use of these weapons within the U.S. homeland. This is not unprecedented.

In executing this strategy, we will build enduring capabilities to meet the enduring IED threat by with a swift C-IED response. It is the synergy of rapid acquisition and fielding, operations and intelligence fusion and analysis, training, weapons technical intelligence, and a whole-of-government approach that coupled with a single focus on the global IED threat ensures our ability to meet the warfighters' requirements. Using the battle-tested LOOs — Attack the Network, Defeat the Device, and Train the Force — we detect, prevent, protect, and mitigate IEDs and their effects. We seek to achieve the stated goals and objectives of this document through our annual planning process, beginning with threat and capability gap analyses, proceeding through the capability acquisition process, and ending with C-IED investment decisions leading to desired solutions. JIEDDO continually assesses these efforts in support of the Combatant Commanders.



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.

Lance Cpl. Arturo Valtierra, a mortarman with Redemption II, Weapons Company, 2nd Battalion, 1st Marine Regiment, scans for IEDs during a foot patrol to a local Afghan National Police near Patrol Base Gorgak, Garmsir District, Helmand province, Afghanistan. (Photo by Sgt. Jesse Stence)

Acronyms

C-IED: Counter-improvised explosive device

COIC: C-IED Operations/Intelligence Integration Center

DoD: Department of Defense

EFP: Explosively formed projectile

IED: Improvised explosive device

JIEDDO: Joint IED Defeat Organization

LOOs: Lines of operation

R&D: Research and development

TTPs: Tactics, techniques, and procedures

WTI: Weapons technical intelligence

JOINT IED DEFEAT ORGANIZATION

(877) 251-3337
www.jieddo.mil

January 1, 2012