Joint Publication 3-15.1

Counter-Improvised Explosive Device Operations

09 January 2012

Intentionally Blank

PREFACE (U)

1. (U) Scope

(U) This publication provides joint doctrine for planning and executing counter-improvised explosive device (C-IED) operations. It outlines responsibilities, provides command and control considerations, discusses organizational options, details the C-IED process and attack the network methodology, and introduces models for coordinating with C-IED supporting organizations.

2. (U) Purpose

(U) This publication has been prepared under the direction of the Chairman of the Joint Chiefs of Staff. It sets forth joint doctrine to govern the activities and performance of the Armed Forces of the United States in joint operations, and provides the doctrinal basis for the planning and conduct of joint C-IED operations. It provides military guidance for the exercise of authority by combatant commanders and other joint force commanders (JFCs) and prescribes joint doctrine for operations, education, and training. It provides military guidance for use by the Armed Forces in preparing their appropriate plans. It is not the intent of this publication to restrict the authority of the JFC from organizing the force and executing the mission in a manner the JFC deems most appropriate to ensure unity of effort in the accomplishment of the overall objective.

3. (U) Application

a. (U) Joint doctrine established in this publication applies to the Joint Staff, commanders of combatant commands, subunified commands, joint task forces, subordinate components of these commands, and the Services.

b. (U) The guidance in this publication is authoritative; as such, this doctrine will be followed except when, in the judgment of the commander, exceptional circumstances dictate otherwise. If conflicts arise between the contents of this publication and the contents of Service publications, this publication will take precedence unless the Chairman of the Joint Chiefs of Staff, normally in coordination with the other members of the Joint Chiefs of Staff,

has provided more current and specific guidance. Commanders of forces operating as part of a multinational (alliance or coalition) military command should follow multinational doctrine and procedures ratified by the United States. For doctrine and procedures not ratified by the United States, commanders should evaluate and follow the multinational command's doctrine and procedures where applicable and consistent with US law, regulations, and doctrine.

For the Chairman of the Joint Chiefs of Staff

WILLIAM E. GORTNEY
VADM, USN
Director, Joint Staff

TABLE OF CONTENTS (U)

FIGURE

EXECUTIVE SUMMARY
COMMANDER'S OVERVIEW (U)

- **(U) Provides Insight on the Improvised Explosive Device Threat**
- **(U) Describes the Improvised Explosive Device Network**
- **(U) Covers Planning for Counter-Improvised Explosive Device Operations**
- **(U) Explains Attacking the Improvised Explosive Device Network**
- **(U) Discusses Staff Responsibilities**
- **(U) Describes Counter-Improvised Explosive Device Task Force**

(U) The Improvised Explosive Device Threat

(U) An improvised explosive device (IED) is a weapon that is fabricated or emplaced in an unconventional manner incorporating destructive, lethal, noxious, pyrotechnic, or incendiary chemicals designed to kill, destroy, incapacitate, harass, deny mobility, or distract.

(U) Improvised explosive devices (IEDs) may incorporate military munitions and hardware, but are generally constructed from components that are nonmilitary in nature. IEDs are employed by threat groups across the globe to achieve their aims. This is, in part, due to IEDs' potential to produce strategic effects beyond their tactical impact. IEDs are designed to kill opponents and influence their actions, discredit them among the populace, and degrade their ability to achieve their objectives. It is projected that such individuals and groups will likely increase their employment of IEDs while enhancing the lethality of their weapons and tactics. These weapons will represent a continuing threat to US forces and multinational forces (MNFs).

(U) IEDs vary widely in shape, size, and form; however, they usually share three common components: main charges, initiating system, and containers.

(U) Methods of IED employment fall within two major categories: suicide and non-suicide. In regard to suicide attacks, insurgents and terrorists can employ IEDs via person or vehicle, both of which are typically disguised as part of the populace. In non-suicide attacks, they conceal IEDs in the ground or in water, inside packages, common containers, vehicles, and even in carcasses.

(U) The IED battle is an evolving contest between the IED network and the

(U) Our enemies employ IEDs to demonstrate their freedom of action; demoralize, distract, and discredit US, multinational, and host nation (HN) security forces; create

US and its multinational partners.

fear within the general population; gain media exposure; and negatively impact US, HN, and partner nation interests. Meeting this threat requires a national effort based on a whole-of-government approach that addresses the device, the network that designs and emplaces the device, and the social-political aspects of the operational environment that facilitates IED employment.

(U) The Improvised Explosive Device Network

(U) The leadership of these IED networks plan, organize, and execute many critical activities necessary to accomplish their objectives.

(U) IED networks are centrally and decentrally organized because of the need to protect relationships and hide activities at the tactical, operational, and strategic levels. Within these IED networks, functional plans and operations are interconnected and may impact each other in direct and indirect ways and at all levels. Recognizing these interrelationships is critical when attempting to attack a network. Fundamental to all networks is an understanding of the resourcing, especially financial resourcing, required to start up, sustain, and grow the organization from the strategic level through to the tactical units.

(U) Virtually all such networked organizations use some variant of a cellular or compartmented structure to enhance security and organize for operations.

(U) Whether the IED is employed by an insurgent, a terrorist, or a criminal gang, it is resourced, manufactured, emplaced, and executed through what is likely a secretive and networked organization. Any group that systematically employs IEDs must perform a series of networked operations or activities to be successful. These operational requirements include resourcing (finance and supply) and personnel (bomb-making specialists and planners), which are driven or guided by ideological or economic motivation. Although some network activities may occur simultaneously or sequentially, activities associated with these operations are frequently conducted independently. Each of the functions may be organized as one or more cells within the network, and participants in each function/cell may be unaware of the others' existence.

(U) The IED Activity Model.

(U) Counter-improvised explosive device (C-IED) operations should begin with a holistic understanding of the enemy and the common activities associated with an IED attack in order to break the enemy's operational cycle. **IED activities can be categorized in four recurring phases—planning, execution, assessment, and exploitation**—and may be conducted concurrently or asynchronously by multiple cells.

(U) Planning for Counter-Improvised Device Operations

(U) Counter-improvised explosive device (C-IED) operations often focus on the device; however, the device is merely the end product of a complex set of activities the adversary executes to achieve his objectives.

(U) An IED attack is the result of a planned operation that can have strategic, operational, and/or tactical effects, not solely because of the military value of the target, but also the psychological effects on units, the local population, the region, and political leadership. **An integrated, synchronized C-IED plan is designed to address all levels of war.** The actions at the strategic level include the coordination of all instruments of national power, the collaboration and cooperation with the combatant commands to deny the enemy funding, supplies, safe havens, and a favorable information environment to influence public opinion. At the combatant command level, the C-IED plan provides guidance for isolation and attacking elements of the IED network, mitigating effects of an IED blast, training the force in C-IED tactics, techniques, and procedures (TTP), and transferring equipment and capabilities to participating MNFs and the HN.

(U) C-IED Concept of Operations.

(U) The foundation of a C-IED concept of operations (CONOPS) is a coherent strategy that links strategic, operational, and tactical activities to objectives, and integrates interagency actions to ensure unity of effort, both inside and outside of the area of responsibility. It describes how the actions of the joint force components and supporting organizations will be integrated, synchronized, and phased to accomplish the mission, including potential branches and sequels. A theater C-IED CONOPS includes the commander's intent, the desired end state, and objectives.

(U) Joint force C-IED activities must be viewed both individually and in the context of their relationship to the other interagency partners' activities conducted using other instruments of national power.

(U) **Joint force C-IED activities fulfill five basic purposes:**

- (U) Protect US, multinational (if applicable), and HN forces and the local populace against the physical effects of IEDs.
- (U) Enable mobility in operational areas.
- (U) Expose and neutralize IED networks.
- (U) Neutralize impact of IED use.
- (U) Stabilize economic activity in the affected locality.

(U) Mission Analysis.

(U) The joint force will conduct C-IED operations within the context of a broader operation or campaign. In certain instances, however, the joint force commander (JFC) may choose to conduct focused C-IED operations to eliminate or neutralize the threat in a specific area. In either case, the mission analysis phase of the joint operational planning process will provide for the effective planning to achieve the commander's objectives.

(U) Lines of Operation.

(U) As JFCs visualize the operational design of the operation, they may use several lines of operation (LOOs) to help visualize the intended progress of the joint force toward achieving operational and strategic objectives. **There are three basic C-IED LOOs that form the basis for the conduct of all C-IED planning and operations: "attack the network" (AtN) "defeat the device," and "train the force."**

(U) A Balanced Approach.

(U) A successful C-IED operation plan is one that employs a mix of lethal and nonlethal actions to deny the enemy access, freedom of movement, and action. Constant pressure on critical nodes in the enemy's infrastructure will keep the enemy off balance and degrade his overall effectiveness. It will also force the enemy to reveal increasing portions of the network as they attempt to reconstitute their activities.

(U) Attacking the Improvised Explosive Device Network

(U) In the context of C-IED operations, "Attack the Network" operations specifically target the enemy's ability to resource and conduct IED attacks.

(U) In order for the IED network to survive in an environment where it is being hunted by friendly forces, the adversary must be able to continuously respond to changing environmental pressures—political, economic, social, and military. Survival and success are directly connected to adaptability and the ability to compete for resources—financial, logistical, and human.

(U) Attacking the Network—General Considerations.

(U) While attacking the adversary's network is a complex, time-consuming task, raising the adversaries' cost of IED employment to unacceptable levels can be accomplished through a focused, continuous series of operations designed to disrupt the people, places, processes, and materials that support the IEDs' design, supply, and employment chain.

(U) Counter-Network Strategy Development.

(U) The ends of an effective counter-network strategy that curtails the IED threat to the joint force or HN population will invariably focus on the operational environment that

allows the threat to take place. The ways of the counter-network strategy use an operation or campaign design process that allows operational art to link ends, ways, and means to reach the desired end state. To AtN, commanders and staffs must first understand the operational environment in network terms. An important feature of any network is its adaptability to a changing environment; one change to a node or link may substantially affect the entire network. Because of this dynamic nature of complex adaptive systems, a second imperative for effective counter network operations is to closely link operations and intelligence. The third essential element for an effective strategy is to rapidly assess the effects created by operations and feed the assessment into the intelligence process.

(U) Attack the Network Across the Levels of War.

(U) **At the strategic, national, and theater levels**, AtN operations are focused on global, international, or transnational threats and networks requiring coordination and integration with interagency partners, MNFs, and multinational organizations. Key AtN operations at this level include positively shaping the strategic environment using the full range of the instruments of national power and developing and providing the partnerships, information, and resources required for strategic success.

(FOUO) **At the operational level**, AtN operations should employ a highly adaptable, collaborative, and decentralized approach, blending physical and cognitive abilities to achieve a desired end state. Through the use of specialized analytical tools, commanders will be able to refine their understanding of the operating environment and focus resources on key nodes in the IED infrastructure.

(U) **At the tactical level**, the focus is on executing AtN operations. Accurate, timely, and relevant intelligence will drive this effort, and tactical units should exercise refined procedures to conduct analysis, template, and target networks.

(U) Targeting the Network.

(U) There are a number of targeting methodologies that have been developed to facilitate AtN. These methodologies (which include find, fix, finish, exploit, analyze, and disseminate and decide, detect, deliver, and assess) can also be merged to complement each other. Regardless of the method employed, established processes and procedures must be identified, standardized, and

exploited to develop and refine a comprehensive picture of the adversary to effectively target and attack an IED network.

(U) Multi-Echelon, Multidiscipline C-IED Fusion.

(U) Organizing and allocating resources for AtN operations requires a coordinated, synchronized, and integrated effort beginning at the tactical level and often involving the use of national-level resources. Intelligence personnel at all echelons must be prepared to employ traditional and nontraditional information sources to build the picture of the adversary's infrastructure and share that information and intelligence across the joint force.

(U) Staff Responsibilities

(U) Intelligence Directorate of a Joint Staff [J-2].

(U) The intelligence directorate of a joint staff's (J-2's) mission is to provide the commander with timely and accurate intelligence to support the commander, joint task force's (CJTF's), objectives, as stated in the C-IED plan, and to meet the information needs of the staff and component commands for operations and planning. The J-2 may elect to create a C-IED intelligence cell in order to focus the analyst's efforts. The mission of the J-2's C-IED intelligence cell is to produce and disseminate timely, all-source fused intelligence that will serve as a basis for the development and conduct of the command's C-IED effort.

(U) Operations Directorate of a Joint Staff (J-3).

(U) The operations directorate of a joint staff (J-3) is responsible for the direction of the joint task force's (JTF's) combat forces. The J-3 ensures that sufficient, properly equipped C-IED forces are available to support the JTF's mission within the operational area. The JTF J-3 C-IED operations intelligence fusion cell is the J-3's focal point to coordinate and synchronize all IED-related matters. Chaired by the J-3, the C-IED working group is tasked to work specific issues relating to the development of the JTF C-IED plan.

(U) Engineering Staff Section.

(U) The engineering staff section (J-7) coordinates combat, general and, in coordination with the J-2, geospatial engineering requirements for the joint force. In the C-IED effort, the J-7 establishes the explosive hazards coordination cell (EHCC) to advise the joint force on developments in adversary IED employment and potential friendly countermeasures. In certain situations, the EHCC

may also forward deploy (with the maneuver units) an explosive hazard awareness team.

(U) Joint Task Force (JTF) C-IED Boards, Working Groups, and Cells.

(U) In order to effectively manage the overall C-IED effort, the JTF will establish a variety of specialized boards, working groups, and cells. The JTF commander may decide to establish a JTF C-IED management board as a senior steering committee to manage the command's C-IED efforts. The purpose of the C-IED management board is to bring together senior JTF leadership with C-IED specialists to shape and direct the C-IED fight. Depending on the commander's requirements, J-3 recommends the formation of a C-IED working group. The working group, consisting of representatives from the J-2, J-2 collection management, J-2 plans, J-7, J-3 plans, J-3 operations, C-IED task force, and other members, as required, is tasked to work specific issues related to the C-IED plan.

(U) Coordinating with Supporting Theater- and National-Level C-IED Organizations.

(U) In organizing the operational area for the C-IED effort, the commander will have the ability to call upon assistance from highly specialized theater military, Department of Defense (DOD), national, and interagency assets that can deploy elements forward to augment the JTF staff. The theater, national, DOD, and interagency assets can perform a wide variety of functions designed to degrade the insurgents' IED infrastructure from detailed forensic/technical evaluations of IEDs, to managing a high-value individual targeting effort.

(U) Counter-Improvised Explosive Device Task Force

(U) The task force construct is useful when a large number of C-IED assets have been deployed to support large-scale, long duration operations.

(U) As an alternative to using the JTF staff to manage the C-IED effort, the CJTF can establish a task force, integrating tactical- and operational-level organizations and streamlining communications under a single headquarters whose total focus is on the C-IED effort. A C-IED task force is normally built around an appropriately augmented brigade-level headquarters or its equivalent (explosive ordnance disposal [EOD] group, ordnance group, engineer brigade, maneuver enhancement brigade, Army EOD battalion or Navy EOD mobile unit). In addition to controlling the subordinate EOD organizations and battalions, the C-IED task force commander is given operational control or tactical control of the JTF's specialized C-IED assets to include weapons intelligence team, combined explosives exploitation cell, C-IED

targeting program, C-IED operations integration center, C-IED training teams, and the technical escort detachment.

(U) The C-IED task force coordinates the overall conduct of C-IED operations through the JTF J-3.

(U) The mission of the C-IED task force is to enable and support the coordination of the JTF's C-IED operations to create the conditions that will deny the IED cells' freedom of action, reduce the IED cells' effectiveness, and lower overall IED activity to a level commensurate with the HN security forces' capabilities. It does so by commanding and controlling specialized C-IED forces as well as coordinating and synchronizing JTF-level C-IED operations, intelligence, technology and training initiatives throughout the operational area.

(U) C-IED Task Force Staff Functions.

(U) One of the most complex challenges in organizing the C-IED effort is in gathering, analyzing, and disseminating information that is relevant to each echelon of the command, from the brigade combat teams that must stay current on the latest adversary IED TTP, to the command that is organizing the fight to defeat the IED supporting infrastructure.

(U) C-IED Task Force Support to the Maneuver Units.

(U) The planning and conduct of C-IED operations is a multi-echelon effort that must be closely coordinated and integrated. The C-IED task force plays a critical role in this effort by attaching specialized C-IED support teams to the land component's subordinate divisions, maneuver brigades, and battalions. These C-IED support elements are designed to assist the maneuver unit in the planning, coordination, and integration of its immediate C-IED operations and act as a liaison to the C-IED task force. The C-IED support element also coordinates the unit's IED infrastructure targeting efforts.

(U) Multinational Considerations.

(U) In multinational operations, many of the participants do not have the trained and deployable EOD units, C-IED technologies, and exploitation capability required to protect their forces and take the fight to the enemy. When participating in a multinational operation that is facing a significant IED threat, the US CJTF may be called upon to provide our partners with a variety of C-IED support.

(U) C-IED Task Force C-IED Working Group.

(U) When the CJTF establishes a C-IED task force, the responsibilities of the JTF J-3's C-IED working group will normally transfer to the C-IED task force. When the C-IED task force commander establishes the working group, it will be responsible for identifying command-wide

C-IED-related issues and initiatives that impact the JTF's C-IED effort.

(U) CONCLUSION

(U) This publication provides joint doctrine for planning and executing C-IED operations. It outlines responsibilities, provides command and control considerations, discusses organizational options, details the C-IED process and AtN methodology, and introduces models for coordinating with C-IED supporting organizations.

Intentionally Blank

CHAPTER I
THE IMPROVISED EXPLOSIVE DEVICE THREAT (U)

(U) "In our laboratory we made powder which we used as a cap, and we invented various devices for exploding the mines at the desired moment. The ones that gave the best results were electric. The first mine that we exploded was a bomb dropped from an aircraft of the dictatorship. We adapted it by inserting various caps and adding a gun with the trigger pulled by a cord. At the moment an adversary truck passed, the weapon was fired to set off the explosion. These techniques can be developed to a high degree. We have information that in Algeria, for example, tele-explosive mines, that is, mines exploded by radio at great distances from the point where they are located, are being used today against the French colonial power."

Che Guevara
***Guerrilla Warfare*, 1961**

1. (U) The Improvised Explosive Device

a. (U) An improvised explosive device (IED) is a weapon that is fabricated or emplaced in an unconventional manner incorporating destructive, lethal, noxious, pyrotechnic, or incendiary chemicals designed to kill, destroy, incapacitate, harass, deny mobility, or distract. IEDs may incorporate military munitions and hardware, but are generally constructed from components that are nonmilitary in nature.

b. (U) IEDs are employed by threat groups across the globe to achieve their aims. This is, in part, due to IEDs' potential to produce strategic effects beyond their tactical impact. IEDs are designed to kill opponents and influence their actions, discredit them among the populace, and degrade their ability to achieve their objectives. Through the proliferation of the Internet and exploitation of readily available off-the-shelf technologies, insurgents, terrorists, and criminals have the capability to develop and employ improvised weapon systems with a relatively small investment. It is projected that such individuals and groups will likely increase their employment of IEDs while enhancing the lethality of their weapons and tactics. These weapons will represent a continuing threat to US forces and multinational forces (MNFs).

c. (U) Methods of IED employment fall within two major categories: suicide and non-suicide. In regard to suicide attacks, insurgents and terrorists can employ IEDs via person or vehicle, both of which are typically disguised as part of the populace. In non-suicide attacks, they conceal IEDs in the ground or in water, inside packages, common containers, vehicles, and even in carcasses. Waterborne improvised explosive devices (WBIEDs) can also be employed in rivers, lakes, and open water to attack not only small boats, but larger commercial or military ships. Surface-to-air IEDs could also be employed against military and civilian aircraft. Suicide and non-suicide tactics may be combined during one attack, or over the course of an operation, and IEDs may be used by irregular forces to augment some conventional tactics, presenting a complex threat to US and multinational forces.

d. (U) IEDs vary widely in shape, size, and form; however, they usually share three common components: main charges, initiating system, and containers. In addition to the three common components, an IED may contain enhancements. An enhancement is any optional component deliberately added to an IED as a secondary hazard. Fuel and fragmentation, as well as chemical, biological, radiological, and nuclear (CBRN) hazards are examples of enhancements. Figure I-1 illustrates the basic components of an IED. This diagram is not representative of the makeup of all IEDs and is only intended for illustration purposes.

(1) (U) **Switch.** A switch is a device for making, breaking, or changing an electrical or nonelectrical connection. Insurgents and terrorists specifically employ switches to fire or arm an IED. Some bomb makers also utilize safe-to-arm switches, so they are able to reduce the risk of accidental detonation during IED emplacement. There are three main categories of switches: command, time, and victim operated.

Figure I-1. (FOUO) Improvised Explosive Device Components

(2) (U) **Initiator.** The initiator is any device that is used to start a detonation or deflagration. In most cases the initiator in IEDs is a blasting cap. Blasting caps can be either electric or nonelectric and are commercially produced; however, insurgents and terrorists have demonstrated the capability to construct improvised initiators.

(3) (U) **Main Charge.** The main charge constitutes the bulk explosive component of an IED and can be configured for directional effects. Explosives fall into two categories: low and high yield. Low-yield explosives are combustible materials that deflagrate, do not produce a shock wave and must be confined to explode (e.g., black powder). High-yield explosives are materials that detonate with a shockwave and do not require confinement (e.g., dynamite).

(4) (U) **Power Source.** A power source either stores or releases electrical or mechanical energy for the initiation of an IED's main charge. The most common power source found in IEDs is batteries; however, insurgents and terrorists have also used alternating current to detonate their devices. In a nonelectric IED, the mechanical energy from a recoiled spring can actuate an initiator, subsequently detonating a main charge.

(5) (U) **Container.** A container is an item or vessel that commonly houses the whole or principal components of an IED. Containers are often designed to conceal the IED.

HISTORY OF IMPROVISED EXPLOSIVE DEVICES (IEDs) ACROSS THE RANGE OF MILITARY OPERATIONS (U)

(U) The IED has increasingly become the weapon of choice for terrorists, insurgents, and criminal organizations; however, the use of IEDs by these groups is not new. Insurgent groups in South America still manufacture IEDs in mountainside labs much like their predecessors of the 1960s. The term "IED" was coined by the British Army in the 1970s when the Irish Republican Army made fertilizer-based bombs boosted by military explosives supplied by Libya. IEDs are cheap, easy to construct, can be emplaced (or driven) anywhere, and can be readily adapted to fit a wide variety of circumstances and targets (Figure I-2). Equally appealing to asymmetric threat groups, is the potential for IEDs to produce strategic and operational effects disproportionate to their tactical impact. Predictably, high-profile attacks such as the bombings of the US Embassy and Marine Barracks in Lebanon (1983), World Trade Center (1993), Khobar Towers (1996), US embassies in Kenya and Tanzania (1998), and USS Cole (2000) have influenced domestic and international public opinion and shaped US foreign policy. However, the pervasive use of IEDs against US and multinational forces, as well as civilians, in both Iraq and Afghanistan has collectively and cumulatively produced strategic and operational effects extending beyond their immediate influence on tactics, techniques, and procedures. The combination of these two factors—low-cost effectiveness and the potential to produce strategic and operational effects—makes the IED an attractive asymmetric option for the foreseeable future.

Various Sources

Some examples of containers are carcasses, pipes, backpacks, jugs, tires, briefcases, vests, and vehicles.

2. (U) The Task of Countering Improvised Explosive Devices

a. (U) Our enemies employ IEDs to demonstrate their freedom of action; demoralize, distract, and discredit US, multinational, and host nation (HN) security forces; create fear within the general population; gain media exposure; and negatively impact US, HN, and partner nation (PN) interests. Actual or perceived successes of these tactical methods and approaches have been demonstrated in Iraq, Afghanistan, Lebanon, and Yemen. Figure I-2 outlines some examples of IED effects that an adversary can seek to create at the tactical, operational, and strategic levels.

b. (U) The IED battle is an evolving contest between the IED network and the US and its multinational partners. In Iraq, it began with command-wired IEDs. When US forces began looking for wires along the road, the IED builders began using remote garage door

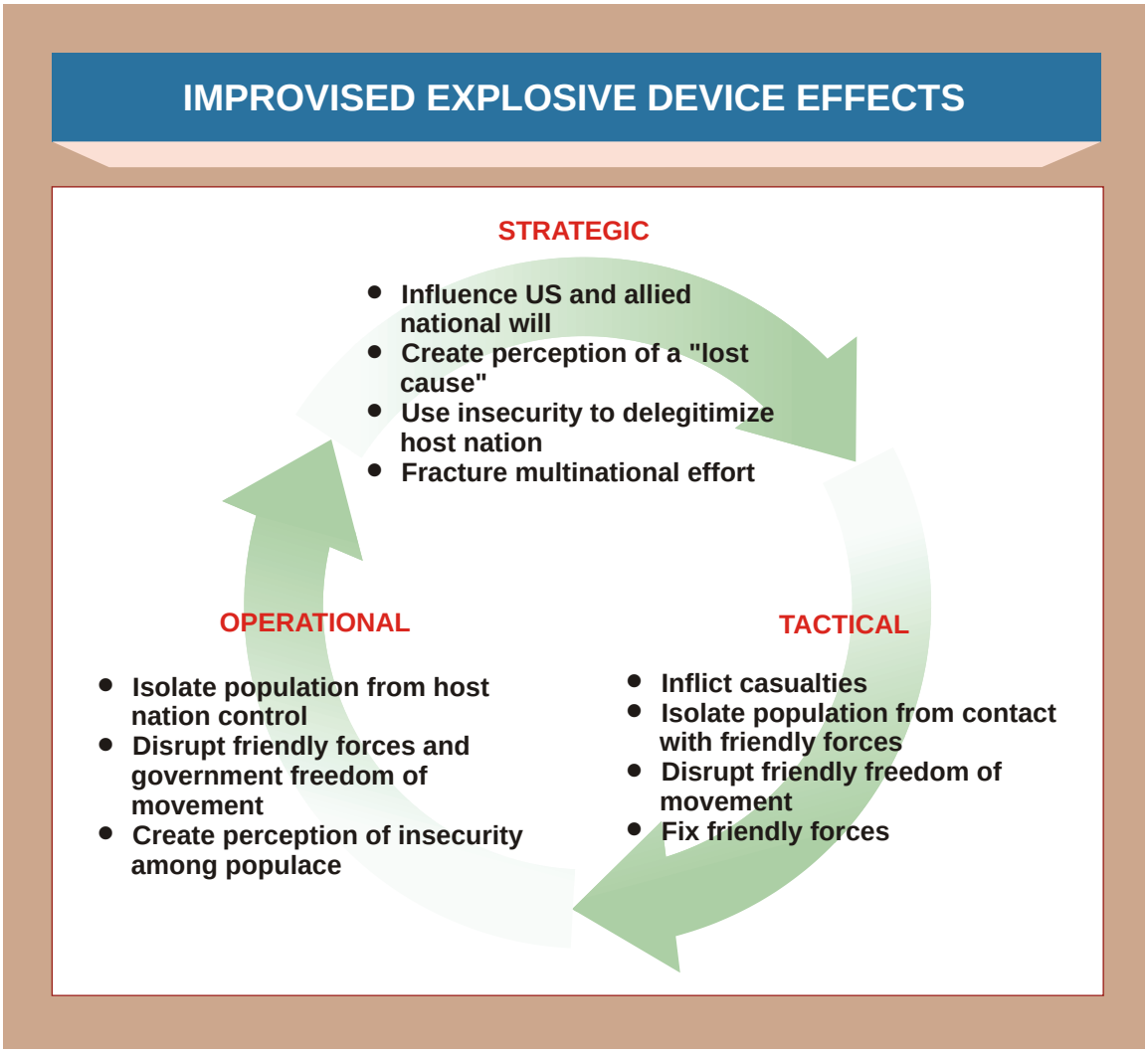


Figure I-2. (U) Improvised Explosive Device Effects

openers, cell phones, or toy car remote controls to detonate the devices. US forces then began jamming these frequencies or broadcasting on them in order to detonate the devices prematurely. The IED builders then returned to command-wired IEDs but buried the wires. In response to the evolving IED threat, the US science community introduced a variety of bomb countermeasures such as explosive sniffers, improved armor, improved explosive ordnance disposal (EOD) robots, and remote circuit detectors. Field commanders responded by conducting aggressive patrolling, employing 24/7 surveillance, grooming and clearing roadsides, and requiring the use of increased air transport to counter the threat. Each of these responses produced a change in the technology of tactics, techniques, and procedures (TTP) of the insurgents, terrorists, or criminals, such as the rise in the use of anti-armor IEDs (including explosively formed projectiles [EFPs]). Persistent intelligence, surveillance, and reconnaissance (ISR) facilitates identification of counter-improvised explosive device (C-IED) lines of operation (LOOs) by piecing together the IED network, identifying TTP being used, and highlighting adversary vulnerabilities.

c. (U) Meeting this threat requires a national effort based on a whole-of-government approach that addresses the device, the network that designs and emplaces the device, and the social-political aspects of the operational environment that facilitates IED employment. The United States Government (USG) has chosen to respond to the IED threat along three basic LOOs:

(1) (U) Attack the Network (AtN). This LOO consists of lethal and nonlethal 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 to enable success of the operation or campaign.

(2) (U) Defeat the Device. This LOO consists of activities to detect and neutralize IEDs before they detonate or mitigate the effects of the detonation at the point of attack to ensure freedom of movement and safer operations. These activities are enabled by rapid identification, development, acquisition, and delivery of capabilities for route clearing, device and explosive detection, improved EOD robots, and better vehicle and personnel protections.

(3) (U) Train the Force. This LOO is designed to mitigate the effects of enemy IED employment through the comprehensive training of US forces deploying to threat areas. Training should ensure that deployed troops are aware of the IED threat in their operational area and have an understanding of their missions, functions, and responsibilities, as well as the capabilities of their equipment to mitigate the effects of an IED attack.

3. (U) Domestic Considerations

(U) IEDs have been used in the US as early as the Civil War. In 1927, hundreds of civilians were killed or injured when a horse drawn cart, filled with explosives, was detonated on Wall Street. In modern times, the bombing of the Alfred P. Murrah Federal Building in Oklahoma City demonstrated the destructive capability of a simple mixture of fertilizer and diesel fuel. With the ready availability of potential IED materials and

components, easy access to instructions on IED construction, and the wide array of easily accessible potential targets, the US homeland is vulnerable to an IED attack at any time. The Department of Justice (DOJ) and Department of Homeland Security (DHS), have the primary responsibility and lead to plan and to prepare, deter, prevent, detect, defend, respond, and recover from terrorist use of IEDs or other activities on US territory. The Department of Defense (DOD) supports their efforts by providing detection, prevention, disruption, preemption, and mitigation of the effects of transnational terrorist actions against the United States, its citizens, and its interests overseas. DOD also shares IED-related information with other USG agencies and departments concerning worldwide threats and the tactical characterization and technical categorization of IEDs encountered by US forces. The technical, forensic, and biometric data recovered from IEDs by DOD is shared with DOJ and DHS in support of domestic counterterrorism activities. Under Homeland Security Presidential Directive-19, *Combating Terrorist Use of Explosives in the United States,* DOD would provide additional C-IED-specific support to civilian agencies. This support specifically includes EOD and support to weapons technical intelligence (WTI) functions. Additional support can include bomb detection equipment, military working dogs, and access to information sharing platforms and other C-IED capabilities as requested.

4. (U) Maritime Considerations

(U) IEDs also pose a significant threat to maritime forces. Terrorist, insurgent, and criminal organization use of the maritime environment, with its proximity to key population centers and inherent integration into transportation hubs and infrastructure, presents a multifaceted security challenge for land and naval forces. The potential for adversary use of WBIEDs has significant capability for impacting access and freedom of movement in areas and environments from blue to green water, the coastal littoral, and stretching far inland. Terrorists, insurgents, and even criminal gangs have demonstrated an ability to attack naval forces with a variety of IEDs, including floating homemade mines and explosive-laden small boats. A modern example is the attack on the USS Cole, which resulted in significant damage and loss of life. C-IED operations must be tailored to operating in a maritime domain that uniquely affects friendly abilities to detect the presence of explosives or explosive devices, locate the explosive or device precisely, diagnose the device to determine its components and how they function, and defeat the device. Navy expeditionary forces, specifically EOD, expeditionary intelligence, security force assistance, riverine, and maritime expeditionary security units, provide the naval component commander and the joint force commander (JFC) with the necessary capabilities to counter IED networks. Maritime forces operating in the littorals must closely coordinate with land component, multinational, and HN forces to establish and maintain a seamless common operational picture (COP) and share information regarding terrorist/insurgent threats and their networks in the operational area.

CHAPTER II
THE IMPROVISED EXPLOSIVE DEVICE NETWORK (U)

(U) "Just attacking the device specifically is not going to solve the IED [improvised explosive device] problem; you also have to look at the network that is in place."

Lieutenant General Michael Oates, US Army
Director, Joint Improvised Explosive Device Defeat Organization

1. (U) Introduction

a. (U) The IED is a weapon used by terrorists, insurgents, and criminal organizations to achieve their objectives. In spite of their diverse purposes, these groups often interact to exchange information, conduct resource transactions, share weapons design and tactics, and otherwise interrelate to achieve efficiencies that would otherwise be impossible (Figure II-1).

b. (U) IED networks are centrally and decentrally organized because of the need to protect relationships and hide activities at the tactical, operational, and strategic levels. The leadership of these IED networks plan, organize, and execute many critical activities necessary to accomplish their objectives (Figure II-2). Within these IED networks, functional plans and operations are interconnected and may impact each other in direct and indirect ways and at all levels. Recognizing these interrelationships is critical when attempting to attack a network.

c. (U) Fundamental to all networks is an understanding of the resourcing, especially financial resourcing, required to start up, sustain, and grow the organization from the strategic level through to the tactical units. Regardless of the network's objectives, money flows enable and empower the network to resource and sustain its activities. Effectively attacking this network requires an understanding of the IED network's business model (Figure II-3).

(1) (U) The diagram illustrates the economic and financial activities of a representative network. It shows that the organization is active in white, gray, and black markets for goods and services, have fixed and variable costs of production, and invest financial capital assets for growth. This financial activity creates opportunity to disrupt or interdict the resource flows and thereby bankrupt or seriously restrict the network and its operations.

(2) (U) In this model, networks profit from the use of IEDs by inflicting casualties on government personnel and innocent civilians, damaging and destroying equipment and infrastructure, and fostering psychological anxiety on the part of target audiences. The IED users successfully raise and receive funds, and maintain a reliable, steady flow of revenues from multiple sources, including quasi-legitimate business operations, gray market sales, criminal money-making activities, laundered investments, and financial backers. They incur operating expenses to maintain and grow profitable, self-sustaining threat organizations. These include the payment of bribes, the purchase of physical capital assets and equipment, and the costs of personnel, raw materials, and intermediate goods. The day-to-day operating routine will also require myriad other planned and unplanned commercial transactions. As

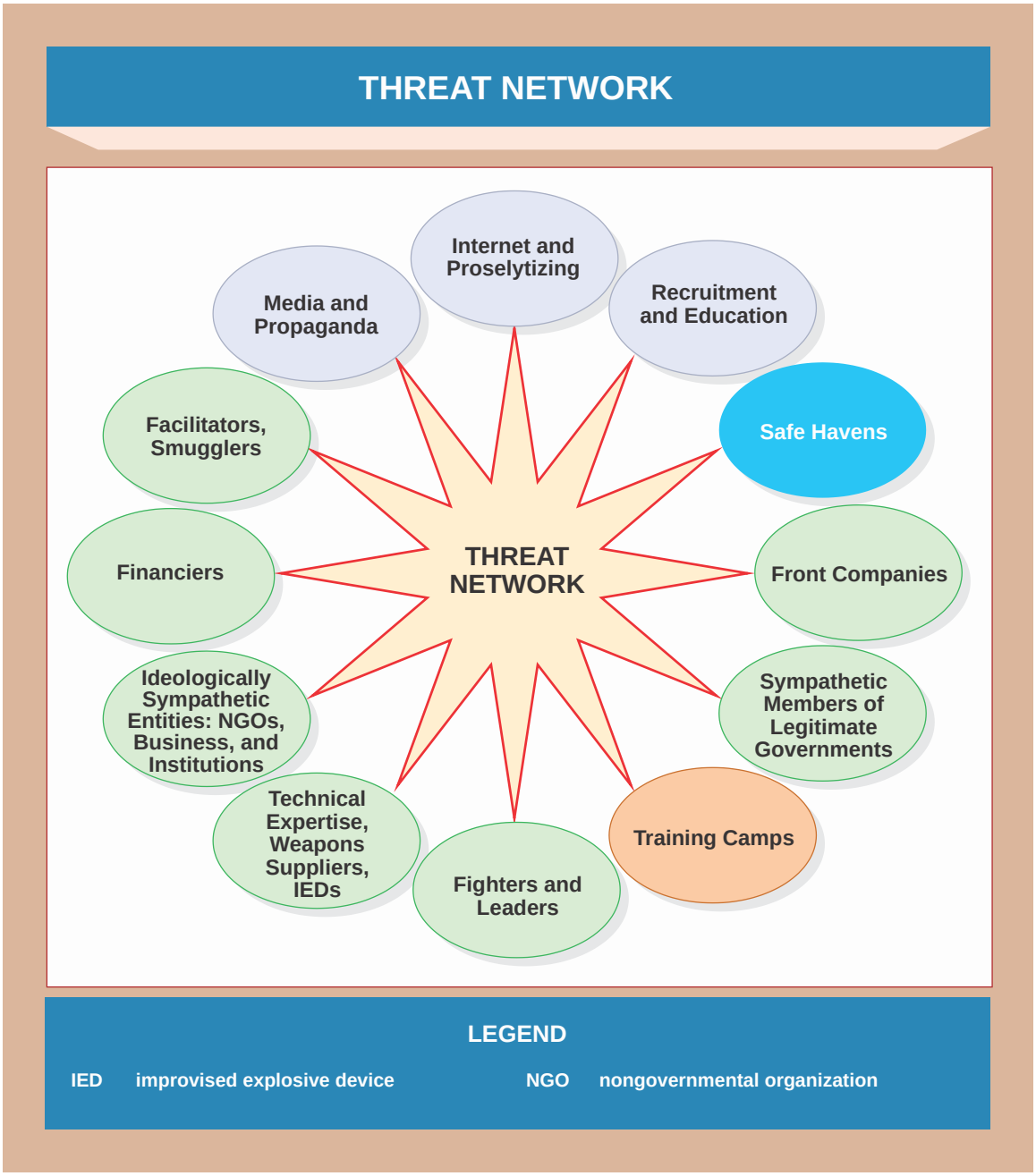


Figure II-1. (U) Threat Network

with any business, it is possible that the notional network may experience a negative net cash flow if operating expenses exceed revenues. This unprofitable state of affairs may require the liquidation of existing financial reserves to cover expected and unexpected expenses.

d. (U) Counter threat finance (CTF) operations may be conducted to bankrupt or shut down networks. CTF operations are often planned and conducted by the cooperating members of the international community and reach from the strategic to the tactical level.

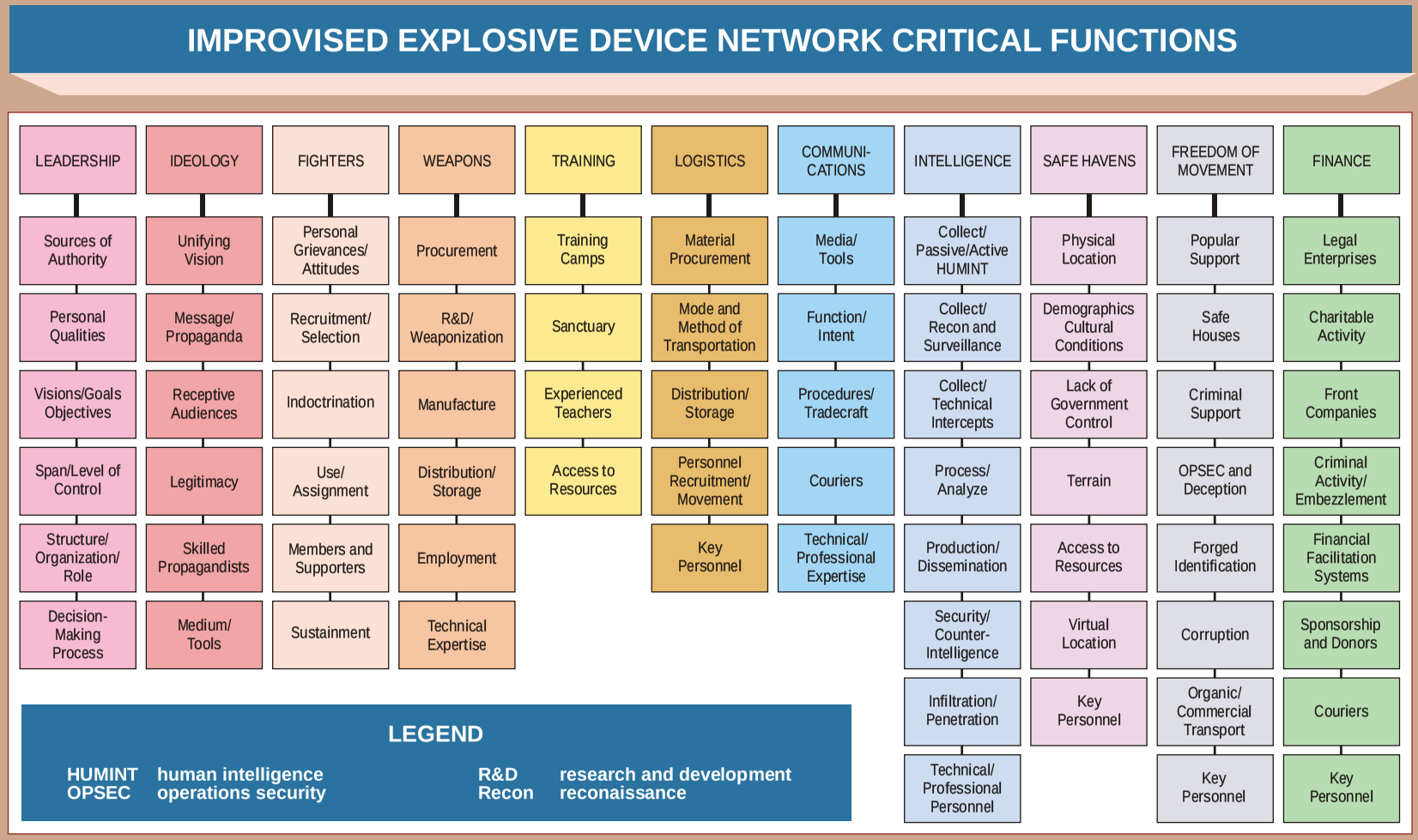


Figure II-2. (U) Improvised Explosive Device Network Critical Functions

CTF operations include squeezing profits and revenue sources and streams; driving up operational, financing, and transactions costs and risks; identifying, tracking, and interdicting commercial and financial transactions and smuggling activities; and freezing or seizing real property and other physical capital assets and financial capital assets and reserves. Typically, DOD would be in a supporting role to CTF operations.

2. (U) Network Characteristics and Components

a. (U) Whether the IED is employed by an insurgent, a terrorist, or a criminal gang, it is resourced, manufactured, emplaced, and executed through what is likely a secretive and networked organization. Virtually all such networked organizations use some variant of a cellular or compartmented structure to enhance security and organize for operations. These networked organizations make full use of the interconnected global environment as a major means of connectivity to direct operations, raise money, obtain and train recruits, and freely exchange technological information.

b. (U) Any group that systematically employs IEDs must perform a series of networked operations or activities to be successful. These operational requirements include resourcing (finance and supply) and personnel (bomb-making specialists and planners), which are driven or guided by ideological or economic motivation. Although some network activities may occur simultaneously or sequentially, activities associated with these operations are frequently conducted independently. Each of the functions may be organized as one or more cells within the network, and participants in each function/cell may be unaware of the others' existence. Many of the network functions supporting IED operations are typically shared with those of a larger network that is also supporting other illicit activities such as drug trafficking and money laundering. In addition to sharing functions with other networks, these IED networks may have ties to external state-sponsored support.

c. (U) Not all network functions are critical, but information derived from noncritical functions can lead to the identification and exploitation of the network's vulnerabilities, contributing to its disruption. Often, through detecting, tracking, and exploiting both general IED and other illicit activities, US and multinational forces can determine how a network is structured, sustained, and conducts its operations."

d. (U) The problem set related to the IED network, depending on its size, scope, and complexity can span the tactical, operational, and strategic levels. While leveraging local perspective and experience is essential to achieving lasting disruptions of network activity in-theater, the requirement to synchronize and integrate tactical activities at the operational and strategic levels to defeat an enemy's IED campaign remains critical. For example, a network's supply chain is global in reach and can move IED components internationally to locations in a commander's operational area. A truly comprehensive counter IED-proliferation program requires a fully integrated set of diplomatic, financial-regulatory, export-control, customs, law enforcement, and military operational intelligence capabilities, systems, and authorities.

e. (U) For an IED network to sustain itself, it must be able to continuously respond to changing environmental pressures—political, economic, social, financial, and military.

Survival and success are directly related to adaptability and the ability to compete for resources—financial, logistical, material and human—successfully. The most important attributes adversary networks require for success are:

(1) (U) A decentralized nonhierarchical structure.

(2) (U) Shared identity among the membership normally based on goals or objectives, grievances, kinship, ideology, religion, and personal relations; shared identity also facilitates recruitment.

(3) (U) Access to IED components, technology, and bomb-making expertise, knowledge, skills, and abilities of group leaders and members.

(4) (U) Access to resources, in terms of money, arms, material, logistical support, and public recognition.

(5) (U) Adaptability, including the ability to learn and adjust behaviors and modify TTP in response to friendly initiatives.

(6) (U) Sanctuary to conduct planning, training, and logistic reconstitution.

3. (U) The Improvised Explosive Device Activity Model

a. (U) While defensive measures against the IED itself are an important part of C-IED operations, focusing exclusively on defeating the device will not produce lasting operational success. C-IED operations should begin with a holistic understanding of the enemy and the common activities associated with an IED attack in order to break the enemy's operational cycle. To this end, the IED activity model (Figure II-3) can help commanders identify and attack potential adversary vulnerabilities to disrupt the IED network, as well as, take defensive measures against IEDs to reduce their effectiveness. IED activities can be categorized in four recurring phases—planning, execution, assessment, and exploitation—and may be conducted concurrently or asynchronously by multiple cells.

(1) (U) During planning and execution, resourcing activities include everything from technical and monetary support to recruiting and training cells and supplying materials needed for IED production. Resourcing also includes the key components of leadership and the will to conduct the continued attacks. It culminates in the planning and construction of IEDs in preparation for an attack.

(2) (U) Execution begins with the surveillance and targeting selection for a specific attack. It includes rehearsals, IED staging, emplacement, and monitoring. This phase ultimately ends with an IED attack and may include egress by the attackers.

(3) (U) The IED users will conduct an assessment of their attack to determine its effectiveness. In some instances immediately subsequent to an event, follow-on forces or first responders may come under attack by secondary IEDs or other fires. The adversary will constantly seek to modify the weapon or alter TTP to improve effectiveness or account for countermeasures.

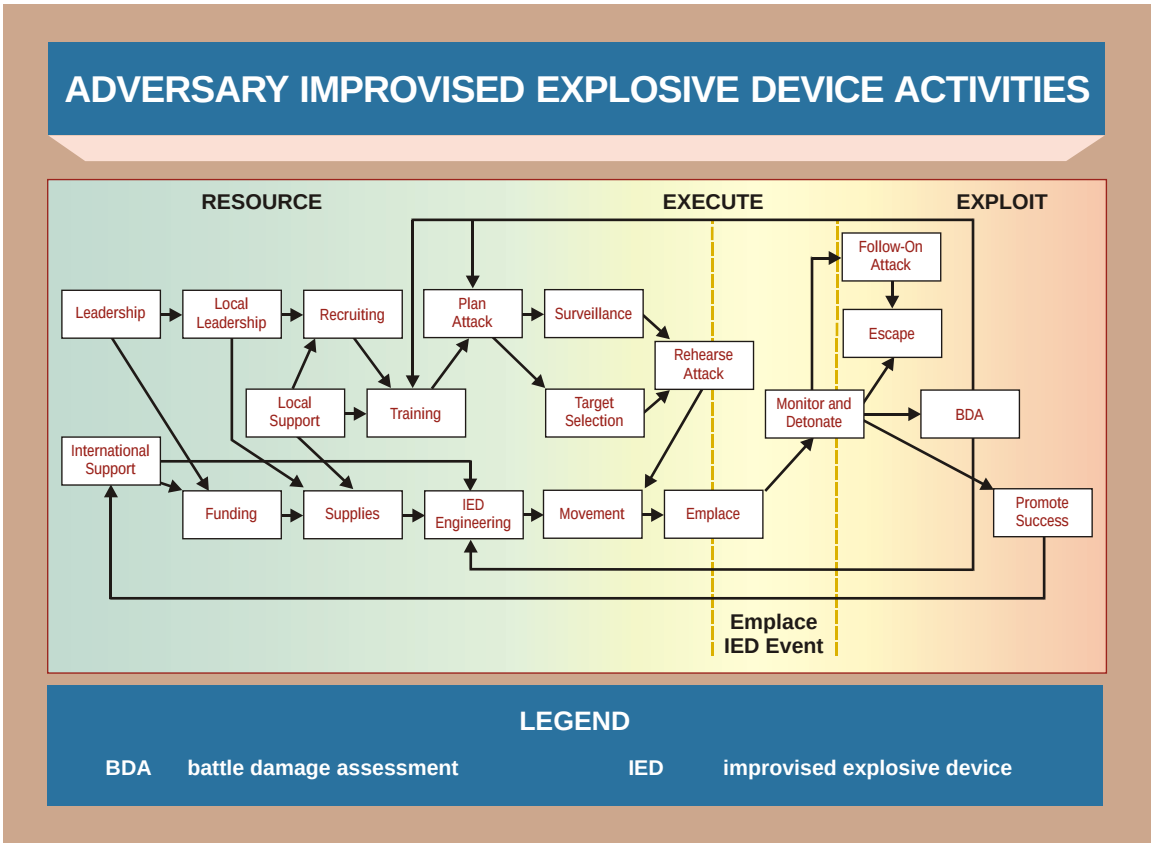


Figure II-3. (U) Adversary Improvised Explosive Device Activities

(4) (U) The IED users will seek to exploit the results of an attack by conducting a propaganda campaign to affect local attitudes, host government security forces, and popular will. Well-publicized successes may also foster or reinforce support to the attackers from domestic or international actors.

b. (U) To successfully mitigate or neutralize the IED threat, it is essential that the freedom of access to, movement in, and action by IED proliferation networks be curtailed or interdicted. AtN operations when executed individually or in a piecemeal fashion may produce short-term tactical success, but may not produce operational or strategic advantages. Attacking the IED network support system requires developing the requisite operational intelligence to target multiple activities simultaneously at the appropriate tactical, operational, and strategic levels. For example, in the early stages of an adversary's IED employment, the joint force can gain the initiative by taking actions to find and seize munitions supplies, logistical managers, and bomb makers. Although equally important at the onset of a conflict, once operations are under way, joint forces may need to focus on securing support from the HN population while bolstering the legitimacy of the HN government to influence and render ineffective an adversary's freedom of movement and freedom of action. For example, in Iraq and Afghanistan, the huge stocks of munitions and ready availability of commercial materials, such as fertilizers, that supply the raw materials for the bomb makers, coupled with the use of dozens of Internet sites providing detailed information on bomb construction, greatly complicated development of a successful C-IED

strategy. Suitable metrics to assess the effectiveness of ongoing C-IED operations should be developed by the JFC and staff. The metrics can take many forms and will normally be closely tied to those developed for assessment of the broader operation or campaign.

Intentionally Blank

CHAPTER III
PLANNING FOR COUNTER-IMPROVISED EXPLOSIVE DEVICE OPERATIONS (U)

1. (U) Introduction

a. (U) C-IED operations often focus on the device; however, the device is merely the end product of a complex set of activities the adversary executes to achieve his objectives. An IED attack is the result of a planned operation that can have strategic, operational, and/or tactical effects, not solely because of the military value of the target, but also the psychological effects on units, the local population, the region, and political leadership. An integrated, synchronized C-IED plan is designed to address all levels of war. The actions at the strategic level include the coordination of all instruments of national power, the collaboration and cooperation with the combatant commands to deny the enemy funding, supplies, safe havens, and a favorable information environment to influence public opinion. At the combatant command level, the C-IED plan provides guidance for isolation and attacking elements of the IED network, mitigating effects of an IED blast, training the force in C-IED TTP, and transferring equipment and capabilities to participating MNFs and the HN. A C-IED plan is an integral part of the overall theater campaign plan and the subordinate plans. The actual design of the theater C-IED plan will depend on the security agreements with HNs, capabilities of HN forces, time phasing of available US capabilities, and the quality of the joint intelligence preparation of the operational environment (JIPOE). The C-IED requirements will be established by the JFC. For C-IED operations to be effective across all levels of war, they must be viewed in the context of the larger whole-of-government operation or campaign plan and integrated across all staff sections and functional areas.

b. (U) Insurgents and terrorists have favored IEDs because they have strategic impact on HN security and peoples' safety, making it imperative that C-IED operations be integrated into counterinsurgency (COIN) or counterterrorism operations. Whatever the enemy's objectives, C-IED operations can protect the civilian population from harm, thereby reinforcing the legitimacy of the HN government. C-IED operations should be designed to allow commanders and staffs at all levels to plan and take proactive measures to identify and target the IED networks, to reduce the employment of IEDs by increasing the cost to the enemy of that tactic. There are key IED network activities and signatures that influence planning at each level of war. These activities must be viewed both individually and in conjunction with the other activities that enable C-IED efforts. C-IED operations must take a holistic approach that incorporates intelligence, information, training, operations, materiel, technology, protection, policy, and resourcing solutions designed to address the strategic, operational, and tactical objectives of the overarching operation/campaign. C-IED operations may be conducted during any phase of a military operation (i.e., shape, deter, seize the initiative, dominate, stabilize, and enable civil authority) and may have to be executed concurrently with other LOOs, each to commence conditionally, and then to continue in parallel throughout an operation/campaign. At a minimum, C-IED operations should include the three LOOs of the C-IED framework—AtN, train the force, and defeat the device. The level of effort for each LOO will vary by phase. While the actual operational

phases will vary depending on the type of operation, appropriate C-IED plans must be developed and executed to ensure comprehensive support.

c. (U) The foundation of a C-IED concept of operations (CONOPS) is a coherent strategy that links strategic, operational, and tactical activities to objectives, and integrates interagency actions to ensure unity of effort, both inside and outside of the area of responsibility (AOR). At the theater and operational levels, the geographic combatant commander (GCC) coordinates with national agencies, such as the Joint Staff, Joint Improvised Explosive Device Defeat Organization (JIEDDO), National Counterterrorism Center, Biometrics Identity Management Agency (BIMA), the National Ground Intelligence Center (NGIC), Defense Intelligence Agency (DIA), and our allies to ensure unity of effort in the planning and conduct of C-IED programs across the AOR. Joint force C-IED activities must be viewed both individually and in the context of their relationship to the other interagency partners' activities conducted using other instruments of national power. Joint force C-IED activities fulfill five basic purposes:

(1) (U) **Protect US, multinational (if applicable), and HN forces and the local populace against the physical effects of IEDs.** Protection of our forces and innocent civilians is paramount to achieving diplomatic and military objectives and bolstering US and HN national will.

(2) (U) **Enable mobility in operational areas.** Effective C-IED operations can enhance the ability of US forces and MNFs to operate freely in the operational area.

(3) (U) **Expose and neutralize IED networks.** C-IED operations must reach beyond countermeasures to eliminate these explosive weapons by attacking and defeating the networks behind IED attacks, their leaders, and supply chains.

(4) (U) **Neutralize impact of IED use.** Effective C-IED reduces IED use and promotes perceptions of a secure environment. A shared perception of a secure environment can enable social and economic stability, return to pre-conflict behaviors, and facilitates the HN government's legitimacy in the eyes of the populace. Effective C-IED also enhances the public's negative perception of IEDs and criminalizes IED use, which directly undermines support for the enemy.

(5) (U) **Stabilize economic activity in the affected locality.** As part of a comprehensive stability operations program, effective C-IED operations contribute to the creation of a secure environment and allow local industries to function at pre-conflict levels conducted before the IED threat appeared. It facilitates the HN government in achieving and maintaining legitimacy in the eyes of the populace, thereby undermining local support for the adversary.

d. (U) A number of important considerations are unique to understanding the design of C-IED operations. First, the IED threat must be addressed within the context of the larger operation/campaign. Second, the joint force must develop a comprehensive and coordinated plan that is proactive and attacks the IED network and avoid focusing C-IED efforts solely on defeating the device. Third, operations and intelligence must be closely linked with

results of operations immediately feeding the intelligence picture. The fusion of the various intelligence methods (human intelligence [HUMINT], signals intelligence [SIGINT], etc.) with information derived from WTI and biometrics provides valuable information that enable joint forces to attack the network and defeat the device. Fourth, C-IED efforts require persistence, because effectively attacking the network, defeating a diverse and plentiful array of IEDs, and training the force take time, and there are no immediate or one-time solutions.

2. (U) Mission Analysis

a. (U) The joint force will conduct C-IED operations within the context of a broader operation or campaign. In certain instances, however, the JFC may choose to conduct focused C-IED operations to eliminate or neutralize the threat in a specific area. In either case, the mission analysis phase of the joint operational planning process (JOPP) will provide for the effective planning to achieve the commander's objectives.

(U) *For a detailed description and explanation of the mission analysis step of JOPP, see Joint Publication (JP) 5-0,* Joint Operation Planning.

b. (U) The commander uses the mission analysis step to develop and focus staff and subordinate commanders' thinking and efforts to achieve the goals and objectives of the force. The commander assesses the guidance from higher authority, analyzes the operational environment, integrates the operational approach (developed via operational design), and produces a restated mission, and commander's intent and planning guidance. Three activities within the mission analysis step are particularly relevant to the conduct of successful C-IED operations.

(1) (U) Determination of Specified, Implied, and Essential Tasks. The staff must have knowledge of the standard C-IED tasks to determine whether or not the purpose of the operation and the expected operating environment will make them essential to success and therefore explicitly stated in the restated mission. At the operational level, those tasks associated with attacking the IED network will often be most important because those tasks will be similar (if not the same) to those of stability and support operations or COIN operations.

(2) (U) Force Allocation Review. The initial force allocation review will reveal the capabilities, limitations, and training levels of the force. When facing an IED threat, in most cases, units will require augmentation with dedicated C-IED enablers. These are non-organic organizations, systems, or training that will best allow a unit to operate safely, to use intelligence resources, and to effectively engage targets.

(3) (U) Development of Risk Assessment. The commander will determine the types and levels of risk that are acceptable in the execution of the operation. The nature and character of the ever-evolving IED weapon will demand focused analysis of intelligence and rapid development and integration of countermeasures. The IED is specifically designed and employed to not only inflict personnel and equipment casualties, but also to create a psychological impact that affects population behavior and national will.

3. (U) Developing a Counter-Improvised Explosive Device Concept of Operations

a. (U) A CONOPS is a verbal or graphic statement that clearly and concisely expresses what the JFC intends to accomplish and how it will be done using available resources. The concept is designed to give an overall picture of the operation. It describes how the actions of the joint force components and supporting organizations will be integrated, synchronized, and phased to accomplish the mission, including potential branches and sequels. The staff writes (or graphically portrays) the CONOPS in sufficient detail so that subordinate and supporting commanders understand their mission, tasks, and other requirements and can develop their supporting plans accordingly. During CONOPS development, the commander determines the best arrangement of simultaneous and sequential actions and activities to accomplish the assigned mission consistent with the approved course of action.

(U) JP 5-0, Joint Operation Planning, *contains more information on operational design as it applies to CONOPS development. Chairman of the Joint Chiefs of Staff Manual (CJCSM) 3122.01A,* Joint Operation Planning and Execution System Volume I: (Planning, Policies, and Procedures), *provides detailed guidance on CONOPS content and format.*

b. (U) The following is an example of a theater C-IED CONOPS and includes the desired end state and campaign objectives.

THEATER COUNTER-IMPROVISED EXPLOSIVE DEVICE CONCEPT OF OPERATIONS EXAMPLE (U)

1. (U) Commander's Intent. Improvised explosive devices (IEDs) are the enemy's primary asymmetric weapon and remain the top cause of casualties among friendly forces. We need to create a counter-improvised explosive device (C-IED) effort that is comprehensive, integrated with our interagency, multinational, and regional partners, timely, holistic and long-term. I expect my commanders at all echelons to integrate C-IED operations into ongoing joint and combined operations. Look at the entire problem. We need to address and attack the entire IED chain of events, not just along single points in the chain. While we can never entirely eliminate the use of IEDs, we can substantially reduce our opponent's ability to employ them. Force protection initiatives are paramount. We need to find solutions that can be applied across the area of responsibility (AOR). Aggressively pursue technological and non-technological solutions, being mindful that the enemy will constantly adapt. Training, tactics, techniques, and procedures (TTP), doctrinal and organizational solutions can be high payoff. Integrate the C-IED effort across all aspects of doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF). Ensure these efforts are interoperable and compatible throughout DOTMLPF. This is a long-term effort; expect no immediate payoffs. We must develop and continuously refine organizations, networks, formal programs, and funding for the long war.

2. (U) End State. The end state for the C-IED operation is a fully integrated and synchronized C-IED effort across the AOR, resulting in a sustained

reduction in the employment and the effects of IEDs as tactical weapons of strategic influence.

3. (U) Objectives. This operation seeks to increase the risks and costs to the enemy of employing IEDs to the point where the enemy no longer employs IEDs as its weapon of choice. We will employ a holistic approach to identifying key elements in the enemy's IED infrastructure, focus on the critical nodes in that infrastructure and apply relentless pressure to curtail or derail efforts of IED networks, utilizing a full array of lethal and nonlethal options. We will make the employment of an IED so expensive for the enemy in terms of material, financing, and personnel—eliminating sources of supply and financing, attacking the bomb makers, and turning public opinion against the enemy that it will seek other means of attack. We increase the risks, along with the economic, financial, and moral costs by engaging partner nation populations and governments in order to make the employment of IEDs a risky, expensive, and unacceptable tactic within the AOR.

4. (U) Lines of Operation

a. (U) As JFCs visualize the operational design of the operation, they may use several LOOs to help visualize the intended progress of the joint force toward achieving operational and strategic objectives. LOOs define the orientation of the force in time, and space or purpose, in relation to an adversary or objective. **JFCs may describe the operation along LOOs that are physical, logical, or both.** Logical and physical LOOs are not mutually exclusive, and JFCs often combine them. Normally, joint operations require JFCs to synchronize activities along multiple and complementary LOOs, working through a series of military strategic and operational objectives to attain the military end state.

b. (U) **There are three basic C-IED LOOs that form the basis for the conduct of all C-IED planning and operations:**

(1) (U) **Attack the Network.** Lethal and nonlethal 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.

(2) (U) **Defeat the Device.** The goal when defeating an IED is to prevent or mitigate its physical effects while neutralizing the adversary's ability to exploit the value of its effects in terms of building a platform to generate fear, terror, or propaganda victories. C-IED device defeat actions begin once the device has been emplaced and include detection, predetonation, rendering safe, and conducting a thorough forensics analysis. Information derived from the physical exploitation of the device and the analysis of how it was employed is used as a basis for a variety of force protection initiatives, to include the development of technologies to detect/neutralize the device and protect individuals.

(3) (U) **Train the Force.** Force providers must ensure that the force is adequately trained prior to deployment. Areas of special interest include the development of relevant and current IED-related TTP, drills, standard operating procedures, and battle staff and leader training in C-IED principles and methodologies to integrate and effectively employ C-IED enablers in theater. Training should be designed to enhance individual and unit protection and the unit's ability to effectively operate in a high-threat IED environment and employ C-IED enablers. Training should also include activities that facilitate the establishment and growth of multinational and PN device defeat capabilities, including the transfer of C-IED technology (previously approved for transfer by competent authority) and the US force's TTP.

c. (U) In designing a C-IED operation, supporting LOOs may be labeled in accordance with mission, enemy, terrain and weather, troops and support available–time available. However, AtN, "defeat the device," and "train the force" remain the threads that are woven appropriately throughout the operation. The C-IED-related LOOs should be nested within the overall joint operation's or campaign's LOOs.

d. (U) Additional LOOs are usually developed to account for the special circumstances or requirements of the mission in a particular operational area. For example, facing a COIN, US Central Command has developed the additional LOO—"Develop Multinational and Host Nation C-IED Capability" (see Figure III-1). Through the execution of each LOO, the

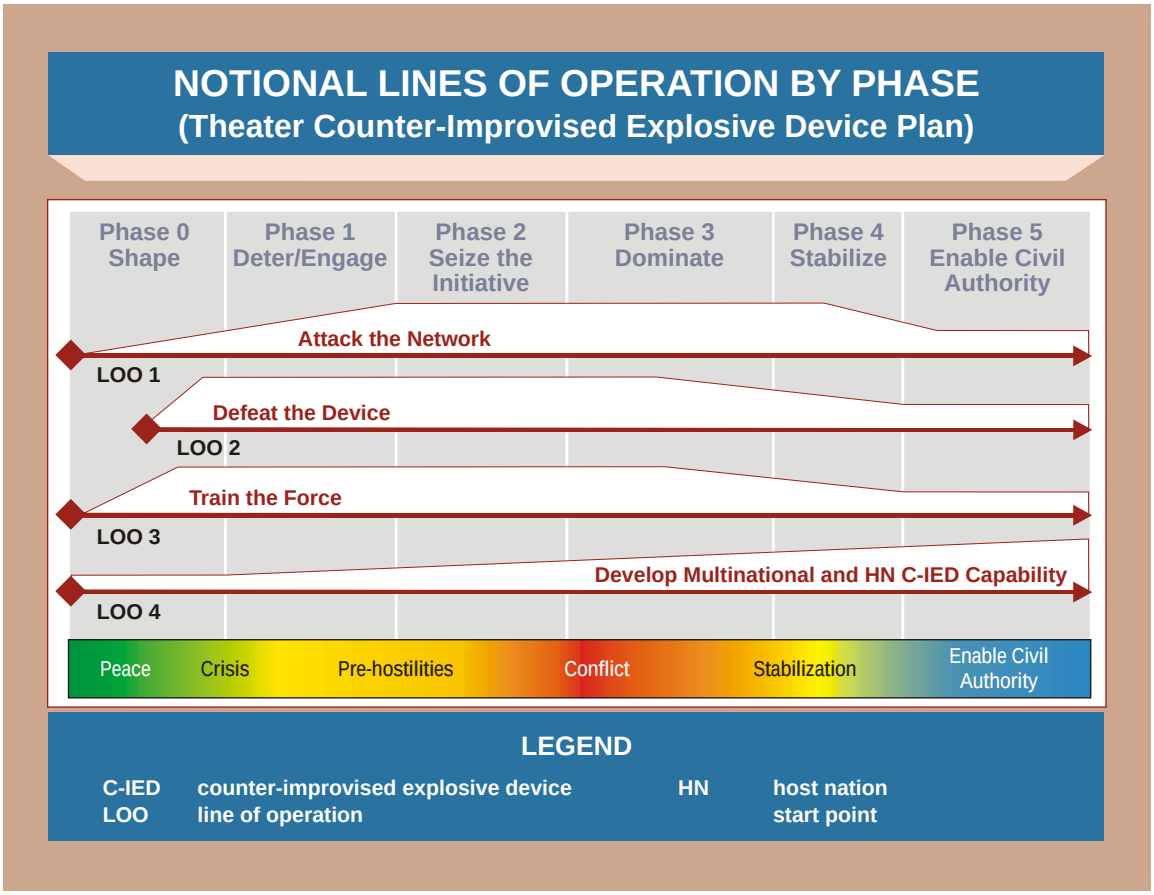


Figure III-1. (U) Notional Lines of Operation by Phase (Theater Counter-Improvised Explosive Device Plan)

adversary's centers of gravity are attacked within each level of war at decisive points disrupting his ability to plan, conduct, and exploit IED operations. C-IED LOOs' objectives are also designed to provide for the protection of friendly forces, equipment, and facilities from IED effects.

e. (U) The following is an example of a theater C-IED CONOPS, where the C-IED LOOs align with the GCC's guidance and intent and provide the groundwork for the development of a CONOPS for the conduct of C-IED operations.

THEATER COUNTER-IMPROVISED EXPLOSIVE DEVICE CONCEPT OF OPERATIONS EXAMPLE (U)

(FOUO) General. The command executes a counter-improvised explosive device (C-IED) effort along lines of operation (LOOs). This C-IED operation plan is based on these LOOs.

(FOUO) LOO 1—Attack the Network. This LOO includes plans and operations designed to reduce improvised explosive device (IED) effects and interrupt the enemy's chain of IED activities by discovering and exploiting vulnerabilities and enabling offensive operations.

(FOUO) LOO 2—Defeat the Device. In order to enhance commanders' freedom of movement and mitigate operational risk, defeat the device actions and activities detect IEDs, neutralize them before they can detonate, or mitigate the effect of IED detonation at the point of attack.

(FOUO) LOO 3—Train the Force. Mitigating the effects of enemy IED employment through comprehensive training of US and partner nation (PN) forces puts troops in the field who understand their mission, function, and responsibilities, and are situationally aware and understand C-IED reporting, response, and equipment use in the field and how best to use it in a force protection capacity. Effectively countering IEDs also requires battle staffs and leaders who understand the C-IED principles and methodologies to integrate and effectively employ C-IED enablers.

(FOUO) LOO 4—Develop Multinational and PN C-IED Capability. The emphasis is to facilitate the establishment and growth of multinational and PN C-IED capabilities, including transfer and sharing of C-IED tactics, techniques, and procedures.

LOO 1—Attack the IED Network (U)

1. (FOUO) The main effort of any operational-level C-IED operation is to isolate the threat network from the population. The decisive operation of the C-IED fight is to enable friendly networks in the government and security services to derail or neutralize IED networks and gain popular support through counterinsurgency (COIN) and stability operations. Within this context, precise and focused "attack the network" operations combine lethal and nonlethal actions and operations against networks conducted

continuously and simultaneously at multiple levels (tactical, operational, and strategic) that capitalize on, or create, key vulnerabilities. These actions are designed to reduce IED activity and effectiveness and create the necessary conditions for COIN and stability operations to succeed.

2. (FOUO) The focus area is intelligence preparation designed to enact successful C-IED operations, which entails: developing an understanding of the enemy's IED capability based on a thorough intelligence preparation of the operational environment; developing a thorough understanding of the enemy's external support for the IED tactic; and ensuring a rapid understanding of the technical aspects of the IED tactic to develop effective countermeasures.

3. (FOUO) In order to succeed in C-IED operations, unrelenting pressure must be applied to IED networks at the strategic, operational, and tactical levels; e.g., denying the adversary's flow of funding, IED training, and interdicting illicit technologies and supplies. Actions to counter the IED tactic must include time-sensitive decision making, direct action execution, and rapid and precise "institutionalization" of C-IED lessons learned, best practices, and training in order to be more proactive than the adversary's adaptive decision-making and execution capability. This asymmetric tactic requires a "quick reaction" mindset, a rapid response planning process, and a time-sensitive targeting capability. Actions that facilitate "attack the network" operations include:

a. (FOUO) The use of the Counter-IED Operations Integration Center, which directly supports the warfighters' efforts to focus attacks on enemy networks employing IEDs; and US, multinational, and PN interagency actions against IED proliferation network actors and activities; the employment of the Naval Explosive Ordnance Disposal Technology Division's combined explosives exploitation cell labs along with the National Ground Intelligence Center's Weapons Technical Intelligence cells to enable the technical and forensic exploitation of recovered devices; the leveraging of the information operations partnership with national organizations such as the Joint Improvised Explosive Device Defeat Organization; the ongoing development and use of material solutions include: National System for Geospatial Intelligence Video Services, Key Hole, Identity InstaCheck, Palantir, Data Tracker software as well as multiple intelligence, surveillance, and reconnaissance platforms and sensors.

b. (FOUO) To provide long-term continuity developed by the first two focus areas, the third focus area is to develop a well-integrated communications strategy. The objective is to influence and turn the local populace from supporting or enabling the insurgent's use of the IED tactic, working against violent extremism. The sympathetic or coerced populations throughout the area of responsibility (AOR), and in the joint operations area (JOA) in particular, facilitate, not only the freedom of action and movement of the insurgents and their ability to employ the IED tactic, but they greatly deny friendly forces the proactive capability to find and strike the IED networks and the devices themselves. By shaping the perceptions of the

indigenous populations to favor our goals and objectives, or at least oppose adversary propaganda and behavior, we deny the insurgents and terrorists the freedom of action they must have to operate so effectively.

c. (FOUO) Decisive Points. The decisive point along this LOO will be reached when the local leadership speaks out against violent extremism and the use of IEDs as an accepted tactic within their communities and borders; the local population constantly provides tips to friendly and PN forces on IED locations and perpetrators; and transnational criminal/terrorist and nationalist insurgent networks are no longer able to employ IEDs as tactical weapons of strategic influence.

LOO 2—Defeat the Device (U)

1. (FOUO) The aim is to defeat the device once it has been assembled and/or emplaced, including detecting emplaced IEDs and rendering them safe, protecting the force by defending against physical effects of IEDs, and mitigating propaganda effects. IEDs are anonymous and both physically and psychologically effective. Master bomb makers have developed thorough knowledge on how to capitalize on readily accessible commercial off-the-shelf technology, available sources of explosive material such as homemade explosives, conventional ordnance, explosive remnants of war and the process for the construction, emplacement, and detonation of IEDs along with personnel needed to employ the devices effectively. Two adverse effects to friendly forces result with each successful IED attack. The first result is the physical damage due to loss of life and property. The second result is the loss of perceived security and prestige or invincibility of the friendly forces and the fledgling HN governments caused by the continuing attacks and the media coverage of the attacks. This result impairs progress toward the COIN objectives. Defending against these effects through force protection measures, operations security measures to minimize adversary knowledge of our capabilities and vulnerabilities, proactive information operations, and strategic communication will reduce the insurgents' and terrorists' most effective weapon.

a. (FOUO) The primary focus of "defeat the device" is countering and neutralizing IEDs. The first step is hardening, equipping, and training the force in C-IED force protection measures. The second step is to disseminate counter IED-related information throughout the AOR and JOA in order to mitigate the enemy's rapid adaptation to our methods, thereby keeping forces one step ahead of the adversary. The third step is executing effective and culturally aware information operations with the communications strategy to counter the adversary media efforts that validate the IED attacks. The third step must run concurrent with the first two steps. In this LOO, we must prioritize our capabilities to take into account operating in a politically restrained environment not commonly planned for in major combat operations. There is more reliance on situational awareness, command and control, and protection measures, while utilizing nontraditional operations to shape the environment.

b. (FOUO) Decisive Points. The decisive point along this LOO is achieved when the capabilities are available in required quantities to defeat present devices throughout the theater, and research and development is focused on anticipated emerging IED capabilities.

LOO 3—Train the Force (U)

(FOUO) The aim is to facilitate the establishment and growth of comprehensive individual, staff, and unit C-IED training programs that will enhance individual protection, maintain our freedom of movement, and carry the fight to the adversary. Personnel will be appropriately trained prior to deployment to the JOA to be able to undertake the theater's missions in light of the conditions and adversary threats. As the adversary is constantly adjusting its TTP, an in-theater training program based on real-time lessons learned will provide ongoing training for deployed individuals and units. Commanders should ensure that staffs are properly trained to plan and conduct C-IED operations.

LOO 4—Develop Multinational and PN C-IED Capability (U)

1. (FOUO) The aim is to facilitate the establishment and growth of multinational and HN C-IED capabilities to target IED proliferation networks including, but not limited to, network sponsors, suppliers, distributors, trade and trade-financing facilitators, and procurement facilities; facilitate the transfer of C-IED technology, information, intelligence, and TTP; and create a socioeconomic environment that actively opposes the use of violence, extremism, or IEDs as a means of political expression. It is the goal of the collective C-IED campaign to not only defeat IEDs as an asymmetric means of attack against multinational forces, leadership, and key infrastructure, but to prepare the HN to assume this role throughout their country. The joint task force (JTF) ensures: HN forces are organized, trained, and equipped to do the mission; gain experience and confidence from conducting C-IED operations with multinational forces throughout the preceding phases of multinational operations; and ensure that the JTF creates and leaves behind a way for them to train themselves. The key is to ensure that they have a capable force to accomplish the mission.

a. (FOUO) The three foci to accomplish this LOO are protecting the multinational and HN while their C-IED capabilities are being developed; developing multinational and HN C-IED capabilities through, but not limited to, force C-IED organization and training, transferring, and sharing of C-IED technologies and TTP; and finally, transferring C-IED responsibilities to the multinational force and HN.

b. (FOUO) Decisive Points. The decisive point along this LOO is reached when IEDs are no longer used systemically as tactical weapons of strategic influence in the AOR and JOA, and HN C-IED capacity is sufficiently advanced to anticipate and deter emerging IED capabilities.

5. (U) Counter-Improvised Explosive Device Annex to the Operation Plan

(U) When analysis of the operational area by the intelligence directorate of a joint staff (J-2) indicates the existence of a real or potential IED threat to friendly operations, commanders should prepare a C-IED annex to the operation plan (OPLAN) based on the previously described LOOs. An example of a C-IED annex is contained in Appendix E, "Counter-Improvised Explosive Device Annex Template."

6. (U) A Balanced Approach

a. (U) A successful C-IED OPLAN is one that employs a mix of lethal and nonlethal actions to deny the enemy access, freedom of movement, and action. Constant pressure on critical nodes in the enemy's infrastructure will keep the enemy off balance and degrade his overall effectiveness. It will also force the enemy to reveal increasing portions of the network as they attempt to reconstitute their activities. A holistic targeting effort will include a mix of direct action against leadership, bomb makers, emplacers and caches, and local infrastructure; interagency actions to disrupt the enemy's value or supply chain and support structure (political, financial, and logistical) outside of the joint operations area (JOA); and information operations (IO) to discredit the enemy and the use of IEDs in the eyes of the local and regional population. It will also ensure that every action is supported by an effort to exploit the results and further refine the targeting process.

b. (U) In the C-IED targeting process, WTI plays a key role in supporting both lethal and nonlethal targeting through the analysis of technical and forensic information that can provide direct intelligence leads on individuals, TTP, and sites associated with the IED proliferation networks. It also supplements and amplifies information derived from other intelligence disciplines to further refine targeting packages and the intelligence collection process. Information derived from WTI may assist HN law enforcement personnel in the identification, investigation, and arrest of perpetrators; raise the level of security in an area; and increase the population's confidence in the ability of the government to provide security. Emphasis on unit collection of biometric information, fusion of multi-intelligence disciplines and requests for further analysis of this information by the JIEDDO Counter-Improvised Explosive Device Operations Integration Center (COIC) can provide commanders with a more defined picture of the IED network, further enabling planning for the lethal or nonlethal targeting of these associated networks.

c. (U) Military information support operations are another nonlethal component of C-IED operations. For example, when the enemy targets friendly military and police forces with IEDs, they frequently result in the indiscriminate killing and wounding of nearby civilians. Used properly, this information can be used against the enemy by:

(1) (U) Informing the local populace of civilian casualties and deaths due to the enemy's use of IEDs.

(2) (U) Informing local populace of the positive, effective security measures being taken by HN forces and MNFs.

(3) (U) Encouraging the local populace to report IEDs, caches, and individuals who support or conduct IED operations.

(4) (U) Developing messages that support the criminalization of IEDs and their associated employment.

CHAPTER IV
ATTACKING THE IMPROVISED EXPLOSIVE DEVICE NETWORK (U)

(U) "The enemy network is a needle in a haystack. We live in the haystack."

Dr. David Kilcullen, Senior Counterinsurgency Advisor
Multinational Force Iraq (2007)

1. (U) Introduction

(U) In the context of C-IED operations, AtN operations specifically target the enemy's ability to resource and conduct IED attacks (Figure IV-1).

a. (U) In order for the IED network to survive in an environment where it is being hunted by friendly forces, the adversary must be able to continuously respond to changing environmental pressures—political, economic, social, and military. Survival and success are directly connected to adaptability and the ability to compete for resources—financial, logistical, and human. While adversary networks possess many attributes, among the ones important to their success are:

(1) (U) A decentralized nonhierarchical structure.

(2) (U) Shared identity among the membership normally based on kinship, ideology, religion, and personal relations; shared identity also facilitates recruitment.

(3) (U) Knowledge, skills, and abilities of group leaders and members.

(4) (U) Resources in the form of arms, money, social connectivity, and public recognition.

(5) (U) Adaptability, including the ability to learn and adjust behaviors and modify TTP in response to friendly initiatives.

(6) (U) Sanctuary to conduct planning, training, and logistic reconstitution.

b. (U) While there are a variety of ways to template an adversary's IED support network, most share common functions, including leadership and planning, logistics support, communications, and finance. These major functions require funding, information and intelligence, personnel, and materiel to maintain the overall network infrastructure. The adversary's IED network (Figure IV-2) is designed to transfer resources from the operational levels down to the local cell executing attacks. In turn, the results of those attacks, properly packaged and distributed, help to provide the propaganda needed to demonstrate the success of a particular network, facilitate criminal money-making activities, assist in fund-raising and recruiting activities, broaden their support base, increase intimidation, and decrease the probability of cooperation with HN and multinational security personnel.

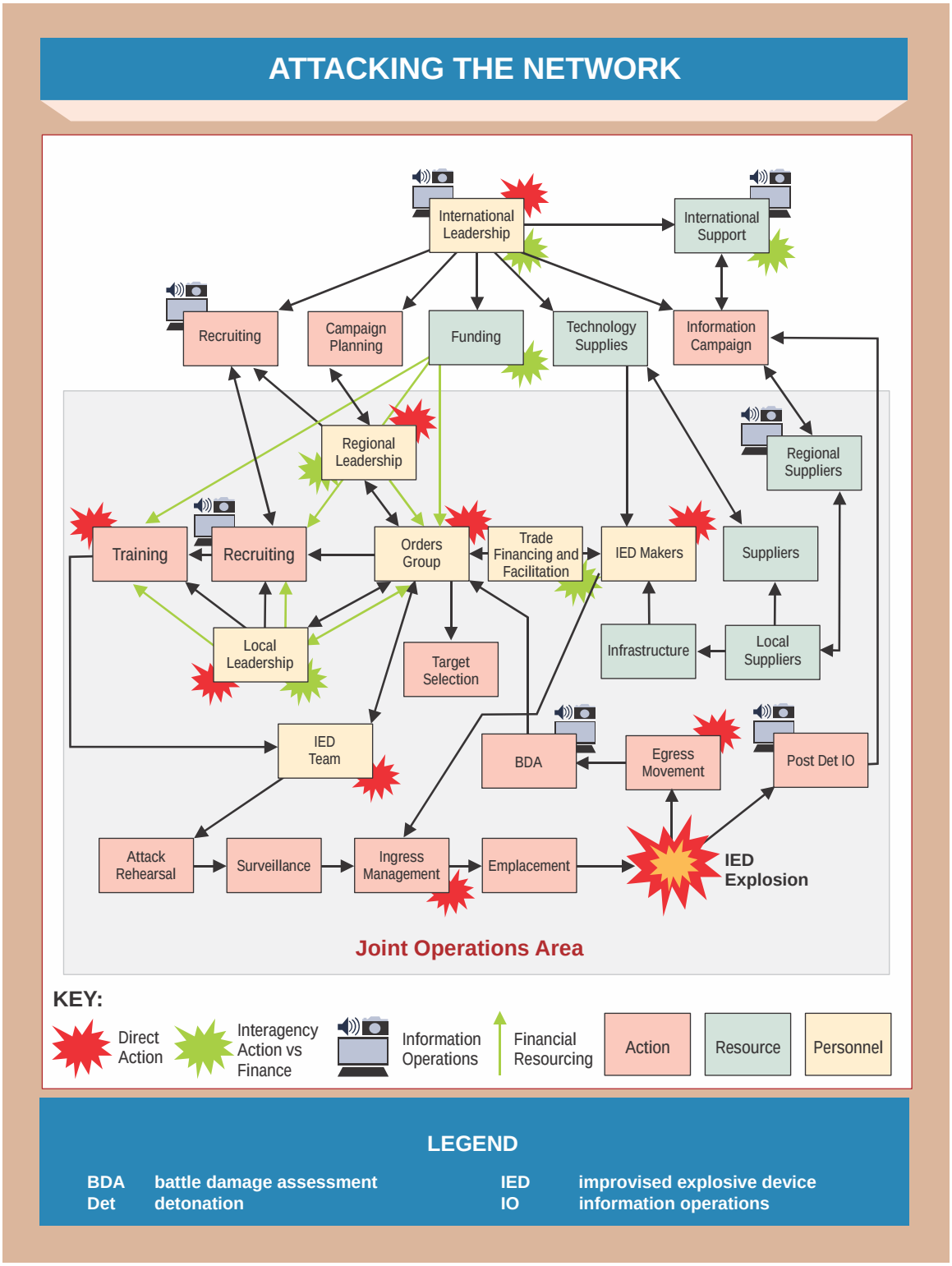


Figure IV-I. (FOUO) Attacking the Network

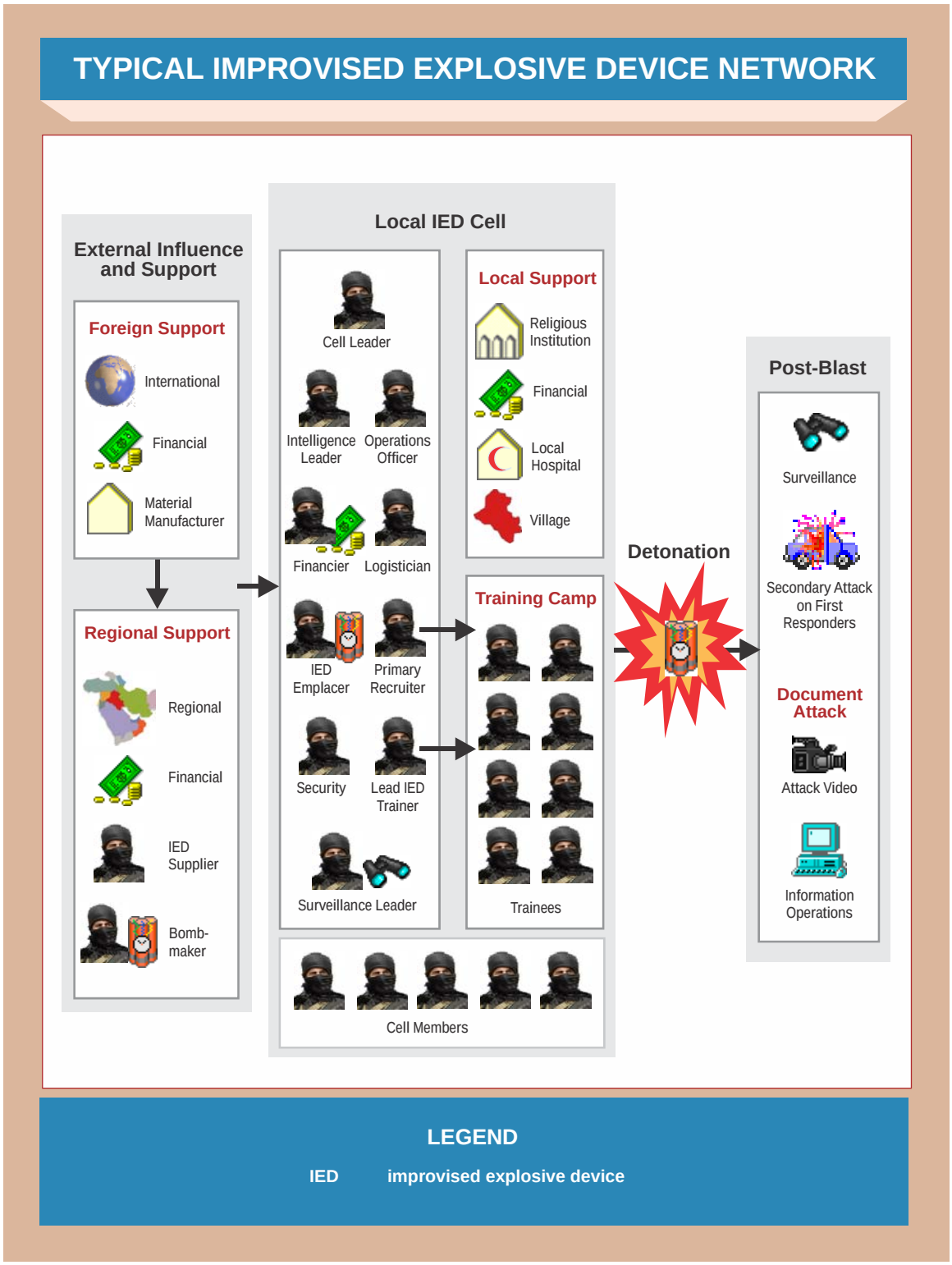


Figure IV-2. (U) Typical Improvised Explosive Device Network

2. (U) Strengths and Weaknesses of a Network

a. (U) Core strengths required to maintain an effective IED network may include:

(1) (U) The ability to adapt over time.

(2) (U) The ability to blend into the operating environment, making it difficult to separate the adversary from the local population.

(3) (U) The ability to rapidly replace personnel losses by recruiting new members, usually through personal relationships and an effective IO program.

(4) (U) A relative high level of insularity makes it difficult to gain intelligence on them for purposes of either destruction or obtaining greater understanding of them. This insularity is based primarily on the bonds of kinship, religion, and purpose that tie members together.

(5) (U) Ability to establish cellular organizations that limit the friendly force's ability to roll up sizable portions of the network.

(6) (U) Networks can be highly connected both internally in terms of their members and to the externally respective country's social structure. Individuals can be connected to one another and their leaders in multiple ways, including kinship, religion, former association, and history, among other factors. This layering of affinity creates densely internally connected networks and supports their cohesiveness. Through their membership, these networks are also connected to major social structures—the tribal system and its associated religious structure—giving them opportunities to acquire both resources and support.

(7) (U) The ability to disassociate from the IED event by paying financially motivated uninformed locals to emplace the IED or by using externally recruited suicide bombers to execute missions, thereby minimizing MNF HUMINT collection capabilities.

b. (U) While adversary networks have inherent strengths, they also have exploitable inherent weaknesses. These may include:

(1) (U) Competition for resources, including the loyalty of the population, often leads to one group working against the other.

(2) (U) Connectivity among cells. Although the cellular structure is a highly secure one, the links between cells can be identified and exploited over time.

(3) (U) The need to conduct activities, for example, reconnaissance, movement, attack rehearsals, etc., that increase the likelihood of detection resulting in the exposure of key network nodes or functions.

(4) (U) Competing interests or objectives among insurgent groups will often lead one group to work against another.

(U) "What behavior do we want? Funerals or diminished/stopped IED [improvised explosive device] activity? If killing leaders doesn't achieve that, what will? This brings us back to what I cited as the two most critical pieces of advice: In order to stop the activity or make them go somewhere else, you have to know more than HOW they set up IEDs, you need to know WHY they are setting IEDs. In order to know that you have to know about the AO [area of operations]—the people, their beliefs about certain behaviors, their goals, their fears, their leaders, their leaders' goals, fears, motivations, etc. The S-2 [intelligence staff officer] doesn't get that data from higher HQ [headquarters] INTSUMs [intelligence summaries] or assessments. He meets with the other intel professionals in the AO; he meets with the PSYOP [psychological operations] guys, the CA [civil affairs] guys, the engineer officer (if he is involved in local projects)—anyone who operates outside the wire—and builds the picture of the AO.

(U) When you can answer "Why do they do this?" you can advise on the HOW to make them stop. If the result of your information gathering indicates that a critical node in the net is a person who, if removed, will seriously disrupt the local network, not just the cell, then removal of that individual may be useful—provided the elimination fits in or can be made to fit in with the larger narrative (messages)."

Bryan N. Karabaich, Colonel, US Army (Retired)

(5) (U) The natural tendency to replicate previous successful actions and unwittingly establish exploitable patterns.

3. (U) Attacking the Network—General Considerations

(U) While attacking the adversary's network is a complex, time-consuming task, raising the adversaries' cost of IED employment to unacceptable levels can be accomplished through a focused, continuous series of operations designed to disrupt the people, places, processes, and materials that support the IEDs' design, supply, and employment chain. However, C-IED operations must be accomplished within the context of successfully targeting the broader adversary infrastructure.

a. (FOUO) There is no guaranteed method of defining and codifying targetable activities and major components of an IED network. To avoid detection and attack, adversary networks camouflage and constantly revise, or adapt, their TTP. At the highest echelons, the leadership rarely communicates openly and generally uses trusted aides and couriers to provide broad guidance to subordinates and direct the network. At the lowest echelons, the local cell members are detectable, targetable, and replaceable. Therefore, eliminating individuals only provides temporary and limited solutions to countering IED threats. But as networks function and move resources (information, money, supplies, recruits) from the highest to the lowest echelons, these activities are detectable and targetable. Disrupting the flow of resources is the most reliable way of neutralizing the adversary's use of IEDs. While ideology may produce recruits, they have to eat, obtain weapons, travel, and build, transport, and emplace bombs. Personnel can be replaced, but the adversary's logistical infrastructure and materials often take more time.

b. (U) When designing an AtN program, the following information requirements must be adequately addressed:

(1) (FOUO) What are the important elements of the IED networks? (Define them in terms of key functions and nodes.)

(2) (FOUO) How do friendly lethal and nonlethal actions directed at different IED network critical functions affect the network?

(3) (FOUO) If a given network critical function is eliminated or degraded, what are its likely successors?

(4) (FOUO) How do removal and influencing actions directed at successors affect the network?

(5) (FOUO) How long does it take for a network to recover when critical nodes are removed?

(6) (FOUO) Which is more effective, removing a network function or influencing it?

(7) (FOUO) Can observed activities be correlated with predictions, using differences or comparisons to gain insight?

(8) (FOUO) How can the effectiveness of friendly actions directed at networks be measured?

(9) (FOUO) How do we determine when a network is no longer capable of accomplishing its mission or is successfully defeated?

(10) (FOUO) How do we influence the population to reduce/eliminate their support to the network?

(11) (FOUO) Who are the local leaders or key actors who can influence the local population and how can they be influenced?

4. (U) Counter-Network Strategy Development and Required Capabilities

a. (U) The ends of an effective counter-network strategy that curtails the IED threat to the joint force or HN population will invariably focus on the operational environment that allows the threat to take place. The perpetrators of IED attacks are motivated by various causes. Political ideology, religious fervor, nationalism, or criminal gain are among the most common reasons. Commanders will rarely attempt to neutralize the IED as the sole purpose of an operation. Rather, effective commanders will understand the IED as a symptom of deeper socio-political-economic issues. A successful long-term counter-IED strategy will seek to find the root cause of the unrest and prevent the decision to use this weapon in the first place.

b. (U) The ways of the counter-network strategy use an operation or campaign design process that allows operational art to link ends, ways, and means to reach the desired end state. The approach will include a description of the operational environment and a statement of the problem to be solved. The operational approach will inform JOPP for course of action determination, creation of the commander's estimate, and plan/order development.

c. (U) To attack the network, commanders and staffs must first understand the operational environment in network terms. The previously described IED network is a subset of the adversary network, and it will interact with the HN population, which can be explained as a neutral network. Friendly forces can also be thought of and considered in network terms as well. An important feature of any network is its adaptability to a changing environment; one change to a node or link may substantially affect the entire network. Because of this dynamic nature of complex adaptive systems, a second imperative for effective counter-network operations is to closely link operations and intelligence. The third essential element for an effective strategy is to rapidly assess the effects created by operations and feed the assessment into the intelligence process. This will include both foreseen and unforeseen results.

d. (U) The means a commander will use to conduct AtN operations is a joint force alongside multinational, intergovernmental, and other like-minded partners that possess the following capabilities and characteristics:

(1) (U) **Analyze.** The ability to apply analytical techniques to information detected and collected to produce intelligence that describes the friendly, neutral, and threat networks and the operational environment.

(2) (U) **Collect.** The ability to continuously and methodically acquire relevant information by any means to gain data and understanding of the operating environment and its friendly, neutral, and threat networks.

(3) (U) **Detect.** The ability to perceive, utilizing technologies or natural sensory abilities, information, activities, material, or persons, potentially related to a friendly, neutral or threat network.

(4) (U) **Disseminate.** The ability to communicate relevant information in a timely manner across the strategic, operational, and tactical levels.

(5) (U) **Engage.** The ability to conduct actions, lethal or nonlethal, on a specific target to create desired results.

(6) (U) **Exploit.** The ability to take full advantage of success in military operations and follow up initial gains by detecting, collecting, and analyzing information, personnel, and materials found during the conduct of operations.

(7) (U) **Target.** The ability and process to methodically select and prioritize an entity, location, object, function, or behavior for possible action to create desired results.

5. (U) Attack the Network Across the Levels of War

a. (U) At the strategic, national, and theater levels, AtN operations are focused on global, international, or transnational threats and networks requiring coordination and integration with interagency partners, MNFs, and multinational organizations. Key AtN operations at this level include positively shaping the strategic environment using the full range of the instruments of national power and developing and providing the partnerships, information, and resources required for strategic success. Success at this level normally depends heavily on influencing a range of audiences including international opinion, network members and supporters, allies, and the US public. Strategic actions can also include specific efforts to gain intelligence, conduct analysis, and target certain nodes and critical functions that require interagency or multinational support.

b. (FOUO) At the operational level, AtN operations should employ a highly adaptable, collaborative, and decentralized approach, blending physical and cognitive abilities to achieve a desired end state. Through the use of specialized analytical tools, commanders will be able to refine their understanding of the operating environment and focus resources on key nodes in the IED infrastructure. For example, geospatial intelligence (GEOINT) can be used to identify portions of the network such as safe houses, bomb-building locations, and cache sites. Commanders and their staffs facilitate and enable AtN operations by developing training activities that lead to better understanding of the operational environment prior to deployment. When operating in sector, units employ their intelligence capabilities to conduct analyses of IED proliferation networks and employ C-IED enablers to develop an extended intelligence picture at the regional and international levels. They coordinate and inform lower echelons of the effects desired, ensure unified actions are taken to favorably shape the operational environment, and employ IO to influence the enemy, the populace, and multinational partners. Most important, commanders should empower leaders at the lowest levels to make timely decisions by pushing to them relevant information and C-IED enabling capabilities. Operational success at this level may also have an impact at the strategic and theater levels, affecting national and military operational strategies and planning.

c. (U) At the tactical level, the focus is on executing AtN operations. Accurate, timely, and relevant intelligence will drive this effort, and tactical units should exercise refined procedures to conduct analysis, template, and target networks. AtN tactical operations include efforts to secure the population, strengthen HN security forces, and counter insurgents' ideology, propaganda, and ability to sustain themselves financially, materially, and logistically. Tactical units will also conduct precise kill/capture operations, often based on time-sensitive targeting. However, engaging in tactical operations against an IED network is not done in isolation but is part of the broader national, strategic, and theater campaigns to eliminate the causes of the insurgency and support the legitimate government.

d. (U) A successful AtN program includes network analysis, templating, and targeting. It is based on the development and exploitation of C-IED-specific intelligence in the form of WTI, usually derived from exploited IEDs, and intelligence derived from all sources to include SIGINT, GEOINT, document and media exploitation (DOMEX), and measurement and signatures intelligence. The central contribution of WTI to the AtN process is linking specific individuals to particular IED events through the use of biometrics enabled

intelligence (BEI) and forensic-enabled intelligence, thus removing insurgents' veil of anonymity and exposing them to a range of counteractions—military, legal, and other. The goal of an AtN program is to provide the commander and staff with an in-depth understanding of the enemy networks in their operational area. In-depth understanding of the network allows for more sophisticated, holistic approaches to attacking it, combining lethal and nonlethal means. Since most unit-level intelligence staffs do not have the personnel resources, time, or software to produce in-depth detailed network analyses, reachback enablers like the JIEDDO COIC, US Army Asymmetric Warfare Group (AWG), and the NGIC capabilities can provide the requisite level of intelligence support for optimized network prosecution.

6. (U) Targeting the Network

a. (U) There are a number of targeting methodologies that have been developed to facilitate AtN. These methodologies (which include find, fix, finish, exploit, analyze, and disseminate [F3EAD] and decide, detect, deliver, and assess) can also be merged to complement each other. Regardless of the method employed, established processes and procedures must be identified, standardized, and exploited to develop and refine a comprehensive picture of the adversary to effectively target and attack an IED network.

b. (U) Every target should be exploited for information. Results from the exploitation are documented and provided to operational-level analysts for further refinement and future targeting actions. Exploitation can include examination of documents, financial ledgers, cell phones, computer hardware, WTI collected from IED components (pre- and post-blast), and biometric data from a variety of sources, and tactical questioning (TQ) or interrogations of detainees. While individual pieces may not seem significant, over time, as information accumulates and is correlated, these actions can reveal significant additional detail about the network's nodes and individual participants. Exploitation should be employed immediately for the collection of WTI from IED components, DOMEX, cellular exploitation (CELLEX), computers, and any other intelligence materials. Even pocket litter may reveal where the individual has been or with whom they have been communicating.

7. (U) Find, Fix, Finish, Exploit, Analyze, and Disseminate

a. (U) F3EAD, a subset of the find, fix, track, target, engage, and assess (F2T2EA) targeting process, may be used to engage selected high-value individuals (HVIs) or activities (caches, bomb-making facilities). It incorporates the same fundamentals of the joint target cycle and facilitates synchronizing maneuver, intelligence, and fire support. F3EAD features massed, persistent ISR cued to a powerful and decentralized all-source intelligence apparatus. The goal is to find an HVI or activity (weapons cache, bomb factory) in the midst of civilian clutter and fix its exact location. This precise location enables surgical finish operations (lethal or nonlethal) that emphasize speed to catch a fleeting target. The emphasis on speed is not only to remove a combatant from the battlefield, but also to take the opportunity to gain more information on the foe. The exploit and analyze steps are often the main effort of F3EAD because they provide insight into the enemy network and may offer new LOOs. The information gleaned during the exploit and analyze steps starts the cycle over again by providing leads, or start points, into the network that can be observed and

tracked. F3EAD is not a replacement for F2T2EA. Rather it is a subset of F2T2EA that refines the actions to be completed when engaging HVIs or high-value activities. The process still begins with a decide function in which decisions are made on priorities and the allocation of resources. It is important to remember that the targeting process is a continuous process. For any given target, the process tends to follow the flow depicted in Figure IV-3. At any given time however, a unit may be at the find step for some targets, the exploit step for several other targets, and at the fix, finish, analyze, or disseminate step for still other targets. Similarly, the unit may disseminate information pertaining to the location of a target prior to the finish or exploit steps. Generally, the process will follow the depicted flow, but don't let the process restrict what needs to happen next. The F3EAD process assists commanders and staffs in:

(1) (U) Analyzing the IED network's ideology, methodology, and capabilities, thereby templating its inner workings—personnel, organization, and activities.

(2) (U) Identifying the links among enemy critical capabilities, requirements, vulnerabilities, and observable indicators of adversary action.

(3) (U) Focusing and prioritizing dedicated ISR assets in support of C-IED efforts.

(4) (U) Providing the resulting intelligence and products to elements capable of rapidly conducting multiple, near-simultaneous attacks against the critical vulnerabilities.

(5) (U) Providing an ability to "see" the operating environment, and array and synchronize forces and capabilities.

b. (U) **F3EAD—Find.** During this step, the intelligence team is building an understanding of the adversary and preparing a JIPOE study, which develops a picture of the IED support infrastructure, to include identifying nodes and functions and working relationships. During the final step (Figure IV-4), all available intelligence sources and resources are utilized but efforts are often heavily weighted to the tactical level, HUMINT-oriented collection capabilities.

(U) *For more information on JIPOE, see JP 2-01.3,* Joint Intelligence Preparation of the Operational Environment.

c. (U) **F3EAD—Fix.** To "fix" the adversary, it is necessary to accurately locate enemy personnel or activities, real time, so that they can be targeted. During this step, intelligence analysts continue to develop and refine the analysis of the network with sufficient detail to produce actionable intelligence and targeting plans. As analysis identifies the network's working nodes, the J-2 prioritizes the collection effort and works with the operations directorate of a joint staff (J-3) to determine an appropriate response. Some nodes require immediate response/attack (lethal or nonlethal), while others require further refinement as they lead to more critical nodes. The commander's guidance will normally provide the criteria for this decision. Practicing "tactical patience" or delaying an attack involves risk. Operational risks must be balanced against the opportunities for further intelligence gains. Fixing (Figure IV-5) potential network targets is also resource-intensive and cannot be conducted indefinitely. For example tactically tracking emplacers back to their safe house or

cache and from there to other links in the network must have a cutoff at some point for action to be taken.

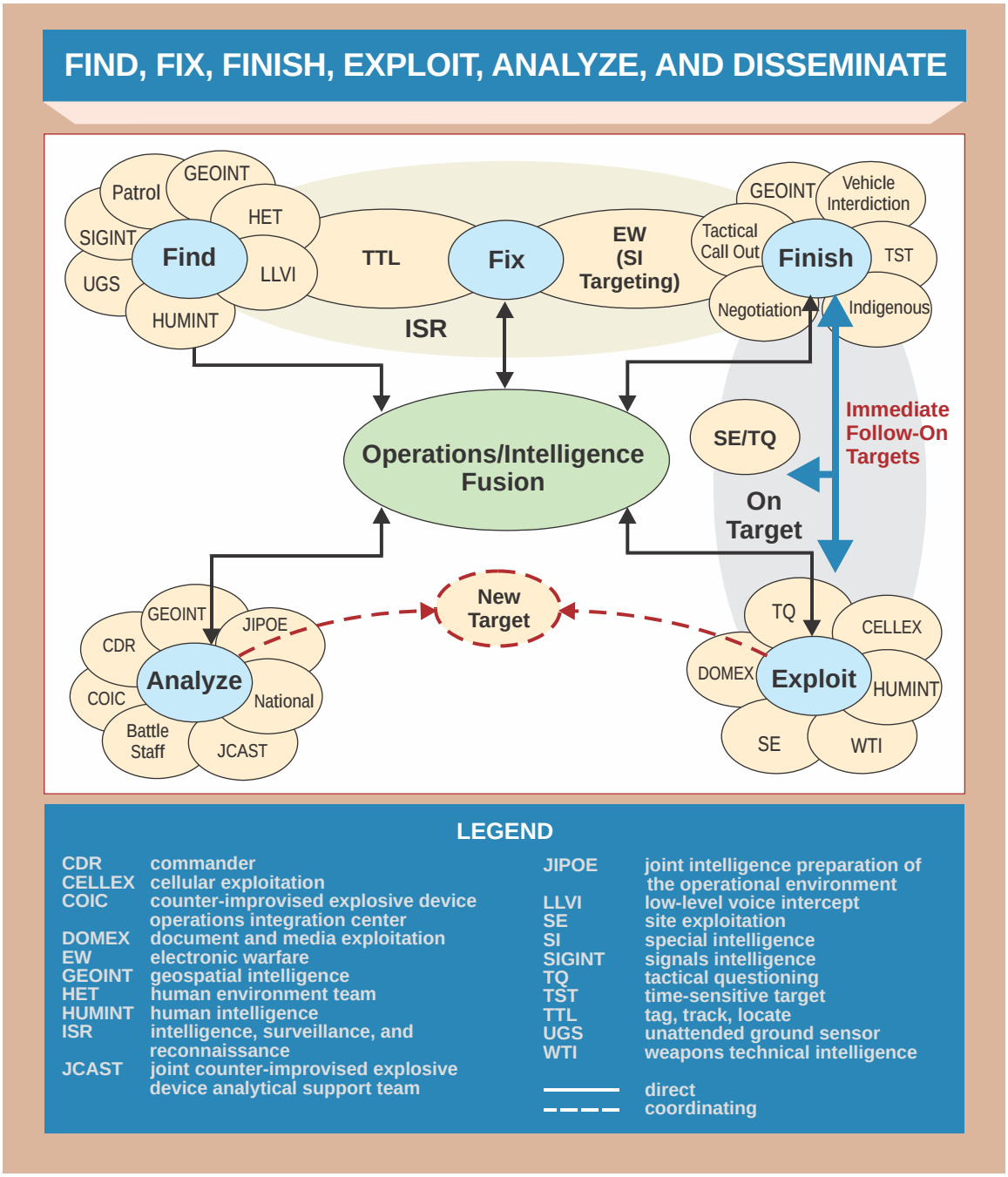


Figure IV-3. (U) Find, Fix, Finish, Exploit, Analyze, and Disseminate

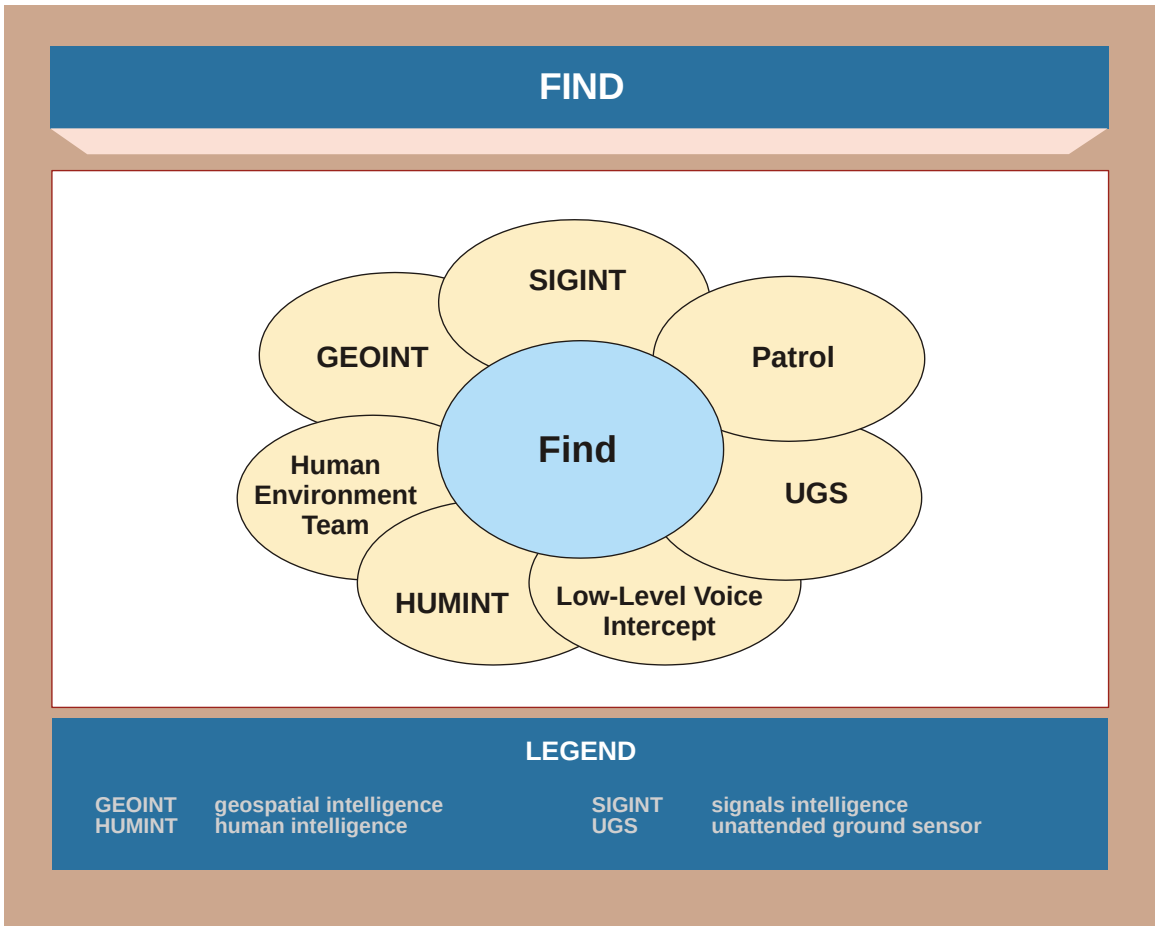


Figure IV-4. (U) Find

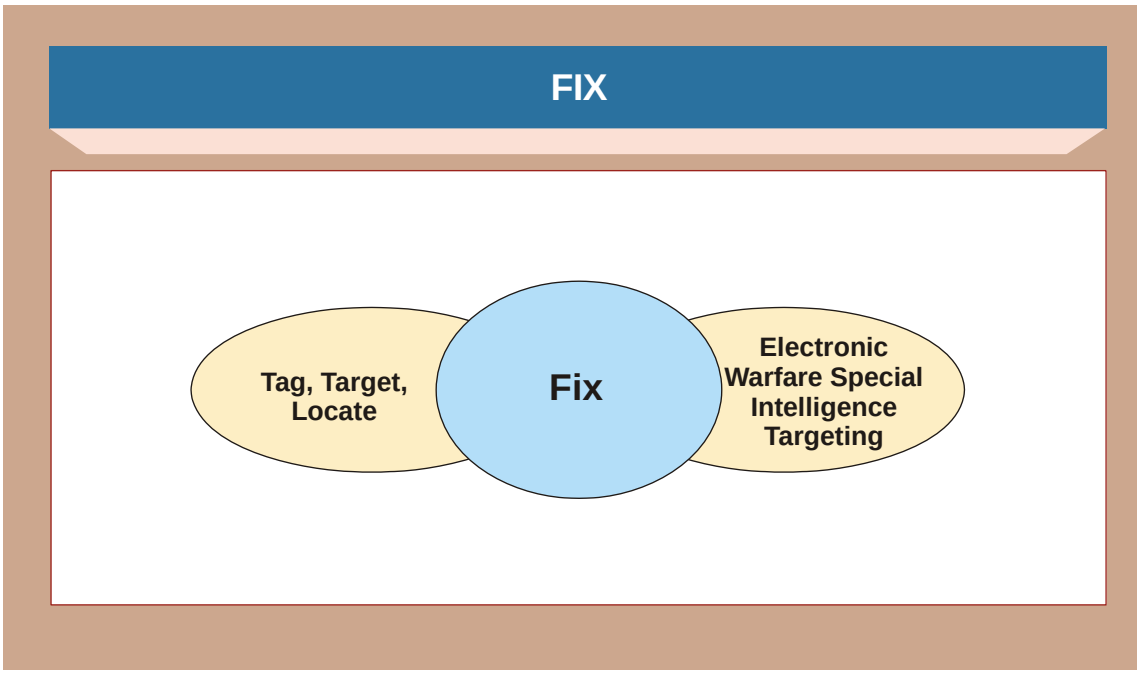


Figure IV-5. (U) Fix

d. (U) **F3EAD—Finish.** See Figure IV-6. J-3 directs the conduct of lethal and nonlethal network-wide engagements. When possible, these actions should be conducted simultaneously. The commander's engagement guidance will determine what specific options will be employed during this step. In an insurgency, nonlethal opportunities, even something as simple as providing jobs for the unemployed (who alternatively will take money to emplace IEDs) can have a measurable impact on IED employment. When executing the preferable option, it is important to employ a multi-echelon approach to disrupt as much of the network as possible and then exploit the results with previously planned

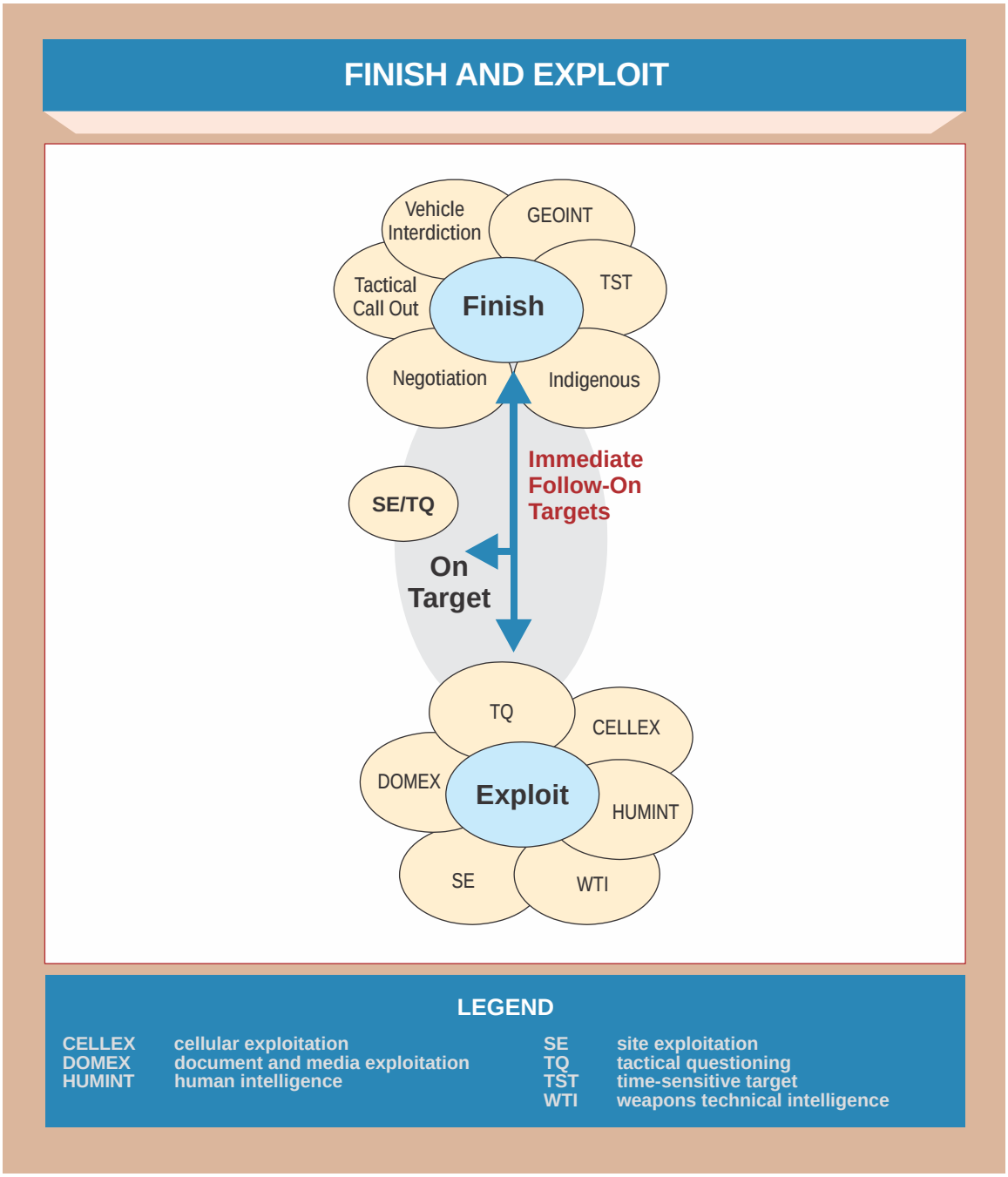


Figure IV-6. (U) Finish and Exploit

collection assets. It is also important to consider conducting near-simultaneous operations to minimize the ability for the target to alert or warn other elements of the network. Where network-wide engagements are not possible, targets of opportunity that may otherwise escape should be engaged.

e. (U) **F3EAD—Exploit.** Information relevant to the C-IED fight comes from many sources. Often, the adversary provides the best information, sometimes without knowing it. Exploitation involves collecting a wide range of information and intelligence from multiple sources, including that which is collected during tactical site exploitation and WTI (pre- and post-blast), and cross-referenced or compared with previously collected intelligence such as DOMEX, CELLEX, computers, and any other relevant materials. WTI is fused with other sources of intelligence to provide critical insights into network members and their activities and can facilitate positively matching specific individuals to particular IEDs or IED events. Whenever a target (individual or material) is attacked (or captured/seized), an attempt should be made to conduct a detailed exploitation (of documents, computer media, cell phones, weapons/explosives, personnel, and other related items) as quickly as possible (Figure IV-7). In addition to being used to populate databases, the information derived from exploitation can often be immediately used to support other operations and to identify follow-on exploitation operations. **Exploitation and analysis activities are continuous and mutually supportive.**

f. (U) **F3EAD—Analyze**

(1) (U) **Analysis.** As exploitation information is received from ongoing collection activities, the intelligence picture of the network is further refined and the foundation is laid for the next set of actions against the network. This process is continuous and results in a return to the first step—refining the JIPOE. During analysis (Figure IV-8) of adversary networks, the joint force should acquire detailed knowledge of the interpersonal dynamics among network members, while maintaining situational awareness of the changing operational environment. The end state of F3EAD analysis is the capability to identify those network members and activities that are most vulnerable to both lethal and nonlethal targeting. Analysis end products should also support those friendly actions that are most likely to yield the desired effects upon IED networks.

(2) (U) **Template.** (Figure IV-9) One means of describing the key output in templating is a modified intelligence synchronization matrix, which is intended to synchronize intelligence asset collection with the AtN operations of maneuver units. The first step in the five-step templating process is to describe the network. Describing the network combines all available analytical and exploitation means, including reachback, in order to uncover threat network personnel and the activities in which they are involved. The second step in templating is to identify and list the adversary's indicators—those enemy activities that we can see (observables) and measure (signatures)—in order to expose potential enemy vulnerabilities. Irregular forces' operations—such as IED manufacturing and employment—must normally be defined in much greater detail than they would be in traditional warfare. Adversary patterns of activity, processes, materials, and networks must be described as highly specific, collectable "indicators" that once collected can either assist in understanding the intentions or capabilities of the enemy, or trigger the commander to take

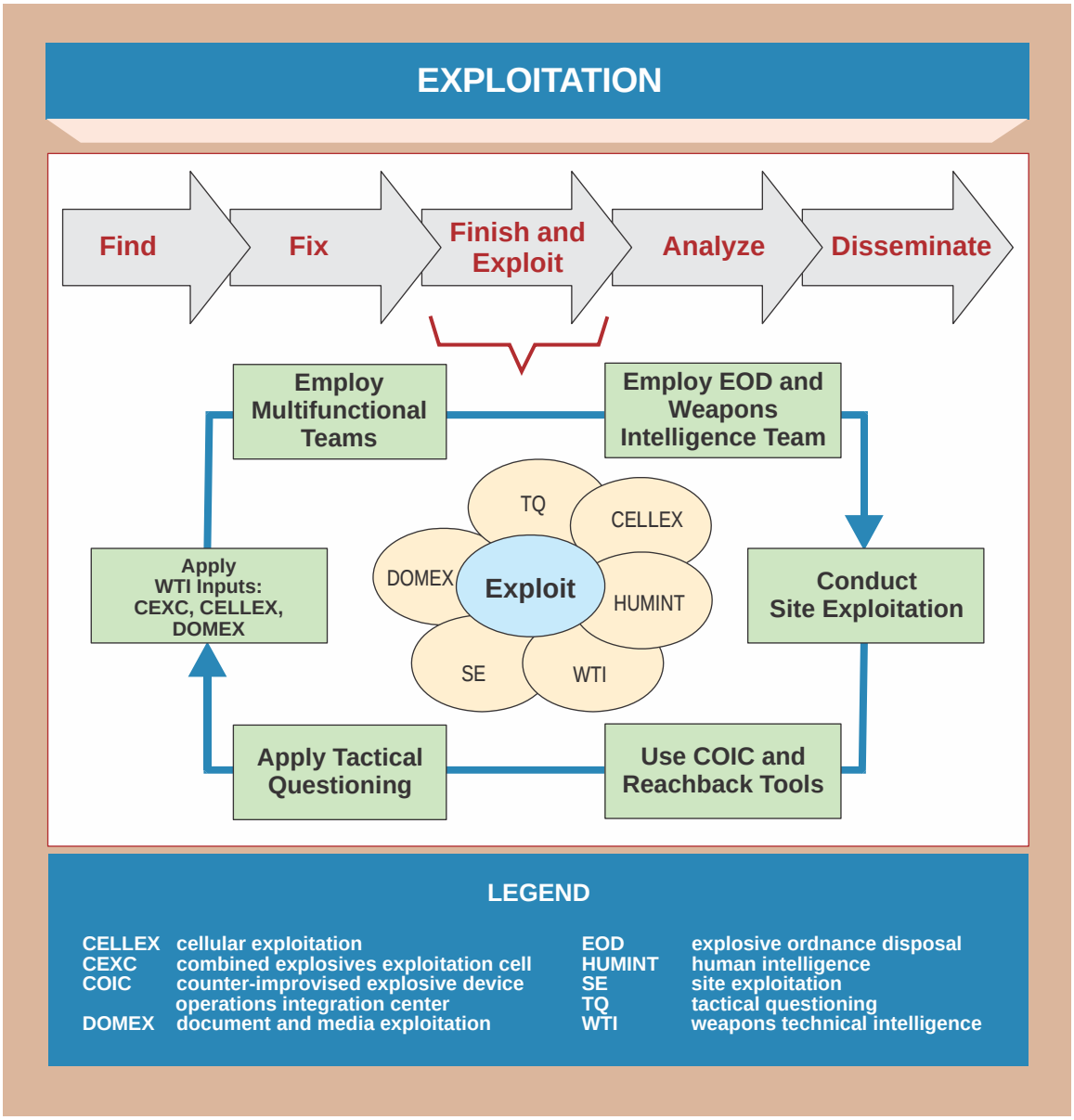


Figure IV-7. (U) Exploitation

action against the enemy capability or activity. Because most of these indicators are less familiar to soldiers, deliberately hidden and often difficult to distinguish from other background activities, many of them can only be inferred through direct observation, indirect observation, or technical measurements. To account for this required level of detailed understanding, indicators are further categorized as "observables" (indicators that can be directly or indirectly observed) and "signatures" (indicators that can be inferred through measurements). The third step is to identify named areas of interest (NAIs)—those areas where friendly collection capabilities can detect enemy activity or individuals and have the greatest decisive effect against the enemy if interdicted—adversary's critical vulnerabilities. The fourth step is to identify both organic and nonorganic collection capabilities required in order to maximize ISR collection against those indicators at their associated NAIs. Finally, in the fifth step, the staff makes targeting recommendations to the commander taking into

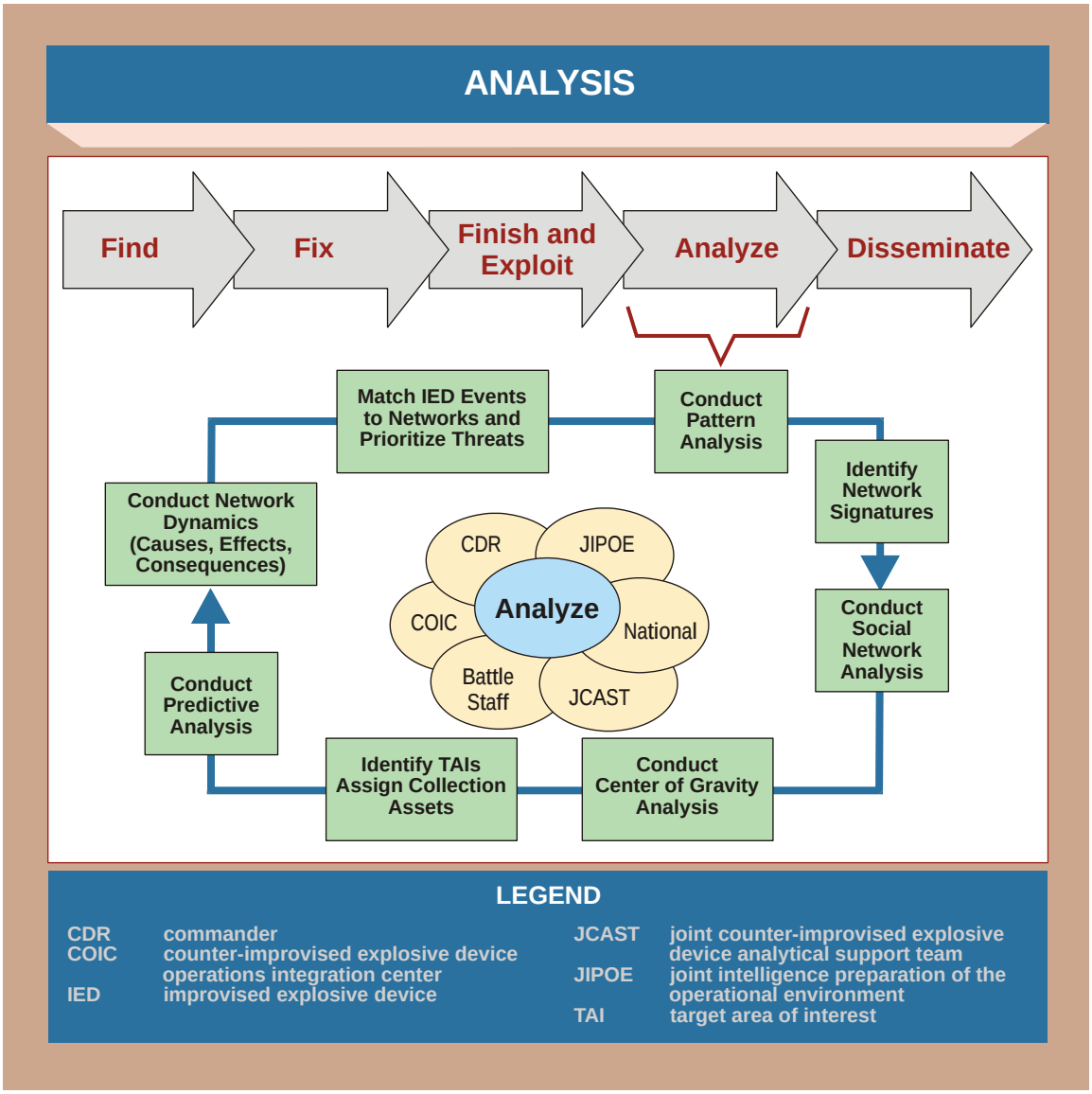


Figure IV-8. (U) Analysis

consideration all **lethal and nonlethal** friendly capabilities available. Throughout this templating process, the staff must draw upon the results of critical factors analysis (CFA)—the analysis of critical capabilities, critical requirements, specific activities, observable and measureable indicators, and critical vulnerabilities—and evaluate CFA along with the activities depicted in the network template. The output of both templating and CFA is captured in the staff synchronization matrix (Figure IV-10). The staff synchronization matrix is a modified intelligence synchronization matrix that portrays specific intelligence requirements, NAIs, ISR capabilities, earliest and latest time the information is of value, threat indicators, and friendly actions and aligns them with potential friendly operations and commander's decision points (shown as red stars).

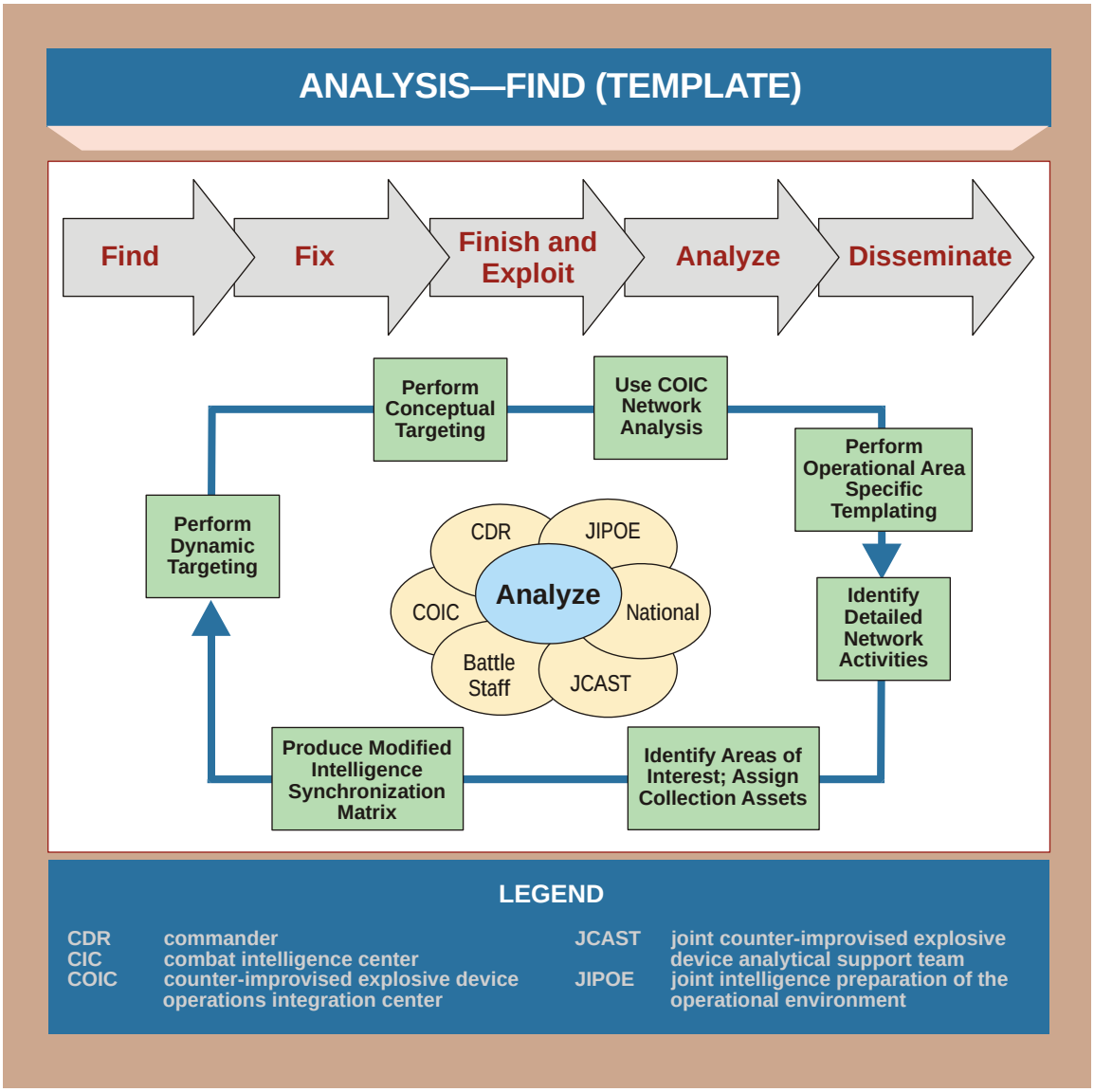


Figure IV-9. (U) Analysis—Find (Template)

(3) (U) **Target Prioritization.** Once analysis and templating have been completed and refined by additional intelligence collection, the next step is targeting. The network targeting process is described in Figure IV-11. There are a variety of mechanisms that can be employed to facilitate the targeting of IED networks. These include the traditional targeting working group process and quick response dynamic targeting cells that usually focus on specific type of targets (HVIs, caches, or emplacers), which vary depending on the echelon conducting the planning. The results of analysis and templating are assessed to ensure that lethal and nonlethal AtN operations are aimed at the right network members and functions using the right means and the best timing. When possible, targeting will result in multiple, near-simultaneous operations aimed at several network targets.

SYNCHRONIZATION MATRIX

Time	1200	1300	1400	1500	1600	1700	1800	1900	2000	2100	2200	2300	0000	0100	0200	0300	0400	0500	0600	0700	0800	0900	1000	1100	1200
Threat Indicators	Movement to Border							Traffic Control Point (TCP) Infiltration						Transportation/Storage				Safe House Operations							
Friendly Actions	**PHASE I**									**HASTY TCP**				**PHASE II**				**CORDON AND SEARCH**							
Task Force 1 (TF1)	**Border Assistance**																								
Task Force 2 (TF 2)	Hasty TCP											Hasty TCP													
Task Force 3 (TF 3)	Cordon and Search																				Cordon and Search				
Capability																									
Full Motion Video (FMV)	Named Area of Interest (NAI) 001, 002																								
FMV									NAI 007, 008																
Signal Intelligence	NAI 001, 002									NAI 007, 008															
Human Intelligence	Interview security forces at TCPs — NAI 003, 004, 005, 006																	Battlefield Interrogation Team/Tactical Questioning (BIT/TQ) in direct support of TF3							
Human Intelligence	Interview locals in remote villages — NAI 002, 005																	BIT/TQ in DS of TF3							
Ground Moving Target Indicator	NAI 011																								

Priority Intelligence Requirements

What types of improvised explosive device (IED) components/materials are being used to conduct attacks?
Which members of the local security force are being influenced by insurgent networks?
Where are the cross-boundary smuggling points, cache locations, meeting locations, distribution points, and IED assembly areas in the area of operations?

Phases of Operation

Phase I — Detect threat activity (movement of lethal aid)
Phase II — Identify tier II targets and capture/kill/influence

Geospatial Intelligence (GEOINT) Collection Focus (Phase I) Task: Monitor sparsely populated boundary areas, cross-cue GEOINT Purpose: Identify (ID) smuggling routes and potential threat activity Priority: Unusual activity along porous boundary areas	**GEOINT Collection Focus (Phase II)** Task: Overwatch Purpose: Force protection Priority: Squirters and potential threat posture
Human Intelligence (HUMINT) Collection Focus (Phase I) Task: Interview security forces and locals, cross-cue SIGINT and GEOINT Purpose: ID smugglers or associates and areas where smuggling takes place Priority: Corrupt security forces, insurgents, smuggling locations, routes, tactics, techniques and procedures	**HUMINT Collection Focus (Phase II)** Task: Conduct BIT/TQ in support of task force elements Purpose: Obtain follow-on targetables Priority: IED emplacement locations, safe houses, cache locations, distribution/assembly areas
Signals Intelligence (SIGINT) Collection Focus (Phase I) Task: Intercept to cross-cue GEOINT Purpose: Personality detection at district boundary areas Priority: Cellular, Push to talk (PTT)	**SIGINT Collection Focus (Phase II)** Task: Intercept/direction find Purpose: Personality detection and location Priority: Cellular/PTT

Figure IV-10. (FOUO) Synchronization Matrix

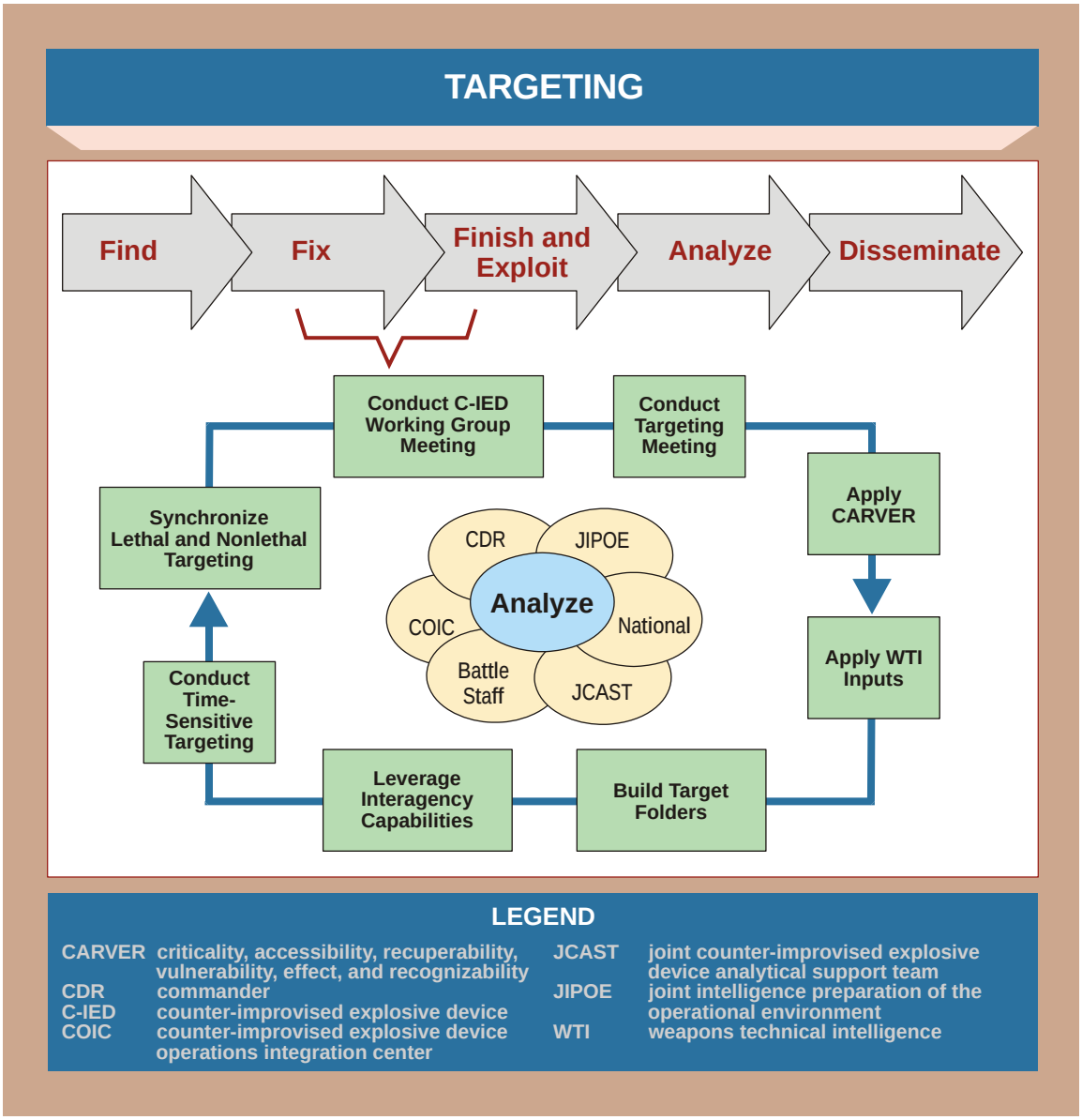


Figure IV-11. (U) Targeting

(a) (U) In the C-IED fight, C-IED working groups at all echelons will take the available intelligence information and the commander's targeting guidance and develop a list of prioritized lethal and nonlethal targets to submit to the targeting board. The goal of a C-IED working group is to provide a series of recommendations to the commander and staff identifying targets and the appropriate method to engage for maximum effectiveness.

(b) (U) The coordination and synchronization between the enablers that make up the C-IED working group is crucial to supporting the commander's targeting guidance. There is a multitude of organizations, within and external to DOD, that provides enablers and crucial technical support, for example, NGIC weapons intelligence team (WIT), combined explosives exploitation cell (CEXC), and other reports of IEDs, and produces analytical products to support targeting of enemy networks. DIA is the lead enabler for WTI process,

(U//FOUO) "Targeting in a COIN [counterinsurgency] environment requires creating a targeting board or working group at all echelons. The intelligence cell provides representatives to the targeting board or working group to synchronize targeting with intelligence sharing and intelligence, surveillance, and reconnaissance operations. The goal is to prioritize targets and determine the means of engaging them that best supports the commander's intent and the operation plan. Effective targeting identifies the targeting options, both lethal and nonlethal, to create effects that support the commander's objectives. Lethal targets are best addressed with operations to capture or kill; nonlethal targets are best engaged with CMO [civil-military operations], IO [information operations], negotiation, political programs, economic programs, social programs and other noncombat methods. Nonlethal targets are usually more important than lethal targets in COIN; they are never less important."

Field Manual 3-24, *Counterinsurgency*

which involves the scientific examination and analysis of materiel as well as data from an event or site involving collected material. The primary function of WTI is to identify associations among events, people, IEDs, improvised weapons, and collected material used to support the IED cycle. Exploitation provides direct support to attacking insurgent and terrorist networks by conducting "supply chain defeat" analysis. WTI facilitates the interdiction of network infrastructures by linking IED supplies to specific individuals or organizations.

(c) (U) Taking the available information (raw and evaluated), the C-IED working group will evaluate it for targetable potential. One method for evaluating potential targets is targets systems analysis (TSA). Criticality, accessibility, recuperability, vulnerability, effect, and recognizability (CARVER) is a well-known TSA tool that can be used to evaluate potential targets. The CARVER criteria are:

1. (U) Criticality—Value of the target to the enemy.

2. (U) Accessibility—Operational element can reach the target with available resources to accomplish its mission.

3. (U) Recuperability—The time it will take to replace, repair, or bypass the destruction or damage of the target.

4. (U) Vulnerability—Operational element has the means and expertise to successfully attack the target.

5. (U) Effect—Effect on the cell or network using political, military, economic, social, information, and infrastructure, including second and third order effects.

6. (U) Recognizability—Degree to which the asset can be recognized by an attacker, intelligence, or reconnaissance.

(d) (U) Once the C-IED working group has developed a prioritized list of recommended targets with recommended means of engagement (lethal and nonlethal), it will

forward that list for consideration and action by the command's targeting board. Again, this recommended targeting can be further enhanced or refined through reachback support from the COIC.

(e) (U) Exploitation continues after the application of lethal or nonlethal fires on the selected target. It involves the application of all available and suitable assets to gather as much information as possible to feed back into the system.

g. (U) **F3EAD—Disseminate.** The success of a counter-network strategy requires a robust communications architecture that connects all the participants in the C-IED process as well as shares data. Additionally, experience, proper training, and established reporting responsibilities and procedures help ensure the timely and accurate sharing of information. While the exact architecture will be determined by the JFC, it should be flexible enough to include multinational partners.

8. (U) Multi-Echelon, Multidiscipline Counter-Improvised Explosive Device Fusion

a. (U) Organizing and allocating resources for AtN operations requires a coordinated, synchronized, and integrated effort beginning at the tactical level and often involving the use of national-level resources. Intelligence personnel at all echelons must be prepared to employ traditional and nontraditional information sources to build the picture of the adversary's infrastructure and share that information and intelligence across the joint force.

b. (FOUO) Modern technology (Figure IV-12) provides the JFC with unprecedented abilities to maintain near-constant surveillance over specific geographic areas using a wide variety of ISR resources to provide continuous coverage. When combined with the real-time imagery downlink provided by the remote operational video enhanced receiver system, aerial surveillance assets of organizations can provide C-IED analysts and targeteers with vital real-time information on insurgent IED activities. This support is also capable of detecting and back tracking emplacers to their safe houses and caches. Once these IED support sites are located, they can be further exploited to identify and locate other network functions. An identified site can be:

(1) (U) Further exploited through more intense all-source based surveillance. The goal is to see if this opportunity will lead to other nodes (individual and support) in the network.

(2) (U) Raided and on-site materials (computers, cell phones, documents [DOMEX], IED components, WTI, other intelligence-related materials) and TQ of detainees (HUMINT) for usable information. This will often require an on-site exploitation capability (EOD, WIT) combined with the ability to immediately respond (with further raids) to any time-sensitive information that may be discovered. It is also critical that recovered materials and data get submitted into the proper channels in order to enable full exploitation and the subsequent dissemination of valuable network intelligence to units.

c. (U) When these enhanced visual surveillance capabilities are combined with the traditional ability to monitor communications means (radio, telephone, Internet) and the use of HUMINT resources (media exploitation, informers, volunteer HN information sources,

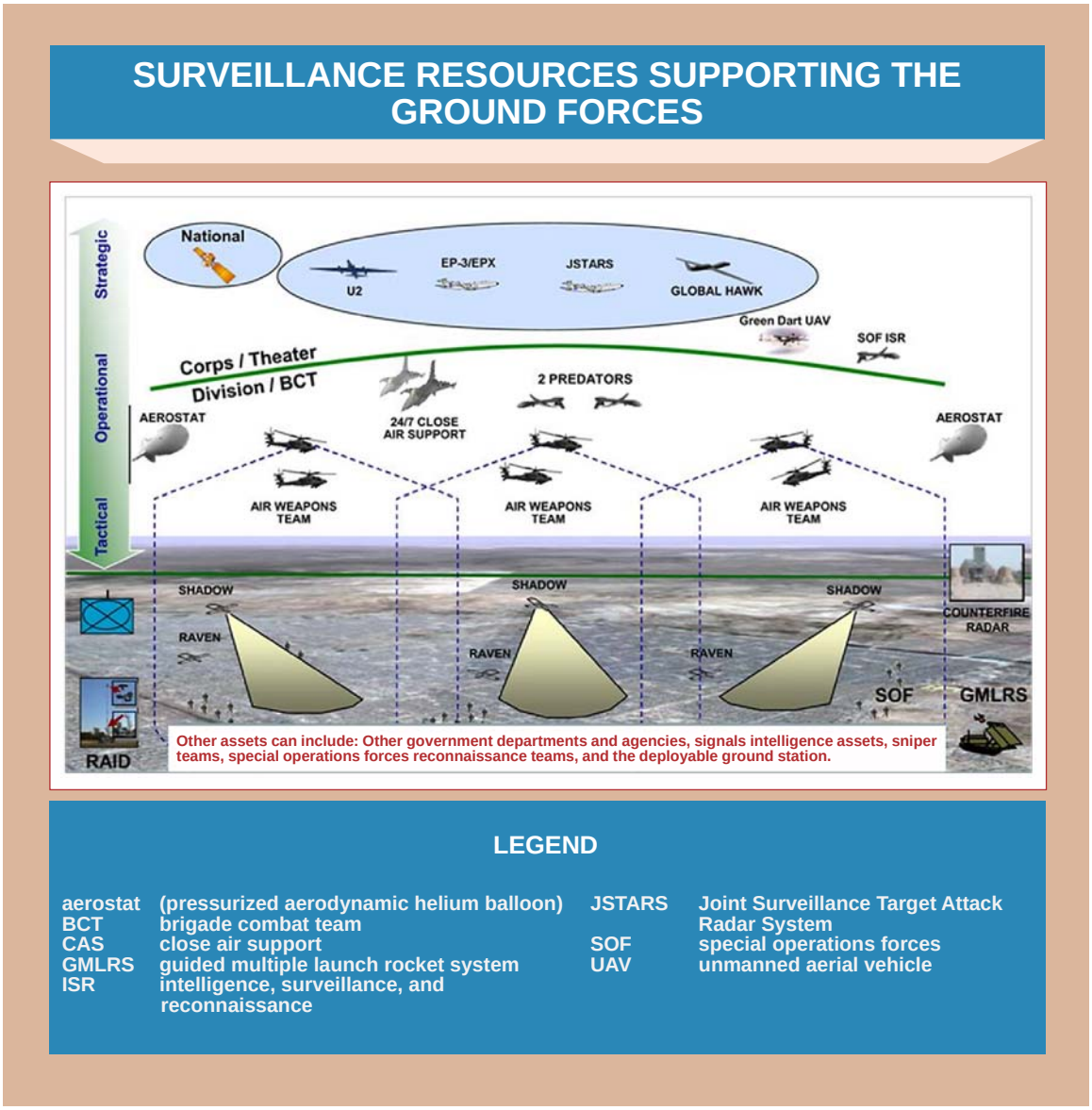


Figure IV-12. (U) Surveillance Resources Supporting the Ground Forces

"every soldier a sensor") and WTI, the C-IED analysts and targeteers will possess information required to help develop an accurate picture of the critical nodes of the various IED networks operating in the operational area. Gathering basic tactical information and utilizing TQ is an essential part of C-IED operations. Whether we are looking at individual soldiers on patrols, or information derived from meeting local leaders, or even conversations with local workers, all of these are information sources. While interactions with the local population and their observations of the physical environment may be considered a tactical concern, when aggregated, they can provide an operational-level picture of adversary IED activities. Over time, this information can be refined sufficiently to produce targetable intelligence and further opportunities for exploitation.

d. (U) The key to success in attacking a network is to maintain disruptive attack pressure on multiple functions simultaneously, forcing the individuals as well as cells out

(U) Threat networks that use improvised explosive devices (IEDs) comprise state and non-state supporters, leaders, core cadre, planners, technology suppliers, financial supporters, trainers, recruiters, transportation agents, logistical storage facilities, IED precursors, surveillance teams, bomb makers, cache locations, emplacers, trigger men, security personnel, people that provide pre- and post-blast safe havens for action and facilitation networks, host nation corrupt political and military officials and personnel who support and collaborate with these networks, etc. In the Operation IRAQI FREEDOM Anaconda Strategy, this entire network system was targeted as a whole. Major named operations were developed in which network critical vulnerabilities (i.e., critical sub-components and supporting requirements of complex adaptive systems), many of which crossed friendly boundaries at tactical through strategic levels, were identified and attacked. Plans were put in place and executed that ultimately "Defeated," not merely disrupted, enemy networks that employed IEDs. Lethal and nonlethal desired effects were identified and measured. There was over a 90% reduction in use of IEDs from April 2007 to April 2009 in Operation IRAQI FREEDOM.

Various Sources

into the open as they take greater risks to continue their IED network operations. As the network attempts to reconstitute the organization, it is vulnerable to detection and targeting actions. While friendly C-IED efforts may not lead to the destruction of the organization, maintaining constant pressure at multiple levels within the network will deny an adversary the freedom of action and movement it needs to conduct operations against the JTF.

9. (U) Deliberate and Dynamic Network Targeting

a. (U) The JFC uses a mix of deliberate and dynamic targeting to actively identify and attack networks that employ IEDs. In deliberate targeting, the joint force **prosecutes planned targets—**the array of critical network components that are essential to the success of that network which have been identified through the fusion of all-source intelligence and C-IED working group information at all levels of command. These are targets that are known to exist in the operational environment, which can be engaged with actions to create effects that support JFC objectives. In the C-IED fight, WTI analysis (including information derived from tactical, technical, and forensic exploitation, biometrics, document exploitation, detainee operations, etc.) combined with information derived from all-source intelligence resources facilitates the precise identification of those portions of the adversary's networks that employ IEDs. Once identified, the JFC can make a better informed decision on how to apply lethal and nonlethal capabilities to attack the IED network before the next IED attack occurs. The second targeting category is dynamic targeting, which prosecutes targets of opportunity, which include targets that are identified too late, or not selected for action in time, to be included in deliberate targeting and which, when detected or located, meet specific criteria to achieving objectives. In the C-IED fight, HVIs are targeted as time-sensitive and cleared for immediate attack when found. These targets are fleeting in nature and are considered high-payoff targets (HPTs). If removed, HVIs/HPTs will significantly "disrupt" activities of the adversary's forces within a commander's operational area. An

approach that focuses only on the engagement of HVIs, without conducting a full-spectrum comprehensive attack against multiple facets of the entire network, allows enemy networks that employ IEDs to reorganize, rearm, refit, and reengage US forces or MNFs. In other words, the network continues to operate.

b. (U) C-IED operations employ a mix of deliberate and dynamic targeting actions and commanders must be prepared to allocate the necessary mix of ISR and attack assets to be able to respond to targets as they are identified. C-IED working groups can facilitate the identification of networks and their critical vulnerabilities and provide the JFC and the joint targeting board with the information needed to more precisely enable attack of networks that employ IEDs.

CHAPTER V
STAFF RESPONSIBILITIES (U)

1. (U) Introduction

a. (U) This chapter examines the roles and responsibilities of the JTF staff with attached and assigned C-IED enabling organizations. Depending on the size and duration of the operation, there are a number of approaches for organizing the conduct of C-IED operations. In small-scale, short duration operations where technical specialist assets are limited, the JTF may create specialized C-IED cells within the J-2, J-3, and engineering staff section (J-7) to plan and oversee the conduct of C-IED operations. This is the normal arrangement in a small-scale operation in the early stages of an insurgency and insurgent IED employment. Another option is to employ a C-IED task force to manage assigned C-IED assets and, in coordination with the JTF staff, plan and conduct C-IED operations. In larger-scale operations or a fully mature insurgency with widespread IED use, the JTF is likely to employ a separate C-IED task force. The C-IED task force has primary responsibility for managing the JTF's C-IED assets and coordinating the activities of many of the assigned/attached C-IED enabling organizations. When a C-IED task force is established, the JTF staff resumes a more traditional staff role in establishing policy and general direction for the JTF's overall C-IED effort.

b. (U) While all elements within the staff are expected to contribute to the C-IED effort, the primary responsibility for organizing and leading the operation lies with the J-2, the J-3, the J-7, and the IO/strategic communication section. The successful conduct of C-IED operations depends on the J-2's ability to organize and direct intelligence operations that are designed to develop timely, predictive, actionable intelligence on specific operational-level IED-related targets, the J-3's ability to direct forces to act on that information, and the J-3's and J-7's ability to ensure that the members of the JTF have individual/unit training packages with the latest available information on the IED threat.

c. (U) At each level of command, the cell or unit assigned the C-IED mission needs to be properly resourced and have the appropriate skills and specialist enablers. Although similar tasks and requirements are present at different levels, proper mission analysis needs to be conducted in order to create an appropriate structure to be able to fulfill those tasks and requirements (see Figures V-1 to V-4). The commander, joint task force (CJTF), should establish a series of staff organizations to assist in the management of the IED-related information flow, to provide direction to attached and supporting C-IED assets (see Appendix A, "Counter-Improved Explosive Device Enabling Organizations") to develop and continuously refine the CJTF's C-IED targeting and countermeasures programs. National, joint, and Service assets in the form of specialized technical, forensic, biometric, and targeting analysis teams will deploy forward to assist organic/assigned EOD teams in the investigation of IED-related incidents and the collection, management, and dissemination of IED information and targeting the IED network. Reporting from those units should be shared immediately within the JTF to help refine unit/individual TTP. It should also be forwarded for more detailed evaluation by specialized national capabilities to help drive the development of improved active and passive force protection measures and develop the information needed to support targeting of the IED support infrastructure. Success normally

relies upon a clear understanding of missions, roles, and responsibilities; a clearly established information gathering, analysis, and dissemination architecture that simultaneously links all participants at all echelons; and an aggressive, innovative, proactive mindset that develops the tools and strategies to carry the fight to the adversary.

(U) Note: In the United States Marine Corps (USMC), C-IED planning and coordination is considered a staff function. The C-IED cell does not control or direct EOD assets. EOD units are organic to the Marine air-ground task force (MAGTF) and employed in direct support of the infantry battalions. EOD officers are assigned as liaison to the regiments. While Marine Corps EOD assets are not usually assigned to the C-IED task force, the JTF's C-IED task force provides WTI teams, C-IED support teams to facilitate planning and specialized C-IED training teams to support Marine Corps forces and share C-IED intelligence and device-specific information with Marine Corps units. Marine Corps representatives participate in the JTF-level C-IED working groups.

2. (U) Intelligence

a. (U) The J-2's mission is to provide the commander with timely and accurate intelligence to support the CJTF's objectives, as stated in the C-IED plan, and to meet the information needs of the staff and component commands for operations and planning. The J-2 is responsible for organizing and directing the operations of the command's intelligence assets. The J-2's C-IED-related information sources within the operations area will include the command's organic intelligence assets (all-source, especially HUMINT); HN and MNF sources, unit level reporting, the command's assigned EOD, WIT, CEXC assets, and national assets (such as WIT, CEXC, etc.) deployed forward to conduct specialized exploitation of IED incidents and devices. In order to manage and exploit this information flow, the J-2 will cooperate with a number of staff organizations and reporting organizations, each with a specific focus on some aspect of the IED problem. The J-2 may elect to create a C-IED intelligence cell in order to focus the analyst's efforts. The mission of the J-2's C-IED intelligence cell is to produce and disseminate timely, all-source fused intelligence that will serve as a basis for the development and conduct of the command's C-IED effort. When the CJTF forms a C-IED task force, the J-2 will support the task force's C-IED intelligence fusion cell, facilitating the collection, analysis, and application of all-source intelligence to the C-IED fight.

b. (U) **Organization.** In addition to AOR-based sources of IED-related information, the JTF J-2 works closely with the combatant command J-2 for ISR support and coordination and to obtain theater analytical products. The combatant command makes a significant contribution to the identification, tracking, and attack of adversary networks and HVI. See Figure V-1.

(U) *For additional information on the relationship between the combatant command intelligence organization and the JTF, see JP 2-0,* Joint Intelligence.

(1) (U) **Joint Intelligence Operations Center (JIOC) or Joint Intelligence Support Element (JISE).** The mission of the JIOC/JISE is to conduct focused all-source analysis to produce target intelligence and participate in the JTF J-3 and the major

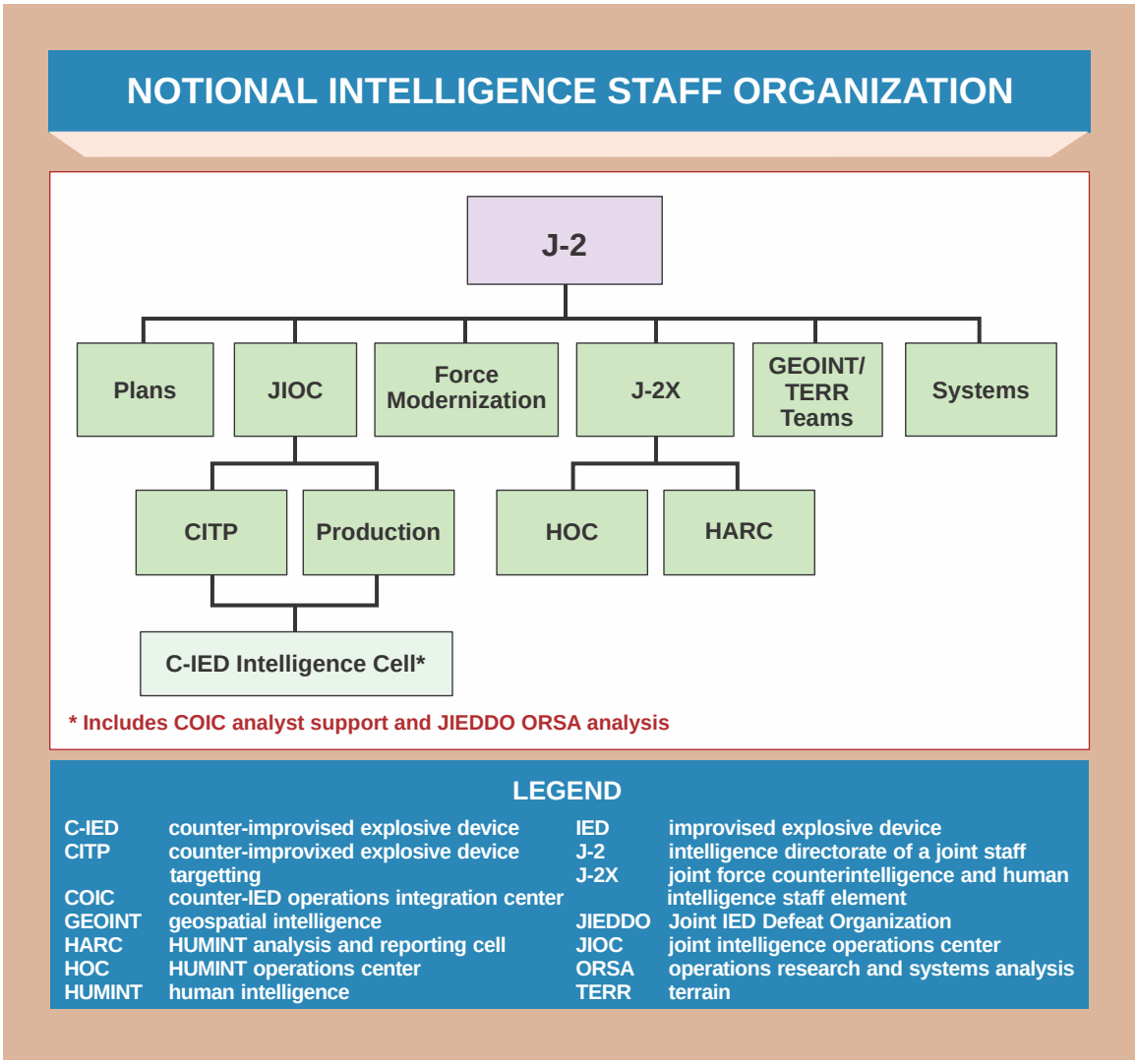


Figure V-1. (U) Notional Intelligence Staff Organization

subordinate commands' (MSCs') dynamic targeting process. The JIOC/JISE is an intelligence fusion cell responsible for developing a current intelligence analysis on the insurgency to include the adversary's activities, objectives and support structure. It produces detailed IED-related assessments on devices and adversary TTP developments. The JIOC/JISE also conducts trend analysis in order to predict future adversary activities. JIOC/JISE reporting is designed to produce intelligence that is tailored to support corps COIN operations and C-IED efforts. In addition to the traditional intelligence summary, the JIOC/JISE develops a variety of general and specialized intelligence reports that are designed to meet the information needs of planners and operators at all echelons within the JTF. The JIOC/JISE may also have a **C-IED intelligence cell** that is responsible for developing all-source reports that are designed to provide friendly forces with detailed C-IED-related assessments on devices and changes in adversary IED-related TTP. The C-IED-related intelligence information flow for the JIOC/JISE is illustrated in Figure V-2. When operating with a C-IED task force that has formed a target development cell (TDC), the JIOC/JISE's IED intelligence reporting supports the C-IED task force's TDC.

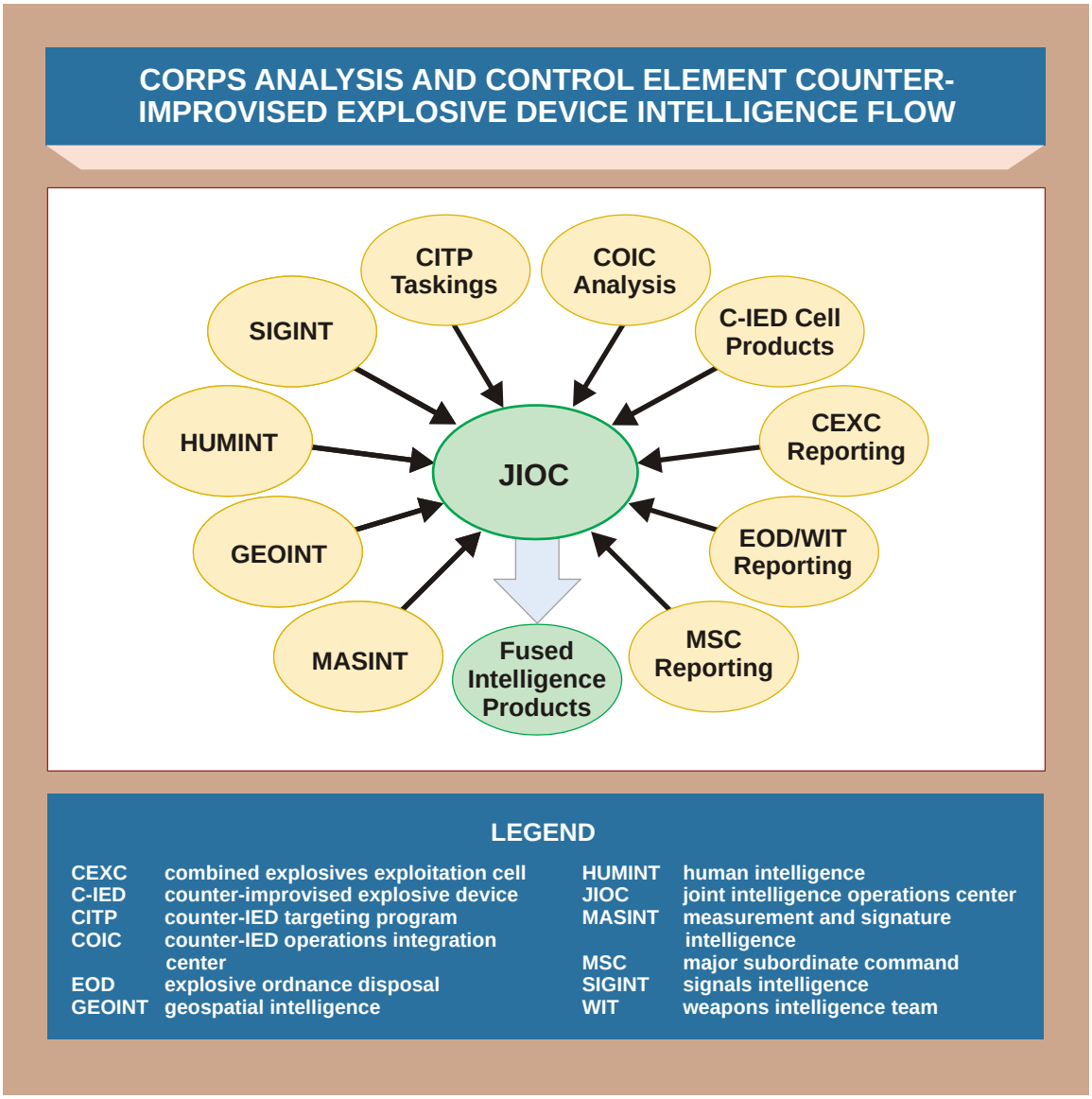


Figure V-2. (U) Corps Analysis and Control Element Counter-Improvised Explosive Device Intelligence Flow

(2) (U) **C-IED intelligence fusion** is accomplished in the JIOC and relies heavily on target intelligence produced by the counter-improvised explosive device targeting program (CITP) cell. The CITP cell, which is also known as a TDC, is responsible for producing target intelligence on high-threat IED networks.

(3) (U) **J-2 C-IED Intelligence Cell.** Consisting of the J-2's C-IED all-source analysis cell and the TDC, the C-IED intelligence cell, consisting of intelligence analysis, collection management, and CITP technical specialists, will normally have the following responsibilities:

(a) (U) Plan the focused employment of intelligence collection assets against the adversary's IED infrastructure.

(b) (U) Serve as the all-source focal point for all IED-related intelligence information originating within the command and from national and multinational/HN sources.

(c) (U) Conduct predictive trend analysis on adversary IED employment and device design to enhance friendly force protection programs and C-IED operational planning.

(d) (U) Identify and produce target intelligence on the critical nodes in the adversary's IED infrastructure to support C-IED operations.

(e) (U) The intelligence cell is the primary agency responsible for fusion of technical assessments, forensic exploitation, and all-source threat intelligence related to the IED threat within the operational area. The cell analyzes developments in the threat's TTP and disseminates advisories to MNFs. The cell also advises the joint forces in IED risk mitigation. Working closely with the J-2 collection manager and the JIOC/JISE, the cell answers all relevant IED-related intelligence requests for information (RFIs). The cell is also responsible for developing intelligence for the J-2's portion of the CITP. In developing their analytical products, the cell reviews all C-IED-related intelligence generated within the command and by the relevant national agencies (NGIC, Terrorist Explosive Device Analytical Center [TEDAC], described in Appendix A, "Counter-Improvised Explosive Device Enabling Organizations"). The cell's reporting on adversary emerging TTP and IEDs are contained in a series of special assessments.

(f) (U) The C-IED intelligence cell fuses information from a variety of sources including:

1. (U) CEXC,

2. (U) WIT,

3. (U) EOD teams,

4. (U) J-2 GEOINT/terrain team,

5. (U) Explosive hazards coordination cell (EHCC),

6. (U) Tactical human intelligence teams (THTs), and

7. (U) COIC analysis.

(4) (U) **Human Intelligence Analysis and Reporting Cell (HARC).** Operating under the J-2X [joint force counterintelligence and HUMINT staff element], this cell is responsible for analyzing information collected through human sources in order to detect potential insurgent activity directed toward friendly forces. Much of the HARC's reporting is designed to support the production of target folders. The HARC accomplishes the following:

(a) (U) Provides HUMINT collection focus and develops HUMINT collection requirements based on the commander's priority intelligence requirements and information requirements.

(b) (U) Incorporates HUMINT into all-source fused products to provide timely, actionable intelligence leading to positive identification, exploitation, or neutralization of high-value targets.

c. (U) The J-2 also obtains information from deployed interagency IED technical exploitation capabilities supporting the JTF. This national support enables the J-2 to better define the operational environment and develop actionable intelligence to target the IED support structure. Organizations that are specifically designed to provide information that supports the development of actionable intelligence to support the C-IED effort are the CEXC manned by joint Service and multinational EOD personnel, the CITP sponsored by the NGIC, WITs deployed to support the command's brigade combat teams (BCTs), and assigned Federal Bureau of Investigation (FBI) Special Agent Bomb Technicians and Bureau of Alcohol, Tobacco, and Firearms and Explosives (ATF) explosives experts (See Appendix A, "Counter-Improvised Explosive Device Enabling Organizations"). In the IED effort, these elements can provide the following:

(1) (U) Databases that track different types of IEDs and can link an IED to a known or suspected bomb maker based on materials and methods used in its construction.

(2) (U) Analysis of found or captured materials to determine if they are in fact IED precursors.

(3) (U) Analysis of current IED construction and initiation methods.

(4) (U) Prediction of IED trends and likely future construction and initiation methods.

(5) (U) Identification of possible sources responsible for IEDs and associated materials based on exploitation and analysis of technical, forensic, and biometric materials and information from site exploitation.

d. (U) The overall C-IED-related intelligence information flow for the JTF is illustrated in Figure V-3.

3. (U) Operations

a. (U) **Mission.** The J-3 (Figure V-4) is responsible for the direction of the JTF's combat forces. The J-3 ensures that sufficient, properly equipped C-IED forces (see Appendix A, "Counter-Improved Explosive Device Enabling Organizations") are available to support the JTF's mission within the operational area. The configuration that is depicted applies in the early stages of an operation when the IED threat is low, the JTF numbers less than a division in size, and a C-IED TF has not been established.

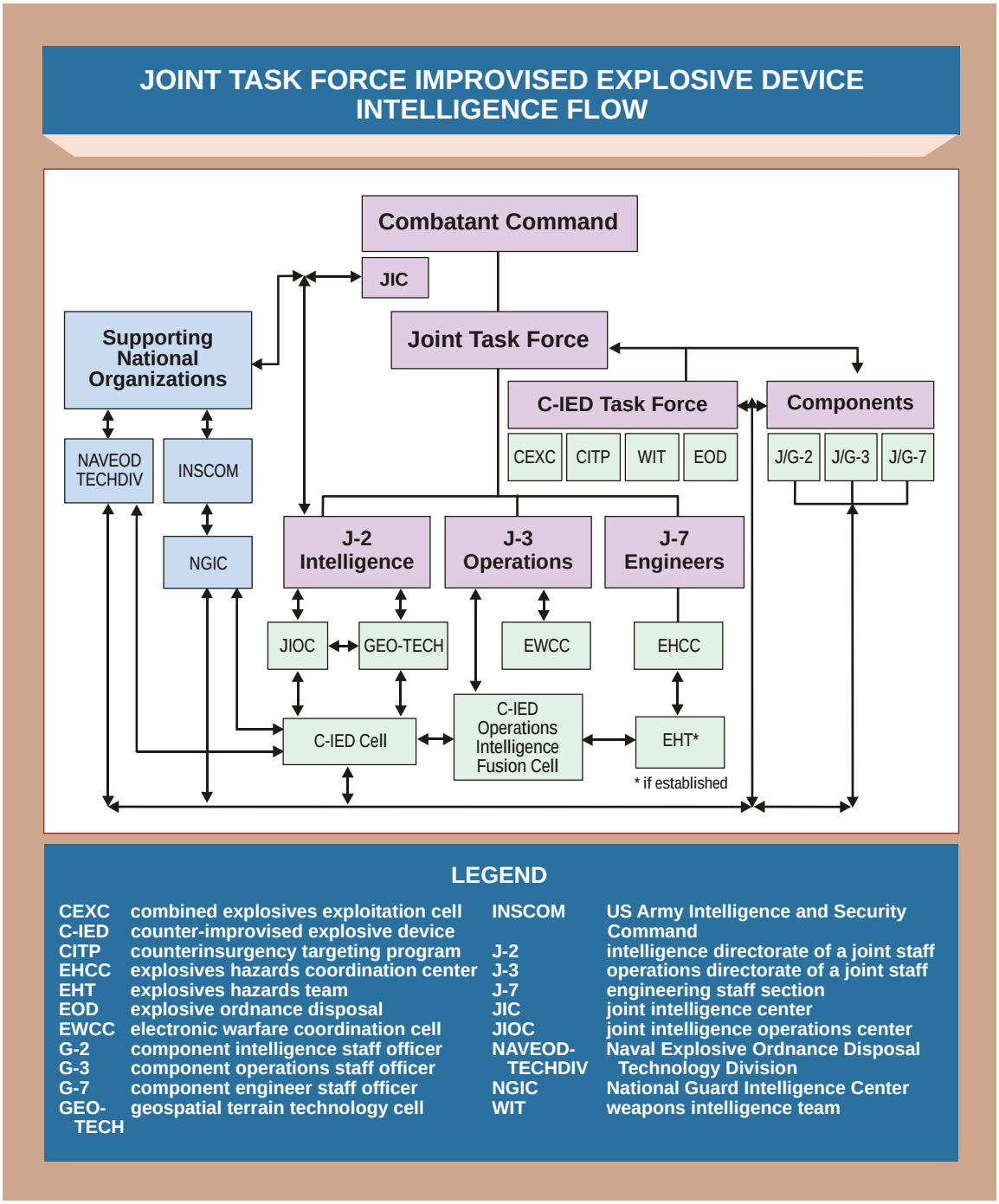


Figure V-3. (U) Joint Task Force Improvised Explosive Device Intelligence Flow

b. (U) J-3 C-IED Operations Intelligence Fusion Cell. The JTF J-3 C-IED operations intelligence fusion cell is the J-3's focal point to coordinate and synchronize all IED-related matters. It approves all friendly TTP and C-IED training packages used in theater and, through the C-IED working group, coordinates C-IED efforts across organizations. It tracks developments in adversary IED employment and TTP and participates with the J-2 in the development of appropriate friendly countermeasures.

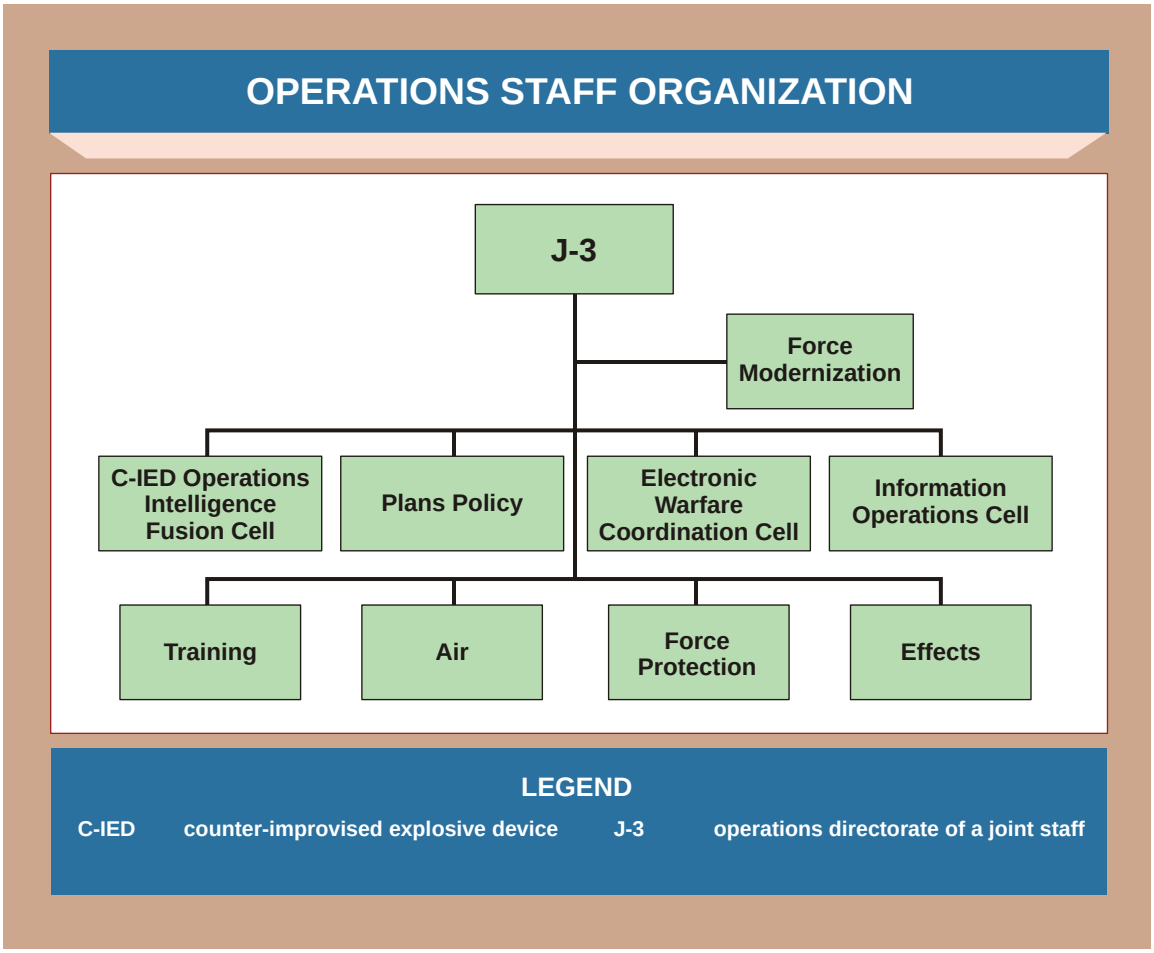


Figure V-4. (U) Operations Staff Organization

c. (U) In some instances, the cell, when augmented by representatives from the operational C-IED assets, can expand its responsibilities to include assisting in prioritizing the C-IED targeting effort, fusing IED-related intelligence and information, providing analytical products to the division and BCT, and providing persistent surveillance on select IED threats. The cell (Figure V-5) produces products for the targeting board and support the planning effort. This "fusion" configuration usually facilitates the synchronization of operations and intelligence activities and is adopted when the JTF is facing personnel constraints and must consolidate its staff functions. The core of the "fusion" cell is normally provided by the C-IED task force and is in direct support of the J-3.

(1) (U) **IO Cell.** IO planning should begin at the **earliest stage** of C-IED operations and must be an integral part of, not an addition to, the overall planning effort. The IO cell should be tailored as necessary to understand the human terrain environment and IED awareness to create a more favorable environment for friendly forces among the local populace.

(2) (U) **J-3 Effects Cell.** The effects cell, when established, coordinates and synchronizes all lethal and nonlethal assets in support of corps operations and conducts assessments of the operations in order to achieve the commander's objectives. This cell is

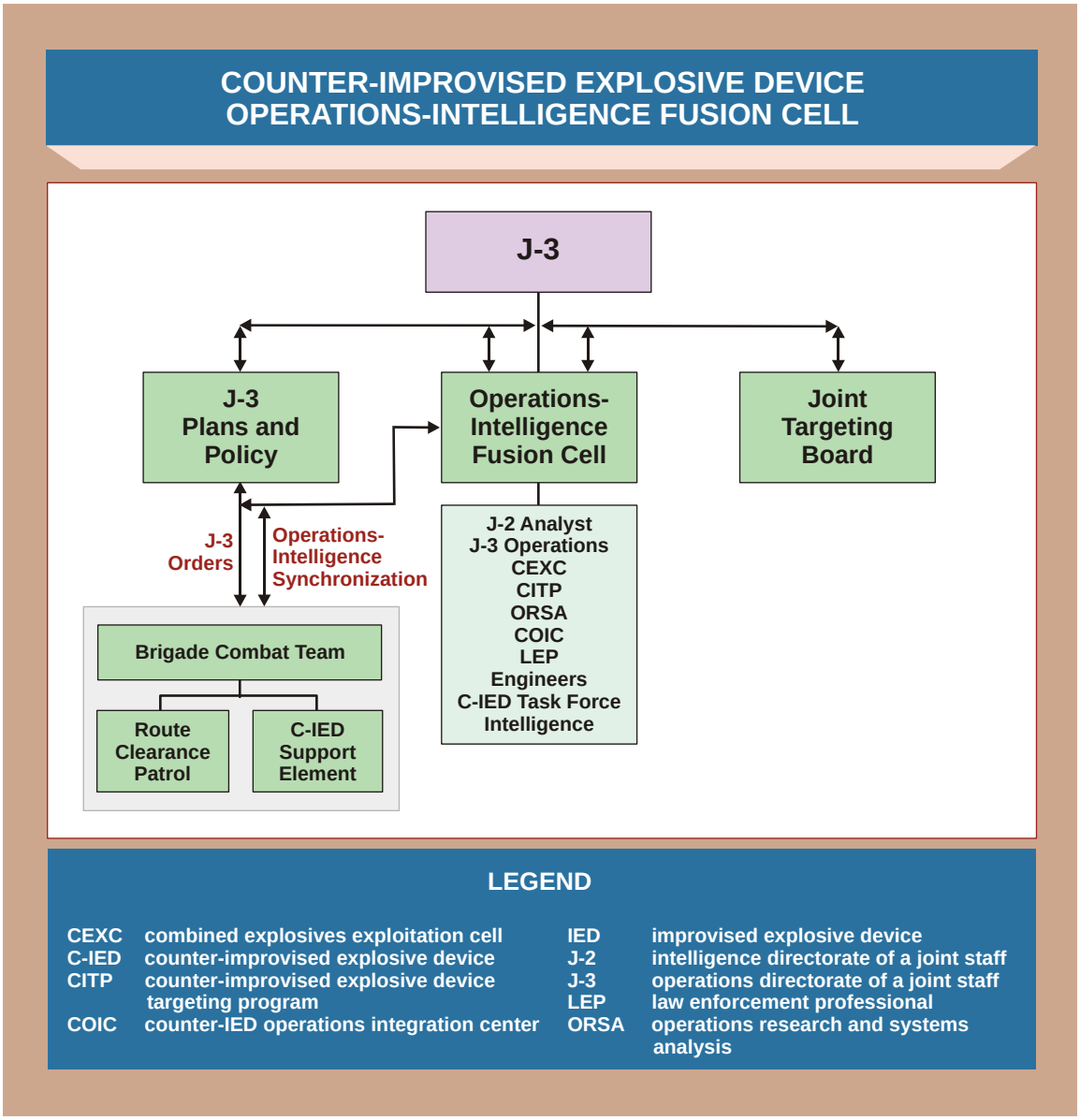


Figure V-5. (U) Counter-Improvised Explosive Device Operations-Intelligence Fusion Cell

normally assigned to the J-3 but can also be a stand-alone staff section, in which case, the electronic warfare coordination cell (EWCC) would be part of the cell. The effects cell develops, executes, and manages a robust and focused C-IED information operation.

(3) (U) **EWCC.** An EWCC can be established at the corps or division to serve as the lead for electronic warfare (EW) coordination, planning, and prioritizing the execution of EW actions in the JOA. The EWCC seeks to deny the adversary the use of the electromagnetic spectrum (EMS) and secure and maintain effective control and use of the EMS in support of the JTF. Depending on the size of the operation, the JTF may be assigned a joint counter radio-controlled improvised explosive device electronic warfare (CREW) unit to manage CREW systems, conduct CREW systems training for the JTF, and develop

CREW-related TTP. The unit will also coordinate with the JTF spectrum manager to deconflict CREW systems employment within the JTF's electronic spectrum.

(4) (U) **J-3 C-IED Working Group.** Chaired by the J-3, the C-IED working group is tasked to work specific issues relating to the development of the JTF C-IED plan. The working group is described in detail in paragraph 5, "Joint Task Force Counter-Improvised Explosive Device Boards, Working Groups, and Cells."

d. (U) **J-3 and Supporting C-IED Enablers.** EOD and WIT assets will normally accompany a JTF when it deploys. Depending on operational requirements, these EOD and WIT assets could range from a few teams to several battalions. Initially, **prior to the creation of C-IED task force,** these assets were placed under the tasking authority of the J-3.

4. (U) Engineers

(U) **Mission.** The J-7 (Engineer) (Figure V-6) coordinates combat, general and, in coordination with the J-2, geospatial engineering requirements for the joint force. The J-7 also provides engineer expertise to many of the JTF's boards, centers, cells, and working groups. In the C-IED effort, the J-7 establishes the EHCC to advise the joint force on developments in adversary IED employment and potential friendly countermeasures. In certain situations, the EHCC may also forward deploy (with the maneuver units) an explosive hazard awareness team.

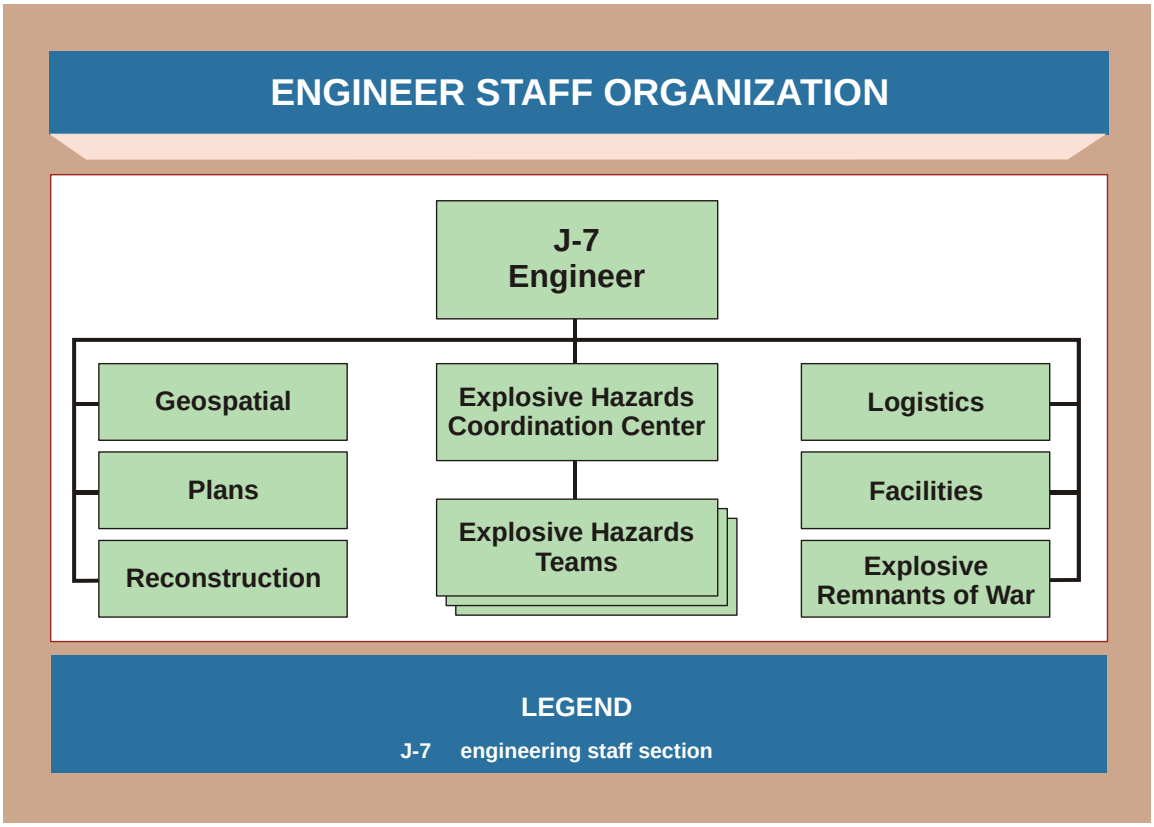


Figure V-6. (U) Engineer Staff Organization

a. (U) The mission of the EHCC is to enable the land component commander to predict, track, distribute information on, and mitigate explosive hazards within the theater by conducting information management and exchanging information concerning explosive hazards with sector and division cells. The EHCC establishes and maintains an explosive hazards database (EHDB). EHCC provides technical advice on the mitigation of explosive hazards, including the development of TTP, and provides training updates to field units, provides explosive hazards awareness and mine detector training teams; and has oversight responsibility for geospatial and topographic products and weapons intelligence. They coordinate explosive hazard teams (EHTs).

b. (U) The EHCC capabilities include:

(1) (U) Establishing, maintaining, and sharing the EHDB within the operational area.

(2) (U) Ensuring accuracy of explosive hazard information distribution via the battle command system.

(3) (U) Coordinating site evaluations and/or strike incident investigations at four sites simultaneously or conducting unit training at four sites simultaneously.

(4) (U) Coordinating technical and tactical training for the BCT by the EHT.

(5) (U) Providing updated TTP and guidance for route and area clearance operations.

(6) (U) Maintaining the EHDB.

5. (U) Joint Task Force Counter-Improvised Explosive Device Boards, Working Groups, and Cells

a. (U) In order to effectively manage the overall C-IED effort, the JTF will establish a variety of specialized boards, working groups, and cells. These organizations are designed to provide time-sensitive, joint, cross-functional C-IED operational unity of effort within the operational area through the integration and synchronization of the C-IED activities of the JTF with enabling theater and national resources. The inclusion of such organizations within the normal staff structures of a JTF may be appropriate for smaller-scale operations to assist the command in organizing and managing the command's C-IED efforts. While several of the organizations have overlapping, even redundant missions, the commander, because of force and resource constraints, will need to design the C-IED construct to pool resources and clearly delineate staff section responsibilities and eliminate unnecessary redundancies in order that the organizations perform their mutually complementary functions with minimum overlap.

b. (U) **JTF C-IED Management Board.** The JTF commander may decide to establish a JTF C-IED management board as a senior steering committee to manage the command's C-IED efforts. The purpose of the C-IED management board is to bring together senior JTF leadership with C-IED specialists to shape and direct the C-IED fight. The C-IED

management board is chaired by the deputy commanding general. It is designed to allocate resources, to include ISR, to support the overall C-IED effort. Membership includes the JTF's primary staff and senior representatives of the component commands. The management board, if established, reviews and decides upon the recommendations developed by the J-3's (or C-IED task forces) C-IED working group. The C-IED management board provides general officer-level updates on the IED threat and trends and MSC concerns relating to C-IED efforts in equipment, training and intelligence. Recommendations produced by the management board include:

(1) (U) C-IED-specific IO recommendations.

(2) (U) C-IED equipment distribution recommendations.

(3) (U) Decisions on C-IED technology requirements.

(4) (U) Priorities for asset allocation as pertains to C-IED efforts (ISR, air platforms, route clearance, and EOD efforts).

c. (U) **J-3 C-IED Working Group.** Depending on the commander's requirements, J-3 recommends the formation of a C-IED working group (Figure V-7). The working group, consisting of representatives from the J-2, J-2 collection management, J-2 plans, J-7, J-3 plans, J-3 operations, C-IED task force, and other members, as required, is tasked to work specific issues related to the C-IED plan. These issues can include anything from developing major refinements to the C-IED plan to developing the command response to major developments in the adversary's employment of IEDs. While the working group usually focuses on a specific IED-related issue of significant importance to the JTF, it can become a standing body to establish, plan, coordinate, and manage the overall C-IED initiatives. IED working groups may also be established at the MSCs. MSC-level working groups are designed to identify C-IED-related issues that require JTF-level action/intervention. MSC-level issues are presented to the J-3 C-IED working group via their working group representatives.

d. (U) **Component Command-Level C-IED Working Groups.** When required, IED working groups are also established at the joint force component commands. These working groups are responsible for focusing C-IED efforts within their respective operational area to mitigate current and future IED threats.

e. (U) **Specialized Cells for C-IED Task Force Operations.** There are a number of specialized cells within the C-IED task force organization that can be created to develop policy and provide direction for the JTF's overall C-IED operations. These cells are normally integrated into the C-IED task force's principal staff (primarily the operations and plans and policy staffs). These cells include:

(1) (U) **C-IED Intelligence Cell.** Discussed in detail in paragraph 2, "Intelligence," this cell is a specialized intelligence cell created to address a wide range of issues related to the command's C-IED plan. The cell, normally placed under C-IED task force J-2, can be assigned a variety of tasks from IED event analysis, determining IED trends, and IED pattern analysis.

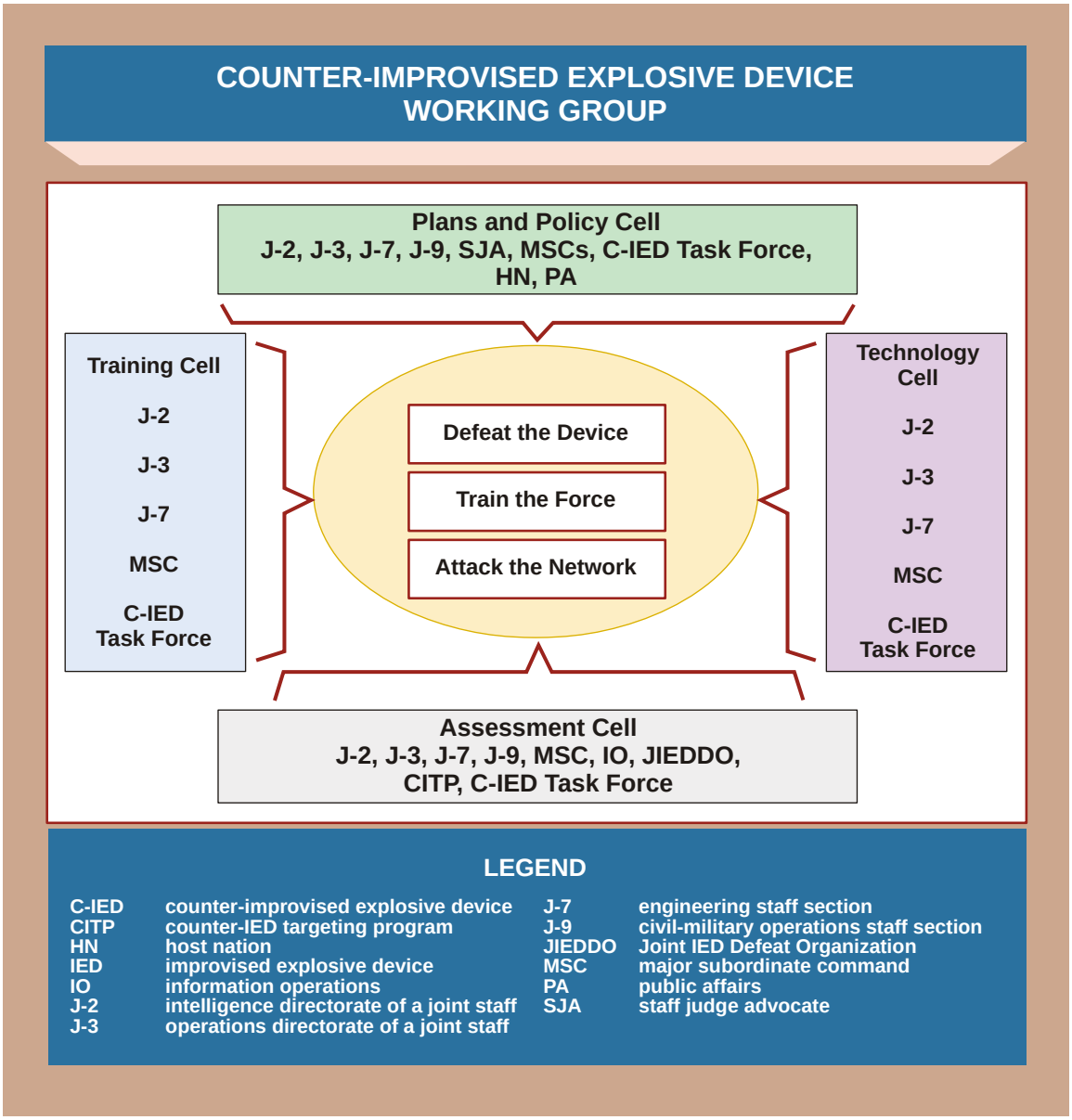


Figure V-7. (U) Counter-Improvised Explosive Device Working Group

(2) (U) **Plans and Policy Cell.** The C-IED task force J-3's plans and policy cell is responsible for developing the command's C-IED plan and for ensuring that the plan is closely tied to the command's overall COIN plan. The cell's tasks include:

(a) (U) Developing the C-IED plan.

(b) (U) In accordance with the CJTF's policy guidance, establishing the command's policies on IED event reporting to include timelines, IED data collection standards, and dissemination of information.

(c) (U) In cooperation with the training cell, establishing policies to update and disseminate C-IED TTP force-wide on a regular basis. Employ specialized mobile training

teams to routinely conduct assistance visits to subordinate units providing the latest information on IED-related TTP and appropriate countermeasures.

(d) (U) **Technology Cell.** This cell is responsible for reviewing friendly force protection and C-IED technologies, identifying potential shortfalls, and recommending near-term solutions. It forwards all short-term recommendations through operations for implementation within the JTF and provides longer-term recommendations through the chain of command and C-IED task force for submission to JIEDDO for action.

(e) (U) **Training Cell.** This cell is responsible for reviewing friendly force C-IED training programs and TTP, identifying potential shortfalls, and recommending near-term (that can be addressed by the force's organic training capabilities, i.e., unit-level TTP or by mobile training teams) and long-term (for service or joint predeployment training) solutions. Near-term recommendations are forwarded through the J-3 for implementation within the command. Longer-term recommendations are forwarded, through the chain of command, to DOD level for action by the appropriate Service.

f. (U) **Targeting.** The C-IED working group plays a critical role in developing and recommending C-IED-related targets for lethal and nonlethal engagement. The C-IED working group develops critical vulnerability candidates in each function area within the overall IED network. Actionable targets and targets for development are matched to these critical vulnerabilities. Targets for development steer requirements for intelligence. Actionable targets that, if actioned together, will disable a critical vulnerability, are prioritized in a list of recommended targets with recommended means of engagement (lethal and nonlethal). This list is forwarded for consideration and action by the command's targeting board.

6. (U) Coordinating with Supporting Theater- and National-Level Counter-Improvised Explosive Device Organizations

a. (U) In organizing the operational area for the C-IED effort, the commander will have the ability to call upon assistance from highly specialized theater military, DOD, national, and interagency assets that can deploy elements forward to augment the JTF staff. The theater, national, DOD, and interagency assets can perform a wide variety of functions designed to degrade the insurgents' IED infrastructure from detailed forensic/technical evaluations of IEDs, to managing an HVI targeting effort. The major theater- and national-level C-IED enablers include:

b. (U) CEXC

(1) (U) The CEXC is a Navy-led task organized unit created to meet technical and forensic intelligence requirements for the combatant commander. It provides expert-level technical and forensic exploitation and analysis of IEDs and associated components, improvised weapons, and other weapons systems in order to determine enemy tactics, identify IED trends and bomb makers, and assist in the development of defensive and offensive C-IED measures. Depending on the theater requirements, the CEXC construct is often augmented by law enforcement professionals (LEPs), CITP personnel, intelligence

analysts, and MNFs work closely with other forensic/exploitation labs and other government departments and agencies to provide more synergetic and extensive exploitation capabilities to the combatant commander. Some of the capabilities include:

(a) (FOUO) Conducting first-line technical and forensic exploitation and evaluation of IEDs and components, and preparing detailed laboratory reports for all exploited materiel.

(b) (FOUO) Providing technical assistance and advice on EOD, force protection, and combat tactics regarding the threat posed by IEDs and counter-IED TTP.

(c) (FOUO) Providing detailed forensic analysis and device profiles to assist the targeting process.

(d) (FOUO) Providing technical assistance to support the interrogation of IED-related detainees.

(e) (FOUO) Assisting in operations against suspected bomb makers and transporters, IED factories, storage locations, and training sites.

(f) (FOUO) Providing briefings, component familiarization, personnel, and subject matter expert support.

(g) (FOUO) Conduct on-scene evaluations of significant IED incidents in order to collect evidence and intelligence on IED-related TTP.

(h) (FOUO) Support site exploitation operations to include accompanying units on raids and searches to exploit caches.

(2) (FOUO) When combined with on-scene reporting from the WITs, EOD teams, detainee reporting, and unit-level information, the CEXC can provide a comprehensive picture of adversary IED developments and TTP that can be used to modify friendly TTP and force protection initiatives.

(3) (FOUO) CEXC exploitation reports are provided to various US national and allied agencies for further technical analysis and EOD-related database development. Additionally, these reports form the basis for targeting programs directed against key nodes in the adversary's IED infrastructure. The main customer for CEXC reports is the TDC in the J-2 JIOC, which also manages the profiles. CEXC reports are also provided to unit-level intelligence cells, and are available through the CEXC Web site. In addition, CEXC generates spot reports for new devices and technical bulletins, which are educational in nature. CEXC analysis provides only a piece of the total insurgent puzzle. Units must fuse the CEXC information with EOD and WIT reports and with their own HUMINT and tactical intelligence to fully understand the bomb maker network.

c. (U) **HVI Targeting Program.** The HVI targeting program is a combatant commander's resource that works closely with the JTF and is designed to capture key adversary personnel including those contributing to the adversary's IED activities. The HVI

targeting program is a joint, interagency task force that plans, manages, and conducts the targeting of HVIs who are in or transiting the operational area in order to capture key individuals who are significantly influencing the operations, directing and/or funding transnational terrorists and local insurgents. The task force is manned by a variety of specialists from the JTF and from supporting interagency partners. Interagency participants could include an on-site team with representation from DOD investigations, legal, DHS, FBI, and the Department of the Treasury. Interagency intelligence reachback for analytical support would also be provided. Liaison officers from the major participants in the JTF would be present to assist in organizing forces to take action against identified targets.

d. (U) **Threat Finance Exploitation (TFE) Unit.** The TFE unit works with DOD and non-DOD intelligence, law enforcement, and regulatory agencies that are responsible for taking action against terrorist and insurgent financial networks. The unit is an integral part of the overall national program to detect, collect, and process information on, and target, disrupt, or destroy the adversary's financial systems and networks. As part of the C-IED effort, the TFE effort denies the adversary the uninterrupted financial resources needed to obtain IED-related supplies and support their personnel (bomb makers, transporters, emplacers). At the JTF level, threat finance information derived from raids, cache exploitation, and interrogations is analyzed and passed through intelligence channels to the TFE unit for target development and further exploitation in coordination with national resources. Appropriate targeting recommendations are then passed back to the JTF for action using lethal and nonlethal means.

CHAPTER VI
COUNTER-IMPROVISED EXPLOSIVE DEVICE TASK FORCE (U)

1. (U) Introduction

(U) As an alternative to using the JTF staff to manage the C-IED effort, the CJTF can establish a task force, integrating tactical- and operational-level organizations and streamlining communications under a single headquarters whose total focus is on the C-IED effort. The task force construct is useful when a large number of C-IED assets (EOD; WIT; C-IED training teams; and chemical, biological, radiological, nuclear, and high-yield explosives [CBRNE] response teams [CRTs], formerly identified as technical escort teams and their supporting organizations, [COIC, LEP, operations research and systems analysis {ORSA}, joint expeditionary team {JET}, etc.]) have been deployed to support large-scale, long duration operations. The organization and employment of the task force will depend on the mission, the threat and the available C-IED enabling forces. Counter-IED resources are scalable to meet not only the size of the supported JTF but also the mission and phase of the operation (Figure VI-1).

2. (U) Organization

a. (U) A C-IED task force is normally built around an appropriately augmented brigade-level headquarters or its equivalent (EOD group, ordnance group, engineer brigade, maneuver enhancement brigade, Army EOD battalion or Navy EOD mobile unit). In addition to controlling the subordinate EOD organizations and battalions, the C-IED task force commander is given operational control (OPCON) or tactical control (TACON) of the JTF's specialized C-IED assets to include WIT, CEXC, CITP, COIC, C-IED training teams, and the technical escort detachment. The combination of EOD assets with specialized C-IED enablers allows the task force to conduct focused C-IED network analysis and targeting, provide direct support packages of C-IED enablers to BCTs, and organize and conduct unit-level C-IED training programs.

b. (U) In establishing a task force to manage C-IED operations, the CJTF will align supporting resources to provide the task force commander with the means necessary to accomplish the mission. Under the task force construct, EOD units are normally OPCON and/or TACON to the C-IED task force commander. The EOD battalion continues to provide EOD teams in direct support of the MSCs. MSCs continue to provide combat service support (CSS) to the assigned EOD team. The EOD battalion provides specialized technical support to the deployed EOD teams and may also be tasked to provide CSS for WIT. An augmented EOD battalion headquarters is well suited to form the nucleus of the maneuver division's C-IED effort, but as previously mentioned, this task could be filled by any battalion staff headquarters augmented with technical experts and additional enablers. In addition to the JTF's attached EOD units that form the basis for the task force, the following C-IED enabling assets will normally be assigned to or under the control of the C-IED task force:

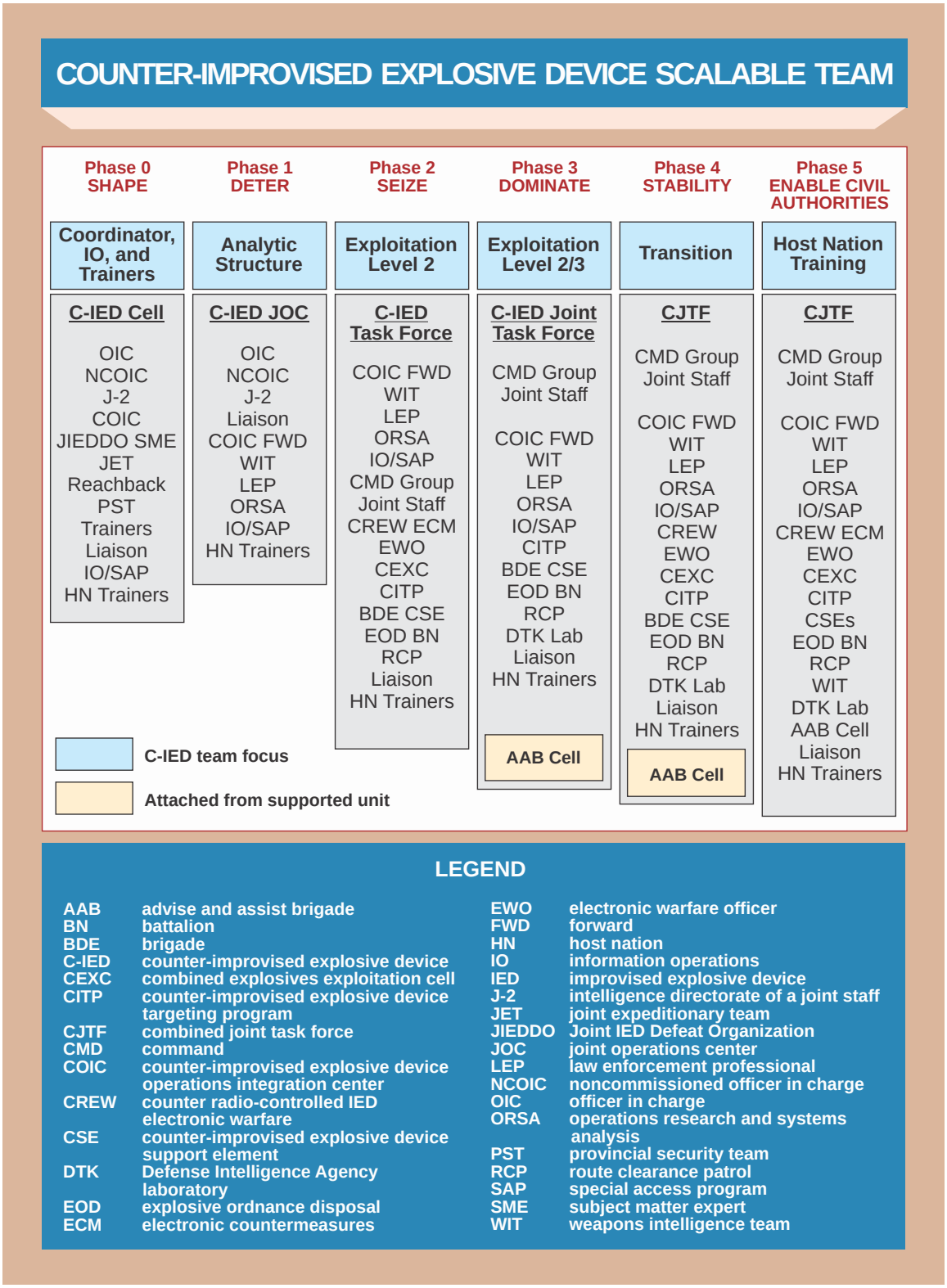


Figure VI-1. (U) Counter-Improvised Explosive Device Scalable Team

(1) (U) The JTF **C-IED intelligence cell** is a JTF J-2 asset that is detailed to the task force commander. The cell consists of the operations section, a network infrastructure analysis and targeting section, the forward deployed CITP cell, the CEXC, and the WIT. The task force C-IED intelligence cell is the primary agency responsible for fusion of technical assessments, forensic analyses, and all-source threat intelligence related to the IED threat within the operational area. Working with the JTF corps analysis and control element and the component commands, the cell develops all-source intelligence products designed to target insurgent IED networks and disrupt the insurgent's ability to effectively employ IEDs as the weapon of choice. The task force C-IED intelligence cell also develops and disseminates information on the latest developments in threat TTP and advises the JTF on IED risk mitigation.

(2) (U) **JTF IO Staff.** The IO staff provides focused IO planning and support to the C-IED TF commander. They coordinate and deconflict related IO capabilities with other staff functions and supporting agencies and organizations.

(3) (U) **CEXC.** The CEXC is normally assigned to the CJTF, who then delegates OPCON to the C-IED task force commander. The CEXC is the core of the task force's C-IED technical intelligence (TECHINT) element facilitating targeting of the adversary's IED infrastructure. Taskings for the CEXC are developed by the CJTF's J-2.

(4) (U) **CBRN Response Teams.** CBRN response teams provide weapons of mass destruction (WMD) site and chemical weapons assessment and exploitation support throughout the theater.

(5) (U) **WIT.** The WITs or C-IED teams are assigned to the C-IED task force. Normally an EOD company, with a direct support WIT, will be placed in direct support of each BCT. The detachments normally will be placed OPCON to the C-IED task force commander.

(6) (U) **CITP.** The NGIC forward deployed CITP cell is assigned to the task force and acts as the focal point for C-IED intelligence fusion. The detachments normally will be placed OPCON to the C-IED task force commander.

(7) (U) **C-IED Training Teams.** The JTF EHCC's training teams normally are placed OPCON to the C-IED task force commander.

(8) (U) **Joint CREW Unit.** The CREW is assigned to the theater C-IED task force. In coordination with the JTF EWCC, the CREW neutralizes the radio-controlled improvised explosive device (RCIED) threat by deconflicting EMS use; conducting EW coordination in support of current operations, training, and readiness; and providing fielding support down to the BCT level. The detachments normally will be placed OPCON to the C-IED task force commander.

(9) (U) **COIC-Forward.** JIEDDO deploys COIC teams forward with the C-IED task force to enable reach back to the full capabilities of COIC analytic centers in theater and at the JIEDDO COIC in the continental United States (CONUS) to enable more precise attacks by the supported commander to defeat networks that employ IEDs.

(10) (U) **JET.** The JET supports all echelons of the joint force, interagency, and multinational partners. Its purpose is to train, advise, observe, analyze, and to collect and disseminate TTP, lessons learned, and best practices to mitigate the IED threat. They will normally operate in two- to three-person teams and be placed OPCON to the task force's C-IED commander.

3. (U) Roles and Responsibilities

a. (U) The mission of the C-IED task force is to enable and support the coordination of the JTF's C-IED operations to create the conditions that will deny the IED cells' freedom of action, reduce the IED cells' effectiveness, and lower overall IED activity to a level commensurate with the HN security forces' capabilities. It does so by commanding and controlling specialized C-IED forces as well as coordinating and synchronizing JTF-level C-IED operations, intelligence, technology and training initiatives throughout the operational area. The C-IED task force optimizes C-IED operations by fusing IED defeat-related intelligence, capabilities, training, equipment, and EOD forces in one organization at the JTF level. The task force acts as the single point of contact for C-IED matters within the operational area. The task force can also be tasked to develop the JTF's C-IED CONOPS and C-IED OPLAN. The C-IED task force's major missions include:

(1) (U) Execution and synchronization of C-IED operations by coordinating and employing C-IED forces and enablers in support of the JTF's C-IED plan. This includes managing the analytical and intelligence assets that feed into the targeting and AtN processes. The C-IED task force provides the CJTF with C-IED subject matter expertise.

(2) (U) Providing C-IED operations planning support. By coordinating with the JTF planning staff, ensuring that the JTF integrates C-IED considerations into its operational plans. Recommending C-IED operational priorities.

(3) (U) Exercising command and control (C2) over C-IED and EOD resources. When C-IED and EOD resources are placed in direct support of component maneuver units, the C-IED task force will maintain responsibility for ensuring those resources have logistical, administrative, planning, and communications support to accomplish their mission-essential tasks.

(4) (U) Managing and developing policy for the WTI and IED exploitation process and managing the IED exploitation architecture. This includes ensuring that the results of the collection, analysis, and dissemination of TECHINT, biometric information, forensics, and media exploitation feed into the C-IED targeting process. It also includes the synchronization of C-IED exploitation in the JOA and the tracking of exploitation labs, personnel, requirements, and forensic material.

(5) (U) Conducting assessments of C-IED capabilities and gaps based on threat and operational environment.

(6) (U) Capturing and analyzing current TTP and best practices in order to support in-theater training updates and refresher training. Coordinating refresher training and

training upon reception, staging, onward movement, and integration (RSOI) of incoming units. Providing support for this training to multinational partners.

(7) (U) Providing constant relevant feedback based on the threat, operational environment, and best practices that feeds into predeployment and IED awareness training.

(8) (U) Organizing the intelligence assets required to determine IED threats and provide analysis on IED cells and sources to feed the targeting process. Assisting units with the employment and integration of C-IED operations within COIN.

(9) (U) Conducting all-source intelligence analysis to build an understanding of the enemy's operations and IED system. Intelligence analysts can gain access to multiple data feeds using COIC tools and taking advantage of US-based reachback support.

(10) (U) Compiling analytically derived, empirically supported, quantitative assessments in support of decision making with regard to targeting and C-IED planning to enhance effectiveness of AtN efforts. Providing impact assessments of operations and solutions on the IED networks.

(11) (U) Developing networks, nominating C-IED targets, developing target packages, and participating in the JTF's joint targeting board to target IED cells and individuals.

(12) (U) Developing and maintaining the ability to share pertinent intelligence across various networks to enable all friendly forces to make necessary linkages that will support both AtN and defeat the device LOOs.

(13) (U) Conducting liaison and sharing information with other organizations involved in the C-IED effort.

(14) (U) Ensuring that there is a unified and coordinated effort for C-IED across MNFs.

(15) (U) Enabling HN training and information sharing to facilitate a transition to the C-IED effort.

(16) (U) Supporting the JTF's strategic communication implementation and IO activities.

(17) (U) Integrating material and nonmaterial solutions to include CONOPs, concepts of employment, and training and sustainment plan development. Conducting ongoing assessments of material and nonmaterial solutions to influence future planning.

b. (U) The C-IED task force coordinates the overall conduct of C-IED operations through the JTF J-3. C-IED task force assets (EOD battalions/mobile units and companies augmented by C-IED enabling assets) deployed in support of maneuver units coordinate their respective operations through the supported unit's J-3/battalion or brigade operations staff officers (S-3s). Through participation in the JTF's (and supported unit's) staff planning

cycle, including applicable boards, working groups, and cells, the C-IED task force synchronizes and integrates its operations into the JTF's and supported unit's overall scheme of maneuver.

c. (U) Service engineer units conducting route clearance operations either in direct support of the maneuver brigades (or their equivalent formation) or on an area support basis will normally coordinate for C-IED task force support through the supported headquarters' J-3/S-3. Engineers identify their C-IED support requirements through participation in the unit's C-IED working groups and planning cells.

4. (U//FOUO) Task Force Intelligence Integrating Functions

a. (U) One of the most complex challenges in organizing the C-IED effort is in gathering, analyzing, and disseminating information that is relevant to each echelon of the command, from the BCTs that must stay current on the latest adversary IED TTP, to the command that is organizing the fight to defeat the IED supporting infrastructure.

b. (U) C-IED Intelligence Cell

(1) (U) **Organization.** Consists of the J-2's C-IED fusion and TDCs. The cell is responsible for integrating the activities of a multitude of intelligence collection and analysis functions to support the task force's many activities. The cell has a number of specific responsibilities including:

(a) (U) Recommending the focused employment of intelligence collection assets against the adversary's IED infrastructure.

(b) (U) Serving as the all-source focal point for IED-related intelligence information originating within the national system, MNF, and HN sources.

(c) (U) Conducting trend analysis on adversary IED employment and device design to enhance friendly force protection programs and IED defeat operational planning.

(d) (U) Identifying and developing information (target packages) on the critical nodes in the adversary's IED infrastructure to support C-IED operations.

(2) (U) **Responsibilities.** This cell is the primary agency responsible for fusion of technical assessments, forensic analyses, and all-source threat intelligence related to the IED threat within the theater of operations. The cell will develop and disseminate threat TTP and advise the MNF in IED risk mitigation. Working closely with the J-2 collection manager and the JIOC/JISE, the cell answers all relevant IED-related RFIs. The cell is also responsible for developing actionable intelligence for the J-2's portion of the CITP. In developing its analytical products, the cell reviews all IED-related intelligence generated within the command and by the relevant entities (NGIC, TEDAC, COIC, etc.), fusing this information from a variety of sources including:

(a) (U) CEXC.

(b) (U) WIT.

(c) (U) EOD teams.

(d) (U) J-2 terrain analysis team.

(e) (U) MSC input.

(f) (U) THTs.

(g) (U) JIEDDO field team after action reports.

(3) (U) **TDC.** The TDC is a consolidated effort of the NGIC and J-2's intelligence assets. The TDC cell, organic to the C-IED JTF intelligence cell, leverages all-source local and national IED intelligence exploits NGIC reachback capability to identify IED cell members and build targeting folders for execution by maneuver or special operations forces.

(a) (U) **Manning.** The TDC contains the following elements:

1. (U) Specialized target analytical team. This team can concentrate on high priority concerns such as EFP manufacture.

2. (U) TECHINT.

3. (U) IED target analytical team.

4. (U) Database.

(b) (U) The majority of the cell's personnel are dedicated to network targeting as directed by J-2 JIOC/JISE officer-in-charge. Regional analysts are dedicated to each MSC to include a joint special operations task force. These analysts have two basic missions: assist the supported intelligence sections in developing targeting packages and act as the C-IED intelligence cell's local source for C-IED-related information that is passed directly to those targeting cells at the JTF.

(4) (U) **Targeting.** In a typical targeting scenario, JTF or locally (BCT/forward operating base level) developed information on a potential target will be compiled from all available local sources. This information will be passed to the CITP at NGIC for further refinement using whatever information is available from national sources. NGIC can also provide imagery of the target area. NGIC will identify any gaps that exist in the available intelligence information. These gaps will be monitored by the intelligence cell at the C-IED task force and, using command resources, the C-IED intelligence cell will attempt to fill those gaps. The final package will then be passed to the appropriate echelon for action.

(5) (U) **Products.** The C-IED intelligence cell develops products designed to meet the specific needs of operational and tactical consumers. These products are based on all-

source inputs and are designed to support the full range of information requirements for organizing the C-IED effort from training on the latest adversary TTP to developing targeting packages.

(a) (U) **Analytical Support Products.** Analysis of IED events detailing both blue and red actions.

(b) (U) **Technical Analysis Products.** Consist of detailed evaluation of the operating characteristics and potential vulnerabilities of IEDs (or their components) that have been recovered by field teams.

(c) (U) **Quick Look Reports.** Consist of quick turn reports with analysis on changes or emerging trends in adversary IED employment TTP.

(d) (U) **Trend and Pattern Analysis.** A detailed analysis of IED events in space and time to identify "hot spots" for C-IED targeting efforts and developments in the adversary's employment of IEDs to support C-IED targeting and force protection initiatives.

(e) (U) **Target Packages.** Provide analysis identifying specific individuals and places associated with the adversary's IED support infrastructure. The packages provide operational planners with sufficient detail to plan and conduct operations focused on disrupting /capturing/neutralizing the identified IED infrastructure components.

(f) (U) **Network Analysis.** Diagrams of IED cells and networks for targeting.

(g) (U) **Detainee Support Products.** Status of detainees with linkage to IED networks.

5. (U) Counter-Improvised Explosive Device Task Force Staff Functions

(U) The C-IED task force has two major responsibilities: directing the assigned EOD units and optimizing the JTF's overall C-IED operation. While it operates as a normal task force headquarters in planning for the employment and support of its assigned forces, the staff have some unique C-IED-related responsibilities including:

a. (U) **C-IED Task Force J-3**

(1) (U) Assist in the development of the JTF's C-IED plans and execute staff supervision over the operational aspects of them (subordinate unit involvement, rules of engagement, training, etc.).

(2) (U) Support the coordination of JTF-level C-IED operations and chair or attend designated C-IED organizations.

(3) (U) Coordinate with JTF's designated engineer brigade on route clearance, sanitation, and improvement operations by providing forces and TECHINT.

(4) (U) Supervise and facilitate the partnering operations with HN force's bomb disposal companies and HN police IED defeat teams.

b. (U) C-IED Task Force Plans

(1) (U) In coordination with J-3, Develop and integrate C-IED enabler support into Future Plans, develop C-IED enabler subject matter expert (SME) input to plans and orders.

(2) (U) In coordination with J-3, develop and manage joint C-IED enabler force generation requirements for support to the MNF.

c. (U) C-IED Task Force J-7 (C-IED Training Team)

(1) (U) Provide a C-IED program (relevant to the in-country threat) in order to provide personnel with the knowledge required to identify IEDs and IED indicators, application of CREW systems, cache search awareness, and the skills required to respond safely to threat situations.

(2) (U) Provide C-IED training teams to support in country RSOI as well as one mobile training team for deployment as required. Coordinate with JIEDDO, JTF J-3 training, and JTF J-7 to provide up-to-date training in C-IED TTP in theater and the CONUS. In conjunction with JIEDDO develop and disseminate C-IED TTP to all forces.

6. (U) Counter-Improvised Explosive Device Task Force Support to the Maneuver Units

a. (U) The planning and conduct of C-IED operations is a multi-echelon effort that must be closely coordinated and integrated. The C-IED task force plays a critical role in this effort by attaching specialized C-IED support teams to the land component's subordinate divisions, maneuver brigades, and battalions. These C-IED support elements are designed to assist the maneuver unit in the planning, coordination, and integration of its immediate C-IED operations and act as a liaison to the C-IED task force. The C-IED support element also coordinates the unit's IED infrastructure targeting efforts.

b. (U) The division C-IED support element coordinates and integrates C-IED operations within the division operational area, and integrates C-IED enablers, analysis, and products into the division targeting process in order to support the division in maintaining freedom of action and defeating insurgent networks. The division C-IED support element is comprised of a mix of specialized C-IED personnel such as CEXC, CITP, intelligence analysis, ORSA, and LEP) along with intelligence and operations staff. Critical division C-IED support element tasks are detailed in Figure VI-2.

DIVISION COUNTER-IMPROVISED EXPLOSIVE DEVICE SUPPORT ELEMENT CRITICAL TASKS (U)	
(U) Execution and synchronization of counter-improvised explosive device (C-IED) operations.	(U) Coordination and employment of forces in support of a C-IED plan. This includes the analytical and intelligence assets that feed into the targeting and "attack the network" processes. Provide the division commander with C-IED subject matter expertise (SME).
(U) Provide C-IED operations planning support.	(U) Planning support to division headquarters with regards to integrating C-IED to operations. Conduct internal planning to better provide SME to leadership and recommend C-IED priorities.
(U) C-IED and explosive ordnance disposal (EOD) forces.	(U) Oversight and life support functions such as logistical, administrative, planning, and communications that enable C-IED forces to perform mission-essential tasks.
(U) Conduct exploitation of improvised explosive device (IED) forensic and biometric material.	(U) Personnel and develop future requirements. Feed data into the incident database and report in accordance with the established forensic tracking process.
(U) Identify and request emerging and immediate C-IED requirements.	(U) Conduct assessments of C-IED capabilities and gaps based on threat and operational environment; document and communicate those gaps through appropriate channels for rapid resolution.
(U) Support and provide in-theater C-IED training and feed information to update predeployment training.	(U) Capture and analyze current tactics, techniques, and procedures and best practices in order to develop in-theater training updates and refresher training. Provide constant relevant feedback based on the threat, operational environment, and best practices that feeds into predeployment and IED awareness training.
(U) Intelligence, analytical and network development support to C-IED operations.	(U) Employment of required intelligence assets to determine IED threats and provide analysis on IED cells and sources that feed the targeting process.
(U) Operations, intelligence, and analysis fusion.	(U) Conduct multidiscipline intelligence analysis to build an understanding of the enemy's operations and IED system. Intelligence analysts can gain access to multiple data feeds using C-IED operations integration center tools and taking advantage of US-based reachback support.
(U) Operational research analysis.	(U) Compile analytically derived, empirically supported, quantitative assessments in support of decision making with regards to targeting and C-IED planning to enhance effectiveness of "attack the network" efforts. Provide impact assessments of operations and solutions on the IED networks.
(U) Support to C-IED targeting.	(U) Working within the joint task force's targeting methodology, lead or participate in the joint targeting board to target IED cells and individuals. Develop networks, nominate C-IED targets, and develop target packages.
(U) Information sharing and archiving.	(U) Ability to share pertinent intelligence across various networks to enable all friendly forces to make necessary linkages that will support both "attack the network" and "defeat the device" lines of operation. Ensure subordinate units collect all data on IED events that occur within their battle space.
(U) Liaison with other organizations.	(U) Ability to link with and include other organizations into the C-IED effort and ensure necessary information is shared.

(U) Multinational operation coordination and support.	(U) Ensuring that there is a unified and coordinated effort for C-IED across multinational forces.
(U) Host nation partnering.	(U) Enabling host nation training and information sharing in order to facilitate a transition of the C-IED effort.
(U) Support C-IED information operations (IO).	(U) Understanding the human environment and supporting division IO campaign for IED awareness and information to create a favorable impression or environment for multinational forces or the host nation among the local populace.

Figure VI-2. (U) Division Counter-Improvised Explosive Device Support Element Critical Tasks

c. (U) The brigade and battalion C-IED support element plans, coordinates, and integrates C-IED operations within the units; and plans, coordinates and integrates C-IED enablers, analysis, and products into the unit's targeting process to support the unit in maintaining freedom of action and defeating insurgent networks. Brigade and battalion C-IED support element tasks are listed in Figure VI-3 and VI-4.

BRIGADE COUNTER-IMPROVISED EXPLOSIVE DEVICE SUPPORT ELEMENT CRITICAL TASKS (U)	
(U) Execution and synchronization of counter-improvised explosive device (C-IED) operations.	(U) Coordination and employment of forces in support of a C-IED plan. This includes the analytical and intelligence assets that feed into the targeting and "attack the network" processes. Provide the brigade commander with C-IED subject matter expertise.
(U) Provide C-IED operations planning support.	(U) Planning support to brigade headquarters with regards to integrating C-IED to operations. Conduct internal planning to better provide subject matter expertise to leadership and recommend integrating C-IED priorities.
(U) C-IED and explosive ordnance disposal force.	(U) Oversight and life support functions such as logistical, administrative, planning, and communications that enable integrating C-IED forces to perform mission-essential tasks.
(U) Conduct exploitation of improvised explosive device (IED) forensic and biometric material.	(U) Integrate IED exploitation into brigade operations, manage and coordinate personnel and exploitation assets to best support collection and the brigade commander's intent. Feed data into the joint operations area incident database and report in accordance with forensic tracking process.
(U) Identify and request emerging and immediate C-IED requirements.	(U) Conduct assessments of C-IED capabilities and gaps based on threat and operational environment; document and communicate those gaps through appropriate channels for rapid resolution.
(U) Support and provide in-theater C-IED training and feed information to update predeployment training.	(U) Capture and analyze current tactics, techniques, and procedures and best practices in order to develop in-theater training updates and refresher training. Provide constant relevant feedback based on the threat, operational environment, and best practices that feeds into predeployment and IED awareness training.
(U) Intelligence, analytical, and network development support to C-IED operations.	(U) Employment of required intelligence assets to determine IED threats and provide analysis on C-IED cells and sources that feed the targeting process.
(U) Operations, intelligence, and analysis fusion.	(U) Conduct multidiscipline intelligence analysis to build an understanding of the enemy's operations and IED network. Intelligence analysts can gain access to multiple data feeds using combined operations integration center's tools and taking advantage of reachback support.

(U) Operational research analysis.	(U) Compile analytically derived, empirically supported, quantitative assessments in support of decision making with regards to targeting and C-IED planning to enhance effectiveness of "attack the network" efforts. Provide impact assessments of operations and solutions on the IED networks.
(U) Information sharing and archiving.	(U) Ability to share pertinent intelligence across various networks to enable all friendly forces to make necessary linkages that will support both "attack the network" and "defeat the device" lines of operation.
(U) Liaison with other organizations.	(U) Ability to link with and include other organizations into the C-IED effort and ensure necessary information is shared.
(U) Host nation partnering.	(U) Enabling host nation training and information sharing in order to facilitate a transition of the C-IED effort.
(U) Support C-IED information operations.	(U) Understanding the human environment and supporting brigade information operations activities for IED awareness and information to create a favorable impression or environment for multinational or host nation forces among the local populace.

Figure VI-3. (U) Brigade Counter-Improvised Explosive Device Support Element Critical Tasks

BATTALION COUNTER-IMPROVISED EXPLOSIVE DEVICE SUPPORT ELEMENT CRITCIAL TASKS (U)	
(U) Advise battalion commander on counter-improvised explosive device (C-IED) matters.	(U) Coordination and employment of forces in support of a C-IED plan. This includes the analytical and intelligence assets that feed into the targeting and "attack the network" processes. Provide the battalion commander with C-IED subject matter expertise.
(U) Provide C-IED operations planning support.	(U) Planning support to battalion headquarters with regards to integrating C-IED to operations. Conduct internal planning to better provide subject matter expertise to leadership and recommend C-IED priorities.
(U) Conduct and manage explosive ordnance disposal/improvised explosive device (IED) disposal operations.	(U) Coordinate and conduct explosive ordnance disposal/IED disposal operations in support of the battalion's operations.
(U) Conduct exploitation of C-IED forensic and biometric material.	(U) Exploit, to the extent possible, all IED incidents within the battalion's operational area. Coordinate proper tracking and evidence handling procedures of all collected material and ship to the appropriate lab for exploitation, taking care that all explosive safety procedures are followed.
(U) Identify and request emerging and immediate C-IED requirements.	(U) Conduct assessments of C-IED capabilities and gaps based on threat and operational environment; document and communicate those gaps through appropriate channels for rapid resolution.
(U) Intelligence, analytical and network development support to C-IED operations.	(U) Employment of required intelligence assets to determine IED threats and provide analysis on IED cells and sources that feed the targeting process.
(U) Operations, intelligence, and analysis fusion.	(U) Conduct multidiscipline intelligence analysis to build an understanding of the enemy's operations and IED system. Intelligence analysts can gain access to multiple data feeds using combined operations integration center's tools and taking advantage of reachback support.
(U) Support to C-IED targeting.	(U) Working within the joint task force headquarters' targeting methodology, participate in the targeting board to target IED

	network cells and individuals. Develop networks, nominate C-IED targets, and develop target packages.
(U) Support C-IED information operations.	(U) Understanding the human environment and supporting battalion's information operations activities for IED awareness and information to create a favorable impression or environment for multinational or host nation forces among the local populace.
(U) Deliver in-theater C-IED update/refresher training and provide information to update predeployment training.	(U) Capture and analyze current tactics, techniques, and procedures and best practices and feed that information to higher headquarters. Deliver in-theater update/refresher training based on the battalion commander's intent

Figure VI-4. (U) Battalion Counter-Improvised Explosive Device Support Element Critical Tasks

7. (U) Multinational Considerations

a. (U) In multinational operations, many of the participants do not have the trained and deployable EOD units, C-IED technologies, and exploitation capability required to protect their forces and take the fight to the enemy. When participating in a multinational operation that is facing a significant IED threat, the US CJTF may be called upon to provide our partners with a variety of C-IED support. At a minimum, this can include one or more of the following:

(1) (U) Providing EOD/WIT support to maneuver units.

(2) (U) Establishing a communications network for the rapid dissemination of IED-related TTP for force protection.

(3) (U) Assistance in organizing and providing individual and unit IED awareness training.

(4) (U) Assistance in organizing and providing specialized training for deployed engineer sapper and EOD personnel.

(5) (U) In some instances, this training and technical assistance could extend to the loan of armored vehicles and CREW equipment.

(6) (U) Upon DOD approval, sharing of C-IED network-related intelligence information derived from various surveillance platforms and other intelligence sources.

b. (U) A GCC, as a part of the theater campaign plan, can seek to facilitate the competency of HN PNs' C-IED capabilities. For a list of those tasks from phase 0 (Shape) to phase 5 (Enable Civil Authority), see Appendix E, "Counter-Improvised Explosive Device Annex Template."

8. (U) Counter-Improvised Explosive Device Task Force Counter-Improvised Explosive Device Working Group

(U) **C-IED Task Force C-IED Working Group.** When the CJTF establishes a C-IED task force, the responsibilities of the JTF J-3's C-IED working group will normally transfer to the C-IED task force. When the C-IED task force commander establishes the working

group, it will be responsible for identifying command-wide C-IED-related issues and initiatives that impact the JTF's C-IED effort. The C-IED task force working group meets on a regular basis with representatives drawn from all the major organizations in the command. It is chaired by the C-IED task force commander, who normally sets the group's working agenda. The working group shares information related to C-IED developments (updated information on adversary TTP modifications and friendly best practices) throughout the area of operations and works to resolve issues related to the JTF's conduct of the C-IED efforts, including resource allocation issues, training, and information dissemination. Issues that have a force-wide impact would be referred to the CJTF through the C-IED management board.

a. (U) **Task Force C-IED Working Group Membership.** The working group normally consists of representatives from the JTF's staff and component commands, the C-IED task force staff and specialized cells (such as the TDC) and representatives of the specialized C-IED organizations supporting the JTF, such as JIEDDO field team, science advisor, IO cell, EWCC, Joint CREW Composite Squadron–One, Army Test and Evaluation Command, Rapid Equipping Force (REF), C-IED targeting cell, and the CEXC. Special attention should be placed on including liaison officers on the task force C-IED working group . Appropriate liaison officers can provide efficient and effective dissemination of emerging adversary TTP, friendly TTP, and best practices throughout the operational area.

b. (U) **Task Force C-IED Working Group Products.** In developing their recommendations for the overall conduct of the JTF's C-IED efforts, the working group reviews the latest intelligence on the IED threat and relevant IED trend analysis; reviews and updates the current C-IED TTP and emerging best practices; and examines the current fielding and testing of the C-IED technologies. The working group's recommendations will normally be in the form of a change (or new guidance) for the JTF's C-IED efforts, and/or the basic issue that will be referred to the JTF's C-IED management board. The C-IED working group process is described in Figure VI-5.

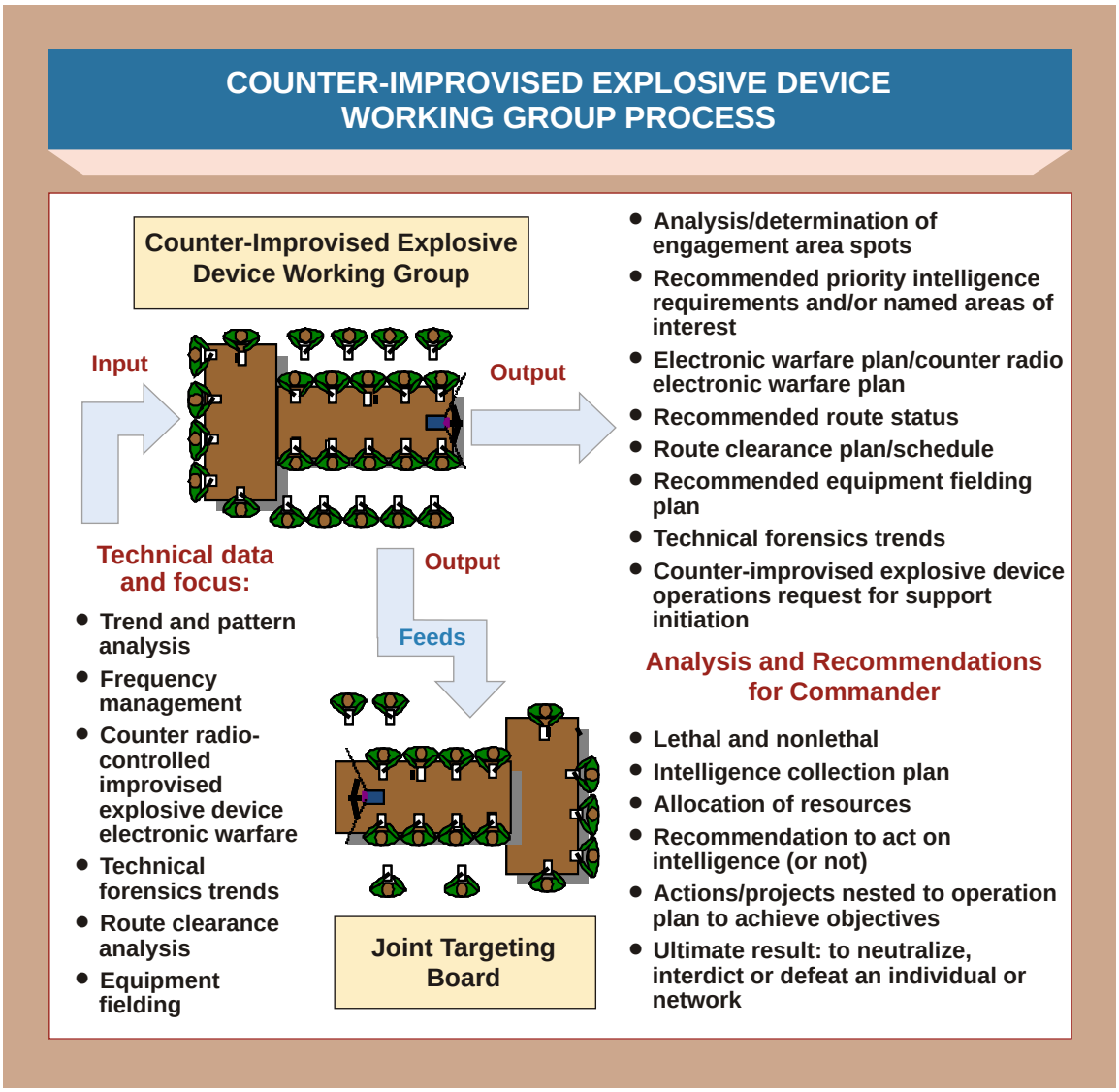


Figure VI-5. (U) Counter-Improvised Explosive Device Working Group Process

Intentionally Blank

APPENDIX A
COUNTER-IMPROVISED EXPLOSIVE DEVICE ENABLING ORGANIZATIONS (U)

1. (U) National Counter-Improvised Explosive Device Enabling Organizations

a. (U) IEDs will certainly be employed in future conflicts. The proliferation of highly detailed bomb-making technologies on numerous sites over the Internet has greatly increased the probability that these asymmetric means will be exploited by our adversaries. To counter IEDs and develop effective technological countermeasures to protect the joint force, the USG has organized a multiagency effort to actively assist DOD in the current C-IED effort and to address emerging threats. This effort assists commanders, material developers, and the strategic community in their C-IED efforts and also provides direct support to attacking insurgent and terrorist networks by conducting "supply chain defeat" analysis. While their overall efforts are complementary, each agency may pursue a different aspect of the IED challenge, but they should be synchronized and integrated. These complementary efforts include:

(1) (U) Technical exploitation of the device to identify the potential technological means of neutralizing or defeating IEDs, i.e., employment of systems similar to CREW.

(2) (U) Forensic and biometric exploitation of the device in order to identify the bomb makers for future targeting.

(3) (U) Technical exploitation of the device and/or its target (post-blast analysis) to develop improved protection systems for personnel/vehicles and develop unit-level IED avoidance TTP and mitigate the IED's effects.

b. (U) National-level agencies conduct detailed analysis and provide the results to interested parties. Much of this information supports in-theater C-IED efforts, providing timely, relevant, and predictive tactical IED intelligence on insurgent IED tactics and trends. National databases and technical IED intelligence also assist operational staffs at all command levels and specialized C-IED units in formulating C-IED TTP.

c. (U) To assist the national agencies in their C-IED efforts, a number of teams (WIT, EOD, JIEDDO, AWG) actively collect information associated with actual devices on-site. After preliminary in-theater technical analysis (CITP, CEXC), this information is forwarded to the national agencies for in-depth evaluation. The principal entities involved in this effort include the multiagency TEDAC and NGIC.

2. (U) Federal Bureau of Investigation

a. (U) **TEDAC.** The TEDAC is within the FBI to coordinate and manage a unified national effort to gather, and technically and forensically exploit, terrorist IEDs worldwide. Together with the ATF and other partner agencies, it works to thoroughly analyze all IED-related information to form actionable intelligence that can be used to assist in terrorist investigations or develop strategies and technologies to counter terrorist attacks. The

TEDAC compiles data and TECHINT and has established direct links between terrorist explosive devices leading to the capture of insurgents. It also functions as a repository and dissemination point for investigative, intelligence, bomb data, and safety information through the exploitation and cataloging of IEDs and the analysis of terrorist explosive incidents. It is responsible for overseeing and facilitating the nation's strategic-level WTI effort in support of strategic attack, targeting, and international policy development by delivering analytical products to the warfighter through CEXC and NGIC based on priorities established by the GCC. Other reports and information may be accessed by customers via the TEDAC's Explosives Reference Tool Program database.

b. (U) **Biometrics.** In an effort to support the overseas contingency operations and information-sharing initiatives, the FBI's Criminal Justice Information Services Division, in conjunction with DOD's BIMA, works to share data collected by military troops deployed internationally. The data consists of fingerprints, photographs, and biographical data of military detainees, enemy prisoners of war, or individuals of interest posing national security threats to the United States.

(U) "Examining tiny bits of bomb housings, wirings, detonation cords, fuses, switches, the chemical composition of the explosives and the electronic signatures of remote switching devices often used to detonate bombs, experts at the center have begun to compile a data bank about terror[ist] bombs. In some cases, forensic scientists have been able to obtain evidence of who made the bomb through a fingerprint or DNA [deoxyribonucleic acid] material left on an explosive part."

***New York Times*, 22 February 2004**

(1) **(U) Automated Biometric Identification System (ABIS).** DOD's ABIS consolidates, formats, and exchanges data equivalent and consistent to the FBI's current state/county/local law enforcement model. The ABIS database provides DOD with the ability to gather, store, share, and enter the information into the FBI's Integrated Automated Fingerprint Identification System, which allows the FBI to disseminate the information to other government and law enforcement agencies.

(2) **(U) Terrorist Identities Datamart Environment (TIDE).** TIDE is the USG's central repository of information (including biometric information) on international terrorist identities. TIDE supports the USG's various terrorist screening systems or "watch lists" and the US Intelligence Community's overall counterterrorism mission. The Terrorist Identities Group, located in National Counter-Terrorism Center's Information Sharing and Knowledge Development Directorate, is responsible for building and maintaining TIDE. The TIDE database includes, to the extent permitted by law, all information the USG possesses related to the identities of individuals known or appropriately suspected to be or have been involved in activities constituting, in preparation for, in aid of, or related to terrorism, with the exception of purely domestic terrorism information.

3. (U) Defense Intelligence Agency—National Ground Intelligence Center

a. (U) **DIA.** The Director, DIA, in coordination with JIEDDO, directs, monitors, and modifies the WTI process, as necessary, to include activities pertaining to the collection, analysis, and primacy for exploitation of IED components, either forensic or force protection. The Directorate for Measurement and Signature Intelligence and Technical Collection's Office of Forensic Intelligence plans, collects, processes, and exploits materiel of intelligence value to associate individuals, weapons and components, and locations and events in support of the DOD and intelligence community requirements. DIA also coordinates more advanced exploitation of specific IEDs by a number of national technical laboratories.

b. (U) **NGIC.** The NGIC fuses EOD, WIT, CEXC, and other reports of IEDs and produces analytical products to support targeting of bomb makers and networks. The NGIC maintains the CITP both in Virginia and forward locations to provide intelligence support to interrogation, targeting of bomb makers and insurgents, detainee management, biometrically enabled watch lists, and threat analysis. The NGIC also produces biometric intelligence analysis reports (BIARs). Additional WTI-related functions within NGIC focus on supporting the warfighter as well as providing solutions for force protection. NGIC provides biometrically focused analysis, tools, training, watch list management, and operational support to enable DOD and its interagency and multinational partners to deny anonymity to our nation's adversaries.

(1) (FOUO) **CITP.** The CITP is designed to collect TECHINT and conducts analysis of IED patterns, IED-related biometric matches, and IED/vehicle-borne improvised explosive device (VBIED) cell structures. CITP is closely integrated with the NGIC's biometrics effort to rapidly match individuals to specific IED incidents. These actions are accomplished by matching and assessing latent prints, fibers, and other data. CITP also supports targeting efforts by conducting personality-based network analysis and device-based network analysis. CITP analysts stationed at forward locations work with targeting cells, attend targeting meetings, and support efforts to identify IED networks by providing relevant information and analysis to targeting packages.

(2) (U) **Anti-Armor Analysis Program.** The Anti-Armor Analysis Program, also located at the NGIC, investigates and analyzes the outcome of insurgent attacks on armored vehicles worldwide. Analysis is provided to operational commanders down to battalion level, materiel and research and development program managers, and DOD leaders. The Anti-Armor Analysis Program uses WTI-derived intelligence to identify trends in the adversary's development, manufacture, and procurement of anti-armor weapons. The Anti-Armor Analysis Program makes TTP and interdiction recommendations to battlefield commanders and the Army staff to mitigate the effectiveness of the adversary's weapon systems.

(3) (U) **NGIC IED/Mines Branch.** The IED branch determines how an IED or an IED component impacts the current and future joint force operations. The IED branch analyzes the technology to understand how it functions, effectiveness of the device, frequency of use, emplacement TTP involving the device placement, how it may be used as

an advantage over current counter-technology, and how it may evolve in the future. This analysis is provided directly to the warfighter and the C-IED developers and related organizations.

4. (U) Joint Improvised Explosive Device Defeat Organization

a. (U) JIEDDO focuses all DOD actions in support of combatant commanders and CJTF efforts to defeat IEDs as weapons of strategic influence. JIEDDO develops force protection requirements and streamlines science and technology (S&T), along with prioritizing research, development, and acquisition. JIEDDO also determines the priority for exploitation of materiel at TEDAC and works with other PNs to assist in the exploitation of IEDs.

b. (U) **COIC.** JIEDDO provides direct support to the deployed warfighter through the COIC. The COIC's mission: "In support of all geographic combatant commands, the COIC harnesses, masses, and fuses information, analysis, technology, interagency collaboration, and training support to enable more precise attacks to defeat networks which employ IEDs. Be prepared to provide analytical support and enemy network information to other USG organizations and multinational partners." The COIC focuses on integrating and analyzing information from multiple intelligence databases and fusing it into products that answer a strategic, operational, and tactical commander's request for support (RFS). Within the latest time of value model, JIEDDO COIC answers RFS directly from joint and Service members in order to alleviate hours of organizational intelligence staff work. The COIC maintains a federated architecture ,which leverages the expertise from the intelligence community as well as national laboratories and academia. Products forwarded from JIEDDO COIC include, but are not limited to, comprehensive persistent views of networks employing IEDs; pattern analysis; geospatial analysis; network dynamics analysis; social network analysis; complex adaptive systems analysis; products that support JIPOE and targeting packages, all focused on defining and enabling the commander to have more lethal and nonlethal desired effects on networks that employ IEDs.

c. (U) **Joint Training Counter-Improvised Explosive Device Operations Integration Center (JTCOIC).** The JTCOIC trains units on COIC tradecraft methodologies prior to their deployment. The JTCOIC replicates JIEDDO COIC's reachback capability and processes, computer-based applications, and AtN methodologies. Training occurs primarily at home station, combat training centers, and mission readiness exercises (MRXs). The JTCOIC develops tactical scenarios to replicate real-world threats within the deploying units' operational area to create training realism and enhance understanding of reachback capabilities that JIEDDO COIC can provide upon deployment. JTCOIC analysts tie into JIEDDO COIC's software applications to obtain actual theater-specific intelligence data. They subsequently sanitize this data and prepare training products for units going through MRXs.

d. (U) **Joint Improvised Explosive Device Defeat Organization Knowledge and Information Fusion Exchange (JKnIFE).** JKnIFE acts as the DOD central repository for IED-related information. Its primary purpose is to exchange information, consolidate best

practices, and respond to RFIs related to the asymmetric application of IED-related TTP by both enemy and friendly forces.

5. (U) Department of Defense, Combating Terrorism Technical Support Office, Technical Support Working Group

(U) The technical support working group is part of the national interagency research and development program for combating terrorism requirements. Its C-IED mission is to identify, prioritize, and execute research and development projects that satisfy interagency requirements to more safely and effectively render terrorist devices safe. Particular emphasis is placed on technologies to access, diagnosis, and defeat terrorist IEDs, improvised CBRN devices, and VBIEDs.

6. (U) Service Counter-Improvised Explosive Device Enabling Organizations

a. (U) The Naval Explosive Ordnance Disposal Technology Division (NAVEODTECHDIV) develops and delivers EOD knowledge, tools, equipment, and life cycle support through an expeditionary workforce that exploits technology and information, contributes to the TECHINT process, and provides expertise which meets the needs of the DOD EOD community, combatant commanders, and interagency partners. NAVEODTECHDIV as the program of record organization for CEXC is also responsible to man, train, and equip the Technical Support Detachment's CEXC platoons in both Level I and Level II exploitation. NAVEODTECHDIV also manages the Joint Digital Information Gathering System (JDIGS), which is the standardized EOD reporting system for the joint EOD community. Data captured by JDIGS is networked to the Combined Information Data Network Exchange (CIDNE) reporting system and is used to produce WTI-related reports for analysis.

b. (U) **US Army Research, Engineering and Development Command—Intelligence and Information Warfare Division (I2WD).** I2WD performs exploitation and characterization of IED components in support of Electronic Warfare Reprogramming, as well as SIGINT systems and countermeasures development. I2WD's intelligence staff also tracks IED and asymmetric technologies worldwide, monitors and analyzes current IED events to document enemy TTP that may be relevant to detect and counter threat systems, and identifies infrastructure requirements for US test sites.

c. (FOUO) **US Army Criminal Investigations Command, Forensic Exploitation Battalion—Joint Expeditionary Forensic Facility (JEFF).** Assigned to the Army's Forensic Exploitation Battalion, the JEFF is a modular and scalable deployable forensic laboratory designed to support targeting, sourcing, prosecution, and detainment and interrogation operations. JEFFs serve as stand-alone facilities for the forensic exploitation of non-IED-related materiel, although they can also provide C-IED-related analysis if needed. JEFF capabilities include fingerprint processing, firearm (including fired bullets and cartridge cases) and tool-mark analysis, and deoxyribonucleic acid (DNA) analysis. JEFF laboratories provide direct support to CEXC by analyzing the tool marks on EFP liners to determine fabrication processes and link EFP liners discovered in caches to caches in adjacent areas.

d. (U) **20th Support Command (CBRNE)** provides C2 of full-spectrum CBRNE forces and is capable of deploying as JTF weapons of mass destruction-elimination (WMD-E) in support of joint and Army force commanders. It provides C2 to all CONUS-based EOD formations. The 20th Support Command also exercises training and readiness oversight of the Army National Guard EOD Group (111th EOD Group). The command's Joint Technical Analysis and Integration Cell (JTAIC) provides CBRNE TECHINT assessments and planning expertise in support of WMD-E to enable worldwide C-IED and WMD-E operations. JTAIC products include: providing analysis and fusion of WTI and CBRNE intelligence; providing support to targeting and RFI management; advising the J-3 on the composition and skill sets required for site exploitation teams; prioritizing the WMD master site list and producing finished TECHINT reports to support force protection, targeting, sourcing and support to prosecution.

e. (U) **REF.** The REF is an organization that takes its operational guidance from the Department of the Army assistant chiefs of staff, operations/plans/information engagement (G-3/5/7), and reports directly to the Vice Chief of Staff of the Army. It has a broad task to rapidly increase mission capability while reducing the risk to Soldiers, Marines, and others. The REF accomplishes this mission by providing the following services:

(1) (U) Equips operational commanders with off-the-shelf (government or commercial) solutions or near-term developmental items that can be developed, tested, and acquired quickly.

(2) (U) Introduces future force technology solutions that support deploying forces' requirements. Actions are accomplished by developing, testing, and evaluating key technologies and systems under specific operational conditions per requiring units CONOPS.

(3) (U) Assesses the capabilities and advises Army and other stakeholders of the findings that will enable forces to rapidly confront an adaptive enemy.

f. (U) **US Army AWG.** The AWG is a sensitive activity under the headquarters, Department of the Army G-3/5/7, that provides operational advisory assistance in support of Army and JFCs. The AWG was created by the Army to enhance the combat effectiveness of the operating force and enable the defeat of asymmetric threats to include IEDs. The AWG deploys its forces worldwide to observe, assess, and analyze information regarding the evolving operating environment and the threat. They also assist in the development, dissemination, and integration of material and nonmaterial solutions including countermeasures. The AWG serves as an agent of change providing key observations and perspectives for leaders when considering policy and resource decisions. The following capabilities summarize the units' contributions to joint force C-IED efforts:

(1) (U) Identifies and develops solutions for capability gaps that:

(a) (U) Exploit adversary vulnerabilities, and

(b) (U) Mitigate friendly vulnerabilities.

(2) (U) Provides a global presence and insight regarding emerging asymmetric threats.

(3) (U) Enhances existing Service capabilities:

(a) (U) Rapid Title 10, US Code (doctrine, organization, training, materiel, leadership and education, personnel, and facilities [DOTMLPF]) solution development through first-hand observations and internal combat/materiel development capabilities.

(b) (U) Operates in support of all types of forces—generating/operating (special operations and conventional forces).

(4) (U) Conducts simultaneous collaboration with geographic combatant commands/Army Service component commands and through the Army's REF for solution development, dissemination, and integration.

g. (U) **US Army Engineer School Counter Explosive Hazards Center (CEHC)**. The CEHC is the Army integrator for all countermeasures involving explosive hazards and serves as a center of excellence to ensure that the US Army maintains superiority in all facets of countermine and counter-explosive warfare. During contingency operations, these countermeasures may include new operational concepts and application of nonstandard materiel or off-the shelf technology into unique conditions. Countermeasures may also include development and training of theater-specific TTP against explosive threats consisting of landmines, unexploded ordnance (UXO), and IEDs. The CEHC remains in continuous contact with the field to identify equipment and training needs or capability gaps in order to immediately provide combat engineers with better mission capabilities. When a requirement is identified, the CEHC coordinates with program managers, combat developers, government laboratories, the REF, JIEDDO, and others to evaluate suitable material systems and candidates for potential integration and rapid fielding. Once a device or item is selected, the CEHC assists in the system's integration, development of its operational concept, training support package, and operational assessment. To ensure countermeasures are up-to-date and relevant, the CEHC gathers the latest intelligence on explosive hazards and adversary TTP as well as TTP employed by friendly units to counter the threat. A key task for the CEHC is training and updating the force in current counter explosive hazards techniques and employment of commercial off-the-shelf and contingency equipment. This instruction enables units to receive theater-specific training prior to deployment and allows them to focus on the mission during transition of authority. Contingency training that will be permanently retained in the Army will eventually be institutionalized and transferred to the official school training curriculum, such as operator training for route clearance vehicles.

h. (U) **United States Marine Corps Warfighting Laboratory (MCWL).** MCWL is the lead USMC agency for IED defeat. MCWL leads a USMC IED working group made up of representatives from the USMC, national-level intelligence agencies, and operating forces. The USMC IED working group rapidly identifies, evaluates, and facilitates the fielding of material and nonmaterial IED defeat solutions to the operating forces. It works in close coordination with the JIEDDO integrated product team to synchronize DOD IED defeat efforts.

i. (U) **Other Marine Corps Organizations That Support C-IED Efforts.** The following Marine Corps organizations provide primary support to the development and implementation of C-IED capabilities within the Marine Corps:

(1) (U) Deputy Commandant, Combat Development and Integration, is the Service advocate for C-IED matters and integrates C-IED operational issues across the DOTMLPF spectrum.

(2) (U) Marine Corps Center for Lessons Learned collects and archives reports of C-IED training and operations. It provides classified and unclassified archives that can be used to identify DOTMLPF trends, materiel requirements, and MAGTF C-IED best practices.

(3) (U) Marine Corps Systems Command performs acquisition and life cycle maintenance of materiel solutions in support of MAGTF C-IED operations. The command's material acquisitions may be in response to an urgent universal need statement or to more deliberate acquisition requirements.

(4) (U) Training and Education Command is responsible for development, standardization, and execution of Marine Corps training at the individual, unit, and force level. It is also responsible for coordinating cross-Service C-IED training.

(5) (U) Marine Corps Tactics and Operations Group (MCTOG) conducts training for the battalion and regimental combat team (RCT) ground combat element headquarters. As the Marine Corps experts on AtN training within the MAGTF C-IED operational environment, MCTOG trains regimental, battalion, and company battle staffs using the Spartan Resolve training exercise.

(6) (U) Marine Corps Engineer School conducts unit and individual C-IED operations (AtN, defeat the device, route reconnaissance, and clearance) training.

(7) (U) Marine Corps Intelligence Activity provides intelligence analysis to support C-IED training and operations.

7. (U) Counter-Improvised Explosive Device Enablers within the Joint Task Force

(U) A number of specialized organizations have been created to assist with the identification of and defeat of individual IEDs and the supporting infrastructure. These enablers are normally found supporting the joint force and its maneuver units and include:

a. (U) **Site exploitation teams** are specifically detailed and trained teams at the tactical level. The teams conduct search operations identifying, documenting, and preserving the cache site and its material. The team also collects material of intelligence evidence value for further analysis and exploitation, including pattern analysis, trend identification, and rule of law.

b. (U) The **DOMEX center** is responsible for the rapid and accurate extraction, exploitation, and analysis of captured enemy documents, media, and material. The NGIC

manages the Army's DOMEX program. DOMEX exploitation and analysis teams are deployed to the brigade level and work with maneuver units.

c. (FOUO) The Navy CEXC conducts investigations of significant events; exploits IEDs and recovering frequencies from RCIEDs to update EW equipment; tests explosive residue; recovers and evaluates forensic and biometric material; identifies IED trends and bomb maker signatures; creates profiles to better enable offensive operations; and conducts limited component tracking. CEXC has direct linkages to NAVEODTECHDIV (as the program of record organization for CEXC), NGIC, COIC, DIA, and TEDAC to support AtN, "defeat the device," and "train the force" LOOs.

d. (U) **EOD** units are the forces employed to render safe and exploit IEDs as well as dispose of UXO and exploit and reduce enemy weapons stores and caches in either a land based or maritime environment. The Army and Navy group headquarters provide command, control, and staff planning for two to six ordnance battalions. It provides technical direction for the EOD mission operations of subordinate units. The group also disseminates TECHINT information throughout the command and to other selected organizations. The group commander acts as the senior EOD land warfare officer for the theater army command. Army and Navy EOD groups are utilized as the core C2 element for C-IED task forces, with C2 over assigned Army, Navy, and Air Force EOD units and specialized C-IED enablers. These formations can be utilized to provide C2 for a two- to three-star-level JTF or joint EOD task force. When a C-IED task force is established, it will direct the employment of Army (and other attached) EOD assets in support of the maneuver force. (Note: The USMC's EOD assets are not normally assigned to a C-IED task force, when established, but do receive a WIT to coordinate with radio battalions, and download cell phone and computer information for local exploitation. USMC EOD units are organic to the MAGTF and provide direct support to Marine infantry battalions. As the Marines retain their assets, the joint force provides enablers in the form of C-IED teams for the headquarters, WIT, to accompany Marine EOD elements, and intelligence support of all types [as requested].)

(U) *For additional information on Service EOD capabilities, see Field Manual (FM) 4-30.16/Marine Corps Reference Publication 3-17.2C/Navy Tactics, Techniques, and Procedures 3-02.5/ Air Force Tactics, Techniques, and Procedures (Instruction) 3-2.32*, Multi-Service Tactics, Techniques, and Procedures for Explosive Ordnance Disposal in a Joint Environment.

e. (U) **EHCC.** Part of the JFC's land component engineer staff, the EHCC assists in the development of the COP and provides informational and situational understanding on explosive hazards to all MNFs, the National Mine Action Authority, and nongovernmental organizations. EHCC enables the land component commander to predict, track, distribute information on, and mitigate explosive hazards within the theater that affect force application, focused logistics, protection, and operational environment awareness. The EHCC supports C-IED efforts throughout the theater and JOA with technical advice and TTP training. The EHCC has oversight responsibility for geospatial and topographic products and manages acquisition and distribution of specialized route clearance equipment. The EHCC:

(1) (U) Provides counter-IED and explosive hazard awareness training to the force.

(2) (U) Provides technical and tactical training using mobile training teams.

(3) (U) Manages acquisition and distribution of specialized route clearance equipment.

(4) (U) Establishes, maintains, and shares the EHDB within the JOA.

(5) (U) Assists intelligence analysts and ISR planners with explosive hazards pattern analysis and intelligence collection management.

(6) (U) Supports efforts with J-7 engineers in sourcing engineer units (mine detection equipment, specialized search dogs, and new technologies).

f. (U) **Service Engineer Units.** Service engineer units perform specific combat engineer missions relating to explosive hazards, including breaching, clearing, and proofing minefields. In extreme high-operational tempo or combat missions, US Army engineers or other non-EOD units may conduct limited reduction or clearing of nonmine explosive and IED hazards, under the technical guidance of Army EOD forces. US Army engineer units involved in addressing IED explosive hazards include:

(1) (U) **US Army Clearance Company.** A clearance company conducts detection and limited IED reduction along routes and within areas of support to enable force application, focused logistics, and protection. It provides training readiness and oversight of assigned route and area clearance platoons. The company provides battle command for three to five route, area, or sapper platoons. It is capable of clearing a total of 255 kilometers of two-way routes per day (three routes of 85 kilometers each) and can clear a total of two acres per day (two areas at one acre each), depending on the enemy situation, terrain, and weather conditions. The company's route clearance platoons and teams are assigned the mission of clearing routes that have had a high incidence of IED activity.

(2) (U) **Engineer Mine Dog Detachment.** Engineer mine detection dogs are trained for the military operating environment to perform area and route clearance and search, minefield extraction, combat patrols, building search (disruptive and nondisruptive), vehicle search, and cave clearance. The dogs can reduce the time spent on a search and can detect metallic and nonmetallic mines, both buried and surface laid.

(3) (U) **Explosive ordnance clearance agent (EOCA)** personnel are Army combat engineers trained to perform limited battlefield disposal of UXO as outlined in the EOCA identification guide and supplemental list of EOCA ordnance provided by the theater EOD commander (part of the ordnance order of battle) during route reconnaissance or route clearance operations or other engineer missions. EOCA personnel are authorized to blow in place single munitions-based IEDs that are positively identifiable in the EOCA identification guide. They are NOT trained to move, combine, and/or destroy multiple UXO (such as a cache or IED incorporating more than one munition) or to perform reconnaissance or handling of IED or VBIED incidents.

(4) (U) **Terrain teams** are deployed at the brigade, division, and corps levels to provide terrain analysis and geospatial support to the field. IED defeat-related support includes route analysis, identification of choke points, assembly areas, line-of-sight analysis, and other tactical decision aids. Terrain teams can also perform geospatial pattern analysis for tracking and locating IEDs.

(5) (U) **EHT.** Assigned to the J-7 EHCC, the mission of an EHT is to provide evaluation of explosive hazard incident sites in support of brigade-size and smaller units and other similar-size joint, interagency, and multinational forces and organizations. The EOD company and EHT coordinate and synchronize explosive hazard information and capability throughout the COP and AOR. The EHT's capabilities include:

(a) (U) Conducting site evaluation of explosive hazard incident sites, and

(b) (U) Conducting TTP training (explosive hazards awareness training, AN/PSS-14, and area clearance) for BCT and RCT and joint, interagency, and multinational personnel on explosive hazard mitigation in a JOA.

g. (U) **Electronic Warfare Officer (EWO).** The EWO is the commander's subject matter expert on CREW. The EWO coordinates spectrum management with the division and brigade's communications officer to deconflict electronic attack, manages and oversees the employment of CREW systems, conducts EW training, and monitors exploitation results for changes in the enemy's use of the spectrum to ensure that load sets are valid.

h. (U) **Marine Corps engineer units** possess personnel that are trained to identify and destroy (blow in place) certain explosive obstacles based upon mission requirements and the supported commander's approval/authorization.

8. (U) Weapons Intelligence Teams

a. (U) WITs consists of four- to five-person elements (Figure A-1). WITs gather data to exploit IED-related intelligence, recreate the scene of attacks to understand adversary TTP, and contribute input to unit after-action reviews and friendly force TTP development. The WIT provides IED intelligence collection capability to support BCT, RCT, and corps intelligence analysis of IEDs and the adversary's IED operations. WIT-derived intelligence also forms the basis for potential targeting of bomb makers and bomb-making networks within the AOR. WIT capabilities include the ability to provide IED reports directly into the theater and national intelligence fusion cells via CIDNE; the ability to conduct complementary IED investigations with EOD, to include assisting in TECHINT collection, cataloging, reporting and evacuation of IED to theater (e.g., CEXC) and national lab (e.g., TEDAC) for exploitation; and the provision of weapons intelligence training for the soldiers in the maneuver units.

b. (U) There are a variety of ways to configure and assign WITs. Organic to the C-IED task force's weapons intelligence flight, individual WITs are normally found at the brigade level responding to IED events. They can be assigned in direct support to the EOD companies that are in direct support to the maneuver BCTs or as part of a brigade C-IED team (consisting of a C-IED training element, a WIT element, a CITP element, and a CREW

Figure A-1. (U) Weapons Intelligence Team

field service representative). In the C-IED team configuration, the WITs usually consist of a CEXC element, an EOD element, and the tactical exploitation team.

APPENDIX B
COUNTER-IMPROVISED EXPLOSIVE DEVICE EXPLOITATION PROCESS (U)

1. (U) Levels of Exploitation and Enablers

(U) The WTI process (Figure B-1) is divided into five distinct levels of exploitation and analysis. Each level focuses on the technical and forensic activities able to be conducted and required outputs, time and location of exploitation, and the user, not on the value of the information. The levels of exploitation are divided due to the category of information that can be gleaned, along with the level of expertise and equipment required to conduct the exploitation and analysis. The information garnered from each level is valuable for analysis from tactical through national levels and is required to provide a complete picture.

2. (U) Level 1—Tactical Exploitation

a. (U) The first level of exploitation (Figure B-2) involves the identification, collection, preservation, transportation, and examination of physical material and contextual information from an event or site involving WTI materiel of interest. It is designed to support the immediate needs of the tactical commanders at the BCT or RCT level and below for information on IED employment in their immediate operational area. This level of exploitation begins at the site of a raid, cache, IED incident site, or post-blast site. Tactical-level exploitation could also involve the initial detainment of individuals suspected of being involved in insurgent activities. Many tactical responses involve site exploitation teams conducting operations to search, locate, identify, and record items of interest. EOD teams will be dispatched to the site to conduct analysis and perform render safe operations. Render safe procedures allow WIT to recover material of WTI interest from the IED incident. EOD teams may have to collect this materiel if WIT is unavailable to attend. WIT personnel produce a technical report (covering “blast in” and “blast out”) in order to gain a full understanding of the event or scene, conduct an initial technical assessment of the device or weapon, provide the tactical commander with relevant and timely information, and evacuate the material to higher-level exploitation forces.

b. (U) The first technical assessment is conducted by an EOD team and results in the complete identification of the IED and its components. The first technical assessment determines the type of IED, the method of employment, intended outcome, type of switch, type and size of explosives, and identification of additional enhancements, to include CBRN material. This assessment produces the following information:

(1) (U) Provides indicators and warnings of the enemy’s introduction of a new or more capable weapon system or munition in the operational area (e.g., batteries and cooling units found in a cache points to man portable air defense missiles in the possession of the enemy).

(2) (U) Provides first reporting of new enemy TTP and devices.

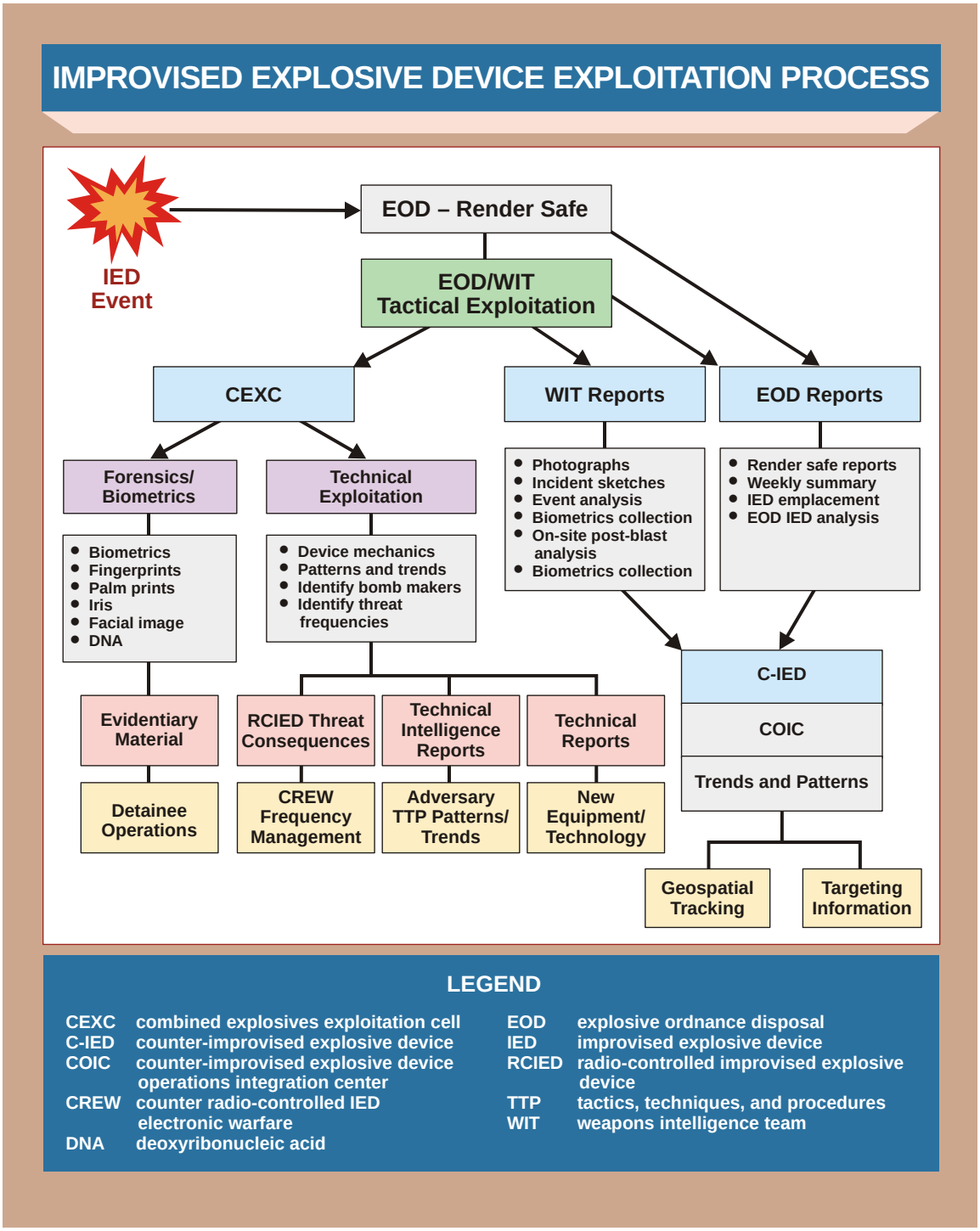


Figure B-1. (U//FOUO) Improvised Explosive Device Exploitation Process

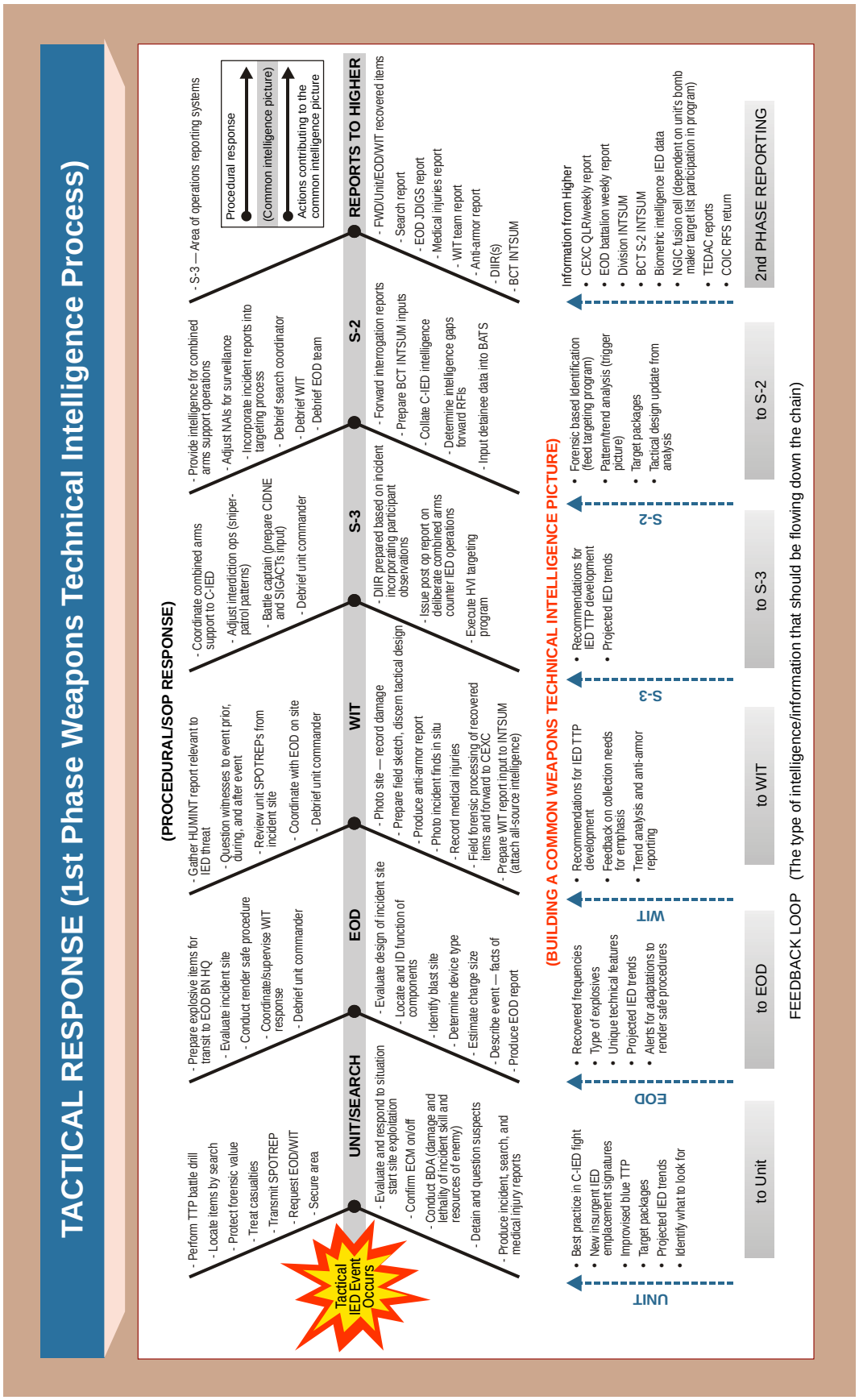


Figure B-2. (U//FOUO) Tactical Response (1st Phase Weapons Technical Intelligence Process)

TACTICAL RESPONSE (1st Phase Weapons Technical Intelligence Process)

LEGEND

BATS	Biometric Automated Tracking System
BCT	brigade combat team
BDA	battle damage assessment
BN	battalion
CEXC	combined explosives exploitation cell
CIDNE	Combined Information Data Network Exchange
C-IED	counter-improvised explosive device
COIC	counter-improvised explosive device operations integration cell
DIIR	draft intelligence information report
ECM	electronic countermeasures
EOD	explosive ordnance disposal
FWD	forward
HQ	headquarters
HUMINT	human intelligence
HVI	high-value individual
ID	identify
IED	improvised explosive device
INTSUM	intelligence summary
JDIGS	Joint Digital Information Gathering System
NAI	named area of interest
NGIC	National Ground Intelligence Center
OPS	operations
QLR	quick look report
RFI	request for information
RFS	request for support
S-2	battalion or brigade intelligence staff officer
S-3	battalion or brigade operations staff officer
SIGACT	significant activity
SOP	standard operating procedure
SPOTREP	spot report
TEDAC	Terrorist Explosive Device Analytical Center
TTP	tactics, techniques, and procedures
WIT	weapons intelligence team

Figure B-2. (U//FOUO) Tactical Response (1st Phase Weapons Technical Intelligence Process) (cont.)

(3) (U) Educates other EOD technicians throughout theater of new or improved render safe procedures.

(4) (U) Provides the technical EOD report required for WIT, the company intelligence support team and the battalion or brigade intelligence staff officer (S-2) to perform pattern and predictive analysis, link diagrams, time-event charts.

(5) (U) Provides critical information to improve TQ.

(6) (U) Enables in-theater C-IED training lanes to be updated quickly to educate the next patrol.

(7) (U) Provides new TTP for home station and RSOI training.

c. (U) WITs are small TECHINT collection teams focused on TECHINT support to the full spectrum of operations and dispatched according to the commanders' intelligence collection requirements. The teams are colocated with an EOD team, given the mutually supporting roles. If necessary, an EOD team can perform the functions of a WIT. While a WIT can also deploy independently, EOD support will still be required by a supported unit. The WIT fully exploits a site of intelligence value by conducting IED-related TQ; collecting forensic materiel, to include latent fingerprints and palm prints; preserving and documenting documents and electronic media, including cell phones and Global Positioning System devices; taking photographs of the scene; preparing material for evacuation; providing in-depth documentation of the scene, including sketches and photographs; and evaluating the effects of threat weapon systems. After examination of the scene and materiel collection, the analytical process takes place to establish, among other things, what happened, what the insurgent/terrorist intended, who the target was, and who is responsible.

d. (U) In addition to EOD teams and WITs, a number of specialized enablers facilitate the processing and interpretation of information of relevance to immediate operations:

(1) (U) The EWO is the commander's CREW SME. The EWO is responsible for coordinating spectrum management with the unit-level communications staff officer to deconflict electronic attack, assist in electronic protection, manage and oversee employment of CREW systems, coordinate the integration of CREW assets, monitor intelligence and ensure load sets of targeted frequencies are valid, and conduct EW training. The EWO is an integral part of the organizational and C-IED working group staffs.

(2) (U) CRTs are specially trained and equipped to conduct deliberate site exploitation operations to support WMD-E operations. CRTs are equipped with state-of-the-art technology and incorporate the latest TTP to identify, neutralize, eliminate, and dispose of chemical and biological agents, hazards, and munitions. CRTs provide theater-level support to the JFC and have limited-capability EOD assets assigned, in order to support CBRNE incidents. CRTs are not a one-for-one substitute for EOD and cannot be utilized in lieu of EOD when JFC requires full-spectrum EOD capability in support of C-IED operations. CRTs are also trained in the hazards and exploitation of clandestine laboratories.

(3) (U) Case managers provide dedicated biometric support to tactical and operational commanders. Case managers are deployed forward and function as a direct liaison, facilitating BEI and ensuring that BEI is integrated into the unit's targeting process. They advise the S-2/component intelligence staff officer on specific IED bomb makers operating in the unit operational area and provide linkages through WTI and biometrics to interrogation activities.

3. (U) Level 2—Operational Exploitation

a. (U) The second level of WTI exploitation (Figure B-3) involves the nondestructive technical and forensic examination as well as analysis of materiel and data. Operational-level WTI exploitation organizations focus their efforts on providing immediate feedback and outputs to the brigade, division, and corps, as well as theater commanders and staff. Level 2 exploitation involves providing laboratory specialties at more forward locations to provide expert level feedback and results to the battlefield commander. Operational-level exploitation is conducted by theater exploitation elements and provides confirmatory analysis of reporting and the first technical assessment, as well as relevant information pertinent to the immediate threat or the identification of individuals responsible for the final construction and emplacement. Additionally, this level of analysis includes combining EOD and WIT reporting with all-source analysis to further enable targeting, force protection (through alerting, informing and training), sourcing, and prosecution. Operational-level forces focus exploitation efforts to produce timely and relevant forensic and technical design information to support the commanders' intelligence requirements. Operational activities require more sophisticated equipment and specialized skills than tactical-level activities but are typically conducted in theater to offset the time required to perform a thorough exploitation at the strategic level. The operational-level activities also serve to select (triage) and prepare materials for strategic-level exploitation and analysis.

b. (U) Outcomes associated with operational exploitation focus on a higher level of evaluation and analysis than can be provided at the tactical level. The outcomes are provided in the form of reports intended to support the theater commander's intelligence requirements. Emphasis is placed on enabling offensive operations to identify, track, and target individuals involved in IED activities and threat networks. The following is a list of additional outcomes associated with Level 2 technical exploitation:

(1) (U) Provide information to enhance BEI for targeting packages.

(2) (U) Provide confirmatory analysis of the tactical characterization and technical categorization.

(3) (U) Identify IED trends.

(4) (FOUO) Identify IED makers and their links in threat networks.

(5) (FOUO) Develop bomb maker profiles and identify signatures to enable pattern analysis and targeting.

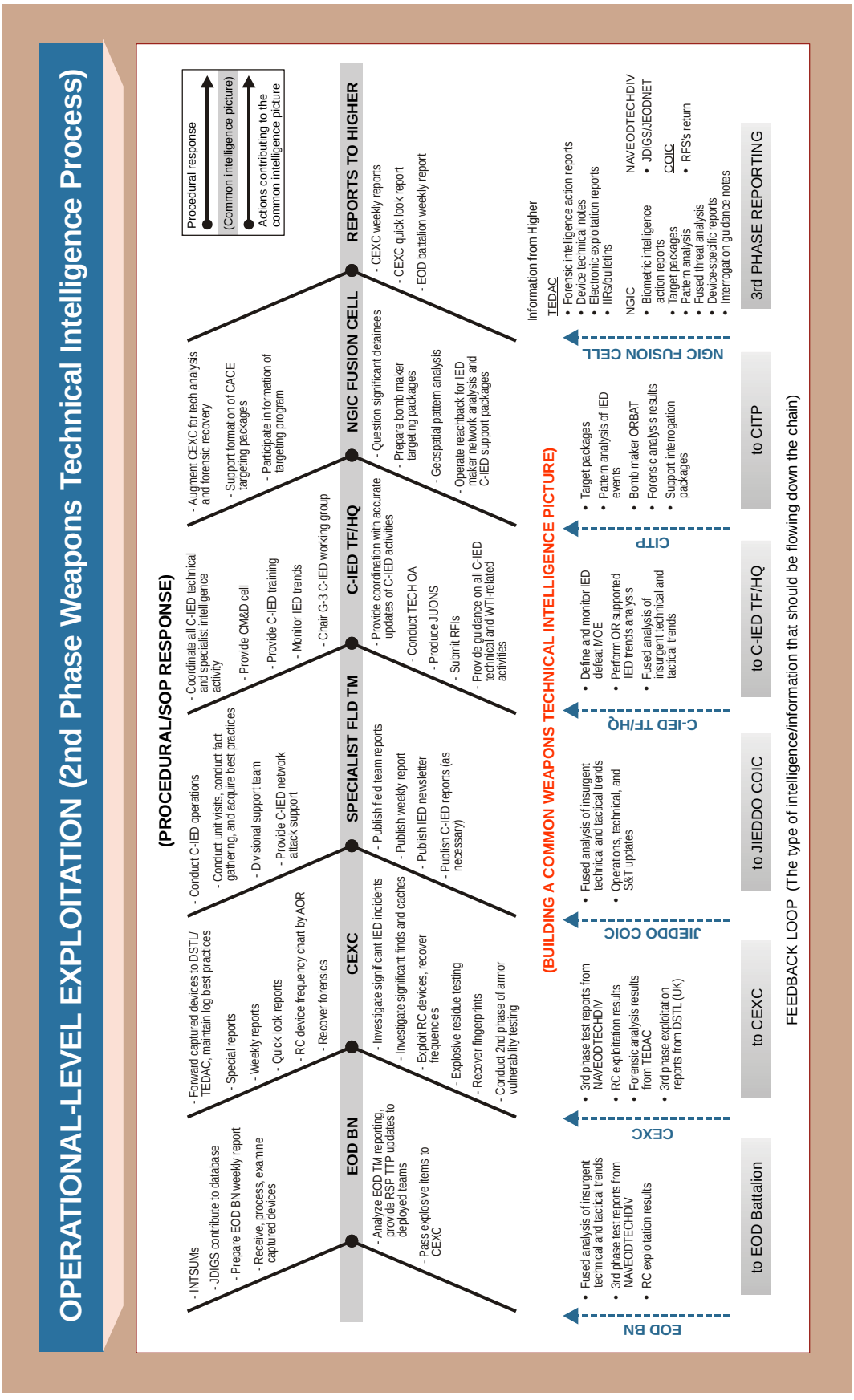


Figure B-3. (U//FOUO) Operational-Level Exploitation (2nd Phase Weapons Technical Intelligence Process)

OPERATIONAL-LEVEL EXPLOITATION (2nd Phase Weapons Technical Intelligence Process)

LEGEND

AOR	area of responsibility	JUONS	joint urgent needs statement
BN	battalion	MOE	measure of effectiveness
C-IED	counter-improvised explosive device	NAVEOD-TECHDIV	Naval Explosive Ordnance Disposal Technology Division
CACE	corps analysis and control element	NGIC	National Ground Intelligence Center
CEXC	combined explosives exploitation cell	OA	operational analysis
CITP	counter-improvised explosive device targeting program	OR	operational research
CM&D	collection management and dissemination	ORBAT	order of battle
COIC	counter-improvised explosive device operations integration cell	RC	radio controlled
		RFI	request for information
DSTL	Defense Science and Technology Laboratory	RFS	request for support
EOD	explosive ordnance disposal	RSP	render safe procedure
FLD	field	S&T	science and technology
G-3	component operations staff officer	SOP	standard operating procedure
HQ	headquarters	TECH	technical
IED	improvised explosive device	TEDAC	Terrorist Explosive Device Analytical Center
INTSUM	intelligence summary	TF	task force
IIR	intelligence information report	TM	team
JDIGS	Joint Digital Information Gathering System	TTP	tactics, techniques, and procedures
JEODNET	Joint Explosive Ordnance Disposal Network	UK	United Kingdom
JIEDDO	Joint Improvised Explosive Device Defeat Organization	WTI	weapons technical intelligence

Figure B-3. (U//FOUO) Operational-Level Exploitation (2nd Phase Weapons Technical Intelligence Process) (cont.)

(6) (U) Update radio-controlled frequency table to enhance EW.

(7) (U) Identify new threat technology or new use of technology.

c. (U) A number of specialized enablers facilitate the processing and interpretation of information of relevance to operational commanders:

(1) (U) The 20th Support Command (CBRNE) integrates, coordinates, deploys, and provides trained and ready specialized C-IED, CBRNE forces. It provides C2 of full-spectrum CBRNE forces and is capable of deploying as JTF WMD-E in support of joint and Army force commanders. The 20th Support Command (CBRNE) can provide a JTF's C-IED task force with a C2 element, staff augmentation, and EOD assets. The unit's CBRNE Analytical and Remediation Activity can also provide deployable laboratories to support CBRNE-related WTI.

(2) (U) The C-IED task force is an operational headquarters providing C2 for all specialized C-IED and CBRNE forces to neutralize the IED/CBRNE threat. The task force coordinates and conducts WTI collection and exploitation to assist the targeting process to defeat IED networks, provides training and recommends material solutions to protect the force, and assists HN security forces in building sustainable security capabilities. The C-IED task force also:

(a) (U) Provides WTI and foreign ordnance collection management and dissemination.

(b) (U) Monitors IED trends, both emerging and migrating.

(c) (U) Produces joint urgent operational needs statements and support to in-theater assessment of new materiel solutions.

(d) (U) Provides guidance on all C-IED technical WTI-related activities.

(e) (U) Trains in-theater forces on C-IED TTP.

(f) (U) Provides a focal point for reachback for WTI and foreign ordnance exploitation.

(g) (U) Provides a focal point for and support to other C-IED initiatives and programs.

(3) (U) The foreign ordnance exploitation cell is a small cell assigned to the C-IED task force and is designed to track and analyze the discovery, collection, transportation, and exploitation of foreign ordnance and weapon systems on the battlefield. The cell is composed of EOD and intelligence professionals from the Services and DIA linked to the intelligence community for reachback assistance and analysis. The cell provides management of captured foreign ordnance in order to facilitate its exploitation by numerous intelligence agencies and organizations.

(4) (U) CEXC. For information on CEXC, see paragraph 6b(1) in Chapter VI, "Counter-Improvised Explosive Device Task Force," and paragraph 7c in Appendix A, "Counter-Improvised Explosive Device Enabling Organizations."

(5) (U) The US Army's forensic expeditionary battalion's JEFF is a deployable forensic laboratory designed to support targeting, sourcing, prosecution, and detainment and interrogation operations. The typical forensic laboratory capabilities include latent print processing, firearm and tool mark analysis, and DNA analysis. While the JEFF laboratories have a primary mission to conduct forensic analysis in support of criminal activity, they provide direct support to CEXC by analyzing the tool marks on EFP liners to determine fabrication processes and link EFP liners discovered in caches to caches in adjacent areas.

4. (U) Level 3—Strategic Exploitation

a. (U) The third level of exploitation (Figure B-4) involves the scientific examination and analysis of materiel as well as data from an event or site involving WTI material. The primary function of Level 3 is to identify associations between events, people, IEDs, improvised weapons, and associated WTI-related materiel. Level 3 exploitation provides direct support to attacking insurgent and terrorist networks by conducting "supply chain defeat" analysis. This level of exploitation utilizes the full spectrum of techniques and equipment, as well as all-source analysis, to fully understand the nature of the threat by providing in-depth technical and forensic analysis. Strategic-level organizations focus efforts to provide precise WTI exploitation and analysis for commanders, the materiel developer, and national policymakers. Support involves providing intelligence to tactical and operational forces. Materiel developer support involves assisting with the development of countermeasures to enhance force protection measures and provide materiel solutions. National policymakers use strategic-level WTI in support of strategic attack, targeting, and international policy. Strategic-level WTI is a CONUS-based activity, supported by allied nations, and currently overseen and facilitated by the FBI TEDAC. The elements of strategic-level WTI, primarily applicable to ground warfare support, are overseen by the NGIC and JIEDDO.

b. (U) Strategic exploitation results in:

(1) (U) Forensic intelligence analysis reports, providing detailed electronic diagrams of IED circuits and interpretation of such.

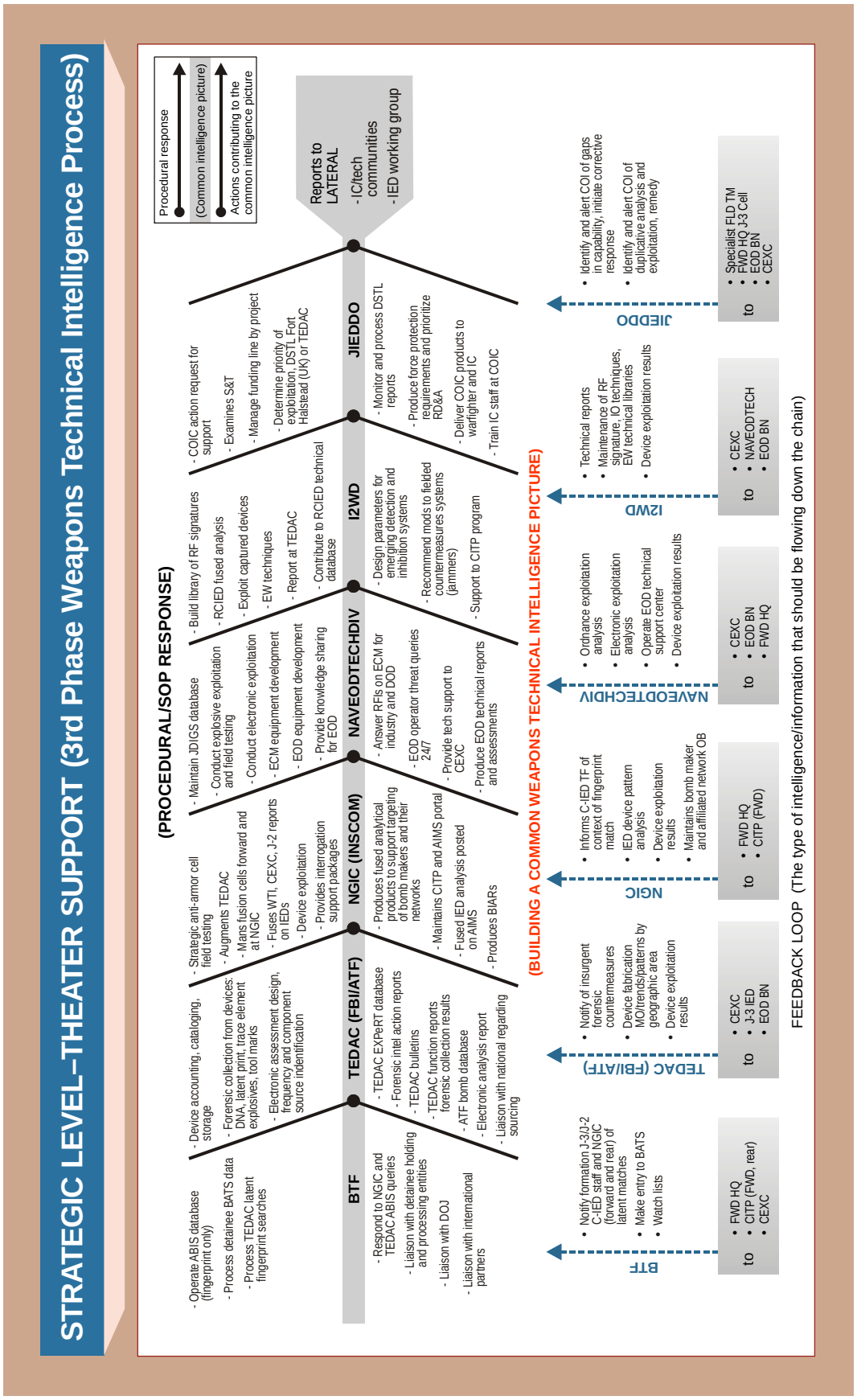


Figure B-4. (U//FOUO) Strategic Level–Theater Support (3rd Phase Weapons Technical Intelligence Process)

STRATEGIC LEVEL–THEATER SUPPORT (3rd Phase Weapons Technical Intelligence Process)

LEGEND

ABIS	Automated Biometric Identification System
AIMS	Automated Identification Management Support System
ATF	Bureau of Alcohol, Tobacco, Firearms and Explosives
BATS	Biometric Automated Tracking System
BIAR	biometric intelligence analysis report
BN	battalion
BTF	biometrics task force
C-IED	counter-improvised explosive device
CEXC	combined explosives exploitation cell
CITP	counter-improvised explosive device targeting program
COI	community of interest
COIC	counter-improvised explosive device operations integration cell
DNA	deoxyribonucleic acid
DOD	Department of Defense
DOJ	Department of Justice
DSTL	Defense Science and Technology Laboratory
EXPeRT	Explosives Reference Tool Program (FBI)
ECM	electronic countermeasures
EOD	explosive ordnance disposal
EW	electronic warfare
FBI	Federal Bureau of Investigation
FLD	field
FWD	forward
HQ	headquarters
I2WD	Intelligence and Information Warfare Division
IC	intelligence community
IED	improvised explosive device
INSCOM	US Army Intelligence and Security Command
IO	information operations
J-2	intelligence directorate of a joint staff
J-3	operations directorate of a joint staff
JDIGS	Joint Digital Information Gathering System
JIEDDO	Joint Improvised Explosive Device Defeat Organization
MO	method of operation
NAVEOD-TECHDIV	Naval Explosive Ordnance Disposal Technology Division
NGIC	National Ground Intelligence Center
OB	order of battle
RCIED	radio-controlled improvised explosive device
RD&A	research, development, and acquisition
RF	radio frequency
RFI	request for information
S&T	science and technology
SOP	standard operating procedure
TECH	technical/technology
TEDAC	Terrorist Explosive Device Analytical Center
TF	task force
TM	team
UK	United Kingdom
WTI	weapons technical intelligence

Figure B-4. (U//FOUO) Strategic Level–Theater Support) 3rd Phase Weapons Technical Intelligence Process) (cont)

(2) (U) Analysis of US TTP and recommendations to mitigate the effects of specific weapons of concern.

(3) (U) Analysis and reports to support interrogation of detainees.

(4) (U) Biometric intelligence analysis to support targeting packages.

(5) (U) Device association through forensic links in support of IED network attack.

(6) (U) Component sourcing activities using non-DOD authorities.

(7) (U) Support to material solutions through JIEDDO, academia, and the industrial base.

c. (U) Appendix A, "Counter-Improvised Explosive Device Enabling Organizations," provides a detailed discussion of the strategic organizations that enable the C-IED exploitation process.

5. (U) National Exploitation

(U) The fourth level of technical exploitation involves the sponsorship of national laboratories to conduct exploitation on specific items across a range of scientific skills. This level of exploitation results in the provision of in-depth reporting, which is linked to other national facilities.

6. (U) Special Activities

(U) The fifth level of technical exploitation is conducted by special activities to support unique collection and investigative activities of national importance. This level includes the collection, analysis, and research of both government departments and agencies and private research firms.

7. (U) Allied Nations

(U) Allied nations provide invaluable assistance and partnerships in the collection and exploitation of WTI materiel. Allied nation support is embedded in every level of the WTI process, providing valuable capabilities, experience, and expertise. The US has developed agreements with other nations to assist with exploitation efforts designed to enhance the technical assessment of IED components. Other nations are also developing similar exploitation capabilities and enablers that provide tactical and operational assistance to US forces.

Intentionally Blank

APPENDIX C
WEAPONS TECHNICAL INTELLIGENCE (U)

1. (U) General

(U) WTI is the result of a paradigm shift from traditional TECHINT activities in order to respond to the threats of COIN and irregular warfare (IW). WTI is a category of intelligence derived from the technical and forensic collection and exploitation of IEDs, associated components, improvised weapons, and other weapon systems. Traditional TECHINT focuses solely on determining the source of a weapon as well as the force protection capabilities to prevent technological surprise on the battlefield. The TECHINT process involves collecting foreign material and providing TECHINT to support the S&T community. WTI goes beyond TECHINT to incorporate the necessary technical, forensic, and biometric disciplines to support force protection, feed targeting information to facilitate attacking the network, enable component sourcing, and support prosecution at all levels of operations. WTI provides US forces and MNFs a multilevel (tactical, operational, and strategic), systematic process to collect information and material from sites, exploit it, and produce analytical outputs that mitigate the threat and get at the crux of the problem—the enemy network.

2. (U) Weapons Technical Intelligence and the Range of Military Operations

a. (U) **Major Operations.** Traditional TECHINT is normally associated with large-scale combat operations involving collecting and exploiting conventional weapons and associated systems. However, the TECHINT process isn't time-sensitive and cannot support a rapid flow of information across all levels of operations. WTI supports large-scale combat operations with the technical and forensic exploitation required to suppress unconventional warfare activities, which normally accompanies large-scale combat operations. WTI provides a process to quickly understand the enemy's capabilities and take advantage of his vulnerabilities and deny the enemy the opportunity to shape battlefield conditions by resorting to improvised weapons. The WTI process shows great utility during large-scale combat operations involving a nation state with a WMD program. The technical exploitation component of WTI will generate intelligence on the manufacturing, synthesis processes, and engineering capability of WMD programs. Nuclear forensics will produce linkages to other sources of materiel, while biological and chemical laboratory analysis of samples will provide information regarding the lethality of agents. The collection and processing of biometric intelligence from research and development facilities will enable the targeting of lead scientists and engineers involved with WMD programs.

b. (U) **IW and COIN.** In IW, the enemy is likely to use improvised weapons and IEDs to inflict casualties, create fear in the local population, and ultimately assist in destabilizing the legitimate government. WTI supports the commander's ability to exploit enemy vulnerabilities to gain or maintain the initiative by characterizing the tactical design of improvised weapons and understand their emplacement, employment, and intended outcome. This is made possible by the tactical and technical exploitation provided through the WTI process.

c. (U) **Peace Operations.** Improvised weapons and terrorism are threats associated with peace operations. WTI conducted during peace operations provides outcomes similar to those of COIN operations. The WTI process feeds information into intelligence cells conducting network analysis and enhance the common intelligence picture for military advisors. Military WTI enablers can conduct collection and analysis in order to feed HN defense and law enforcement agencies. This relationship should be designed to eliminate information gaps and enhance targeting in order for police to apprehend and prosecute criminals involved with insurgent operations and terrorism.

3. (U) Weapons Technical Intelligence Exploitation Process and Functions

a. (U) The WTI process involves a systematic approach to conduct exploitation of WTI material. Exploitation is based on the commander's priorities for information and not based on the sequential order the material is received. The WTI process may be altered or adjusted based on the tactical situation, type of mission, and the required outputs. Key to its overall success, the WTI process is a combined joint, interdepartmental, and interagency process. The results of the WTI process affect the design of force protection initiatives, the production of actionable intelligence for targeting of networks, the identification of IED sourcing, and support for prosecution of bomb makers and others associated with the production and emplacement of IEDs.

b. (U//FOUO) The WTI exploitation functions are the technical and scientific methods and procedures applied systematically to solve a problem. The functions are a blend of traditional TECHINT functions coupled with forensic examination to fully understand a weapon, how it was employed, who employed it, and how to mitigate the effects. Technical exploitation is taking full advantage of the information garnered from examining and analyzing the design, material, and suitability of mechanical and electronic components of IEDs and improvised weapons. This examination involves the operability and relationship of components in comparison with others and how the item functions to produce a resulting action. Forensic exploitation is the application of multidisciplinary scientific processes to establish facts involving the use of physical science to link people with locations and events. (See Appendix B, "Counter-Improvised Explosive Device Exploitation Process," for a detailed examination of the actual WTI exploitation process.)

c. (U) **Technical exploitation** includes:

(1) (U) **Electronic.** Electronic exploitation of WTI material centers on how IED switches, both arming and firing, function, whether in relation to mechanical components such as washing machine timers or other electrical components such as dual tone multifrequency integrated circuit boards. Electronic exploitation also provides a description of how the device functions, potential sources for the IED's components, the arming and firing sequence and codes, the frequency the device operates at for RCIEDs, and a record of functioning times for electronic events.

(2) (U) **Mechanical.** Mechanical exploitation of WTI material focuses on devices incorporating manual operations, the combination of mechanical/physical parts that transmits forces, motion, and energy. An example of a mechanical IED switch requiring exploitation

is a washing machine timer. These timers have physical parts that move several contacts together to complete a circuit. Mechanical exploitation involves the exploitation of the mechanical functioning of improvised weapons and their associated launch platforms.

(3) (FOUO) **Explosive.** Initial identification and analysis of explosives is conducted by EOD for use at the tactical level while confirmatory analysis is performed by CEXC and other laboratories in theater. The goal is to identify the main charge and precursor elements and evaluate the detonating cord. CEXC also has the capability to conduct trace analysis of explosive residue recovered from a post-blast investigation. Explosive analysis utilizing laboratory equipment can provide an analysis of explosive materials, and in some cases, the lab can source the explosive back to the country or region of manufacture. In the case of homemade explosives, produced from locally obtained base materials, this analysis can provide information regarding the types of equipment Service members should look for when conducting raids and site exploitation as well as identifying the source of the precursors used in manufacturing.

(4) (U) **CBRN.** The collection, identification, characterization, and analysis of CBRN material is conducted at the tactical and operational levels by EOD, CBRN response teams, and DIA laboratories operating in theater. Field laboratories at the operational level provide scientific data regarding the use of chemical warfare agents and toxic industrial material enhancements used in IEDs.

(U) *For further guidance on CBRN hazards, their effects, and operational considerations, refer to JP 3-11,* Operations in Chemical, Biological, Radiological, and Nuclear (CBRN) Environments.

d. (U) **Forensic exploitation** includes:

(1) (FOUO) **Photography.** Photography is one of the first steps in the forensic exploitation process. Detailed photographs are important for examiners and analysts to identify profiling data and signatures, establish links to other devices seen in the operational area, and identify manufacture information that could lead to identifying possible supply routes.

(2) (FOUO) **Biometric.** Biometric exploitation is defined as taking full advantage of the measurable physical characteristics or personal behavioral traits used to recognize the identity or verify the claimed identity of an individual. Biometric modalities range from fingerprints, DNA, and iris identification to face or palm prints. Key to identifying insurgents living among the population is the use of biometric exploitation fused with other intelligence such as SIGINT and HUMINT. The fusion of biometric intelligence with other forms of intelligence facilitates targeting individuals and groups associated with insurgent and criminal activity. Biometrics modalities include:

(a) (FOUO) **Latent Fingerprints.** Latent fingerprints are collected in theater by WIT and CEXC as well as by TEDAC. Fingerprints and palm prints are the most common and successful means to verify individuals who may be involved in IED activity. The analysis of latent fingerprints can be completed within hours and the results

disseminated in the form of a BIAR. The BIAR is posted by NGIC's Automated Identification Management Support System portal on the SECRET Internet Protocol Router Network (SIPRNET) and pushed to tactical units via e-mail. BIARs aid the development of target support packages, interrogation support packages, and warrant support packages.

(b) (FOUO) **DNA.** Mitochondrial deoxyribonucleic acid (mtDNA) is extracted from hairs found on WTI materials, while nuclear DNA analysis is possible on samples of bodily fluids taken from materials, with nuclear analysis being the more precise. The DNA profile is then compared against other catalogued profiles previously collected from post-blast sites, caches, the internal and external areas of IED components, bomb makers, detainees, and suicide bombers. JEFF labs are capable of performing nuclear analysis, while TEDAC is capable of mtDNA analysis.

(3) (FOUO) **Trace Analysis.** Trace evidence includes hairs and fibers discovered at a site or caught in a device or in tape adhesive. Since these fibers are normally removed from the internal area of the device or weapon, they were likely left by the bomb maker or someone involved with the construction of the weapon. Hair is removed and processed for mtDNA analysis, while fibers are analyzed visually under a microscope, compared to existing samples, and retained for future comparison. Trace analysis supports pattern analysis to determine the number of fabricators involved. This form of analysis is primarily Level 3 exploitation and analytical activity.

(4) (FOUO) **Tool Marks.** Tool mark analysis involves studying characteristics created on WTI-related items during the manufacturing process, such as marks left by machinery, for the purpose of identifying the machinery and tools used to manufacture the device. The JEFF and TEDAC are capable of analyzing tool marks and conducting comparative analysis for manufacturing marks on EFPs by microscopically examining milling and strike marks. Tool marks can often determine whether a device was fabricated locally or by a foreign supplier, how many steps were required in the manufacturing process, and the type of machinery involved in making the IED.

4. (U) The Outcomes of the Weapons Technical Intelligence Process

(U) WTI analysis supports a wide variety of activities from the commander's decision-making cycle to the design of improved individual protection equipment. The benefits of the WTI process are illustrated in Figure C-1.

Figure C-1. (U) Weapons Technical Intelligence Outcomes

Intentionally Blank

APPENDIX D
WEAPONS TECHNICAL INTELLIGENCE CONSTRUCT OF IMPROVISED EXPLOSIVE DEVICES (U)

1. (U) Levels of Exploitation and Enablers

a. (U) The WTI construct of IEDs is intended to provide a coherent conceptual framework and an operational vocabulary to address the IED threat worldwide, encompassing the broad spectrum of IED employment scenarios, the variety of IEDs, and their critical components. The basic construct is illustrated in Figure D-1.

b. (U) The WTI construct of IEDs is designed to:

(1) (U) Standardize IED reporting and improve database content management.

(2) (U) Enable IED-related education and training.

(3) (U) Support development of WTI IED policy and doctrine.

2. (U) General Terms

a. (U) **As Intended.** An IED that has detonated against the intended target.

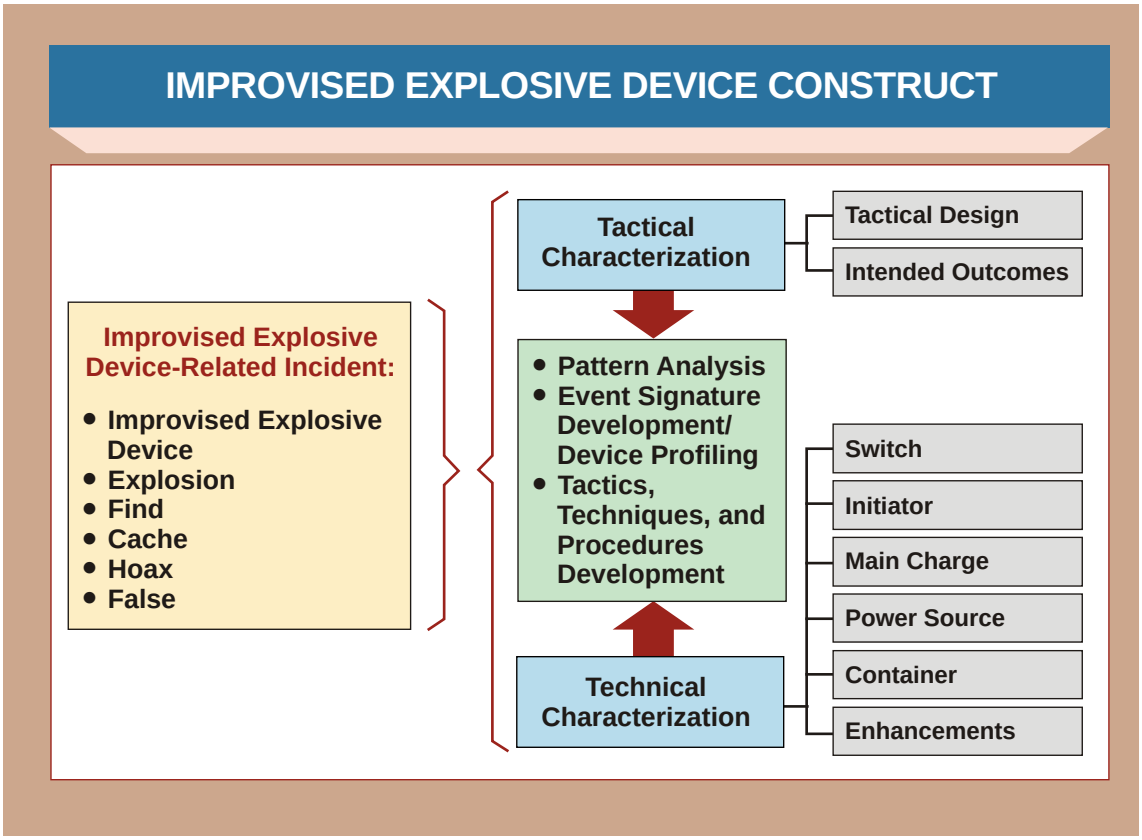


Figure D-1. (U) Improvised Explosive Device Construct

b. (U) **Associated Components.** Components that are part of an IED or improvised weapon system, the tools required to produce the components, or precursors to the manufacture of IED components to include explosives.

c. (U) **Blown in Place.** Actions taken at the discretion of the tactical commander to clear an IED by detonating it where discovered.

d. (U) **Cache.** An IED incident that involves the discovery and/or recovery of unarmed devices, IED components, and IED paraphernalia, or explosive ordnance that involves long-term storage in a permanent, fixed location.

e. (U) **Event Signature Development and Device Profiling.** The process of analyzing the tactical and technical identifiers of an IED incident to support force protection, targeting, prosecution, and sourcing.

f. (U) **Explosion.** Occurs when gaseous products are rapidly produced from a single substance (high explosives or low explosives with a fuel and oxidant).

g. (U) **Explosive Train.** A train of combustible and explosive elements arranged in order of decreasing sensitivity. Its function is to accomplish the controlled augmentation of a small impulse into one of suitable energy to cause the main charge to function.

h. (U) **False.** An incident incorrectly identified though reported in good faith as an IED that is subsequently categorized as a false alarm after positive EOD action.

i. (U) **Find.** An IED incident that involves the discovery or turning in of devices or IED components in a temporary and/or transitory location.

j. (U) **Force Protection.** Preventive measures taken to mitigate hostile actions against DOD personnel (to include family members), resources, facilities, and critical information.

k. (U) **Found and Cleared.** An IED incident that involves an armed and emplaced IED that has been discovered and rendered safe by EOD personnel or has been discovered and blown in place.

l. (U) **Hoax.** An IED incident that involves a device fabricated to look like an IED and is intended to purposely simulate one in order to elicit a response.

m. (U) **IED.** A device placed or fabricated in a creative manner incorporating destructive, lethal, noxious, pyrotechnic, or incendiary chemicals and designed to destroy, incapacitate, harass, deny mobility, gather intelligence, or distract. It may incorporate military stores, but is normally devised from nonmilitary components. Refers to a complete functioning device.

n. (U) **IED-Related Incident.** An event that involves one or more of the following types of IED-related actions/activities: IED, explosion, find, cache, false, hoax.

o. (U) **Improvised Weapons.** A nonexplosive device placed in an improvised manner designed to destroy, incapacitate, harass, or distract. It may incorporate military stores, but is normally devised from nonmilitary parts.

p. (U) **Other Weapons Systems.** Military weapons associated with a terrorist or insurgent group's method of operations that involve IEDs or improvised weapons.

q. (U) **Pattern Analysis.** Using prior actions and activities to identify trends in activities or behaviors. Once identified, these patterns can be used to predict future enemy actions and plan ISR activities.

r. (U) **Premature Detonation.** An IED that has denoted unintentionally during the emplacement or construction of the device. Does not refer to an IED incident involving an ineffective detonation against an intended target due to inaccurate timing or placement.

s. (U) **Prosecution.** The process of associating IED-related people, places, devices, or equipment to an individual for evidentiary purposes in a recognized court of law.

t. (U) **Render Safe Procedure.** The portion of the EOD procedures involving the application of special EOD methods and tools to provide for the interruption of functions or separation of essential components of UXO to prevent an unacceptable detonation.

u. (U) **Sourcing.** The process of determining the origination point (such as a production facility or person, a geographic location, or a specific country of origin) for IED components.

v. (U) **Tactical Characterization.** A characterization of how an IED incident was conducted or planned to be conducted (the tactical design) and/or how an IED incident was used or intended to be used (the intended outcome).

w. (U) **TTP Development.** Using the lessons learned from an IED attack to refine and improve the tools and methods used during all missions in which an IED may occur (e.g., convoys, tactical suppression efforts, ISR, C-IED missions). The authority to change or modify friendly C-IED TTP within an operation should be vested in a single authority that will also be responsible for disseminating the approved changes.

x. (U) **Technical Categorization.** A description of an IED using a hierarchical construct to identify its key components. The components identified in this categorization are the elements from which technical and forensic information is recovered and exploited.

y. (U) **Weapons Technical Intelligence.** A category of intelligence and process derived from the forensic and technical collection and exploitation of IEDs, associated components, improvised weapons, and other weapon systems.

3. (U) Tactical Characterization—Tactical Design

a. (U) **Tactical Design.** The specific design of an IED attack, including but not limited to, position of the IED, type of IED, method of actuation, intended target, type of road

segment used, concealment technique, use of secondary devices, and time of day. Tactical design addresses the questions of why here, why now, and why in this way. Terms used to describe a specific type of device or component of a device (e.g., VBIED) are often used to describe all or part of the tactical design. See Figure D-2.

b. (U) **Airborne.** An IED held aloft by aerodynamic means or buoyancy that serves as concealment means for explosives with an initiating device. Also known as ABIED.

c. (U) **Attack Geography.** A description of the geography surrounding the IED incident, such as road segment, buildings, foliage, etc. Understanding the geography indicates enemy use of landscape to channel tactical response, slow friendly movement, and prevent pursuit of enemy forces.

d. (U) **Blast Crater Characteristics.** Observations and measurements of the blast crater, to include depth, diameter, debris field size, and surface description (soil, sand, concrete, etc).

e. (U) **Elevated.** IED emplaced above the surface: hanging from an overpass, on a roof, etc.

f. (U) **Estimated Size of Main Charge.** A reference to the estimated weight of the main charge derived from observation of the blast effects and crater characteristics.

g. (U) **Incident Atmospherics.** A description of the demeanor of the civilian population at an IED event, to include mood, absence or presence, changes in previously experienced interactions, etc.

h. (U) **Incident Environmental Conditions.** A description of the ambient surrounding conditions, to include weather conditions, such as temperature, precipitation, fog, dust, etc.

i. (U) **Large VBIED.** An IED built into any large ground-based vehicle (e.g., dump truck, panel truck, bongo truck, commercial bus, tanker) that serves as the concealment means for explosives with an initiating device.

j. (U) **Low-Metal Content IED.** An IED designed with few or no metallic parts.

k. (U) **Magnetic Attachment.** A type of IED employment in which the device is attached to the target with magnets.

l. (U) **Method of Device Emplacement.** A description of how the device was delivered to the target.

m. (U//FOUO) **Nonmagnetic Attachment.** A type of IED employment in which the device is attached to the target using nonmagnetic means.

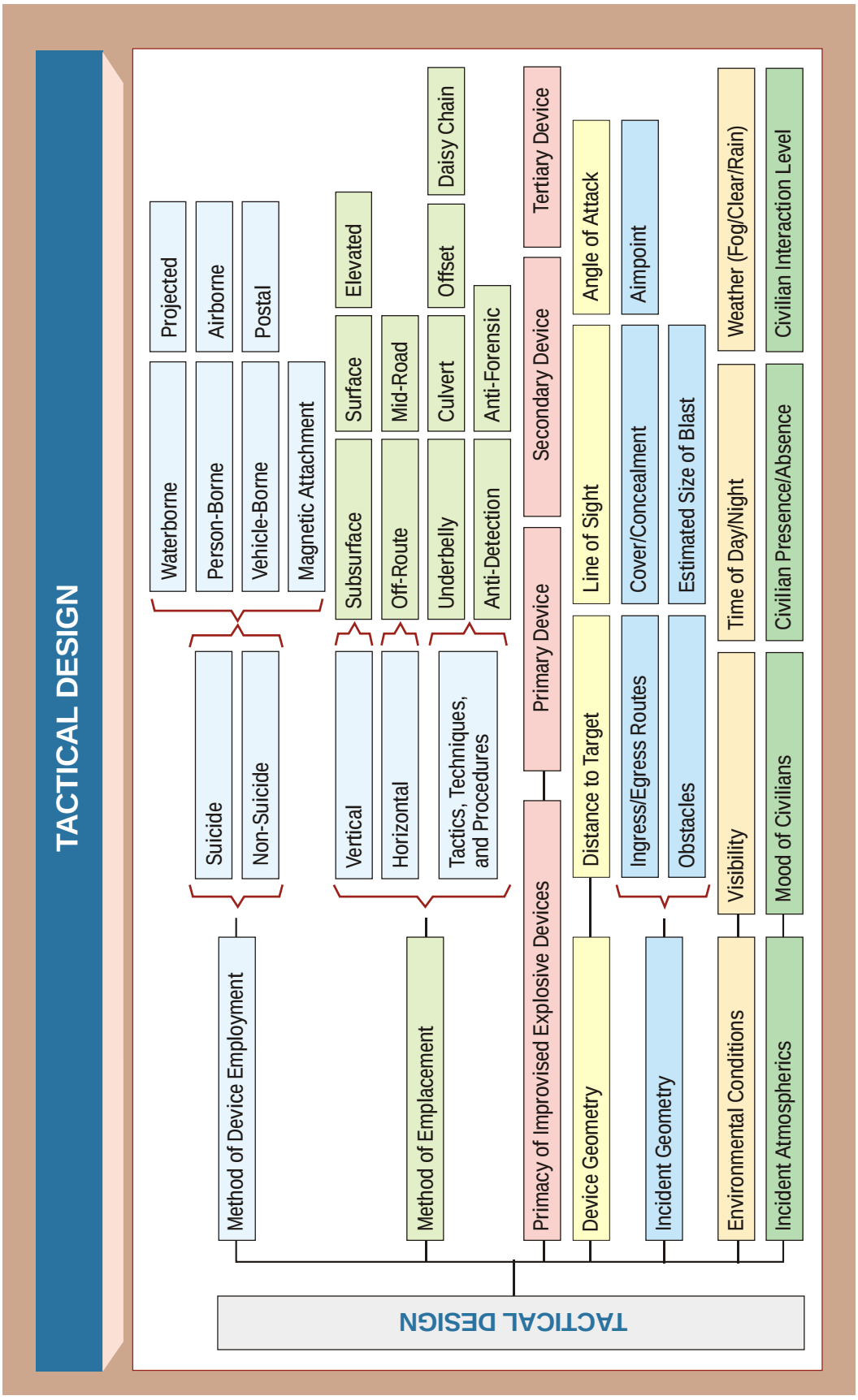


Figure D-2. (U) Tactical Design

n. (U) **Non-Suicide.** An IED in which the insurgent/terrorist does not intentionally kill himself or herself as part of an attack.

o. (U) **Overhead.** IED emplaced above the intended target (e.g., hanging from an overpass, on a roof, etc.).

p. (U) **Person-Borne Improvised Explosive Device (PBIED).** An IED worn by a person either willing or unwillingly, such as a vest, belt, backpack, etc., in which the person houses the whole IED or principal IED components and/or serves as the delivery or concealment means for explosives with an initiating device. It is often initiated by the person wearing the IED (suicide). However, not all PBIEDs are triggered by the person wearing the IED (proxy).

q. (U) **Postal.** An IED introduced or delivered through a postal system.

r. (U) **Primary Device.** An IED emplaced to attack an initial target.

s. (U) **Projected.** An improvised weapons system that delivers the main charge through the air to its target.

t. (U) **Secondary Device.** An additional device emplaced in the target area to attack individuals or vehicles after the initial event. This device would normally be placed in an obvious or pre-employed incident control point or first responder/EOD team location.

u. (U) **Surface.** IED emplaced directly on the ground.

v. (U) **Subsurface.** IED emplaced under the surface or below the intended target (e.g., buried, in a culvert, underwater).

w. (U) **Suicide.** An IED initiated by an insurgent or terrorist at a time of his or her choosing in which the operator intentionally kills himself or herself as part of the attack or to deny his or her capture.

x. (U) **Tertiary Device.** An additional IED emplaced in the target area to attack individuals or vehicles after the initial and secondary attacks.

y. (U) **Underbelly.** A type of IED employment in which the device targets the underside of a vehicle, using large amounts of explosives buried to deliberately defeat armor (can include conventional land mines).

z. (U) **Under Vehicle IED.** An IED that is placed on the underside of a vehicle (using string, tape, magnet, etc. as a form of attachment). Also known as a UVIED.

aa. (U) **VBIED.** An IED delivered by any small ground-based vehicle (e.g., passenger vehicle, motorcycle, moped, bicycle); the vehicle serves as the concealment means for explosives with an initiating device. It will also become the main source of fragmentation.

bb. (U) **WBIED.** An IED delivered by floating, drifting, anchored, or propelled on or below the water.

4. (U) Tactical Characterization—Intended Outcomes (Figure D-3)

(U) Longer-term strategic and immediate or direct tactical intentions of the IED incident include the making of political statements at the strategic level and/or more immediate objectives such as disruption of normal activities, anti-material, antipersonnel, criminal, TTP identification, experimentation, and obstacle creation at the tactical level. IEDs can have multiple intended outcomes.

a. (U) **Antiaircraft.** An IED primarily intended to damage or destroy aircraft and/or their payload as well as to kill or wound individuals inside the aircraft.

b. (U) **Anti-Armor.** An IED primarily intended to penetrate armored vehicles and/or to kill or wound individuals inside armored vehicles.

c. (U) **Anti-EOD.** An IED primarily intended to kill or wound EOD personnel, or to impede render safe procedures.

d. (U) **Anti-First Responder.** An IED primarily intended to kill or wound first responders, such medics, firefighters, etc.

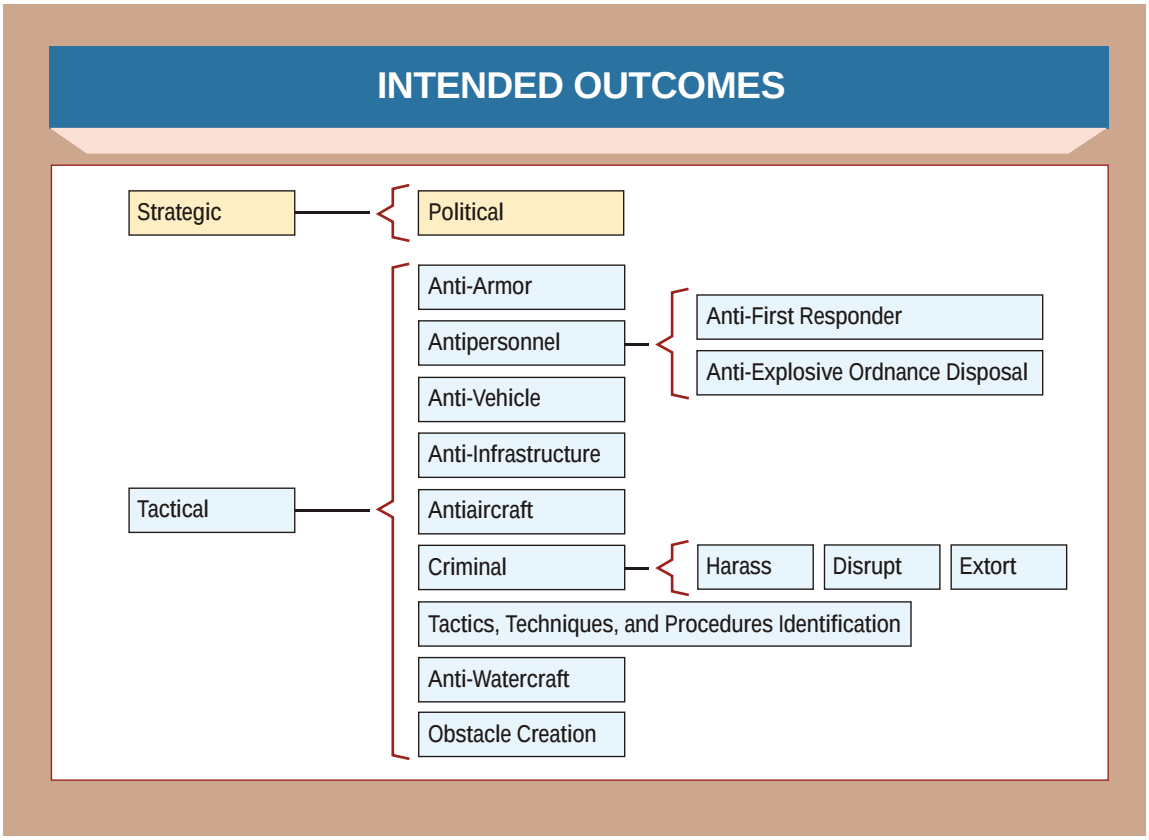


Figure D-3. (U) Intended Outcomes

e. (U) **Anti-Infrastructure.** An IED primarily intended to damage or destroy physical infrastructure such as pipelines, communications towers, bridges, buildings, utility lines, and/or facilities such as electrical transformers or water pump houses.

f. (U) **Antipersonnel.** An IED primarily intended to kill or wound people.

g. (U) **Anti-Vehicle.** An IED primarily intended to damage or destroy vehicles, excluding armored vehicles and/or their cargo, as well as to kill or wound individuals inside such vehicles.

h. (U) **Anti-Watercraft.** An IED primarily intended to damage or destroy watercraft and/or their payload, as well as to kill or wound individuals inside the watercraft.

i. (U) **Criminal.** An IED primarily intended to harass, disrupt, or extort as part of criminal activity.

j. (U) **Experimental.** An IED primarily intended to increase the effectiveness of a subsequent device with respect to its intended outcome.

k. (U) **Obstacle Creation.** An IED primarily intended to create an obstacle to impede movement or channel movement into a desired location, possibly as part of a complex attack or ambush.

l. (U) **Political.** An IED primarily intended to make a political statement in addition to the more immediate tactical outcome.

m. (U) **TTP Identification.** An IED primarily intended to cause a reaction by forces in an effort to learn and understand employed tactics. This knowledge is then used by the attacker to plan new attacks incorporating the lessons learned to inflict additional casualties or to avoid countermeasures. The IED need not function to serve this purpose. A hoax IED can have TTP identification as its intended outcome.

5. (U) Technical Categorization—Switches (Figures D-4 and D-5)

(U) A device for making, breaking, or changing a connection in an IED is a switch. A single switch can have multiple functions (e.g., safe-to-arm and firing). IEDs are classified by their firing switches.

a. (U) **Active Infrared Sensor Switch.** A sensor that emits an infrared beam to a receiver forming an invisible link that, when broken, acts as a trigger to initiate the IED. These sensors act like an electronic version of the trip wire.

b. (U) **Anti-Tamper Switch.** A victim-operated switch designed to initiate an IED when it is tampered with or disturbed in a particular manner. Sometimes referred to as an anti-handling or anti-disturbance switch

c. (U) **Chemical Switch.** A timing switch using the reaction of chemical compounds as a switch to provide a delay before starting the initiation train.

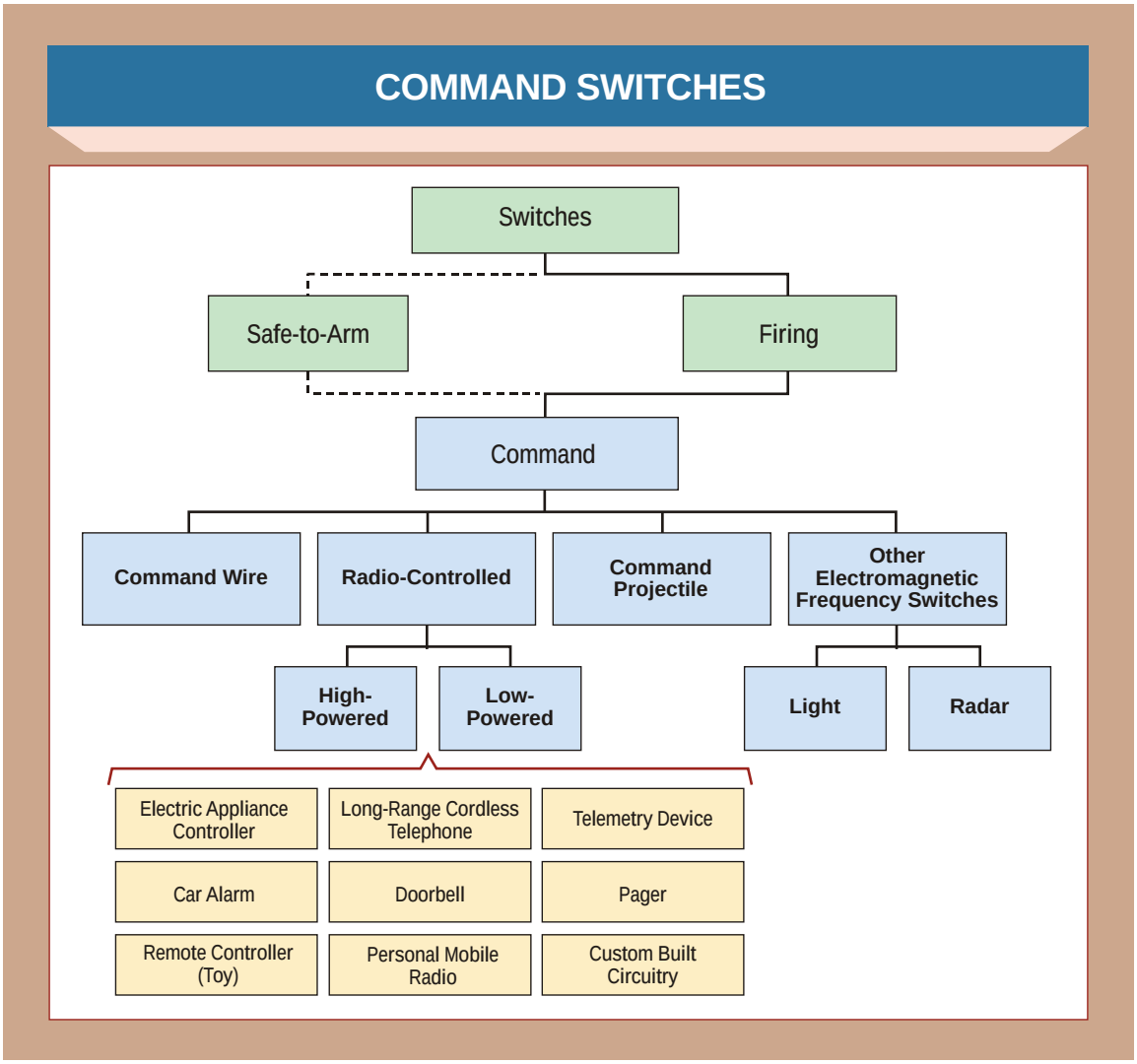


Figure D-4. (U) Command Switches

d. (U) **Command Switch.** A type of switch that is activated by the attacker in which the attacker controls the device.

e. (U) **Command Projectile Switch.** The use of a small arms bullet to close the circuit by penetrating two metal plates. This provides standoff between firing point and contact point.

f. (U) **Command Wire Switch.** An IED where the firing point and contact point are separate but joined together by a length of wire.

g. (U) **Electronic Time Switch.** A timing switch using a commercial or improvised electronic timer or integrated circuit to start the initiation train.

h. (U) **Firing Switch.** Component that initiates the firing train.

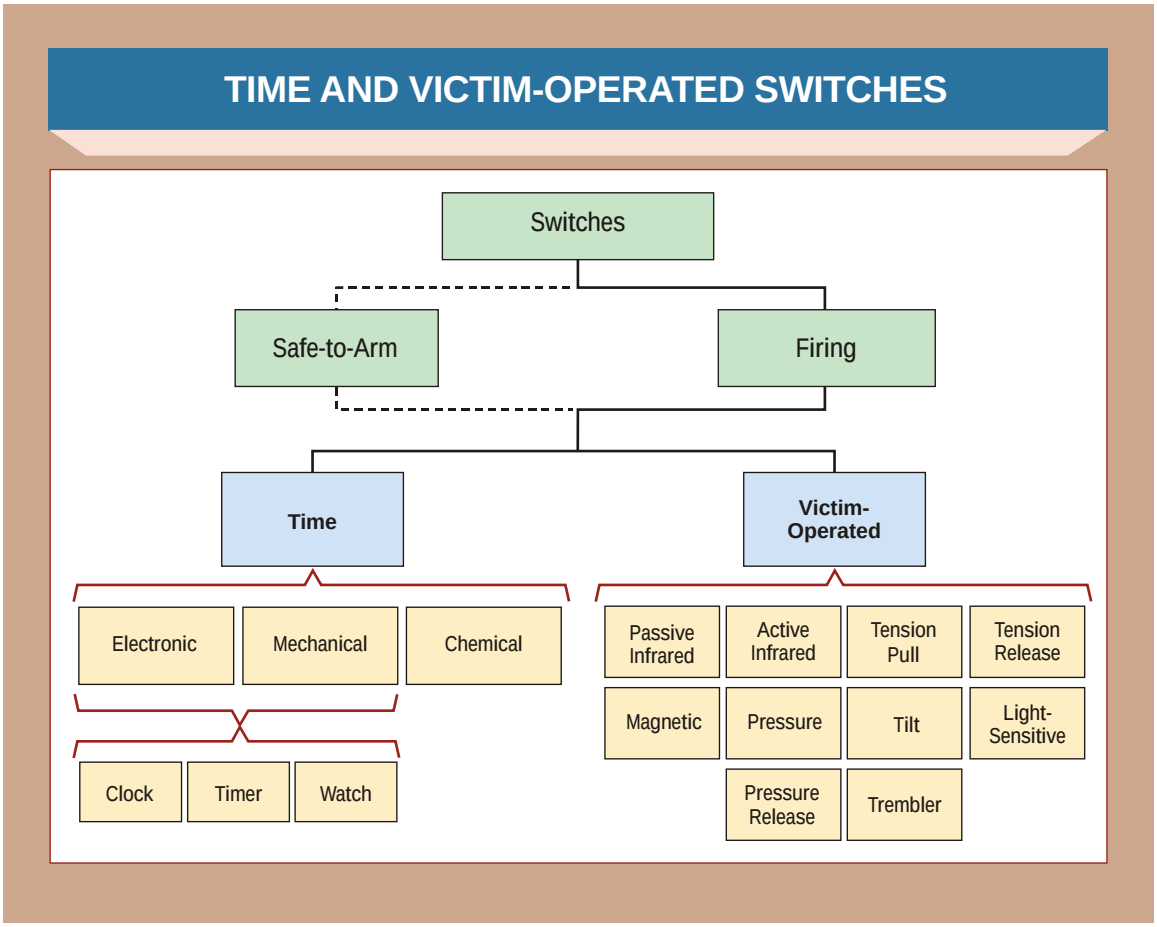


Figure D-5. (U) Time and Victim-Operated Switches

i. (U) **High-Power Transmitter.** An RCIED transmitter with an output power greater than or equal to 0.35 watt.

j. (U) **Light-Sensitive Switch.** A type of proximity trigger that senses changes in the amount of light in the environment near the sensor. When this happens, the sensor causes a circuit to be completed, firing the device.

k. (U) **Low-Power Transmitter.** An RCIED transmitter with an output power less than 0.35 watt.

l. (U) **Magnetic Switch.** A type of proximity trigger that senses magnetic alterations in the area around the sensor. When this happens, the sensor causes a circuit to be completed, firing the device.

m. (U) **Mechanical Time Switch.** A timing switch (e.g., clock, timer, drip timer) constructed or modified so that physical contact between two parts of the timing device complete an electrical circuit, initiating the device.

n. (U) **Other Electromagnetic Frequency (Non-Radio Frequency) Switches.** Electromagnetically operated command switches that do not operate in the radio frequency band.

o. (U) **Passive Infrared Sensor Switch.** A sensor that detects movement of a heat source. When the change in ambient temperature is detected, the sensor acts as a trigger to initiate the IED.

p. (U) **Pull Switch.** An IED initiated by a person using a "command pull" action.

q. (U) **Pressure Switch.** A method for activating a device that occurs when an object is used to complete a circuit when pressure is applied in a predetermined direction. Many pressure initiated IEDs explode when pressure plates are compressed under the weight of passing vehicles or foot soldiers.

r. (U) **Pressure Release Switch.** A method for activating a device that occurs as a result of reductions in pressure. Such devices may employ mechanical, pneumatic, or hydraulic systems to signal a detonator that a vehicle or individual has released pressure to a pressure plate or similar mechanism. Pressure release triggers are often used in the design of military booby traps or victim-operated IEDs.

s. (U) **RCIED.** An IED initiated electronically in a wireless method consisting of a transmitter and receiver (e.g., personal mobile radio, cell phone, cordless phone, pager).

t. (U) **Safe-to-Arm Switch.** A device used to arm the IED to ensure that the emplacer can safely employ or emplace the IED.

u. (U) **Target Selection Switch.** A victim-operated switch used to select a particular target based on its particular characteristics such as weight, place in a convoy, etc.

v. (U) **Tension/Pull Switch.** A victim-operated device that triggers an explosion when tension is applied to a firing mechanism—such as pulling a trip wire. The tension causes an action that releases a firing pin or activates an electrical or electronic switch.

w. (U) **Tension Release Switch.** A victim-operated trigger that, when tension is released, such as when a taut wire or cord is cut or broken, releases a spring-loaded firing pin or closes electrical contacts, initiating the device.

x. (U) **Tilt Switch.** A device that allows voltage to flow to the output wires after a conductive material (e.g., mercury or a ball bearing) is moved enough (up/down, left/right) to flow onto the switch contacts, completing the circuit.

y. (U) **Time Switch.** A type of switch that functions after a set time. Used widely against infrastructure targets.

z. (U) **Trembler Switch.** A device that allows current to flow to output wires after movement causes two metal parts to make contact, completing the circuit.

aa. (U) **Victim-Operated Switch.** A type of switch that is activated by the actions of an unsuspecting individual. These devices rely on the target for the device carrying out some form of action that will cause the device to function. Can include target selection switches or anti-tamper switches.

6. (U) Technical Categorization—Initiators

(U) Any component that may be used to start a detonation or deflagration is an initiator; it may or may not be a detonator.

a. (U) **Blasting Cap/Plain Detonator.** A device containing a sensitive explosive intended to produce a detonation wave. Can be either electric or nonelectric (plain).

b. (U) **Electric Initiator.** An initiator for which functioning is initiated by an electrical impulse that creates heat or a spark.

c. (U) **Exploding Bridge Wire.** An initiator or system in which a very high-energy electrical impulse is passed through a bridge wire, literally exploding the bridge wire and releasing thermal and shock energy capable of initiating a relatively insensitive explosive in contact with the bridge wire.

d. (U) **Heat Initiator.** A type of initiator that serves as an igniting element through the application of heat. This may include direct heat to a sensitive explosive.

e. (U) **Light/Flash Bulb Initiator.** Devices used as electric initiators that incorporate an improvised use of the bulb to initiate primary or low explosives.

f. (U) **Nonelectric Initiator.** An initiator for which functioning is initiated by nonelectric means.

g. (U) **Percussion Initiator.** An initiator that serves as an igniting element when mechanically struck.

h. (U) **Shock Tube.** A thin, plastic tube of extruded polymer with a layer of high explosive deposited on its interior surface that propagates a detonation wave to the blasting cap.

i. (U) **Squib/Igniter.** A device used to initiate low explosives or high explosives when used in an appropriate firing train. In general, any chemical, electrical, or mechanical device used to ignite a combustible material.

j. (U) **Time Fuse/Safety Fuse.** A pyrotechnic contained in a flexible and weatherproof sheath burning at a timed and constant rate; used to transmit a flame to the detonator or a low explosive charge with a predetermined delay.

7. (U) Technical Categorization—Main Charge

(U) The explosive charge that is provided to accomplish the end result in a munition is the main charge. Note: Examples for end results are bursting a casing to provide blast and fragmentation, splitting a canister to dispense submunitions, or producing other effects for which it may be designed.

a. (U) **Blasting Accessory.** Devices and materials used in blasting, such as, but not limited to, cap crimpers, tamping bags, blasting machines, blasting galvanometers, and detonation cord.

b. (U) **Bulk Explosives.** Manufactured explosive charges in their original packaging or that have been removed from weapons or munitions.

c. (U) **Commercial Explosives.** Explosives produced and used for commercial, industrial, or recreational applications.

d. (U) **Directional Effect.** Type of main charge configuration in which the explosive effect is channeled to an intended area.

e. (U) **EFP.** Specially designed main charge configuration incorporating an explosive charge with a machined or pressed concave metal plate which by the force of the charge reshapes the plate into a high-temperature, high-velocity metal slug capable of penetrating armored vehicles.

f. (U) **High Explosives.** Materials that detonate; they do not require confinement as they react chemically to produce heat, gas, a rapid expansion of matter, and a shock wave in the explosion.

g. (U) **Improvised Claymore.** An improvised weapon, military or homemade, designed to explosively propel a fan shaped pattern of ball bearings or other fragmentation in an aimed direction.

h. (U) **Improvised Explosives.** Nonstandard explosive mixtures/compounds that have been formulated/synthesized from available ingredients. Most often utilized in the absence of commercial/military explosives. Also referred to as homemade explosives.

i. (U) **Improvised Grenade.** An improvised weapon, military or homemade, designed to explode when a restraint is removed (usually handheld, but can be projected).

j. (U) **Improvised Mortar.** An improvised weapon, military or homemade, designed to launch an explosive charge to the target.

k. (U) **Improvised Rocket.** An improvised weapon, military or homemade, designed to propel an explosive charge to the target.

l. (U) **Incendiary.** Chemical mixtures that are intended and designed to cause fires.

m. (U) **Low Explosives.** Combustible materials that are characterized by deflagration. They do not produce a shock wave, generally requiring confinement to explode.

n. (U) **Main Charge Configuration.** The arrangement or design of the main charge and other materials (usually metal) to create an effective weapon to attack personnel, vehicles, or structures.

o. (U) **Military Explosives.** Explosives manufactured for military use.

p. (U) **Munitions.** Ammunition, ordnance, or demolition charges containing explosives, propellants, pyrotechnics, initiating composition, or nuclear, biological, or chemical material for use in military operations.

q. (U) **Omni-Directional Effect.** An aspect of main charge configuration in which the explosion is omni-directional and expands in all directions; includes improvised rockets, mortars, and grenades.

r. (U) **Platter Charge.** The use of an explosive to propel a metal plate toward a target in a manner in which the plate remains intact.

s. (U) **Propellant.** An energetic explosive that produces high volumes of gas when ignited. Propellant product gasses are utilized in work suitable for affecting the controlled propulsion of a solid body, such as a projectile or rocket. Propellants are classified as low explosives.

t. (U) **Shaped Charge.** A main charge configuration incorporating a metal liner shaped so as to concentrate its explosive force in a particular direction in order to cut or penetrate (e.g., a plasma jet).

8. (U) Technical Categorization—Power Sources

(U) A device that stores or releases electrical or mechanical energy. The key elements of information about a power source are its type/source, number of batteries and their configuration (series or parallel), its voltage (if electrical), and how it is connected to close an IED switch.

a. (U) **Alternating Current.** Electric current that flows through a circuit in both directions with the change in direction occurring with a well-defined and specified frequency.

b. (U) **Direct Current.** Electric current that flows through a circuit in just one direction.

c. (U) **Mechanical Energy.** A retained spring that acts as the energy source.

9. (U) Technical Categorization—Container

(U) A vessel commonly used to conceal the principal components of an IED is a container.

a. (U) **Concealment Container.** A vessel commonly used to prevent the discovery of an IED by visual inspection.

b. (U) **Confinement Container.** A vessel commonly used to hold the main charge together.

10. (U) Enhancements (See Figure D-6)

(U) An optional additional component deliberately added as opposed to a secondary hazard that modifies the effects of the IED. The IED would be effective, yet produce a different measurable result, if this material were not added. The effect can be additional physical destruction, proliferation of dangerous substances (e.g., radiation, chemicals), or other results to enhance the effect of the IED.

a. (U) **Biological Enhancement.** A microorganism and/or biologically derived compound or molecule that causes disease in people, plants, or animals, or causes the deterioration of material.

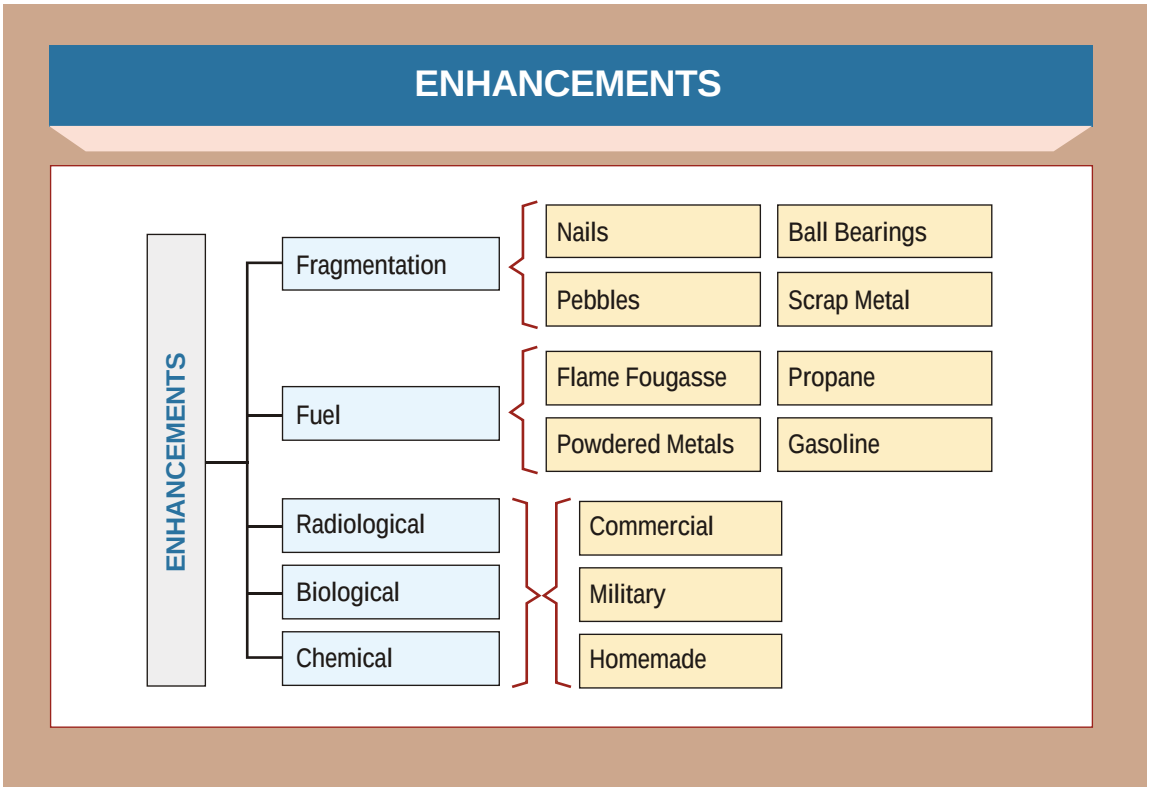


Figure D-6. (U) Enhancements

b. (U) **Chemical Enhancement.** Chemical agent included in an IED and specifically designed to cause death or other harm through toxic properties.

c. (U) **Flame Fougasse.** Typically a mixture of petrol (gasoline) and oil in a 40/60 ratio.

d. (U) **Fragmentation Enhancement.** Shrapnel and small objects designed to be accelerated by explosive forces.

e. (U) **Fuel Enhancement.** An incendiary material designed to enhance the burning and visual effect of the device.

f. (U) **Radiological Enhancement.** Radioactive materials that cause casualties or restrict the use of terrain when dispersed by an explosive charge. May also be described as a radiological dispersal device.

APPENDIX E
COUNTER-IMPROVISED EXPLOSIVE DEVICE ANNEX TEMPLATE (U)

(U) SECTION A. INTRODUCTION

(U) Below is a sample format that a joint force staff can use as a guide when developing a C-IED annex for a joint OPLAN. The exact format and level of detail may vary somewhat among joint commands, based on theater-specific requirements and other factors. However, joint OPLANs will always contain the basic five paragraphs (such as paragraph 3, "Execution") and their primary subparagraphs (such as paragraph 3a, "Concept of Operations").

(U) CJCSM 3122.01, *Joint Operation Planning and Execution System (JOPES) Volume I: (Planning, Policies, and Procedures)*, describes joint operation planning interaction between the President, the Secretary of Defense, the Chairman of the Joint Chiefs of Staff, the supported joint commander, and other joint planning and execution community members, and provides models of planning messages and estimates. CJCSM 3122.03, *Joint Operation Planning and Execution System (JOPES) Volume II: (Planning Formats)*, provides the formats for joint OPLANs when commanders must submit OPLANs in accordance with JOPES policy requirements.

(U) SECTION B. OPLAN FORMAT

(U) Copy No. _____

(U) Issuing Headquarters

(U) Place of Issue

(U) Effective Date/Time Group

(U) OPERATION PLAN: (Number or Code Name)

(U) USXXXXCOM OPERATIONS TO…

(U) References: (List any maps, charts, and other relevant documents deemed essential to comprehension of the plan.)

1. (U) Situation

a. (U) **General.** The use of IEDs has proven to be an effective tactic and weapon of strategic influence. IEDs are complex, adaptive systems. Challenging and unpredictable employment tactics, successful attacks without central direction, the social complexity of IED networks, and the strategic impacts caused by IEDs create an ill-structured strategic problem for US forces. C-IED is a focus of special effort for the command due to the unique and challenging nature of an IED attack, the extreme difficulty in defeating the IED threat, the adverse psychological effects a successful IED campaign has on friendly forces and local

populations, and the overall confidence of an adaptive enemy. C-IED is a combination of collective efforts and operations that include the offensive and defensive measures taken to defeat the IED network.

b. (U) **Purpose.** This annex describes C-IED functions and assigns responsibilities for the execution of Plan XX. It provides the concept for the scheme of C-IED operations, gives employment guidelines, and assigns missions to component command C-IED Task Forces.

c. (U) **Enemy Forces.** Annex B (Intelligence). Refer to (Intelligence Estimate) for the typical structure of an IED network (each network is unique yet contains the same functions in varying capacity).

d. (U) **Friendly Forces.** Annex A (Task Organization)

2. (U) Mission

(U) Mission. Basic Plan.

3. (U) Execution

a. (U) **Concept of Operations.** In order to achieve goals outlined in the basic plan, Combatant Command X conducts simultaneous C-IED actions coordinated through the six planning phases: Phase 0—Shape, Phase I—Deter/Engage, Phase II—Seize the Initiative, Phase III—Dominate/Decisive Operations, Phase IV—Stabilize, and Phase V—Enable Civil Authority. While some JOAs are further along in the phases individually, across the whole AOR, we are currently in Phase X. (General note: The combatant command should establish a core set of C-IED enablers that run through each phase. As the phases progress, the enabler will take on more fidelity or responsibility for action. An example would be dynamic network analysis for IED network modeling (nonmaterial solution) or supply chain countermeasures (materiel solution).)

(1) (U) Phase 0—Shape: This phase will set conditions that provide friendly forces (US and partners) the freedom of action to conduct operations against the enemy and deter the use of IEDs. These activities will be designed to enhance US and partner access to priority and high-priority countries and develop the appropriate theater infrastructure required to support C-IED operations against the enemy. By shaping the environment, Combatant Command X will create conditions that inhibit the IED threat from gaining a foothold. This phase will establish an environment hostile to the IED network and establish the battlefield infrastructure required to execute Plan XX.

(a) (U) Phase 0—Operational Objectives:

1. (U) Shape future behavior within regional area by expanding security cooperation with allies and PN to protect US interests and prevent the spread of extremist ideology.

2. (U) Develop relationships with and ensure operational access to allies and PNs to enable effective partnerships in times of crisis.

3. (U) Propagate memorandums of agreement and memorandums of understanding with the interagency to prevent bureaucratic restrictions.

4. (U) Establish mechanisms through the HN or the Department of State to leverage commercial supply chains.

5. (U) Establish mechanisms through the HN to leverage local telecommunication networks and to provide support to the communications strategy within the local, national, and regional media sources.

6. (U) Adapt to changing and complex security environment.

(b) (U) Phase 0—Essential Capabilities:

1. (U) Network Attack. Establish a federated node and integrate into the C-IED federated enterprise for access to C-IED information. Develop a phased ISR plan for multilayered C-IED operations. Perform military intelligence operations to identify IED networks and their supporters. Conduct dynamic network analysis to define IED network structures and relationships.

2. (U) C-IED Training. Ensure friendly forces, individuals and staffs, are appropriately postured and trained to conduct C-IED operations as Plan XX is executed.

3. (U) International. Establish relationships with partner organizations and nations through embassy and country teams, military attachés, and other multiagency efforts for information and capability sharing to build C-IED capacity throughout the region.

4. (U) Planning. Develop model for a joint C-IED task force if Plan XX enters offensive operations.

(c) (U) Phase 0—End State: This phase ends with providing a security environment favorable to US interests and HN objectives. The results of the shaping activities will be a favorable environment established for friendly forces to interdict the target set at the place and time of their choosing.

(2) (U) Phase 1—Deter: This phase will set the conditions required to conduct offensive actions against the IED threat network and achieve decisive results outlined in Plan XX and facilitate the competency of allied and PN C-IED organizations.

(a) (U) Phase 1—Operational Objectives:

1. (U) Bilaterally with HN, conduct direct action against known bomb makers and facilitators

2. (U) Monitor environment to detect and predict IED trends and attacks.

3. (U) Exploit IED network C2 and decision-making capability.

4. (U) Defend MNFs from the effects of IEDs.

5. (U) Develop proper C2 infrastructure with defined command relationships and robust communications to link the strategic, operational, and tactical levels of the C-IED campaign.

6. (U) Establish procedures to collect, consolidate, and disseminate IED and C-IED lessons learned throughout the AOR.

7. (U) Establish procedures to identify capability needs, request new technologies, and prioritize technology programs.

8. (U) Conduct JIPOE to identify key sources of IED supplies and critical IED production facilities.

9. (U) Identify existing C-IED organizations within the AOR and establish procedures for coordinated and supported efforts.

10. (U) Protect PNs from the effect of IEDs.

11. (U) Engage PN governments to assist in developing their C-IED capabilities.

12. (U) Conduct joint C-IED exercises and training with allies and PNs.

13. (U) Conduct C-IED operations to implement strategic communication guidance.

14. (U) Use elements of IO targeting AOR populations in order to discredit the use of IEDs as an accepted tactic.

(b) (U) Phase 1—Essential Capabilities:

1. (U) Network Attack. Perform multilayered, multi-intelligence analysis to identify IED networks. Conduct dynamic network analysis to define IED network structures and relationships.

2. (U) C-IED Training. Ensure friendly forces, individuals and staffs, are appropriately postured and trained to conduct C-IED operations as enemy tactics evolve.

3. (U) International. Share information through embassy and country teams, military attachés, and other multiagency efforts to build C-IED capacity throughout the region.

4. (U) Planning. Implement model for a joint C-IED task force appropriately staffed for the threat level.

(c) (U) Phase 1—End state: This phase ends with:

1. (U) Establishment of competent allied and HN C-IED organizations.

2. (U) Establishment of an environment and indigenous population that is non-supportive of IED activity and its supporting network.

3. (U) The emplacement of a C2 structure that synchronizes all strategic-, operational-, and tactical-level C-IED efforts and establishes unity of effort throughout the AOR.

4. (U) Establishment of procedures to capture TTP and technology lessons learned; technology capabilities and limitations; and methods to share lessons learned with forces throughout the theater.

(3) (U) Phase 2—Seize the Initiative: This phase will shift the main effort to the destruction of enemy IED networks and contain the spread of IEDs throughout the area of operations.

(a) (U) Phase 2 Operational Objectives:

1. (U) Conduct detailed JIPOE focused upon the specific IED networks the JOAs and conduct tailored CFA on the networks.

2. (U) Identify effective TTP and technologies to defeat IEDs.

3. (U) Source, in significant quantities, networks proven effective against emplaced devices.

4. (U) Execute the explosive remnants of war (ERW) reduction plan to decrease the supply of IED components.

5. (U) Test and develop technologies to defeat anticipated future devices and emplacement tactics.

6. (U) Initiate joint interdiction operations that neutralize bomb makers, facilitators, and resources.

7. (U) Transition applicable C-IED solutions to HN forces and MNFs.

8. (U) Engage HN governments to assist in developing their C-IED capabilities.

9. (U) Execute IO targeting AOR populations in order to discredit the use of IEDs as an accepted tactic.

(b) (U) Phase 2 Essential Capabilities:

1. (U) Network Attack. Perform multilayered, multi-intelligence analysis to identify, attack, and defeat IED networks. Conduct dynamic network analysis to define IED network structures and relationships.

2. (U) C-IED Training. Ensure friendly forces, individuals and staffs, are appropriately postured and trained to conduct C-IED operations as enemy tactics evolve.

3. (U) International. Share information through embassy and country teams, military attachés, and other multiagency efforts to build C-IED capacity throughout the region.

4. (U) Planning. Implement model for a joint C-IED task force appropriately staffed for the threat level.

(c) (U) Phase 2—End state: This phase ends with:

1. (U) Effective technologies fielded in significant quantities to defend all MNFs in theater against current IED techniques.

2. (U) C-IED joint interdiction operations established.

3. (U) ERW reduced to a manageable level. Accountability and security maintained over remaining ERW stockpiles.

4. (U) HN has a trained and ready C-IED force.

5. (U) Focused research and development on anticipated IED techniques.

6. (U) Institutionalize C-IED efforts throughout DOTMLPF.

(4) (U) Phase 3—Dominate: This phase will focus on defeating IED networks and reduce IED employment throughout the area of operations.

(a) (U) Phase 3 Operational Objectives:

1. (U) Identify, target, and interdict all elements of the IED network, with specific emphasis on critical nodes and commodities of network.

2. (U) Continue ERW reduction plan.

3. (U) Continue to target and neutralize bomb makers and facilitators.

4. (U) Continue to engage HN governments to assist in developing their C-IED capabilities.

(b) (U) Phase 3—Essential Capabilities:

1. (U) Network Attack. Perform multilayered, multi-intelligence analysis to identify, attack, and defeat IED networks. Conduct dynamic network analysis to define IED network structures and relationships.

2. (U) C-IED Training. Ensure friendly forces, individuals and staffs, are appropriately postured and trained to conduct C-IED operations as enemy tactics evolve.

3. (U) International. Share information through embassy and country teams, military attachés, and other multiagency efforts to build C-IED capacity throughout the region.

4. (U) Planning. Implement model for a joint C-IED task force appropriately staffed for the threat level.

(c) (U) Phase 3 End State:

1. (U) Severely restrict insurgent and terrorist IED networks' freedom of action and movement.

2. (U) Destroy and disrupt IED networks.

3. (U) PN populations unsupportive of IED use within the AOR.

4. (U) IED critical components developed out of theater are tracked and interdicted.

5. (U) ERW reduced to a manageable level. Accountability and security maintained over remaining ERW stockpiles.

(5) (U) Phase 4—Stabilize the Environment: This phase will shift the main effort from US forces defeating IED networks to HN forces responsible for C-IED operations.

(a) (U) Phase 4 Operational Objectives:

1. (U) Protect the US, MNF (if applicable), and HN from the effects of IEDs.

2. (U) Develop and share C-IED capability within the MNF and HN.

3. (U) Transition control of the C-IED effort from US to HN.

(b) (U) Phase 4—Essential Capabilities:

1. (U) Network Attack. Perform multilayered, multi-intelligence analysis to identify, attack, and defeat IED networks. Conduct dynamic network analysis to define IED network structures and relationships.

2. (U) C-IED Training. Ensure that friendly forces, with special emphasis on HN forces, are appropriately postured and trained to conduct C-IED operations as enemy tactics evolve.

3. (U) International. Share information through embassy and country teams, military attachés, and other multiagency efforts to build C-IED capacity throughout the region.

4. (U) Planning. Implement model for a joint C-IED task force appropriately staffed for the threat level.

(c) (U) Phase 4—End State:

1. (U) HN assumes lead role in executing C-IED efforts.

2. (U) HN manned, trained, and equipped to execute C-IED efforts.

(6) (U) Phase 5—Enable Civil Authority: This phase will shift the main effort to support legitimate civil governance in the theater and ensure that the HN military can effectively and independently perform C-IED operations.

(a) (U) Phase 5—Operational Objectives:

1. (U) Enable viability and provision of essential civil services.

2. (U) Train HN forces.

(b) (U) Phase 5 Essential Capabilities:

1. (U) C-IED Training. Ensure friendly forces, individuals and staffs, are appropriately postured and trained to conduct C-IED operations as enemy tactics evolve.

2. (U) International. Share information through embassy and country teams, military attachés, and other multiagency efforts to build C-IED capacity throughout the region.

(c) (U) Phase 5—End State: HN conducts C-IED operations autonomously.

b. (U) Tasks

c. (U) Coordinating Instructions. *[Expand this section as necessary.]*

4. (U) Administration and Logistics

[Expand this section as necessary.]

5. (U) Command and Control

[Expand this section as necessary.]

APPENDIX F
IMPROVISED EXPLOSIVE DEVICE NETWORK ACTIVITIES (U)

(U) C-IED operations should begin with a thorough understanding of the enemy and the common activities associated with an IED attack. IED attacks are the results of many interrelated activities, including planning, financing, material procurement, bomb making, target selection, recruiting, and attack execution. Understanding each activity can assist commanders and their staffs in identifying adversary vulnerabilities and points of attack. Once identified, these vulnerabilities can be exploited to disrupt the IED network and break the enemy's operational chain of events.

1. (U) **Strategic Leadership.** A person or group that provides the strategic direction and purpose for the network. This leadership may coordinate the activities between regional and local nodes.

2. (U) **Regional and Local Leadership.** A person or group that carries out the operations delegated by the international leadership. A network can also be made up of many splinter organizations carrying out specific orders from a larger, more centralized group.

3. (U) **Recruiting.** Recruiting includes the activities related to the act of building a force of operatives, including trainers, technicians, bomb makers, treasurers, comptrollers or accountants, emplacers, fighters, suppliers, distributors, fund-raisers, donors, and financial service providers to carry out the group's campaign.

4. (U) **Training.** Training is the act of providing a means to educate recruited personnel in a skill needed to perform a role in the overall effort. Some personnel may be trained as engineers, while others may be trained to emplace IEDs.

5. (U) **Target selection and planning.** Planners must first select a target before mission planning can begin; this will be based on ISR assessments and overall campaign objectives of network leadership. Target selection and planning will become more complex as friendly security and C-IED capabilities grow.

6. (U) **Surveillance.** Includes observing and assessing potential targets to collect information used in the planning of IED operations. Through observation, the enemy collects valuable information on troop movements, times of vulnerability, and target vulnerability. These observations also aid the enemy planner with critical information, such as ideal IED emplacement locations, high-traffic areas, concealment data, observation points, and avenues of approach, escape, and reinforcement.

7. (U) **Attack Rehearsal.** A rehearsal prepares the IED team for its actions and tests and evaluates the plan of attack.

8. (U) **Movement.** Movement is the physical transport of devices, supplies, personnel, and possibly money (cash funds) into and out of an operational area during pre- and post-

detonation phases. Movement may also take place during an incident that distracts friendly forces.

9. (U) **Financing.** This includes the fund-raising, funding, and financial facilitation activities required to establish, maintain, and grow networks of IED cells and pay for the cost of their operations, including, but not limited to, the cost of planning and executing IED attacks. Financing also includes the electronic transfer of funds and other methods of finance required to procure IED parts, components, and technology.

10. (U) **Supplies.** The materials required to execute IED operations.

11. (U) **IED Makers.** People involved in the design and fabrication of an IED.

12. (U) **IED Team.** The personnel who emplace, monitor, and detonate the IED. The team may also include an element to videotape the explosion for exploitation/propaganda purposes.

13. (U) **International Support.** Support in the form of funding, financial facilitation, training, organization, recruiting, publicity, and planning assistance that is provided to the group from nonlocal sources, including sympathetic foreign nations and states, nongovernmental organizations, terrorist organizations, media outlets, and other organizations or individuals.

14. (U) **Regional and Local Support.** Active local support consists of efforts on the part of citizens and other locals to assist enemy IED efforts (such as looking out for troops while IEDs are being placed or donating supplies). Active local support may also be the result of the local or regional IED networks providing employment opportunities to individuals who would otherwise be unemployed. Passive local support for insurgent IED efforts consists of the refusal of citizens and other locals to give US or multinational troops information or assistance. Passive local support of IED efforts results in part from fear of reprisal, but may also be attributed to sympathy with enemy objectives.

15. (U) **Orders Group.** The orders group (which may have no formal name) is a small cell made up of one or more members of the regional and/or local leadership and possibly the IED maker(s). It is designed to coordinate the IED effort including the procurement of IED components while compartmenting information in case of infiltration or discovery.

16. (U) **Battle Damage Assessment.** Battle damage assessment is the act of observing, which may include videotaping the event for propaganda purposes, the detonation or aftermath of an explosion to evaluate the destruction of the IED. Often this is a decision point for the enemy to initiate a follow-on attack or egress out of the kill zone.

17. (U) **Emplacement.** This is the positioning of an IED for the purpose of conducting an attack. It may be simply placing an IED by a road or burying a large device at a specific location.

18. (U) **Monitor and Detonate.** The act of observing the area of emplacement in order to command detonate an IED.

19. (U) **Ideology and Other Motivating Factors.** The set of reasons, including the body of ideas shaped by social, religious, cultural, and criminal factors, that drive the formation of a network, dictate function, and govern behavior. Regardless of motivation, the TTP, or business model, for planning, executing, assessing, and exploiting IED attacks or events may be the same.

20. (U) **Infrastructure.** IED makers require an infrastructure of safe houses, work areas, storage facilities, and transport or courier facilities to move devices, supplies, cash, and personnel.

21. (U) **IO.** The enemy can be very effective in using IO as a method of promoting group success; for example, the filming of attacks may enhance recruiting efforts and encourage support by portraying a positive image of the group's operations.

Intentionally Blank

APPENDIX G
REFERENCES

The development of JP 3-15.1 is based upon the following primary references:

1. Strategic Guidance and Policy

a. *The National Security Strategy of the United States of America.*

b. *National Defense Strategy of the United States of America.*

c. *National Military Strategy.*

d. Department of Defense Directive 2000.19E, *Joint Improvised IED Defeat Organization.*

2. Joint Publications

a. JP 2-01.3, *Joint Intelligence Preparation of the Operational Environment.*

b. JP 3-0, *Joint Operations.*

c. JP 3-11, *Operations in Chemical, Biological, Radiological, and Nuclear (CBRN) Environments.*

d. JP 3-13, *Information Operations.*

e. JP 3-16, *Multinational Operations*.

f. JP 3-33, *Joint Force Headquarters.*

g. JP 5-0, *Joint Operation Planning.*

3. Allied Joint Publications

Allied Joint Publication-3.15, *Counter-Improvised Explosive Device Operations.*

4. Service Publications

FM 3-90.119 (Field Manual Interim 3-34.119/Marine Corps Interim Publication 3-17.01). *Combined Arms Improvised Explosive Device Defeat Operations.*

5. General

a. US Army Center for Army Lessons Learned Handbook 09-49, *IED-Defeat Leader's Handbook,* 2009.

b. Defense Intelligence Agency and Joint IED Defeat Organization Handbook, *Weapons Technical Intelligence Handbook,* 2009.

Intentionally Blank

APPENDIX H
ADMINISTRATIVE INSTRUCTIONS

1. User Comments

Users in the field are highly encouraged to submit comments on this publication to: Joint Staff J-7, Deputy Director, Joint and Coalition Warfighting, Joint and Coalition Warfighting Center, ATTN: Joint Doctrine Support Division, 116 Lake View Parkway, Suffolk, VA 23435-2697. These comments should address content (accuracy, usefulness, consistency, and organization), writing, and appearance.

2. Authorship

The lead agent for this publication is the XXX. The Joint Staff doctrine sponsor for this publication is the Director for Operations (J-3).

3. Change Recommendations

a. Recommendations for urgent changes to this publication should be submitted:

TO: DA WASHINGTON DC// G35-SSP//
INFO: JOINT STAFF WASHINGTON DC//J-7-JEDD//
CDRUSJFCOM SUFFOLK VA//JT10//

b. Routine changes should be submitted electronically to the Deputy Director, Joint and Coalition Warfighting, Joint and Coalition Warfighting Center, Joint Doctrine Support Division and info the lead agent and the Director for Joint Force Development, J-7/JEDD.

c. When a Joint Staff directorate submits a proposal to the Chairman of the Joint Chiefs of Staff that would change source document information reflected in this publication, that directorate will include a proposed change to this publication as an enclosure to its proposal. The Services and other organizations are requested to notify the Joint Staff J-7 when changes to source documents reflected in this publication are initiated.

5. Distribution of Publications

Local reproduction is authorized and access to unclassified publications is unrestricted. However, access to and reproduction authorization for classified JPs must be in accordance with DOD 5200.1-R, *Information Security Program*.

6. Distribution of Electronic Publications

a. Joint Staff J-7 will not print copies of JPs for distribution. Electronic versions are available on JDEIS at https://jdeis.js.mil (NIPRNET) and https://jdeis.js.smil.mil (SIPRNET), and on the JEL at http://www.dtic.mil/doctrine (NIPRNET).

b. Only approved JPs and joint test publications are releasable outside the combatant commands, Services, and Joint Staff. Release of any classified JP to foreign governments or

foreign nationals must be requested through the local embassy (Defense Attaché Office) to DIA, Defense Foreign Liaison/IE-3, 200 MacDill Blvd, Joint Base Anacostia-Bolling, Washington, DC 20340-5100.

c. JEL CD-ROM. Upon request of a joint doctrine development community member, the Joint Staff J-7 will produce and deliver one CD-ROM with current JPs. This JEL CD-ROM will be updated not less than semi-annually and when received can be locally reproduced for use within the combatant commands and Services.

GLOSSARY

PART I—ABBREVIATIONS AND ACRONYMS

ABIS	Automated Biometric Identification System
AOR	area of responsibility
ATF	Bureau of Alcohol, Tobacco, Firearms, and Explosives (DOJ)
AtN	attack the network
AWG	Asymmetric Warfare Group (Army)
BCT	brigade combat team
BEI	biometrics-enabled intelligence
BIAR	biometric intelligence analysis report
BIMA	Biometrics Identity Management Agency
C2	command and control
CARVER	criticality, accessibility, recuperability, vulnerability, effect, and recognizability
CBRN	chemical, biological, radiological, and nuclear
CBRNE	chemical, biological, radiological, nuclear, and high-yield explosives
CEHC	Counter Explosive Hazards Center (Army)
CELLEX	cellular exploitation
CEXC	combined explosives exploitation cell
CFA	critical factors analysis
CIDNE	Combined Information Data Network Exchange
C-IED	counter-improvised explosive device
CITP	counter-improvised explosive device targeting program
CJCSM	Chairman of the Joint Chiefs of Staff manual
CJTF	commander, joint task force
COIC	counter-improvised explosive device operations integration center
COIN	counterinsurgency
CONOPS	concept of operations
CONUS	continental United States
COP	common operational picture
CREW	counter radio-controlled improvised explosive device electronic warfare
CRT	chemical, biological, radiological, nuclear, and high-yield explosives response team
CSS	combat service support
CTF	counter threat finance
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DNA	deoxyribonucleic acid

DOD	Department of Defense
DOJ	Department of Justice
DOMEX	document and media exploitation
DOTMLPF	doctrine, organization, training, materiel, leadership and education, personnel, and facilities
EFP	explosively formed projectile
EHCC	explosive hazards coordination cell
EHDB	explosive hazard database
EHT	explosive hazard team
EMS	electromagnetic spectrum
EOCA	explosive ordnance clearance agent
EOD	explosive ordnance disposal
ERW	explosive remnants of war
EW	electronic warfare
EWCC	electronic warfare coordination cell
EWO	electronic warfare officer
F2T2EA	find, fix, track, target, engage, and assess
F3EAD	find, fix, finish, exploit, analyze, and disseminate
FBI	Federal Bureau of Investigation
FM	field manual (Army)
G-3	assistant chief of staff, operations
G-5	assistant chief of staff, plans
G-7	assistant chief of staff, information engagement
GCC	geographic combatant commander
GEOINT	geospatial intelligence
HARC	human intelligence analysis and reporting cell
HN	host nation
HPT	high-payoff target
HUMINT	human intelligence
HVI	high-value individual
I2WD	Intelligence and Information Warfare Division (Army)
IED	improvised explosive device
IO	information operations
ISR	intelligence, surveillance, and reconnaissance
IW	irregular warfare
J-2	intelligence directorate of a joint staff
J-3	operations directorate of a joint staff
J-7	engineering staff section
JDIGS	Joint Digital Information Gathering System
JEFF	Joint Expeditionary Forensic Facility (Army)

JET	joint expeditionary team
JFC	joint force commander
JIEDDO	Joint Improvised Explosive Device Defeat Organization
JIOC	joint intelligence operations center
JIPOE	joint intelligence preparation of the operational environment
JISE	joint intelligence support element
JKnIFE	Joint Improvised Explosive Device Defeat Organization Knowledge and Information Fusion Exchange
JOA	joint operations area
JOPES	Joint Operation Planning and Execution System
JOPP	joint operation planning process
JP	joint publication
JTAIC	Joint Technical Analysis and Integration Cell (Army)
JTCOIC	Joint Training Counter-Improvised Explosive Device Operations Integration Center
JTF	joint task force
LEP	law enforcement professional
LOO	line of operation
MAGTF	Marine air-ground task force
MCTOG	Marine Corps Tactics and Operations Group
MCWL	Marine Corps Warfighting Lab
MNF	multinational force
MRX	mission readiness exercise
MSC	major subordinate command
mtDNA	mitochondrial deoxyribonucleic acid
NAI	named area of interest
NAVEODTECHDIV	Naval Explosives Ordnance Disposal Technology Division
NGIC	National Ground Intelligence Center
OPCON	operational control
OPLAN	operation plan
ORSA	operations research and systems analysis
PBIED	person-borne improvised explosive device
PN	partner nation
RCIED	radio-controlled improvised explosive device
RCT	regimental combat team
REF	Rapid Equipping Force (Army)
RFI	request for information
RFS	request for support
RSOI	reception, staging, onward movement, and integration

S&T	science and technology
S-2	battalion or brigade intelligence staff officer (Army; Marine Corps battalion or regiment)
S-3	battalion or brigade operations staff officer (Army; Marine Corps battalion or regiment)
SIGINT	signals intelligence
SIPRNET	SECRET Internet Protocol Router Network
SME	subject matter expert
TACON	tactical control
TDC	target development cell
TECHINT	technical intelligence
TEDAC	Terrorist Explosive Device Analytical Center (FBI)
TFE	threat finance exploitation
THT	tactical human intelligence team
TIDE	Terrorist Identities Datamart Environment
TQ	tactical questioning
TSA	target system analysis
TTP	tactics, techniques, and procedures
USG	United States Government
USMC	United States Marine Corps
UXO	unexploded ordnance
VBIED	vehicle-borne improvised explosive device
WBIED	waterborne improvised explosive device
WIT	weapons intelligence team
WMD	weapons of mass destruction
WMD-E	weapons of mass destruction-elimination
WTI	weapons technical intelligence

PART II—TERMS AND DEFINITIONS

asymmetric. In military operations the application of dissimilar strategies, tactics, capabilities, and methods to circumvent or negate an opponent's strengths while exploiting his weaknesses. (Approved for inclusion in JP 1-02.)

attack the network operations. Lethal and nonlethal 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. Also called **AtN operations.** (Approved for inclusion in JP 1-02.)

counter-improvised explosive device operations. The organization, integration, and synchronization of capabilities that enable offensive, defensive, stability, and support operations across all phases of operations or campaigns in order to defeat improvised explosive devices as operational and strategic weapons of influence. Also called **C-IED operations.** (Approved for inclusion in JP 1-02.)

explosive hazard incident. The suspected or detected presence of unexploded or damaged explosive ordnance that constitutes a hazard to operations, installations, personnel, or material. Not included in this definition are the accidental arming or other conditions that develop during the manufacture of high explosive material, technical service assembly operations, or the laying of mines and demolition charges. (Approved for replacement of "explosive ordnance disposal incident" and its definition in JP 1-02.)

explosive ordnance disposal procedures. None. (Approved for removal from JP 1-02.)

final disposal procedures. None. (Approved for removal from JP 1-02.)

improvised explosive device. A weapon that is fabricated or emplaced in an unconventional manner incorporating destructive, lethal, noxious, pyrotechnic, or incendiary chemicals designed to kill, destroy, incapacitate, harass, deny mobility, or distract. Also called **IED.** (Approved for incorporation into JP 1-02.)

intelligence summary. None. (Approved for removal from JP 1-02.)

man portable. None. (Approved for removal from JP 1-02.)

recovery procedures. None. (Approved for removal from JP 1-02.)

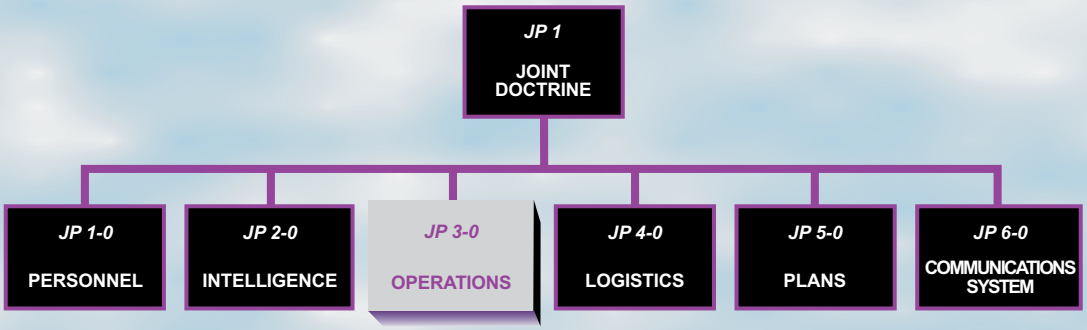
render safe procedures. The portion of the explosive ordnance disposal procedures involving the application of special explosive ordnance disposal methods and tools to provide for the interruption of functions or separation of essential components of unexploded explosive ordnance to prevent an unacceptable detonation. (Approved for incorporation into JP 1-02.)

technical escort. An individual technically qualified and properly equipped to accompany designated material requiring a high degree of safety or security during shipment. (Approved for incorporation into JP 1-02 with JP 3-15.1 as the source JP.)

technical evaluation. The study and investigations by a developing agency to determine the technical suitability of material, equipment, or a system for use in the Services. (Approved for incorporation into JP 1-02.)

weapons technical intelligence. A category of intelligence and processes derived from the technical and forensic collection and exploitation of improvised explosive devices, associated components, improvised weapons, and other weapon systems. Also called **WTI.** (Approved for inclusion in JP 1-02.)

JOINT DOCTRINE PUBLICATIONS HIERARCHY



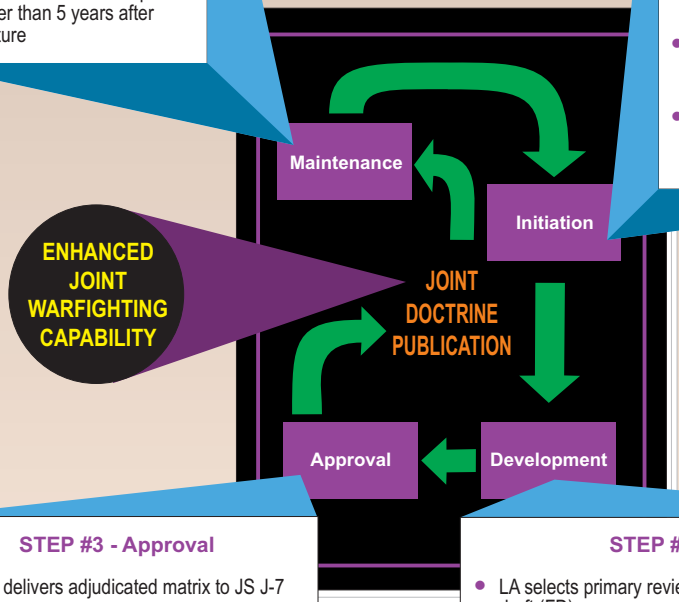
All joint publications are organized into a comprehensive hierarchy as shown in the chart above. **Joint Publication (JP) 3-15.1** is in the **Operations** series of joint doctrine publications. The diagram below illustrates an overview of the development process:

STEP #4 - Maintenance

- JP published and continuously assessed by users
- Formal assessment begins 24-27 months following publication
- Revision begins 3.5 years after publication
- Each JP revision is completed no later than 5 years after signature

STEP #1 - Initiation

- Joint doctrine development community (JDDC) submission to fill extant operational void
- Joint Staff (JS) J-7 conducts front-end analysis
- Joint Doctrine Planning Conference validation
- Program directive (PD) development and staffing/joint working group
- PD includes scope, references, outline, milestones, and draft authorship
- JS J-7 approves and releases PD to lead agent (LA) (Service, combatant command, JS directorate)



STEP #3 - Approval

- JSDS delivers adjudicated matrix to JS J-7
- JS J-7 prepares publication for signature
- JSDS prepares JS staffing package
- JSDS staffs the publication via JSAP for signature

STEP #2 - Development

- LA selects primary review authority (PRA) to develop the first draft (FD)
- PRA develops FD for staffing with JDDC
- FD comment matrix adjudication
- JS J-7 produces the final coordination (FC) draft, staffs to JDDC and JS via Joint Staff Action Processing (JSAP) system
- Joint Staff doctrine sponsor (JSDS) adjudicates FC comment matrix
- FC joint working group


JOINT
CHIEFS OF STAFF