Joint Publication 3-26

Joint Combating Terrorism

30 July 2020

PREFACE

1. Scope

This publication provides fundamental principles and guidance to plan, execute, and assess military activities to combat terrorist threats to US forces, allied and partner nations, and foreign and domestic civilian populations through a combined and coordinated application of offensive counterterrorism and protective antiterrorism activities and operations.

2. Purpose

This publication has been prepared under the direction of the Chairman of the Joint Chiefs of Staff (CJCS). It sets forth joint doctrine to govern the activities and performance of the Armed Forces of the United States in joint operations, and it provides considerations for military interaction with governmental and nongovernmental agencies, multinational forces, and other interorganizational partners. It provides military guidance for the exercise of authority by combatant commanders and other joint force commanders (JFCs) and prescribes joint doctrine for operations and training. It provides military guidance for use by the Armed Forces of the United States in preparing and executing their plans and orders. 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 objectives.

3. Application

a. Joint doctrine established in this publication applies to the Joint Staff, commanders of combatant commands, subordinate unified commands, joint task forces, subordinate components of these commands, the Services, the National Guard Bureau, and combat support agencies.

b. This doctrine constitutes official advice concerning the enclosed subject matter; however, the judgment of the commander is paramount in all situations.

c. If conflicts arise between the contents of this publication and the contents of Service publications, this publication will take precedence unless the CJCS, 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:

DAVID R. IVERSON
Major General, US Air Force
Vice Director, Joint Force
Development

SUMMARY OF CHANGES
REVISION OF JOINT PUBLICATION 3-26
DATED 24 OCTOBER 2014

- **Changes the title of this publication to *Joint Combating Terrorism.***
- **Consolidates counterterrorism and antiterrorism doctrine into one publication.**
- **Rescinds Joint Publication (JP) 3-07.2 *Antiterrorism;* retains United States Special Operations Command as the lead agent for JP 3-26.**
- **Adds combating terrorism-related content on cyber operations, countering threat networks, joint security areas, and force protection with reference to the JPs that cover these topics in greater detail.**
- **Adds discussion of violent extremist organizations as they relate to combating terrorism efforts.**
- **Updates definitions and terminology with approved joint or pertinent Service positions.**
- **Updates figures, quotes, and vignettes.**
- **Adds Appendix G, "Combating Terrorism in the Information Environment."**

Intentionally Blank

TABLE OF CONTENTS

Intentionally Blank

EXECUTIVE SUMMARY
COMMANDER'S OVERVIEW

- **Describes the relationship and synergy between counterterrorism (CT) and antiterrorism (AT) activities and operations by combining these discussions under the broader construct of combating terrorism (CbT).**

- **Outlines CbT activities, organizations, responsibilities, and authorities and explains the relationship with force protection.**

- **Describes the terrorist threat and identifies specific types of threats, to include terrorist networks.**

- **Discusses the fundamentals and principles of CT operations and activities across the competition continuum, to include command and control (C2), planning, targeting, assessment, and support operations.**

- **Outlines the fundamentals of AT and examines the key aspects of AT programs, to include responsibilities, C2, assessment, incident response, and support activities.**

Introduction to Combating Terrorism

The challenge for the Department of Defense (DOD) and the United States Government (USG) is how to best apply the instruments of national power to defeat terrorists and violent extremist organizations (VEOs) that threaten the United States, its citizens, and its vital interests and protect friendly forces, populations, and allies, while assisting and enabling friendly forces to deter and defeat terrorists. The answer to this challenge is a balanced and integrated approach that maintains an aggressive, offensive counterterrorism (CT) capability coupled with robust and proactive antiterrorism (AT) measures. CT are activities and operations tasked to neutralize terrorists and their organizations and networks to render them incapable of using violence to instill fear and coerce governments or societies to achieve their goals. AT measures are used to reduce the vulnerability of individuals and property to terrorists' acts, to include rapid containment by local military and civilian forces. This publication emphasizes the relationship and synergy between CT and AT activities and operations by combining these discussions under the broader construct of combating terrorism (CbT).

Strategic Context

Individual terrorists and VEOs are potentially grave dangers to the national security and interests of the United States, at home and abroad. Additionally, some traditional criminal activities, such as counterfeiting or illegal drug trafficking, may be terrorist-related if used to fund terrorist acts. Trends in the strategic environment require the United States to revalidate its assumptions about CbT and the methods to address existing and emerging threats. The joint force coordinates with and operates in support of interagency partners and partner nations (PNs) to dissuade individuals and groups from turning to terrorist tactics and to disrupt terrorist development and employment of capabilities that create lethal effects. DOD must seek to build closer relationships at the tactical, operational, and strategic levels to ensure its efforts complement diplomatic, intelligence, and law enforcement (LE) efforts and do not duplicate or disrupt them. Efforts to deter, delay, degrade, disrupt, and defeat or defend against terrorist actions and their organizations must address the entirety of threat networks and pathways.

Combating Terrorism Activities

CbT remains an approach with defensive and offensive components. AT activities are used to reduce the vulnerability of individuals and property to terrorist acts. AT activities include containment of terrorist activities by local military and civilian forces. CT operations are executed to neutralize individual terrorists, terrorist organizations, and their networks to render them incapable of using terrorist tactics to kill innocent people, instill fear, and coerce governments or societies to achieve their objectives. Critical supporting activities of CbT operations are intelligence support, information sharing, and incident management, which, together, serve to support and link AT and CT in the achievement of common strategic objectives. Other defensive and offensive elements are force protection (FP), personnel security, operations security, continuity of operations, countering weapons of mass destruction (CWMD), and defense critical infrastructure protection.

Combating Terrorism Organizations, Responsibilities, and Authorities

The National Security Council manages the interagency process concerning CT and all national security-related issues and specific, selected action. The Homeland Security Council (HSC) is an entity within the White House Office created in 2001. The HSC coordinates across a broad spectrum of federal, state, local, and

private-sector entities to reduce the potential for terrorist attacks and other threats and mitigates damage should an incident occur. The Department of Homeland Security (DHS), in conjunction with other USG departments and agencies, plays a crucial role in the protection of critical infrastructure. DHS provides strategic guidance to public and private partners, promotes unity of effort, and coordinates the overall USG effort to promote the security and resilience of the nation's critical infrastructure. The Department of State (DOS) has six regional bureaus that address foreign policy considerations on a regional basis. The assistant secretaries of the regional bureaus are key leaders in CT activities, policy, and operations in their assigned regions. Furthermore, the DOS Bureau of Counterterrorism publishes an annual country report on terrorism and manages US policy for a whole-of-government approach to CT. The DOS Bureau of Counterterrorism maintains the Foreign Terrorist Organizations List that provides justification for the President to block or freeze tangible property and freeze financial accounts of individuals or terrorist organizations pursuant to Executive Order 13224, *Blocking Property and Prohibiting Transactions With Persons Who Commit, Threaten to Commit, or Support, Terrorism.* The Attorney General investigates acts or incidents that may constitute a violation of federal laws related to acts of terrorism or the use or threatened use of weapons of mass destruction. This authority is exercised through the Federal Bureau of Investigation (FBI). The US Department of the Treasury's role in CT is to lead the USG efforts to locate, track, and seize suspected terrorist financial assets. Aligned under the Office of the Director of National Intelligence, the National Counterterrorism Center mission is to analyze terrorist threats, share information with PNs, and integrate all instruments of national power to ensure unity of effort. The National Joint Terrorism Task Force is an interagency coordination organization that provides liaison from FBI headquarters to local joint terrorism task forces and participating agencies and serves as a conduit for information on threats and leads. Within DOD, CT activities and operations are normally executed by combatant commanders (CCDRs), subordinate theater special operations command commanders, and other joint force commanders (JFCs). Commander, United States Special Operations Command (CDRUSSOCOM),

exercises coordinating authority for planning global operations against VEOs and for planning DOD CWMD efforts, in coordination with other CCDRs, the Services, and, as directed, other USG departments and agencies. The Defense Intelligence Agency (DIA) Defense Combating Terrorism Center (DCTC), in accordance with Department of Defense Instruction (DODI) 2000.12, *DOD Antiterrorism (AT) Program*, serves as the lead national-level, all-source, international terrorism intelligence effort within DOD and the analytic lead and mission manager for CbT analysis pertaining to domestic and international terrorist threats to DOD elements and personnel.

Terrorist Threat

Terrorist Organizational Structure, Membership, Networks, and Functions

Terrorist groups typically utilize one of two types of organizational structures: hierarchical or networked. Within either of those two larger organizational structures, however, virtually all terrorist groups organize as smaller cells at the tactical level. These organizations have a well-defined vertical chain of command and responsibility. Information flows up and down organizational channels that correspond to these vertical chains but may not move horizontally through the organization. Unlike hierarchies, networks distribute authority and responsibility throughout an organization, often creating redundant key functions. Terrorist groups are now increasingly part of a far broader but indistinct system of networks than previously experienced. A threat network consists of interconnected nodes and links and may be organized using subordinate and associated networks and cells. Understanding the individual roles and connections of each element is as important to conducting operations as is understanding the overall network structure, known as the network topology.

Lone Terrorists

As compared with a typical networked or hierarchical terrorist organization, lone terrorists, or "lone wolves" as they are commonly referred to, are often the hardest to detect, which presents a formidable challenge for JFCs, LE, and intelligence agencies. Typically, the lone terrorist shares an ideological and sympathetic identification with an extremist organization and its goals and may have had some limited level of direct affiliation in the past, but the lone terrorist does not

communicate with any group when fashioning political aims and committing acts of terrorism.

Identity-Based Terrorism

Identity and intent are linked closely to the underlying ideology and the corresponding strategic objectives of terrorists and terrorist organizations. Some of the common categories are: ethnocentric, nationalistic, and revolutionary separatist. Ideological categories describe the political, religious, or social orientation of the group.

Violent Extremist Organizations

VEOs are the collective grouping of extremists, terrorist enablers, and/or terrorists with a common goal to conduct acts of terrorism in pursuit of ideological objectives. VEOs may have state and non-state sponsorship. VEOs have spread globally and continue to threaten the US homeland, US territories, US citizens, US allies, and US partners by conducting attacks, inspiring violence, and creating destabilizing conditions that divert military resources from other priority challenges. VEOs continue to evolve over time. This evolution includes innovations in the ability to antagonize, induce, and exploit existing grievances to mobilize support for violent change; find, influence, and mobilize populations locally, regionally, and globally; spread information and disinformation to elicit tacit and active support or acceptance of their views and actions; and conduct, direct, support, or inspire a mix of lethal and nonlethal actions to create physical and psychological effects, gain notoriety, garner attention, sustain and increase their base, and advance their cause.

Terrorist State, Affiliation, Non-State Affiliation, and Criminal Nexus

Terrorists and their organizations operate in interrelated networks. The nexus between these state, non-state, criminal, and terrorist networks happens when each element and network, operating in its own self-interest, sees an opportunity for mutual benefit. The terrorist and criminal nexus can also involve both types of groups having common sources of support. Both terrorist and criminal networks can use the same enablers, such as forgers, money laundering, corruption, permissive environments, trans-border movement, cyberspace "crime-for-hire" services, or other criminal-related services. Criminal network and terrorist network recruiting can also overlap.

Terrorist Tactics, Techniques, and Procedures

Terrorism is a tactic used by organizations or individuals trying to achieve specific objectives. Terrorist tactics are used by a wide variety of groups, including insurgents. Terrorists employ a variety of tactics, techniques, and procedures (TTP)—some small-scale, some large-scale—to produce fear in their intended audience. A few of the most common TTP employed by terrorist groups are assassination, arson, bombing, kidnapping and hostage taking, hijacking, piracy, seizure, raids or ambushes, sabotage, threats or hoaxes, environmental destruction, active shooter, and insider threat. Terrorists prefer to attack their enemies asymmetrically, circumventing an opponent's strength and exploiting weaknesses. Notably, these methods constantly evolve and often vary according to target and terrorist cell. Asymmetric tactics routinely employed by terrorists include denial and deception, human shields, ambush and surprise, attacks, and misinformation. Terrorists may leverage space and cyberspace capabilities to oppose CbT efforts by DOD forces and those of our allies. Terrorists can use cyberspace operations as an asymmetric means to counter traditional advantages by selectively targeting US space and cyberspace operations, capabilities, and infrastructure.

Terrorist Threats to the Homeland

In the most general statutory terms, a domestic terrorist engages in terrorist activity that occurs in the homeland. Domestic terrorism can be described as violence perpetrated by individuals or groups inspired by or associated with primarily US-based movements that espouse extremist ideologies of a political, religious, social, racial, or environmental nature. The FBI has lead responsibility for terrorism investigations at the federal level. The current domestic threat has expanded considerably; three factors have contributed to the evolution of the terrorism threat: the Internet, use of social media, and homegrown violent extremists. Commanders and policy makers are affected by the following aspects of domestic terrorism: level of activity, use of nontraditional tactics, exploitation of the Internet, decentralized nature of the threat, radicalization, insider threat, and active shooter.

Counterterrorism Operations and Activities

Fundamentals of Counterterrorism

To succeed at the tactical, operational, and strategic levels, civilian leadership should develop rapid, coordinated, and effective CT efforts that reflect and leverage the full capabilities and resources of the entire USG. CT operations should be planned and executed to support US diplomatic or informational initiatives, balancing near- and long-term CT considerations.

Principles, Activities, and Operations

The principles of joint operations are formed around the traditional nine principles of war—objective, offensive, mass, economy of force, maneuver, unity of command, security, surprise, and simplicity. To these, joint doctrine adds three principles based on operations over the last few decades—restraint, perseverance, and legitimacy. In addition to the traditional warfighting tenets, CT requires collaboration, balance, and precision.

National Strategy for Counterterrorism

The *National Strategy for Counterterrorism of the United States of America* outlines how the United States will combat terrorism at home and abroad. The strategic objectives support the following CT end states: the terrorist threat to the United States is eliminated; US borders and all ports of entry into the United States are secure against terrorist threats; terrorism, radical Islamist ideologies, and other violent extremist ideologies do not undermine the American way of life; and foreign partners address terrorist threats so they do not jeopardize the collective interests of the United States and its partners.

Counterterrorism Across the Competition Continuum

JFCs use capabilities in a wide variety of combat and noncombat situations to build a cohesive CT operation or support the combatant command campaign plans (CCPs). The primary purpose of military engagement and security cooperation (SC) activities, which may include CT activities, is to enable the CCDR to build indigenous capabilities that deter terrorist acts and shape the operational environment (OE) to a desired set of conditions that facilitate stability activities and future operations. CT, as a part of military engagement, is a noncombat activity conducted by specifically trained forces. SC that involves interaction with PN or host nation (HN) CT defense forces builds relationships that

promote US CT interests and develops indigenous and PN CT capabilities and capacities. Deterrence prevents terrorist acts by presenting a credible threat of specific counteraction that would deny the success of an organization's use of terrorism and degrade its legitimacy or capabilities and influence over a population.

Military Objectives Across the Competition Continuum

It is important to recognize that CT operations and activities can be executed simultaneously across the competition continuum during the same campaign. The operations and activities differ depending on the situation and relationship among participants.

Levels of Warfare and Counterterrorism

At the strategic level, the Secretary of Defense (SecDef) translates national CT strategic objectives into military strategic objectives that facilitate theater planning. Theater planning links national strategic policy, strategy, objectives, and end states that address global and transregional adversaries to DOD global objectives and end states. DOD then develops global campaign plans to address inherently global and transregional threats that exceed the authority of a single CCDR. The operational level links the national and military CT strategic objectives and end states to the tactical level by the planning and execution of CCPs with day-to-day activities and contingency plans. At the tactical level, special operations forces (SOF) contain units dedicated to CT operations and should be a JFC's first choice. When SOF are not available, the most appropriate and available force may be used.

Command, Control, Plan, and Assess Counterterrorism Activities and Operations

The nature of terrorist threats requires SecDef, CDRUSSOCOM, CCDRs, and JFCs to establish flexible and often complex command relationships to ensure the joint force has the required agility to coordinate with all DOD, interagency, and foreign partners and to pursue terrorists across military and governmental boundaries.

Organize for Counterterrorism Activities and Operations

SOF provides an array of command and control (C2) options that enables effective CT mission command throughout the competition continuum, which spans daily activities supporting a CCP, competitive activities against adversaries, and conflict. Planning for SOF CT C2 requires an understanding of the differences of the

SOF components and their C2 nodes, which contributes to the knowledge and ability to articulate the SOF C2 requirements for US Special Operations Command validation.

Execute Counterterrorism Activities and Decisive Operations

Executing CT activities and operations require the formulation of approaches, lines of effort, and decisive points that lead to an acceptable end state. When dealing with terrorists, the JFC must consider how actions against decisive points will affect not only the enemy but also the relevant population and their behavior and relationships with the terrorist and friendly forces. A JFC employing forces must selectively focus a series of actions against terrorists' critical vulnerabilities until the cumulative effects lead to achieving the objectives and attaining the end state.

Combat Terrorist Networks

An objective of CbT operations may be to influence neutral networks to establish conditions within the OE that make it more difficult for threat networks to conduct attacks. Network engagement is particularly important in CbT, as those operations are intertwined with friendly, neutral, and threat networks

Network Targeting Considerations

Initial analysis provides the commander with the basic justification for targeting a particular network. Refined analysis, which happens continuously throughout staff processes, will provide the commander with a comprehensive targeting plan for specific nodes, links, or other network components. It also includes analysis of other networks, providing potential indicators of second- and third-order effects impacting mission accomplishment.

Target Terrorists and Their Organizations

Using both military and nonmilitary capabilities, JFCs target terrorists and terrorist groups who pose the greatest threat to American citizens and interests. Forces use the find, fix, finish, exploit, analyze, and disseminate process to plan for and execute all CT operations against terrorists, terrorist organizations, and terrorist networks. This process analyzes a terrorist organization structure, capabilities, and intentions to help develop courses of action to eliminate its capability to commit terrorist acts.

Cyberspace Operations in Support of Combating Terrorism

Cyberspace operations are used by insurgents, VEOs, and terrorist organizations as a tool for radicalization and recruitment; a method of propaganda distribution, operational communications, and financial transactions; and a platform for training. The USG has organizations that conduct communications and public diplomacy activities, offensive cyberspace operations, and defensive cyberspace operations. To assist in planning and execution, cyberspace can be described in terms of three interrelated layers: physical network, logical network, and cyber-persona. Each layer represents a different focus from which cyberspace operations may be planned, conducted, and assessed.

Information Considerations for Combating Terrorism

Information activities are key to influencing the target audience and bolstering the legitimacy of CbT. Integrated with US efforts, PNs and HNs conduct operations and information activities to effectively strengthen and defend support for CbT objectives. These operations and activities help isolate terrorists from the public. Military information support operations are an essential part of the DOD psychological operations capabilities required for CbT, in particular, in application of the indirect approach to shape, stabilize, and influence the environment in which terrorist organizations operate. Civil affairs operations also support CbT by gaining civil information through civil reconnaissance, civil engagement, and civil information management to develop the civil component of the supported commander's common operational picture.

Antiterrorism Activities

Operational Context

AT is one of several requirements under a commander's overall responsibility to provide protection. Commanders routinely use a breadth of complementary programs to protect designated personnel, assets, processes, information, and interdependent networks and systems from a variety of threats, including terrorism. AT is not only a sub-element of CbT, it is also a subset of the broader FP construct. While AT programs also integrate various FP-related programs to protect against terrorist attacks, they do not include all aspects of FP. Plans and capabilities developed for AT should be coordinated with

other crisis management efforts to prevent or minimize redundant programs.

Fundamentals of Antiterrorism

As with CT operations, accurate, timely, and relevant intelligence is critical in identifying and assessing terrorist capabilities, plans, intent, emerging trends, magnitude, probable courses of action, and possible targets. By integrating all available sources of intelligence, commanders have the basis for the development of an effective AT program. Enemy capabilities have increased the need for a resilient joint force. The joint force achieves resiliency through professional military education and development, FP measures, depth, exchangeability, interoperability, and dispersal. DOD components, elements, and personnel shall be protected from terrorist acts through a high-priority, comprehensive AT program using an integrated systems approach.

Antiterrorism Intelligence Roles and Responsibilities

Within the United States, the FBI collects and processes terrorist information to protect the United States from terrorist attacks. Overseas, intelligence on terrorist threats is principally a Central Intelligence Agency (CIA) responsibility, but DOS, DIA, and the HN are also participants. DIA's DCTC provides a wide range of intelligence on terrorist threats for DOD components, to include warning intelligence, current intelligence, assessments, in-depth analysis, DOD terrorism threat assessments/levels, and the maintenance of a CbT database. CCDRs, through the intelligence directorate of a joint staff, joint intelligence operations center, command counterintelligence (CI) coordinating authority, and subordinate component command CI and AT organizations, and in consultation with DIA, CIA, the US country team, and applicable HN authorities, collect intelligence and CI information specific to the operational area and issue intelligence and CI reports, advisories, and assessments. DODI 2000.12, *DOD Antiterrorism (AT) Program*, and DODI 2000.26, *Suspicious Activity Reporting (SAR)*, task the Secretaries of the Military Departments to ensure Service component commands have the capability to collect, receive, evaluate, analyze, and disseminate all relevant data on terrorist activities, trends, and indicators of imminent attack and to develop the capability to fuse suspicious activity reports from military security, LE, and CI organizations with national-level intelligence, surveillance, and reconnaissance

collection activities. Service criminal investigative services collect and evaluate criminal information and disseminate terrorist-related information to supported installation and activity commanders, as well as to the Service lead agency.

Antiterrorism Programs

AT programs consist of defensive measures to reduce the vulnerability of individuals and property to terrorist acts, including rapid containment by local military and civilian forces. As a subset of the overarching FP program, the AT program is a collective, proactive effort focused on the prevention and detection of terrorist attacks against DOD personnel and their families, facilities, installations, and infrastructure critical to mission accomplishment, as well as the preparation to defend against and planning for the response to the consequences of terrorist incidents. The minimum elements of an AT program are AT risk management, planning, training and exercises, resource management, and a program review.

Command, Control, Plan, and Assess Antiterrorism Activities and Operations

AT planning is the process of developing specific guidance, measures, and instructions to deter, mitigate, and prepare for a terrorist incident. The AT plan contains command-specific guidance to establish and maintain an AT program as outlined in DODI O-2000.16, Volume 1, *DOD Antiterrorism (AT) Program Implementation: DOD AT Standards.* During the planning process, the JFC should consider the need for exploitation support to help fulfill the requirements for information about the OE, identify potential threats to US forces, and understand the capabilities and capacity of adversary networks.

Organize for Antiterrorism Activities and Operations

A joint task force (JTF) may have several elements supporting CbT. Historically, the JTF provost marshal has been seen as the principal staff advisor to the JTF commander on AT and FP matters. While the provost marshal is a logical choice to provide overall AT matters, other staff sections and individuals play a critical role in establishing an expanded CbT fusion cell or group.

Joint Security Area Antiterrorism Activities

A joint security area is a specific surface area designated by the JFC to facilitate protection of joint bases and their connecting lines of communications that support joint

operations. AT are a large part of the base security plan and consist of defensive measures to reduce the vulnerability of individuals and property to terrorist acts, including rapid containment by local military and civilian forces.

Terrorist Incident Response

The response to a terrorist incident includes procedures established to mitigate the effects of the incident. An important objective of AT incident response is to mitigate the number and severity of casualties resulting from a terrorist attack. Well-developed response measures, to include intermediate force capabilities, employing the use of nonlethal weapons, can save lives, preserve health and safety, protect and secure property, and eliminate the hazard.

Cyberspace Operations in Support of Antiterrorism Operations

The DOD Defense Cyber Crime Center serves as DOD's operational focal point for the Defense Industrial Base Cybersecurity Program that incorporates a voluntary cyberspace threat information sharing and incident reporting program.

Space Operations in Support of Antiterrorism

Space control operations include offensive measures to deceive, disrupt, degrade, deny, or destroy the space systems or services that terrorists may exploit to support their operations. Space control operations also include active and passive measures taken to protect friendly space capabilities from a terrorist attack on any segment of a space system.

Information Considerations for Antiterrorism Activities

Generally, installation commanders inform an internal and external public audience of AT activities. The installation public affairs officer (PAO) supports the commander's AT plan. The installation PAO and AT planners work together to build an information plan.

CONCLUSION

This publication provides fundamental principles and guidance to plan, execute, and assess military activities to combat terrorist threats to US forces, allied and PNs, and foreign and domestic civilian populations through a combined and coordinated application of offensive CT and protective AT activities and operations.

Intentionally Blank

CHAPTER I
INTRODUCTION TO COMBATING TERRORISM

"But above all, we must be united in pursuing the one goal that transcends every other consideration. That goal is to meet history's great test—to conquer extremism and vanquish the forces of terrorism."

President Donald J. Trump Speech at Arab Islamic American Summit, May 2017

1. Overview

a. Terrorism is the unlawful use of violence, or threat of violence, often motivated by religious, political, or other ideological beliefs, to instill fear and coerce governments or societies in pursuit of goals that are usually political. Terrorism is a longstanding illegal and violent tactic, specifically targeting innocent populations, to further terrorist objectives through violence, fear, and intimidation. From the "Reign of Terror" of the French Revolution to the terrorist attacks of September 11, 2001, both state and non-state actors have used terrorist tactics, in one form or another, to achieve mostly political objectives.

b. The challenge for Western-style civil societies is how to effectively deal with these threats while maintaining individual liberty, democratic institutions, and economic freedom. The challenge for the Department of Defense (DOD) and the United States Government (USG) is how to best apply the instruments of national power to defeat terrorists and violent extremist organizations (VEOs) that threaten the United States, its citizens, and its vital interests and protect friendly forces, populations, and allies, while assisting and enabling friendly forces to deter and defeat terrorists. The answer to this challenge is a balanced and integrated approach that maintains an aggressive, offensive counterterrorism (CT) capability coupled with robust and proactive antiterrorism (AT) measures, both relying on a shared common intelligence picture. CT are activities and operations tasked to neutralize terrorists and their organizations and networks to render them incapable of using violence to instill fear and coerce governments or societies to achieve their goals. AT measures are used to reduce the vulnerability of individuals and property to terrorists' acts, to include rapid containment by local military and civilian forces.

c. Too often in the past, commanders, staffs, and policy makers tended to treat CT operations and AT separately. CT was considered a narrow, offensively focused mission area, mainly composed of direct action, targeting individual terrorists and their organizations, and largely the purview of special operations forces (SOF). AT activities, on the other hand, tend to be treated as purely defensive actions nested under the larger force protection (FP) and mission assurance (MA) umbrellas and primarily the purview of the provost marshal's office or civilian law enforcement (LE) agencies. A joint force commander (JFC) should not consider AT and CT unrelated and separate activities but rather as mutually supporting and complementary activities that help defeat terrorists and their organizations while simultaneously enabling and assisting friendly forces and protecting populations from the effects of terrorist attacks. Robust AT activities serve an important, and many times overlooked, deterrent function that, when coupled with

aggressive CT operations, provides an effective counter to terrorism. The key element to both effective CT and AT operations and activities is a comprehensive and integrated intelligence collection and analysis capability which produces a shared understanding of not only local terrorist threats but also transregional threats.

d. This publication emphasizes the relationship and synergy between CT and AT activities and operations by combining these discussions under the broader construct of combating terrorism (CbT). See Chapter III, "Counterterrorism Operations and Activities," for more information on the competition continuum.

2. Strategic Context

a. **Threat.** Individual terrorists and VEOs are potentially grave dangers to the national security and interests of the United States, at home and abroad. Additionally, some traditional criminal activities, such as counterfeiting or illegal drug trafficking, may be terrorist-related if used to fund terrorist acts. Terrorists use many forms of unlawful violence or threats of violence to further a variety of political, social, criminal, economic, and religious ideologies. Terrorism threatens the national power, sovereignty, and interests of the United States and allies and partner nations (PNs). Terrorists organize and operate in many ways—some operate within transnational networks; others operate as small, independent groups; and others operate alone. The terrorist threat is amplified by the Internet; social media; commercially available, advanced technologies; and the proliferation of weapons of mass destruction (WMD) and their potential use by terrorists. Additionally, within the United States, an increasing trend is the growth of homegrown violent extremists (HVEs), which includes those who have become ideologically radicalized. The United States strives to enlist the support of the international community, adapt alliances, and create new partnerships to facilitate regional solutions that stem the growth of terrorism and contain and defeat terrorists, their organizations, and their networks.

b. **Trends.** The increasingly transregional and complex problem of CbT frustrates area of responsibility (AOR)-specific planning efforts and operations, national policy and strategy, and cooperation with PNs. Trends in the strategic environment (e.g., the rapid evolution and spread of technology, increased global connectivity, erosion of state sovereignty, and shifting population affiliation identities) require the United States to revalidate its assumptions about CbT and the methods to address existing and emerging threats. The influence of rapidly evolving strategic trends has produced a greater diversity of terrorists, networks, and enablers, resulting in an increased potential for coercion or attack against the United States or its interests. Addressing strategic environmental trends and the ever-evolving terrorist threat requires an approach that disrupts threat pathways and generates shared awareness, active assessment, and coordinated activities (both offensive and defensive) across DOD and with interagency partners. Additionally, awareness of strategic trends, evolving terrorist tactics, and advancements in technology will enable commanders to set in-place protective measures to better thwart terrorist attacks and mitigate the effects of an attack if it should occur. Strategic trends provide the context for understanding the evolving characteristics of terrorism. The exponential growth and

spread of technology places significant capability in the hands of greater numbers of actors, especially in the case of WMD, which is a significantly more destructive capability.

(1) Global connectivity expands access to ideas and resources across borders and geographical divides. The erosion of state sovereignty leads to an increased number of empowered non-state actors capable of vying for influence over, and competing with, states on a number of levels. Also, the convergence of new social networks and non-state actors leads to increasingly unfamiliar and unpredictable relationships and interactions between state and non-state actors. These trends confound our efforts to decide how best to apply resources transregionally to counter terrorism threats. Moreover, increased global connectivity via cyberspace and human networks improves the ability to collaborate and share expertise across great distances and access resources in the most remote parts of the planet.

(2) This increased connectivity challenges countermeasures by overwhelming the ability to identify and respond to it. This trend enables potential terrorist threats to move transregionally and globally—beyond the confines of any borders or regional demarcations. When combined with emerging technologies (e.g., three-dimensional printing), this evolution of terrorist capabilities demands adaptive approaches to keep pace. Adding to the expansion of technology and interconnectivity, the erosion of state sovereignty and shifting population identities has given rise to increasingly empowered and unfamiliar non-state actors with state-like powers. State monopolies on setting the rules of behavior and establishing international norms are being contested by multinational corporations, supranational organizations, and VEOs. These recently emerged, non-state entities offer little history or familiarity for assessing behavior and intentions and oftentimes have no observable territory in which to monitor activity. Understanding the behaviors and motives of these new entities will become increasingly important to understanding the problem and designing the right approach to address it.

c. **Approach.** In the past, traditional approaches to CbT (domestic and regional security operations) have worked to adequately contain known threats, but they were largely focused on threats within the confines of a specific combatant command's (CCMD's) AOR and did not sufficiently address the increasingly transregional and global aspects of emerging terrorist operations and trends.

(1) With increasing advancements in global communications and social network interactions between heretofore disparate groups and individuals, a globally accessible 24-hour news cycle, and the unhindered availability of advanced technology, the world has become smaller and populations more vulnerable to extremist influence. The lack of shared awareness and dialogue about terrorist threats and activities between CCMDs, international partners, LE agencies, and the private sector have fostered AOR-specific approaches that often stop at the boundary and not the terminus of the threat network. Furthermore, without a unified understanding of campaign activities at the tactical, operational, and strategic levels, departmental coordination with interagency partners becomes disjointed and fragmented.

(2) The joint force coordinates with and operates in support of interagency partners and PNs to dissuade individuals and groups from turning to terrorist tactics and to disrupt

terrorist development and employment of capabilities that create lethal effects. As such, DOD must seek to build closer relationships at the tactical, operational, and strategic levels to ensure its efforts complement diplomatic, intelligence, and LE efforts and do not duplicate or disrupt them. Similarly, efforts to detect and disrupt terrorist capability development are greatly enhanced when the United States leverages the aid of PNs. Besides traditional partners, a JFC should explore opportunities to work cooperatively with nontraditional partners such as private businesses and nongovernmental organizations (NGOs).

(3) Efforts to deter, delay, degrade, disrupt, and defeat or defend against terrorist actions and their organizations must address the entirety of threat networks and pathways. The supply and demand characteristics of threat pathways mean any transfer involves a minimum of two nodes and conveyance across a virtual or physical route. Both the sender and receiver within a pathway are vulnerable to discovery, disclosure, and, ultimately, targeting by friendly forces. In transit along pathways, information and things are susceptible to interception and manipulation. Monitoring and disrupting along the entirety of the pathways increases the likelihood of success.

3. Combating Terrorism Activities

a. **Background.** Historically, CbT has been both a battle of arms and ideas against terrorists and the ideology that drives them. CbT are actions, including AT and CT, taken to oppose terrorism throughout the competition continuum. DOD, along with other USG organizations, PN, and allies, strives to prevent terrorist ideology from spreading, protect societies from terrorist violence, and maintain a strong capability to directly target terrorists. CbT remains an approach with defensive and offensive components. AT activities are used to reduce the vulnerability of individuals and property to terrorist acts. AT activities include containment of terrorist activities by local military and civilian forces. CT operations are executed to neutralize individual terrorists, terrorist organizations, and their networks to render them incapable of using terrorist tactics to kill innocent people, instill fear, and coerce governments or societies to achieve their objectives. The vignette, "A Pathogenic Approach to Combating Terrorism," that follows, offers a comparison between terrorism and pathogenic disease to illustrate a long-term balanced proactive approach to CbT.

b. **DOD CbT Approach.** DOD uses a comprehensive, prioritized, life-cycle approach to CbT (see Figure I-1). This approach aims to diminish contributing root causes of terrorism, discredit violent extremists, disrupt terrorist enablers, degrade or defeat terrorist organizations, and defend targets from terrorists to protect the US homeland, citizens, and vital interests and US allies and partners against terrorist acts.

c. **Supporting Activities.** Critical supporting activities of CbT operations are intelligence support, information sharing, and incident management, which, together, serve to support and link AT and CT in the achievement of common strategic objectives (see Figure I-2). Other defensive and offensive elements that overlap in the operational environment (OE) are FP, personnel security, operations security (OPSEC), continuity of operations (COOP), countering weapons of mass destruction (CWMD), and defense critical infrastructure (DCI) protection. Identity activities, consisting of identity exploitation operations (document and media exploitation, forensics, and biometrics) and

A PATHOGENIC APPROACH TO COMBATING TERRORISM

Violent extremism and terrorism are "memetic"--communicable ideas and actions--wherein societies are the infected hosts, and violent extremist organizations and individual terrorist are the pathogens.

If one takes this pathogenic approach to combating terrorism (CbT) and systematically applies a balance of simultaneous preventive (antiterrorism) and pro-active invasive (counterterrorism) measures, the Department of Defense can begin to develop a more effective long-term terrorism prevention, mitigation, and perhaps potential eradication objectives. Additionally, like pathogens, terrorism can spread from one host to another. In the case of terrorism, afflicted victims are nations, civil societies, or individuals. However, just as with a pathogen, terrorist tactics and motivations may mutate into heretofore new areas such as artificial intelligence or genetic engineering technology.

Terrorist ideologies take root when societal conditions foster radicalization of a few people who believe that only violent extremist actions can cure perceived societal ills. CbT activities and operations play a similar role as preventive medicine and invasive surgical measures. Security cooperation, foreign internal defense, and civil-military operations help build resilient and secure societies, partners, and allies. Intelligence support to CbT, akin to advance to medical diagnostics, aids in early detection, identification, and prevention of terrorist threats.

Ideally, military actions must ultimately support programs leading to societal reform by promoting security and defeating terrorist efforts to recruit and radicalize new adherents. Just as in disease prevention and treatment, to be most effective, CbT activities not only require focus on potentially infected parties, they also require nations and societies to help themselves; this requires patience and persistence across generations to ultimately eradicate terrorists and the ideologies that drive them.

Various Sources

identity intelligence (I2) derived from those activities and operations, are critical supporting activities, before and after a terrorist incident.

See Joint Publication (JP) 3-40, Countering Weapons of Mass Destruction, *for more information on CWMD.*

4. Combating Terrorism Organizations, Responsibilities, and Authorities

a. **National Security Council (NSC).** The NSC manages the interagency process concerning CT and all national security-related issues and specific, selected action. The interagency process advances the President's policy priorities and serves the national interest by ensuring all agencies and perspectives that can contribute to achieving these priorities participate in making and implementing policy. The NSC is the key integrator of the President's whole-of-government CT policy and strategy, which requires

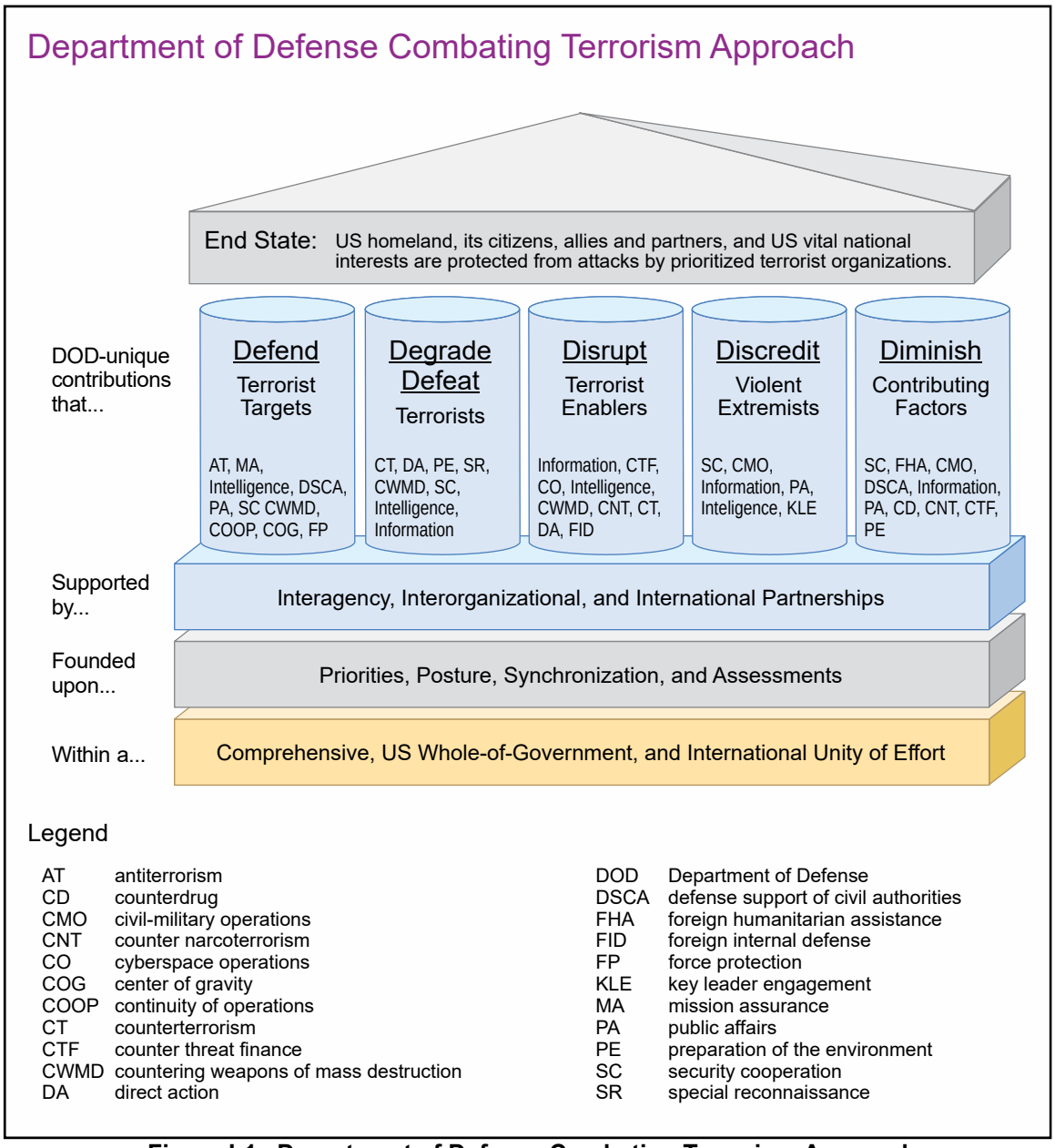


Figure I-1. Department of Defense Combating Terrorism Approach

interagency coordination at the Principals Committee, Deputies Committee, supporting interagency policy coordination committees, and the efforts of the NSC Staff. The President chairs the NSC. Its regular attendees (both statutory and non-statutory) are the Vice President, Secretary of State (SECSTATE), Secretary of the Treasury, Secretary of Defense (SecDef), and Assistant to the President for National Security Affairs. The Chairman of the Joint Chiefs of Staff (CJCS) is the statutory military advisor to the NSC, and the Director of National Intelligence is the intelligence advisor. The chief of staff to the President, counsel to the President, and the Assistant to the President for Economic Policy are invited to attend any NSC meeting. The Attorney General and the Director of the Office of Management and Budget are invited to attend meetings pertaining to their responsibilities. The heads of other executive departments and agencies, as well as other senior officials, are

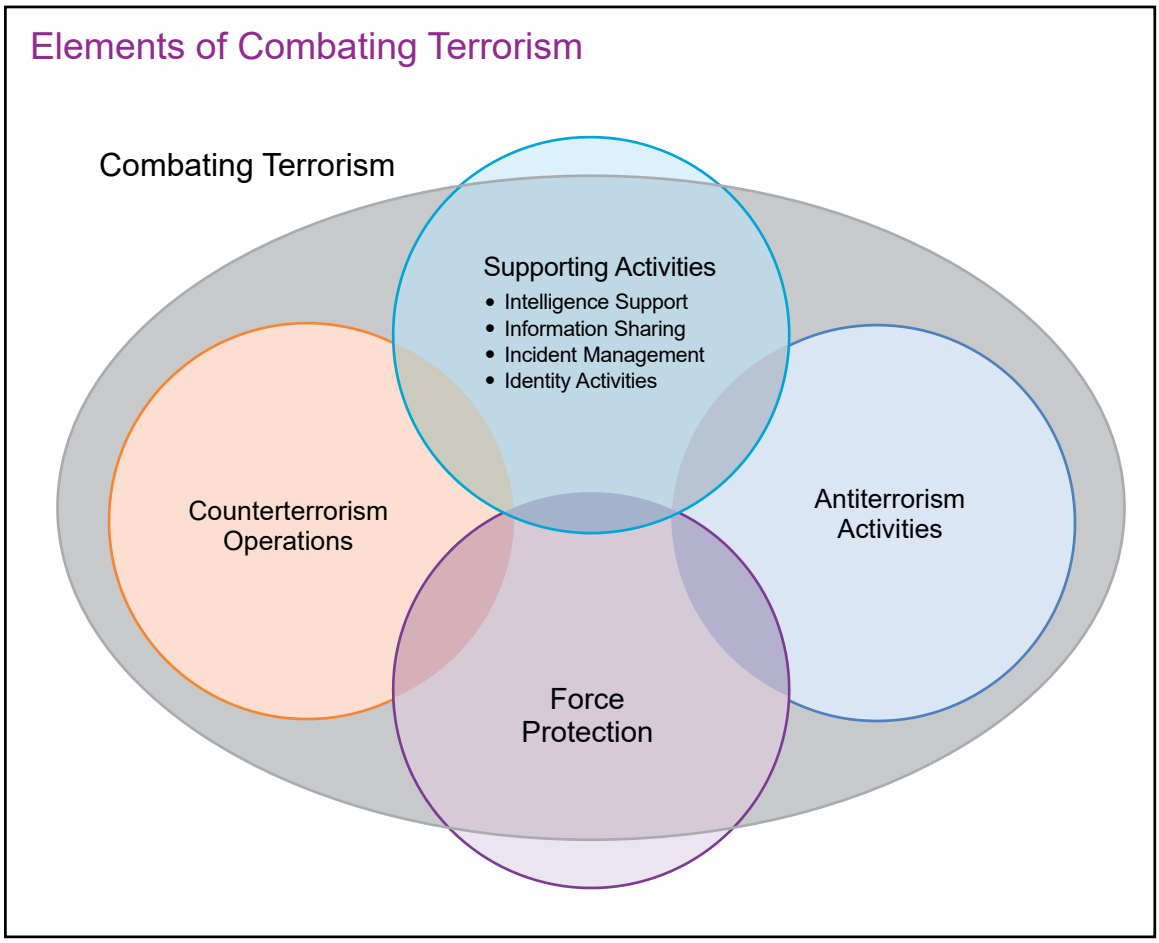


Figure I-2. Elements of Combating Terrorism

invited to attend meetings of the NSC when appropriate. The NSC manages the interagency process with respect to CT and all national security-related issues and certain selected actions. The interagency process is designed to advance the President's policy priorities and to serve the national interest by ensuring all agencies and perspectives that can contribute to achieving these priorities participate in making and implementing policy. The key interagency policy committee of CT is the Counterterrorist Security Group, which is led by the Assistant to the President for Homeland Security and Counterterrorism.

b. **Homeland Security Council (HSC).** The HSC is an entity within the White House Office created in 2001. It served as the successor to the Office of Homeland Security, established on September 20, 2001, immediately after the September 11, 2001, attacks. Congress subsequently codified the HSC in the Homeland Security Act of 2002, charging it with advising the President on homeland security (HS) matters. In 2009, the HSC and NSC staffs were merged into one, the National Security Council Staff. The HSC and NSC continue to exist by statute as independent councils of leadership advising the President. The HSC coordinates across a broad spectrum of federal, state, local, and private-sector entities to reduce the potential for terrorist attacks and other threats and mitigates damage should an incident occur.

c. **USG**

(1) **Department of Homeland Security (DHS).** DHS leads the unified national effort to secure the United States. Key among its strategic goals is to prevent, protect against, respond to, and recover from acts of terrorism. DHS, in conjunction with other USG departments and agencies, plays a crucial role in the protection of critical infrastructure. Critical infrastructure describes the physical and cyberspace systems and assets that are so vital to the United States that their incapacity or destruction would have a debilitating impact on our physical or economic security or public health or safety. The nation's 16 critical infrastructure sectors (see Figure I-3) provide the essential services that underpin American society. DHS provides strategic guidance to public and private partners, promotes unity of effort, and coordinates the overall USG effort to promote the

Critical Infrastructure Sectors

Sector	Sector-Specific Agency
Chemical	Department of Homeland Security
Commercial Facilities	Department of Homeland Security
Communications	Department of Homeland Security
Critical Manufacturing	Department of Homeland Security
Dams	Department of Homeland Security
Defense Industrial Base	Department of Defense
Emergency Services	Department of Homeland Security
Energy	Department of Energy
Financial Services	Department of the Treasury
Food and Agriculture	Department of Agriculture and Department of Health and Human Services
Government Facilities	Department of Homeland Security and Government Services Administration
Public Health and Healthcare	Department of Health and Human Services
Information Technology	Department of Homeland Security
Nuclear Reactors, Materials and Waste	Department of Homeland Security
Transportation Systems	Department of Homeland Security and Department of Transportation
Water and Wastewater Systems	Environmental Protection Agency

Figure I-3. Critical Infrastructure Sectors

security and resilience of the nation's critical infrastructure. Presidential Policy Directive-21, *Critical Infrastructure Security and Resilience*, advances a national policy to strengthen and maintain secure, functioning, and resilient critical infrastructure. The term "sector-specific agency" refers to the USG department or agency designated under Presidential Policy Directive-21, *Critical Infrastructure Security and Resilience*, that provides institutional knowledge and specialized expertise, as well as leading, facilitating, or supporting the security and resilience programs and associated activities of its designated critical infrastructure sector in the all-hazards environment.

(2) **Department of State (DOS).** As the lead US foreign affairs agency, DOS formulates, represents, and implements the President's foreign policy. SECSTATE is the President's principal advisor on foreign policy and the person chiefly responsible for US representation abroad, except for regions where the responsibility lies with the military commander as designated by the President. DOS has six regional bureaus that address foreign policy considerations on a regional basis. The assistant secretaries of the regional bureaus are key leaders in CT activities, policy, and operations in their assigned regions. Furthermore, the DOS Bureau of Counterterrorism publishes an annual country report on terrorism and manages US policy for a whole-of-government approach to CT. The DOS Bureau of Counterterrorism maintains the Foreign Terrorist Organizations List that provides justification for the President to block or freeze tangible property and freeze financial accounts of individuals or terrorist organizations pursuant to Executive Order (EO) 13224, *Blocking Property and Prohibiting Transactions With Persons Who Commit, Threaten to Commit, or Support, Terrorism.* This tool is designed to sever terrorist organizations' logistics and resources. These efforts are worked through PNs where the United States maintains country teams under the leadership of chiefs of mission (COMs).

(3) **COM.** The COM is the personal representative of the President and the official USG representative in the host nation (HN). The COM is responsible for the conduct of relations with the host government and is the primary channel for communications with that government. The COM directs, coordinates, and supervises all USG executive branch employees in that effort, except those under the command of a US military commander. CT activities and operations conducted by DOD and other USG departments and agencies require COM concurrence prior to execution, unless otherwise directed by the President.

(4) **Department of Justice (DOJ).** The Attorney General investigates acts or incidents that may constitute a violation of federal laws related to acts of terrorism or the use or threatened use of WMD. This authority is exercised through the Federal Bureau of Investigation (FBI). The Attorney General, generally acting through the FBI, in coordination with SECSTATE and the COM, will assume lead responsibility for the LE investigation of terrorist or WMD incidents abroad. The FBI's tasks may include taking custody of suspected terrorists, lawful transfer of custody of suspected terrorists, forensic examination of material collected of possible intelligence or criminal prosecution value, and hostage negotiation support.

(5) The **US Department of the Treasury**'s role in CT is to lead the USG efforts to locate, track, and seize suspected terrorist financial assets. The US Department of the

Treasury may use a variety of presidential, statutory, and regulatory authorities, including economic and financial sanctions. For threats not responsive to diplomatic outreach and not suitable for military action, the US Department of the Treasury's economic and financial capabilities often provide unique tools to contribute to CT policy and strategies.

(6) **National Counterterrorism Center (NCTC)**

(a) The NCTC is aligned under the Office of the Director of National Intelligence. The mission of the NCTC is to analyze terrorist threats, share information with PNs, and integrate all instruments of national power to ensure unity of effort. The NCTC also provides assistance to the operational elements of the USG that disrupt, isolate, and dismantle terrorist organizations and prevent future attacks.

(b) The NCTC is staffed by personnel from multiple USG departments and agencies. The NCTC serves as the primary organization in the USG to integrate and analyze all intelligence pertaining to CT, except for information pertaining exclusively to domestic terrorism. It serves as the USG's central and shared database on known and suspected terrorists and international terrorist groups. The NCTC also provides USG departments and agencies with intelligence analysis on terrorist threats and other information.

(c) The NCTC conducts strategic planning for CT activities across the USG, integrating all instruments of national power to ensure unity of effort. The NCTC ensures effective integration of CT plans and synchronization of operations across more than 20 USG departments and agencies conducting CT efforts.

(d) The NCTC maintains the authoritative database of all known or suspected terrorist identifiers maintained by the USG. This feeds the National Known or Suspected Terrorist Watch List maintained by the Terrorist Screening Center and disseminated to front-line screening organizations, like Customs and Border Patrol, Consular Affairs, and state and local LE. Complete and accurate collection of identity data (e.g., biometric, biographic, and behavioral attributes) and derogatory information is critical to supporting nominations to the National Known or Suspected Terrorist Watch List.

(7) **National Joint Terrorism Task Force (NJTTF).** The NJTTF is an interagency coordination organization that provides liaison from FBI headquarters (HQ) to local joint terrorism task forces and participating agencies and serves as a conduit for information on threats and leads. It is located in the NCTC, where it also works with NCTC personnel to analyze data and plan AT strategies. The NJTTF shares information among its 80 members—officers, agents, and analysts—who then pass the information onto the 48 different agencies they represent, from the LE, intelligence, HS, defense, diplomatic, and public safety sectors, including DHS; the US military; and federal, state, and local partners.

(8) **DOD.** Within DOD, CT activities and operations are normally executed by combatant commanders (CCDRs), subordinate theater special operations command (TSOC) commanders, and other JFCs. Conventional forces (CF) and SOF each bring certain competencies to CT efforts. CF and SOF skills and capabilities complement each other. The scope, intensity, and duration of each specific operation will dictate the missions

to be accomplished, and the JFCs must determine the right joint force mix to employ. CF and SOF each possess unique capabilities that can produce even greater warfighting potential for the JFCs when integrated into a holistic global CT campaign with numerous theater CT operations. Critical capabilities in CT are I2, biometrics, forensics, and document and media exploitation. Flexible command and control (C2); specific mission-generation processes; clear mission approval levels; and the integration of all appropriate partners at the strategic, operational, and tactical levels improve the CT effectiveness of both CF and SOF. CT is a core task of SOF, but global demand for CT activities and the varied conditions under which the broad range of CT activities occur dictate that SOF cannot be the sole force conducting CT operations.

(a) **CCDRs.** As the principal JFCs responsible for CT activities and operations, CCDRs detect, deter, and prevent attacks against the United States, its territories, and its bases and employ appropriate force to defend the nation should deterrence fail. The CCDR is also the single point of contact for military matters within the assigned AOR or global functional responsibility, excluding areas within the United States.

(b) A TSOC is a subordinate unified command, under combatant command (command authority) (COCOM) of Commander, United States Special Operations Command (CDRUSSOCOM). It is the primary theater special operations organization capable of performing synchronized, continuous CT activities and operations. It is the organization through which a CCDR exercises C2 of attached SOF. SecDef has delegated operational control (OPCON) of TSOCs and attached SOF tactical units to their respective CCDRs via the *Global Force Management Implementation Guidance.* The CCDR may exercise OPCON of subordinate forces directly through the TSOC or a special operations command-forward (SOC-FWD), which is a small, scalable, operational-level HQ that provides a forward-deployed, persistent presence and C2 capability. If conditions warrant larger special operations, a SOC-FWD can transition to a joint task force (JTF) called a special operations JTF. The SOC-FWD develops a close working relationship with members of the country team, PN armed forces, and HN security forces and helps the TSOC commander execute their role as a JFC and theater special operations advisor.

(c) **United States Special Operations Command (USSOCOM)**

1. USSOCOM is a CCMD with global responsibilities. CDRUSSOCOM exercises coordinating authority for planning global operations against VEOs and for planning DOD CWMD efforts, in coordination with other CCDRs, the Services, and, as directed, other USG departments and agencies. During the conduct of global operations against VEOs and DOD CWMD efforts, CDRUSSOCOM is normally a supporting commander to the CCDR in whose AOR the operations occur. While CT is a core task of SOF, global demand for SOF actions, and the varied conditions under which the broad range of SOF activities occur, dictate that SOF cannot be the sole force conducting CT operations.

2. The Service component commands and other subordinate commands of USSOCOM have assigned and attached subordinate units and may deploy to support a CCDR's training, exercises, activities, and operations.

3. In addition to the responsibilities assigned in Title 10, United States Code (USC), Section 167, CDRUSSOCOM is responsible for the planning and execution of global special operations activities and missions, as directed, in coordination with or in support of other CCMDs, the Services, DOD agencies, and, as directed by the President or SecDef, other USG departments and agencies. These responsibilities include the following tasks:

a. Integrate DOD strategy, plans, and intelligence priorities for operations against VEOs and other threat networks.

b. Integrate DOD plans and intelligence priorities to support operations against state and non-state networks that possess or seek WMD.

c. Plan preparation of the environment (PE) and, as directed, execute PE in coordination with other CCDRs.

d. Execute operations against VEOs and other threat networks, as directed, and execute global operations against state and non-state networks that possess or seek WMD, in coordination with other CCMDs, as directed.

See JP 3-05, Special Operations, *for a detailed description of SOF core activities.*

(d) The Defense Intelligence Agency (DIA) Defense Combating Terrorism Center (DCTC), in accordance with Department of Defense Instruction (DODI) 2000.12, *DOD Antiterrorism (AT) Program*, serves as the lead national-level, all-source, international terrorism intelligence effort within DOD and the analytic lead and mission manager for CbT analysis pertaining to domestic and international terrorist threats to DOD elements and personnel (excluding threats posed by US persons who have no foreign connections). DCTC operates the Defense Terrorism Threat Warning System, disseminating intelligence on international terrorist threats, including warning of specific threats, against DOD elements and personnel. DCTC functions as the DOD intelligence lead for the intelligence community (IC) terrorist watch-list effort in support of Homeland Security Presidential Directive (HSPD)-6, *Directive on Integration and Use of Screening Information to Protect Against Terrorism,* and National Security Presidential Directive (NSPD)-59/HSPD-24, *Biometrics for Identification of Screening to Enhance National Security*. DCTC operates a 24-hour terrorism intelligence Warning and Fusion Center as the CT adjunct to the National Joint Operations and Intelligence Center, ensuring terrorist threat intelligence is disseminated to the appropriate DOD components.

(e) DOD counter threat finance (CTF) activities and capabilities. Per Department of Defense Directive (DODD) 5205.14, *DOD Counter Threat Finance (CTF) Policy,* USSOCOM is the lead component for synchronizing DOD CTF activities. The CCDRs are responsible for DOD CTF activities within their AORs or functional areas. CTF cells, while complying with all USG authorities and procedures, deny, disrupt, destroy, or defeat finance systems and networks that negatively affect US interests. To see the breakdown of CTF and threat finance intelligence cell actions and activities, refer to JP 3-25, *Countering Threat Networks.* This includes those activities and capabilities undertaken with other USG departments and agencies and PNs. DOD CTF counters

financing used to support terrorist activities and illicit networks that traffic narcotics; WMD; improvised explosive devices (IEDs); other weapons, persons, and precursor chemicals; and related activities that support an adversary's ability to negatively affect US interests. Threat finance intelligence cells are charged with providing all-source intelligence related to illicit financial networks globally. The Under Secretary of Defense for Intelligence is the lead component for threat finance intelligence.

1. The majority of DOD CTF cells are currently funded by the Office of the Deputy Assistant Secretary of Defense for Counternarcotics and Global Threats, which places the focus of their CTF activities under Title 10, USC, Section 284, and CT-related support under Title 10, USC, Section 271, to conduct CT actions and activities with counter narcotics funding. Under these authorities, CTF cells are principally aligned to provide support, when requested, to other USG departments and agencies, along with PNs.

2. Military forces under Title 10, USC, have authority to pursue a broader selection of CTF activities more directly in alignment with JFC CT priorities. Military support to CTF is not limited to a distinct type of military operation action or activity; rather, it can draw on a wide array of operations to create desired effects on a terrorist organization's financial network. Military personnel do not conduct CTF directly. Rather, they take actions to support USG departments and agencies with the authority to affect terrorist financial nodes. These actions are the essence of CTF.

3. In support of CbT operations, CTF can reduce or eliminate the terrorist organization's operational capability by affecting its means to pay members, procure weapons and supplies, collect intelligence, project force, or recruit new members. In addition to CbT operations, CTF supports military operations and activities such as:

a. **Security Cooperation (SC).** US CTF personnel, while participating in foreign internal defense (FID) activities, can provide training on CTF to PN and HN LE, as well as provide CTF capabilities as a defense-related service under SC with specific authorities to assist nations in CbT.

For additional information, refer to JP 3-20, Security Cooperation, and *JP 3-22,* Foreign Internal Defense.

b. **Enforcement of Sanctions.** CTF encompasses all forms of value transfer, not just currency. DOD organizations can provide assistance to other USG departments and agencies that are interdicting the movement of goods and any associated value remittance in support of terrorism as a means to enforce sanctions against desired DOD-targeted individuals, entities, or nations involved.

c. **Counterinsurgency Operations.** CTF can be used to counter, disrupt, or interdict the flow of resources to an insurgency. Insurgent groups tend to lean toward terrorist-type activities, or attempt to affiliate themselves with terrorist organizations, to gain legitimacy or influence. Additionally, CTF can be used against corruption, as well as drug and other criminal revenue-generating activities that fund or

fuel insurgencies and undermine the legitimacy of the HN government. For more information, refer to JP 3-24, *Counterinsurgency*.

d. **DOD Support to Counterdrug Operations.** The US military may conduct training of PN/HN security and LE forces to assist in intelligence collection and the detection, monitoring, and communication of movements outside the geographic boundaries of the United States. Disrupting the flow of drug profits via CTF may also expose vulnerabilities in terrorist organizations' financial infrastructures, which often use narcotics as a means to generate operational funding.

e. Figure I-4 shows a notional criminal/terrorist enterprise business model and highlights potential targeting opportunities. For more information on CTF operations, see the Joint Staff J-7 [Joint Force Development] *Commander's Handbook for Counter Threat Finance* at https://jdeis.js.mil/jdeis/index.jsp?pindex=124&catindex=16.

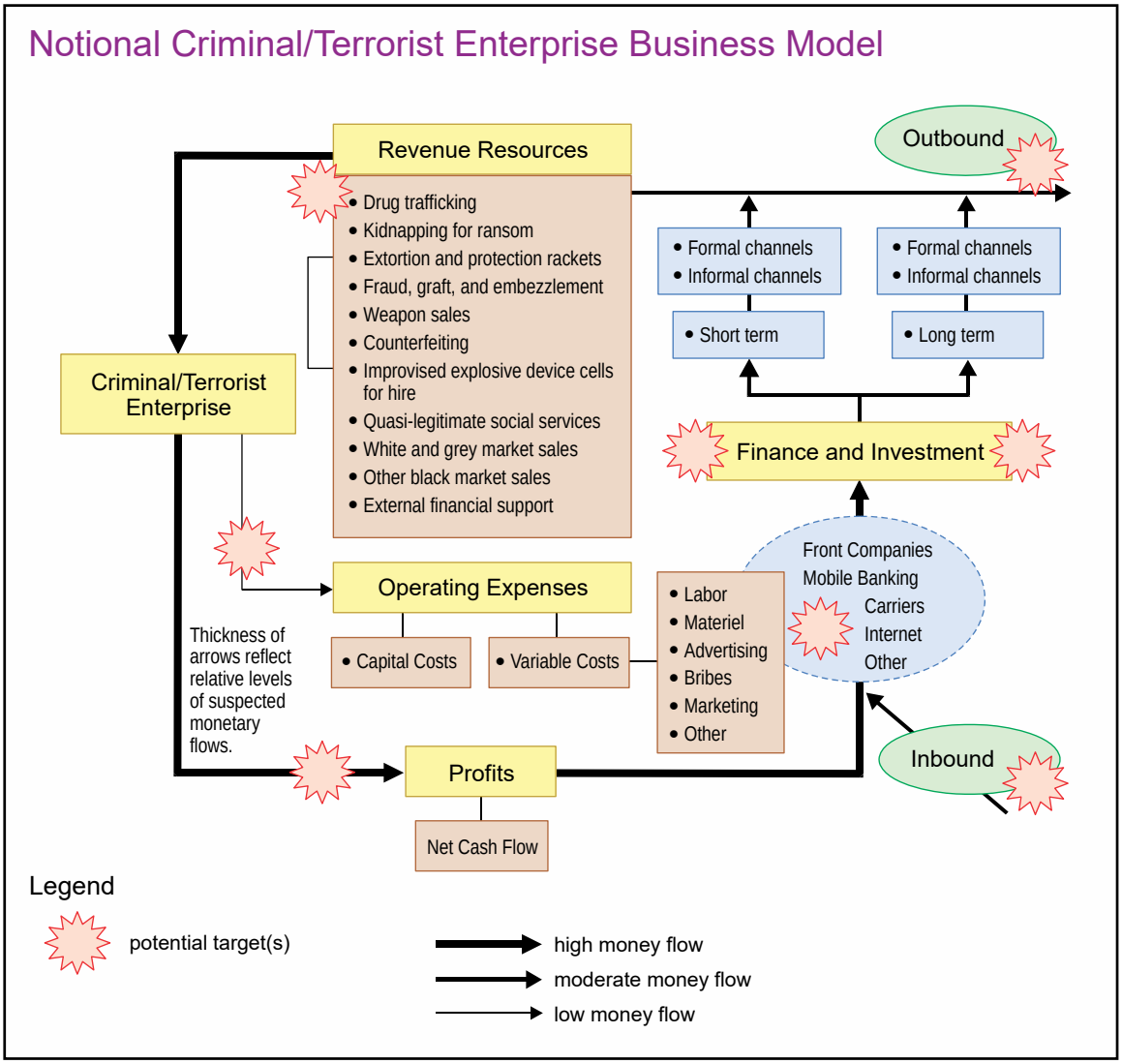


Figure I-4. Notional Criminal/Terrorist Enterprise Business Model

CHAPTER II
TERRORIST THREAT

1. Terrorist Organizational Structure, Membership, Networks, and Functions

General knowledge of prevalent terrorist organizational structures helps leaders to understand their capabilities and the types of threats they pose. A terrorist organization's structure, along with membership, resources, and security, determine, in part, its capabilities, influence, and reach. Terrorist groups, regardless of ideology, location, or structure, have common organizational imperatives—the need to survive and to pursue the goals of the organization, while remaining credible to their followers.

a. **Basic Organizational Structure.** Terrorist groups typically utilize one of two types of organizational structures: hierarchical or networked. Within either of those two larger organizational structures, however, virtually all terrorist groups organize as smaller cells at the tactical level. Typically, there are four different levels of commitment within a terrorist organization. Leaders of the organization provide direction and policy, approve goals and objectives, and produce overarching guidance for operations. The zealots of a terrorist organization, who not only plan and conduct operations but also manage technology, intelligence, finance, logistics, information activities, and communications, can be considered cadre. Active supporters participate in the political, fund-raising, and information activities of the group, while passive supporters are typically individuals or groups that are sympathetic to the announced goals and intentions of the terrorist organization but are not committed enough to take action.

b. **Hierarchical Structure.** These organizations have a well-defined vertical chain of command and responsibility. Information flows up and down organizational channels that correspond to these vertical chains but may not move horizontally through the organization. Hierarchies are traditional and common to larger groups that are well established with a command and support structure. Hierarchical organizations feature greater specialization of functions in their subordinate cells (support, operations, intelligence). In the past, some significant "traditional" terrorist organizations influenced by revolutionary theory or Marxist-Leninist ideology used this structure: the Japanese Red Army, the Red Army Faction in Germany, the Red Brigades in Italy, the Palestine Liberation Organization, the Provisional Irish Republican Army (IRA), the Weather Underground, the Symbionese Liberation Army, and the New World Liberation Front. These organizations had a clearly defined set of political, social, or economic objectives and tailored aspects of their organizations (such as a "political" wing or "social welfare" group) to facilitate their success. The necessity to coordinate actions between various "fronts," some political and allegedly nonviolent, and the use of violence by terrorists and some insurgents favored a strong hierarchical structure. The benefits of hierarchies include greater efficiency due to specialization and the ability to coordinate actions toward a common goal.

c. **Networked Structure.** Unlike hierarchies, networks distribute authority and responsibility throughout an organization, often creating redundant key functions. Effective networks require a unifying idea, concern, goal, or ideology. Without a unifier,

networks may take actions that are counterproductive, and independent nodes may not develop the necessary cohesiveness for the success of the network. General goals and targets are announced, and individuals or cells with redundant capabilities are expected to use flexibility and initiative to conduct the necessary actions.

(1) Networks with cell structures allow anonymity of individuals operating throughout the organization. Only a limited number of people within a cell may have full visibility of the entire organization. The various cells do not need to contact other cells, except for cells essential to a particular operation with which they are working in common. The avoidance of unnecessary coordination or command approval for action provides deniability to the leadership and enhances OPSEC. Furthermore, breaches in security do not paralyze or cripple the entire organization.

(2) Terrorist groups are now increasingly part of a far broader but indistinct system of networks than previously experienced. Rapid changes in leadership, whether through a generational transition, internal conflict, or attrition or as a response to enhanced security operations, may signal significant adjustments to terrorist group organizational priorities and capabilities.

(3) A network structure may be a variation of several basic nodal constructs: a node being an individual, a cell, another networked organization, or even a hierarchical organization. A terrorist network may consist of parts of other organizations (even governments), which are acting in ways that can be exploited to achieve the network's organizational goals. Networks need not be dependent on the latest information technology (IT) to be effective. The organizational structure and the flow of information inside the organization (i.e., their information management plan) are the defining aspects of networks. While IT can make networks more effective, low technology means, such as couriers, often provide a simple and redundant means of communication that is less vulnerable to compromise or surveillance.

(4) **Networks Terminology.** A threat network consists of interconnected nodes and links and may be organized using subordinate and associated networks and cells. Understanding the individual roles and connections of each element is as important to conducting operations as is understanding the overall network structure, known as the network topology. The overall structure, as it has formed over time and adapted to its environment, impacts the behavior of the networks, nodes, and cells. The strength and number of links provide the initial insight into network capabilities, strengths, weaknesses, and centers of gravity (COGs). Network boundaries must also be determined, especially when dealing with overlapping networks and global networks. Operations will rarely be possible against an entire threat or its supporting networks. Understanding the network topology allows planners to develop an operational approach and associated tactics necessary to create the desired effects against the network.

(a) **Network.** A network is a group of elements consisting of interconnected nodes and links representing relationships or associations. Sometimes, the terms network and system are synonymous. This publication uses the term network to distinguish threat

networks from the multitude of other systems, such as an air defense system, communications system, and transportation system.

(b) **Cell.** A cell is a subordinate organization formed around a specific process, capability, or activity within a designated larger organization.

(c) **Node.** A node is an element of a network that represents a person, place, or physical object. Nodes represent tangible elements within a network or OE that can be targeted for action. Nodes may fall into one or more political, military, economic, social, information, and infrastructure categories.

(d) **Link.** A link is a behavioral, physical, or functional relationship between nodes. Links help the JFC and staff visualize the internal nodal functions and interactions with other nodes such as command or supervisory arrangements that connect a superior to a subordinate, the relationship of a source of weapons to an arms dealer, and the ideology that connects a propagandist to a group of terrorists. Links establish the interconnectivity between nodes that enables them to work together as a network—to behave in a specific way (accomplish a task or perform a function). Nodes and links are useful in identifying COGs, networks, and cells the JFC may wish to influence or change during an operation.

For more information on threat networks, see JP 3-25, Countering Threat Networks.

2. Lone Terrorists

a. As compared with a typical networked or hierarchical terrorist organization, lone terrorists, or "lone wolves" as they are commonly referred to, are often the hardest to detect, which presents a formidable challenge for JFCs, LE, and intelligence agencies. The lone terrorist's tactics are conceived entirely on his or her own without any direction from a terrorist commander. Typically, the lone terrorist shares an ideological and sympathetic identification with an extremist organization and its goals and may have had some limited level of direct affiliation in the past, but the lone terrorist does not communicate with any group when fashioning political aims and committing acts of terrorism. Notably, it can be difficult to distinguish between a lone terrorist aiming for political results and another criminal, such as a serial killer, who utilizes the same tactics. Traditional CT measures, such as military, economic, and diplomatic actions, will not work against the lone terrorist, nor will travel bans from various countries, since lone terrorist attacks are as likely to originate from individuals already residing in the United States as they are to come from recent immigrants. Lone terrorists cut across the entire political and religious spectrum. There are Islamic extremist lone terrorists and white supremacist lone terrorists. There are "single-issue" lone terrorists who act in the name of a particular issue (e.g., anti-abortion, environmental, or animal rights). There is also the "wild card" lone terrorist, namely the idiosyncratic lone wolf who uses ideology, real or self-created, to justify their actions.

b. Another characteristic of lone terrorists is their immunity from group decision making. Group decision-making processes or inter-group dynamics can sometimes stifle creativity in formulating plans and operations. Therefore, lone terrorists are free to develop any scenario and act upon it since they are only accountable to themselves, although it is

important to remember that while atypical, lone terrorists may recruit other individuals who wittingly or unwittingly participate or facilitate the terrorist activity. This freedom to think "outside the box" is why lone wolves have been responsible for introducing several new terrorist tactics in the United States, including the first vehicle bombing (1920); the first major, midair plane bombing (1955); the first US airline flight hijacking (1961); the first major consumer product contamination (1982); and the first terrorist use of anthrax (2001). Furthermore, because lone terrorists are not part of a group, they may not be concerned, as some terrorist groups are, about alienating supporters, using WMD, or attacking the wrong type of target.

3. Identity-Based Terrorism

a. **Identity and Intent Categories.** Identity and intent are linked closely to the underlying ideology and the corresponding strategic objectives of terrorists and terrorist organizations. Political or religious identity expressed in ideology is often all-encompassing and determines the general parameters— the "why" and "where"—of the terrorist operations. These factors determine the desired end state and measures of success for terrorists. Operational tactics, techniques, and procedures (TTP); specific targets; and timing are often constrained or limited by ideological frameworks—this may not be the case for some apocalyptic religious ideologies or political constructs. To make matters even more difficult, many categories overlap, even when there would seem to be inherent ideological conflict. Some of the common categories are:

(1) **Ethnocentric.** Groups of this persuasion see race or ethnicity as the defining characteristic of a society and, therefore, a basis of cohesion. These groups often desire full and independent sovereignty, thus making ethnonational terrorist groups among the most prevalent type of terrorist organization.

(2) **Nationalistic.** Loyalty and devotion to a nation-state and the national consciousness derived from placing one nation's culture and interests above those of other nations or groups is the motivating factor behind these groups. Often, displaced minorities living in other states (diaspora) display this fierce nationalistic loyalty.

(3) **Revolutionary.** These groups are dedicated to the overthrow of the established order and replacing it with a new political or social structure. Most terrorist groups are opposed to the established order and use terrorism as a revolutionary tactic to achieve their goals. Some state-directed terrorist groups may use terrorism as a means to preserve and extend their power and as a strategic deterrent.

(4) **Separatist.** Separatist groups are those with the goal of separation from existing entities through independence, political autonomy, or religious freedom or domination. The ideologies separatists subscribe to include social justice or equity, anti-imperialism, and the resistance to conquest or occupation by a foreign power.

b. **Ideological Categories.** Ideological categories describe the political, religious, or social orientation of the group. While some groups will be seriously committed to their avowed ideologies, for others, ideology is poorly understood and primarily a rationale used

to justify their actions to outsiders or sympathizers. It is a common misperception to believe that ideological considerations will prevent terrorists from accepting assistance or coordinating activities with terrorists or states on the opposite side of the religious or political spectrum. Quite often, terrorists with differing ideologies have more in common with each other than with the mainstream society they oppose, and they will settle into pacts of non-aggression to achieve a common goal. Common ideological categories include:

(1) **Political.** Political ideologies are concerned with the structure and organization of the forms of government and communities. While observers outside terrorist organizations may stress differences in political ideology, the violent activities of groups that are politically opposed are similar to each other in practice. Examples of political ideologies that terrorists might ascribe to or identify with include, but are not limited to, fascism, nationalism, neo-Nazism, Marxist-Leninism, and anarchism, as well as extreme forms of environmental and animal rights activism.

(2) **Religious.** Many terrorist organizations and individual terrorists have taken up violence to further their extremist religious goals. Religiously motivated terrorists see their ultimate objectives as divinely sanctioned and, therefore, infallible and nonnegotiable. The religious motivations of terrorists can sometimes be tied to ethnic and nationalist identities, especially when they are intertwined in geographic locations, such as the Taliban, who are comprised mostly of Pashtuns in Afghanistan and Pakistan.

(3) **Social (Special Interest).** Often particular social policies or issues will be so contentious that they will incite extremist behavior and terrorism. Frequently, this is referred to as "single-issue" or "special-interest" terrorism. Special-interest terrorism is used to describe people and groups who commit violence on behalf of a very specific cause.

4. Violent Extremist Organizations

VEOs are the collective grouping of extremists, terrorist enablers, and/or terrorists with a common goal to conduct acts of terrorism in pursuit of ideological objectives. VEOs may have state and non-state sponsorship. VEOs have spread globally and continue to threaten the US homeland, US territories, US citizens, US allies, and US partners by conducting attacks, inspiring violence, and creating destabilizing conditions that divert military resources from other priority challenges.

a. **Violent Extremism.** Violent extremism refers to advocating, engaging in, preparing, or otherwise supporting ideologically motivated or justified violence to further social, economic, and political objectives. Terrorism is a tactic VEOs use to advance their interests. VEOs may initially start as adherents of a localized or transnational political movement, bound together by ethnicity, religious belief, caste affiliation, or common goal. Such groups are dedicated to radicalizing populations, spreading violence, and leveraging terrorism to impose their visions of societal organization. They are strongest where governments are weakest, exploiting people trapped in fragile or failed states. While these groups tend to be motivated by real or imagined unjust treatment from a government (or governments), these VEOs may turn to transnational criminal organizations to provide

financial, material, or personnel support, despite a purported abhorrence for criminal or immoral activity. In many locations, violent extremists coexist with transnational criminal organizations, where they conduct illicit trade and spread corruption, further undermining security and stability. VEOs can exist in permissive environments, as well as in uncertain and hostile ones associated with insurgencies. In certain cases, violent extremism and insurgency can overlap. The Al-Qaeda reliance on the Haqqani criminal network in Afghanistan and Pakistan is an example. Additionally, many criminal and terrorist organizations have developed political branches to offer legal protection, obfuscation, and a means to develop the trappings of a state (e.g., Lebanese Hezbollah). Violent extremism often manifests itself at the individual level and in highly informal diffuse networks. Such networks are often transnational in character. "Push" factors are important in creating the conditions that favor the rise or spread in appeal of violent extremism. Push factors are socioeconomic, political, and cultural in nature. "Pull" factors are necessary for push factors to have a direct influence on individual-level radicalization and recruitment. Pull factors are associated with the personal rewards which memberships in a group or movement, and participation in its activities, may confer. The preferred way to counter VEOs is by way of sustained pressure using local forces augmented by specialized US and multinational military strengths such as intelligence, surveillance, and reconnaissance (ISR) precision strike, training, and logistical support. Defeating VEOs ultimately requires providing security and economic opportunities to at-risk populations. Thus counter-VEO campaigns demand that JFCs, in close coordination with other USG departments and agencies and international organizations, assist local governments in addressing the root causes of conflict.

b. Ideologically motivated extremist insurgencies and terrorism are increasingly conducted in the broader context of extremist transnational social movements. This transnational appeal can lead to substantial flows of support from international sources for both insurgent or terrorist groups and can provide a unifying ideology and narrative across groups, countries, or regions. The shared ideology and narrative of VEOs can provide commonality of objectives and mutual understanding among participants, which, in turn, can foster transregional cooperation or coordination among groups. Even if no material cooperation or direct coordination has occurred, disparate groups or even lone wolves can share similar general objectives.

c. Not all extremist ideologies promote violence nor are all extremists violent. Determining whether an individual or group is driven more by promotion of the "cause" or destruction of those who oppose it can help make the distinction between an extremist and a terrorist. Regardless of tactics employed, all VEOs pose a threat to the United States and its forces, citizens, allies, and partners. VEOs continue to evolve over time. This evolution includes innovations in the ability to:

(1) Antagonize, induce, and exploit existing grievances to mobilize support for violent change.

(2) Find, influence, and mobilize populations locally, regionally, and globally.

(3) Spread information and disinformation to elicit tacit and active support or acceptance of their views and actions.

(4) Conduct, direct, support, or inspire a mix of lethal and nonlethal actions to create physical and psychological effects, gain notoriety, garner attention, sustain and increase their base, and advance their cause.

d. Continuous changes in demographics, economics, and the global security environment continue to shape the OE and will enable more entry points for VEOs to exploit. Trends and analysis indicate that VEOs will not only endure into the future but will likely be more adaptive, coalesce quicker, increase in numbers and varieties, be harder to identify, and be more lethal.

e. JFCs continue to defeat threats to US vital interests through targeted lethal and nonlethal actions, but maintaining local-level management of VEO threats will increasingly rest with our interorganizational partners.

f. Adaptive cooperative military engagement is an approach that addresses changes in the OE and emerging capabilities that affect the military's ability to understand and influence the competitive space. This approach leverages the JFC's ability to generate and exploit information to enable effective decision making while increasing integration, interoperability, and interdependence between international partners to manage VEO threats and achieve sustainable strategic success. Adaptive cooperative military engagement empowers the JFC to support, and be supported by, interorganizational partners through information, intelligence, planning, coordination, synchronization, and execution. This military engagement enables the JFC to sustain a competitive advantage over VEO threats and rebalances civil-military efforts when addressing VEO problem sets.

5. Terrorist State Affiliation, Non-State Affiliation, and Criminal Nexus

Terrorists and their organizations operate in interrelated networks. The nexus between these state, non-state, criminal, and terrorist networks happens when each element and network, operating in its own self-interest, sees an opportunity for mutual benefit.

a. An example of disparate threat networks partnering is the IRA seeking out Libyan leader Muammar Gaddafi to supply it with arms, training, and sanctuary. The IRA (an armed, Irish Catholic, nationalist organization) and Gaddafi (a fervent Islamist state-supporter of anti-Western and anti-Israel terrorism) were at opposite ends of the spectrum. The nexus between them was based on the old adage, "The enemy of my enemy is my friend." In this case, the enemy was the United Kingdom for the IRA and the United States and the West for Libya. To add to this mix, most of the funding and weapons that passed through Libya on their way to Northern Ireland in the late 1960s were supplied by the Soviet Union and other Eastern-Bloc countries. To counter threat networks, it is imperative to understand the converging nature of the relationship among terrorist groups, insurgencies, and transnational criminal organizations. The proliferation of these illicit networks and their activities globally threaten US national security interests. Together,

these groups not only destabilize environments through violence but also become dominant in shadow economies, distorting market forces.

b. A criminal nexus example is narcoterrorism, which can be described as either narcotics networks or traffickers who use terrorism against civilians to advance their agenda or as terrorists who use drug money to further their cause (also known as "narco-driven terrorism"). US security strategy recognizes that some of the billions of dollars generated yearly by the global illicit drug trade goes toward funding terrorism. Sanctuaries may be created by drug organizations, other criminals, terrorists, or insurgents. In some parts of the world, such as Colombia and Afghanistan, connections between drug producers and terrorists can be very significant. In other circumstances, connections between drug criminals and terrorists may be "transactional," involving payment for specific goods and services. Such transactions may provide weapons, false identities and travel documents, money laundering and movement, armed protection, and intelligence and clandestine communications. For more information on terrorist and criminal network connections, see JP 3-07.4, *Counterdrug Operations,* and JP 3-25, *Countering Threat Networks.*

c. The terrorist and criminal nexus can also involve both types of groups having common sources of support. Both terrorist and criminal networks can use the same enablers, such as forgers, money laundering, corruption, permissive environments, trans-border movement, cyberspace "crime-for-hire" services, or other criminal-related services. Criminal network and terrorist network recruiting can also overlap. This can be for a variety of factors, such as opportunities to transfer existing skill sets to supporting threat activities; a "redemption" narrative, particularly in the case of prison networking and recruiting; social norms promoting the use of crime to advance ideology; and the use of white-collar and other financial crimes to finance terrorism. Fully addressing terrorist network threats may involve disrupting or neutralizing the connections between common enablers.

6. Terrorist Tactics, Techniques, and Procedures

a. **Terrorist Tactics.** Terrorism is a tactic used by organizations or individuals trying to achieve specific objectives. Terrorist tactics are used by a wide variety of groups, including insurgents, such as Al-Qaeda, in Iraq's effort to replace what they identified as a Shia-led government; nationalists, such as Pakistan-based Lashkar-e-Tayyiba's efforts to eliminate the influence of a foreign power; armed separatists, such as the Euskadi Ta Askatasuna in Spain; or a state attempting to influence another by the murder, kidnapping, or hostage taking of another state's diplomats or citizenry. The defeat of terrorism is, therefore, better understood through the prism of terrorists' goals rather than their acts of terrorism. Terrorists employ a variety of TTP—some small-scale, some large-scale—to produce fear in their intended audience. A few of the most common TTP employed by terrorist groups are: assassination, arson, bombing, kidnapping and hostage taking, hijacking, piracy, seizure, and raids or ambushes. Terrorists prefer to attack their adversaries asymmetrically by circumventing an opponent's strength and exploiting any weaknesses. Using this approach, terrorists pick the time, place, and manner of the attack, while controlling contact with their targets. To instill fear and coercion, terrorists often select vulnerable and unanticipated targets, such as civilian transportation infrastructure,

economic hubs, and cultural centers. Target selection is what distinguishes a terrorist attack from a traditional attack on an enemy military force. An attack on an enemy military force is a widely accepted act of war and generally executed to either provoke a political reaction or degrade, disrupt, or defeat the targeted force, not to instill fear. The terrorist goal is not just to win favor for their causes but to erode the confidence, capability, and legitimacy of the government or societies they wish to coerce. The term terrorism is often used interchangeably with the term insurgency. Indeed, several of the tactics discussed in this chapter may also be used in an insurgency. An insurgency is the organized use of subversion and violence to seize, nullify, or challenge political control of a region. What typically distinguishes terrorism from insurgency is that, while both terrorism and insurgency seek political aims, terrorism is always unlawful and specifically intended to inculcate fear to achieve its aims. While terrorist and insurgent groups are often viewed as distinct entities, in many cases, the same group may use both terrorism and insurgent tactics. Insurgent groups often employ terrorism tactics to intimidate opponents. Terrorist groups may conduct guerrilla attacks on their enemy's military capabilities. Further, threat networks have demonstrated the ability to shift between insurgent style of activities and terrorist activities as their environment changes to suit one form over the other. Insurgencies may shift to terrorism as they lose control of territory, while terrorist groups may behave more like insurgencies in permissive environments. These shifts can change what approaches and capabilities are needed to counter changing threats. The following list highlights the most common TTP employed by terrorist groups:

(1) **Assassination.** An assassination is a deliberate action to kill specific, usually prominent, individuals such as political leaders, notable citizens, collaborators, or particularly effective government officials, among others. A terrorist group will assassinate people it cannot intimidate, those who have left the group, people who support the "enemy," people who cause significant challenges to the terrorist strategic agenda through their individual or collective actions, or people who have some symbolic significance to the enemy or world community. Terrorist groups may refer to these killings as "punishment" or "justice" as a way of legitimizing them. Assassinations are an effective psychological tool. Also see paragraph 6.b.(3)(d), "Attacking Local Government Officials and Civilians."

(2) **Arson.** Less dramatic than most tactics, arson has the advantage of low risk to the perpetrator and requires only limited technical knowledge. It is most often used for symbolic attacks and to create economic effects.

(3) **Bombing.** The IED is often the terrorist's weapon of choice. IEDs can be inexpensive to produce and, because of the various detonation techniques available, may be a low risk to the perpetrator. Another common method of attack is suicide bombings. Advantages to these tactics include their attention-getting capacity and the ability to control casualties through targeted planning and selection of time, location, and means of execution. Announcing responsibility for the bombing or denying responsibility for the incident, should the action produce undesirable results, generates media interest and may lead to increased coverage of a terrorist group's agenda and activities and may be a means of support and recruitment of additional supporters. Also see paragraph 6.b.(3)(e), "IED," and paragraph 6.b.(3)(f), "Suicide-Bomber Attacks," for more information.

(4) **Kidnapping and Hostage Taking.** Kidnapping is the unlawful seizure and captivity of one or more individuals. Kidnappings usually result in the individual being held hostage to extract specific demands but may be for intelligence collection, financial gain, or execution. A successful kidnapping usually requires elaborate planning and logistics. Similarly, hostage taking is the seizure of one or more individuals, usually overtly, with the intent of gaining an advantage, such as publicity, ransom, political concessions, and release of prisoners. Targets of terrorist-related kidnappings and hostage taking are usually prominent individuals, such as high-ranking foreign diplomats or officers, or of symbolic value, such as government, military, or LE personnel; foreign businesspeople; or tourists. Hostages can also serve as human shields, increasing terrorists' chances of success in carrying out a mission or to use in exchange for other government detainees or prisoners (see paragraph 6.b.(2), "Human Shields"). While dramatic, hostage and hostage barricade situations are risky for the perpetrator. Killing of hostages may occur once the terrorist group believes it has fully exploited the media coverage from the situation. Likewise, kidnapped personnel are also likely to be executed once the terrorist group achieves their objectives, be it ransom or publicity.

(5) **Hijacking.** Hijacking involves the forceful commandeering of a mode of conveyance. Normally associated with aircraft—often referred to as skyjacking—it may also include ships, trains, or other forms of conveyance. Hijacking is normally carried out by terrorists to produce a spectacular hostage situation or provide a vehicle for carrying out a lethal mission (e.g., using an aircraft as a weapon), but it is also employed as a means of escape.

(6) **Piracy.** Piracy is an illegal act of violence, depredation (e.g., plundering, robbing, or pillaging), or detention in or over international waters, committed for private ends by the crew or passengers of a private ship or aircraft against another ship or aircraft or against persons or property on board such ship or aircraft. Piracy may be used in itself as a terrorist tactic or as a means to support other terrorist activities.

(7) **Seizure.** Seizure usually involves occupying and holding a prominent building or object of symbolic value (e.g., a US embassy, DOD Website, or cyberspace node). There is usually considerable risk to the terrorist because security personnel have time to plan and react. Security personnel are more likely to use force to resolve the incident, if few or no innocent lives are involved.

(8) **Raids or Ambushes.** A terrorist raid is similar to a conventional military operation but is usually conducted with smaller forces against targets marked for destruction, hijacking, or hostage and barricade operations. Some raids are conducted with the intent of creating insecurity within the region. In these instances, the objective is to cause chaos and disorder, while accomplishing as much destruction as possible for the small raiding force. In some cases, the raid is designed to allow control of the target for the execution of another operation. An ambush is a surprise attack characterized by violent execution and speed of action.

(9) **Sabotage.** Sabotage is an act or acts with intent to injure, interfere with, or obstruct the normal or intended functionality of a vital resource, industry, or capacity. The

objective in most sabotage incidents is to demonstrate how vulnerable society and its critical infrastructure are to terrorist actions and the inability of the government to stop terrorism. Industrialized societies are more vulnerable to sabotage than less highly developed societies. Utilities, communications, and transportation systems are so interdependent that a serious disruption of any one affects all of them and attracts immediate public and media attention. Information systems, commercial industry, human resources, mass transit, and energy and communication infrastructures are examples of attractive targets of terrorist sabotage.

(10) **Threats or Hoaxes.** Any terrorist group that has established credibility can employ a hoax with considerable success. A credible threat causes time and effort to be devoted to increased security measures. A bomb threat can close a commercial building, empty a theater, or delay an aircraft flight at no cost to the terrorist. Threats may also be used by terrorists to probe and observe security procedures. Repetitive false alarms may dull the analytical and operational efficiency of key security personnel, thus creating complacency in reacting to threats.

(11) **Environmental Destruction.** Although this tactic has not been widely used, the increasing accessibility of sophisticated weapons to terrorists has the potential to threaten damage to the environment. For example, possible tactics may include the intentional dumping of hazardous chemicals into the public water supply, poisoning or destroying a nation's food supplies through introduction of exotic plants or animals, destroying oil fields, or attacking an oil tanker to cause ecological harm. The use of exotic insects, animals, or plants to poison or damage the food supply or ecosystem is a potential low-cost weapon.

(12) **Active Shooter.** An active shooter is an individual or individuals actively engaged in killing or attempting to kill people in a confined and populated area; in most cases, active shooters use firearms but can use any other deadly weapon (e.g., knife, club, bow and arrow, explosive, vehicle). There is no pattern or method to their selection of victims. In some cases, active shooters use IEDs to create additional victims and to impede first responders. For more information, see CJCS Guide 5260, *A Self-Help Guide to Antiterrorism*.

(13) **Insider Threat.** An insider threat, with respect to DOD, is a threat presented by a person who has, or once had, authorized access to information, a facility, a network, a person, or a resource of DOD and wittingly, or unwittingly, commits an act in contravention of law or policy that resulted in, or might result in, harm through the loss or degradation of information, resources, or capabilities or a destructive act, which may include physical harm to another in the workplace. An insider threat is commonly associated with cybercrimes and financial and commercial espionage; an insider threat may also include active shooters, bombers, and "inside the wire" (sometimes referred to as green-on-blue) threats.

For more information, see DODI 5240.26, Countering Espionage, International Terrorism, and the Counterintelligence (CI) Insider Threat; *Title 10, USC, Sections 1564 and 2222; and Title 50, USC, Sections 3024 and 3043a.*

b. **Terrorist Use of Asymmetrical Tactics.** As stated earlier, terrorists prefer to attack their enemies asymmetrically, circumventing an opponent's strength and exploiting weaknesses. Notably, these methods constantly evolve and often vary according to target and terrorist cell. The following provides descriptions of asymmetric tactics routinely employed by terrorists.

(1) **Denial and Deception**

(a) **Dispersing and Hiding.** Dispersion and hiding in complex terrain and urban environments degrade situational awareness and complicate US intelligence and targeting efforts. Urban areas offer excellent cover and concealment because building interiors and subterranean areas are hidden from airborne observation and vertical obstructions hinder line of sight to ground targets. Terrorists tend to blend in among a dense civilian populace in urban areas.

(b) **Exploitation of Sensitive Infrastructure.** Urban infrastructure such as buildings, shrines, and ruins can be "sensitive" for political, religious, cultural, or historic reasons. Terrorists deliberately occupy sensitive buildings under the assumption US forces will refrain from entering or returning fire.

(c) **Perfidy.** Terrorist forces have used civilian vehicles to help maneuver, supply, and transport insurgents around on the battlefield. In addition, terrorists have configured all types of motorized vehicles as vehicle-borne improvised explosive devices (VBIEDs). In one example, enemy forces reconfigured a white van into a VBIED with red crescents painted on the front and sides (similar to impersonating an International Red Cross and Red Crescent Movement vehicle), which was later detonated near a local hotel.

(2) **Human Shields**

(a) In addition to deliberately targeting civilians, terrorists may use civilians as human shields. This tactic forces friendly forces to adopt more stringent rules of engagement (ROE).

(b) Terrorists purposefully conduct operations in close proximity to civilians. In some instances, terrorists may prevent civilians from evacuating likely engagement areas to ensure a source of human shields remains available. Terrorists may also instigate situations such as work strikes or school closures that produce crowds of civilians in potential battle areas. Attackers may also use mass demonstrations to conceal their escape after executing an attack.

(c) **Maneuver Within Crowds of Civilians.** Terrorists may use crowds of civilians to conceal their movements and negate ingress and egress by first responders.

(d) **Attack Targets from Residential Areas.** Terrorists have launched attacks from residential areas to invite return fire into civilian homes and designated protected structures.

(3) **Ambush and Surprise Attacks**

(a) In general, terrorists avoid direct attacks against strong military forces and prefer to engage civilian "soft" targets. Terrorists tend to use standoff tactics and weapons to allow for escape from the target area and to avoid immediate response by military or LE forces.

(b) **Shoot and Move Tactics.** Mortars and rockets are the primary weapons of choice used by terrorists for applying shoot and move tactics in urban terrain. Attackers can use mounted mortars in truck beds and inside of automobiles by cutting holes in the roofs of the car to fire the weapon. Attackers fire a few rounds from these systems before moving to a new location. Terrorists may leave these systems behind to quickly egress the area or to avoid counterbattery fire. Sometimes the equipment left behind is rigged with bombs or is targeted by another indirect fire system to engage first responders.

(c) **Standoff Weaponry.** Mortars, rockets, and their ammunition are available worldwide, are relatively easy to maintain, and are easy to employ. They are easy to hide, have high rates of fire, and can quickly relocate. Mortars do not require large firing areas, and they are ideal for urban attacks as their arcing trajectory can clear high buildings. Rockets require more planning and more set-up time, but they increase attacker survivability and deliver a larger warhead. Terrorists have also manufactured improvised standoff weaponry such as the FARC's [Revolutionary Armed Forces of Colombia's] use of explosive-filled propane tank mortars in Colombia.

(d) **Attacking Local Government Officials and Civilians.** This tactic avoids the strength of military forces and concentrates on the various levels of the public servants and innocent civilians. Such attacks undermine the government's efforts to maintain stability, prevent the provision of basic services to the population, and attempt to intimidate other individuals from supporting or assisting the government. Terrorists may publicize their attacks on the Internet or other media to garner credibility, demonstrate their capabilities, and spread fear or panic to a wider audience.

(e) **Improvised Threats.** Improvised threats are devices, systems, and associated TTP designed, fielded, or employed unconventionally that are intended to adversely impact US forces and partners. Terrorist groups have been known to develop and adapt improvised weapons and systems under a variety of circumstances. Improvised threats are adaptively applied and leveraged to overcome a friendly advantage and capable of producing cascading tactical, operational, and strategic effects. Once known to be successful, they are replicated by enemy forces and can quickly affect an entire theater or even pose a transregional threat. Improvised threats include IEDs and small unmanned aircraft systems (UASs), and new improvised threats can be expected to emerge. Commanders should remain alert for improvised threat development in their OEs.

(f) **Small UASs.** Small UASs are commercially available and can be improvised or locally fabricated and employed in the OE. These small UASs are typically under 55 pounds. Terrorist attacks have been conducted with small UASs, which can provide a standoff capability and ability to bypass ground-oriented defenses. Further, small UASs can provide an over the horizon capability for surveillance, reconnaissance, and vectoring of attacks.

(g) **IED.** An 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.

For more information on IEDs, see JP 3-15.1, Counter-Improvised Explosive Device Activities.

(h) **Suicide-Bomber Attacks.** Terrorists may employ suicide bombers to precisely control the time, place, and target of an attack. Suicide bombers are the delivery vehicles and triggering devices for the explosives they are transporting, with the added benefit of demoralizing the opponent and by proving the volunteer suicide bombers' extreme commitment to their cause. Many suicide bomb attacks use VBIEDs, though, in some areas, personnel-borne IEDs are the prevalent tactic. Multiple VBIEDs have also been employed, with the first vehicle explosion designed to open a breach into a hardened facility or perimeter barrier and a second bomb to penetrate through the opening to attack the target.

(4) **Misinformation.** Terrorists may use misinformation to garner support both locally and from a wider, regional, or international audience. Terrorists are adept at disseminating information quickly, thus putting friendly information-related activities in a defensive posture. Methods might include:

(a) **Spreading Rumors.** Rumors have always been a powerful force. News from the marketplaces and cafés has always been used to offset official information. Terrorists plant many rumors and initiate disinformation to discredit information from PNs and the USG. Rumors in Operation IRAQI FREEDOM, which took months to disprove, included the distribution of disease-laden toys by coalition soldiers to Iraqi children and the harvesting of human organs by US personnel for sale on the Internet.

(b) **Releasing Favorable Combat Footage.** Terrorists rely heavily on video to distribute their propaganda. For example, crude digital video discs (DVDs) containing footage of attacks on multinational forces, wounded women and children, and damaged local infrastructure may appear in regional marketplaces immediately after attacks. DVDs will usually praise the bravery of residents "who didn't submit to humiliation by the Americans" and include scenes depicting the bravery of fighters as they engage multinational forces.

(c) **Posting Video on the Internet.** Terrorists can use the Internet to disseminate their message as quickly as events happen. An immediate press release from a Website is not only cheap but offers direct control over the content of the message. Sites are managed to manipulate images in support of the terrorists and to create special effects or deception. Video footage of terrorist successes are used for recruitment and to sustain morale. Multimedia and social media sites display manufactured evidence of USG and allied "atrocities and war crimes" to turn domestic and international opinion against the USG.

(d) **Ensuring Media Access.** Terrorists rely on media coverage to reinforce their messages. Some media companies repeatedly display images of casualties, massive collateral damage, and the accusation that government forces use excessive force.

c. **Space and Cyberspace Threats.** Terrorists may leverage space and cyberspace capabilities to oppose CbT efforts by DOD forces and those of our allies. The diffusion of advanced technology in the global economy means terrorists and affiliated non-state actors can now muster weaponry and leverage capabilities through commercial providers that were once available only to technologically advanced nations. Consequently, the capability advantage that US forces have had will likely erode in the future. Terrorists will not only have more advanced capabilities but may also develop abilities to fight in a coordinated manner across multiple AORs and throughout the OE.

(1) Terrorists will also attempt to deny operational use of space and cyberspace by DOD and other friendly forces conducting CbT operations. Concurrently, AT protections should be added to all essential military capabilities. Joint forces must also be trained to operate in contested, degraded, and operationally limited space and cyberspace.

(2) Terrorists can use cyberspace operations as an asymmetric means to counter traditional advantages by selectively targeting US space and cyberspace operations, capabilities, and infrastructure. These tactics may enable strategic attacks against the United States—without resorting to nuclear weapons—in ways that could cripple our economy and our ability to deploy our military forces. For example, terrorists could use cyberspace attacks against financial and industrial sectors while simultaneously launching physical attacks. VEOs currently use space and cyberspace capabilities to communicate anonymously, asynchronously, and without being tied to set physical locations. They attempt to shield themselves from US LE, intelligence, and military operations through use of readily available commercial cyberspace security products and services. Defensive cyberspace operations and defensive space control operations conducted to mitigate terrorist threats (or others) are not conducted as AT activities.

See JP 3-14, Space Operations; *JP 3-12,* Cyberspace Operations; *and JP 3-25,* Countering Threat Networks, *for additional guidance in the conduct of space and cyberspace operations.*

7. Terrorist Threats to the Homeland

a. In the most general statutory terms, a domestic terrorist engages in terrorist activity that occurs in the homeland. The FBI has lead responsibility for terrorism investigations at the federal level. The FBI generally relies on two fundamental sources to define domestic terrorism. First, Title 28, Code of Federal Regulations, Section 0.85, characterizes terrorism as "the unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives." Second, Title 18, USC, Section 2331, more narrowly defines domestic terrorism and differentiates it from international terrorism and other criminal activity (see Figure II-1).

Domestic Terrorism Definition

Activities that:

Involve acts dangerous to human life that are a violation of the criminal laws of the United States or of any State;

Appear to be intended—

- To intimidate or coerce a civilian population;
- To influence the policy of a government by intimidation or coercion; or
- To affect the conduct of a government by mass destruction, assassination, or kidnapping.

Occur primarily within the territorial jurisdiction of the United States.

Source: Title 18, United States Code, Section 2331

Figure II-1. Domestic Terrorism Definition

b. Domestic terrorism can be described as violence perpetrated by individuals or groups inspired by or associated with primarily US-based movements that espouse extremist ideologies of a political, religious, social, racial, or environmental nature. The April 15, 2013, Boston Marathon bombing, where two homemade pressure cooker bombs detonated near the finish line of the race, killing three people and injuring several hundred others is an example. The bombers were two Chechen Kazakhstani-American brothers surnamed Tsarnaev. The surviving brother claimed their motivation was extremist Islamist beliefs and the wars in Iraq and Afghanistan; he also claimed that they were self-radicalized and unconnected to any outside terrorist groups.

c. The current domestic threat has expanded considerably, though it is important to note that the more traditional threat posed by organizations such as the Islamic State of Iraq and Syria, Al-Qaeda, and their affiliates, is still present and active. The threat of domestic terrorism also remains persistent overall, with terrorists crossing the line from First Amendment-protected rights to committing crimes to further their political agenda. Three factors have contributed to the evolution of the terrorism threat:

(1) **The Internet.** International and domestic terrorists have developed an extensive presence on the Internet through messaging platforms and online images, videos, and publications, which facilitate the groups' ability to radicalize, recruit, and inspire individuals receptive to extremist messaging. Such messaging is constantly available to people participating in social networks dedicated to various causes, particularly younger people comfortable with communicating in the social media environment.

(2) **Use of Social Media.** In addition to using the Internet, social media has enabled both international and domestic terrorists to gain unprecedented, virtual access to people living in the United States in an effort to enable homeland attacks.

(3) **HVEs.** Domestic LE and DHS cannot focus solely on terrorist threats emanating from overseas; they must also identify those persons most vulnerable to become

radicalized and become HVEs and aspire to attack our nation from within. HVEs can be described as global-jihad-inspired individuals who are based in the United States, have been radicalized primarily in the United States, and are not directly collaborating with a foreign terrorist organization.

d. Commanders and policy makers are affected by aspects of domestic terrorism.

(1) **Level of Activity.** Domestic terrorists have orchestrated more than two-dozen incidents since September 11, 2001, including terrorist attacks. There also appears to be growth in antigovernment extremist activity as measured by watchdog groups in the last several years.

(2) **Use of Nontraditional Tactics.** A large number of domestic terrorists do not necessarily use tactics such as suicide bombings or airplane hijackings. Instead, they have been known to conduct activities such as vandalism, arson, and mass shootings.

(3**) Exploitation of the Internet.** Domestic terrorists are often Internet-savvy and use the medium as a resource for their operations.

(4) **Decentralized Nature of the Threat.** Many domestic terrorists rely on the construct of **leaderless resistance.** This involves two levels of activity. On an operational level, militant, underground, ideologically motivated cells or individuals conduct illegal activity without any participation in or direction from an organization that maintains traditional leadership positions and membership rosters. On another level, the above-ground public face (the "political wing") of a domestic terrorist movement may focus on propaganda and the dissemination of ideology—using protected speech.

(5) **Radicalization.** Radicalization can occur through various means, such as online radical Websites, membership in gangs, or personal contact with terrorist recruiters. Prison has been highlighted as an arena in which terrorist radicalization can occur. Some prison gangs delve into radical or extremist ideologies that motivate domestic terrorists, and, in a number of instances, these ideologies are integral to fashioning cohesive group identities within prison walls. It must be reiterated, however, that even for gangs that exhibit these ideological dimensions, criminal enterprises such as drug trafficking—not radical beliefs—largely drive their activities.

(6) **Insider Threat.** See paragraph 6.a.(13), "Insider Threat."

(7) **Active Shooter.** See paragraph 6.a.(12), "Active Shooter."

Intentionally Blank

CHAPTER III
COUNTERTERRORISM OPERATIONS AND ACTIVITIES

1. Fundamentals of Counterterrorism

a. **Pursuing a Whole-of-Government Effort.** To succeed at the tactical, operational, and strategic levels, civilian leadership should develop rapid, coordinated, and effective CT efforts that reflect and leverage the full capabilities and resources of the entire USG. This approach integrates the capabilities and authorities of each USG department and agency, ensuring the right tools are applied at the right time for the right situation in a manner that is consistent with US law and supports USG objectives.

b. Network engagement provides a framework to understand and effectively manage partner-friendly networks and engage with neutral networks in comprehensive and whole-of-government efforts. It can support understanding networks, member motivations, and their interrelationships. Building and facilitating a shared understanding is key to enabling unity of effort and unified action with partners in friendly networks. The JFC may need to consider strategies to enable partners who have authority the JFC lacks but do not have sufficient resources. Engaging neutral networks often involves efforts to turn those individuals, groups, or organizations away from supporting groups or networks that oppose JFC objectives and toward supporting friendly networks. This can be achieved directly by the joint force or through leveraging the larger friendly network, whose members may have different authorities or capabilities.

For more information, refer to JP 3-25, Countering Threat Networks.

c. **Balancing Near- and Long-Term CT Considerations.** CT operations should be planned and executed to support US diplomatic or informational initiatives. Certain tactical successes can have unintended strategic consequences. For example, if a lethal strike kills a known terrorist but also causes unintended casualties, which may lead to greater recruitment of terrorist operatives, the near-term success might have a detrimental effect on long-term objectives. The use of deadly force must be exercised in a thoughtful, reasoned, and proportionate way that both enhances US security and discredits terrorists. A legal basis must exist for every decision to use military force, including CT operations.

d. While there will never be a complete eradication of terrorism, the *National Strategy for Counterterrorism of the United States of America* [short title: *National Strategy for CT*] reflects the reality that success will only come through the sustained, steadfast, and systematic application of all instruments of national power simultaneously across the globe. The United States must use all means to defend against terrorist attacks on the United States, its citizens, and its interests around the world. It is imperative not only to forge a diverse and powerful coalition to combat terrorism today but to also work with our international partners to build lasting mechanisms for CbT, while fostering trust, coordination, and cooperation.

2. Principles, Activities, and Operations

a. The principles of joint operations are formed around the traditional nine principles of war—objective, offensive, mass, economy of force, maneuver, unity of command, security, surprise, and simplicity. To these, joint doctrine adds three principles based on operations over the last few decades—restraint, perseverance, and legitimacy. The principles of joint operations apply to CT activities and operations but of particular importance are legitimacy and objective.

(1) **Legitimacy.** Legitimacy is a condition based upon the perception by specific audiences of the legality, morality, or rightness of a set of actions and of the propriety of the authority of the individuals or organizations in taking them. Legitimate CT operations strengthen support for the objectives and activities of CT and help isolate terrorists from the public. Legitimacy can be decisive in addressing enduring terrorist threats.

(2) **Objective.** Objectives direct operations toward a clearly defined, decisive, and achievable goal. Clear objectives enable effective collaboration and unity of effort, which focuses CT operations to use scarce resources efficiently. Finally, by identifying and pursuing appropriate goals, CT may enhance legitimacy and earn enduring support.

b. In addition to the traditional warfighting tenets, CT requires collaboration, balance, and precision.

(1) **Collaboration.** Collaboration between USG departments and agencies, PNs, and allies is necessary to ensure unity of effort through ongoing coordination, cooperation, and information sharing. CT operations include interagency and multinational partners during both planning and execution. Collaboration creates a common and increased understanding of the OE and must be managed to preserve the precision and capabilities of forces conducting CT operations.

(2) **Balance.** The purpose of balanced action is to provide the appropriate type and scale of operations and activities to create desired effects. Balance is critical to CT operations as overly offensive or aggressive action risks eroding the legitimacy and support. Conversely, overly defensive action cedes the initiative to the terrorists and provides them the time and space to potentially grow into strategic threats.

(3) **Precision.** The purpose of precision is to limit unnecessary collateral damage. CT operations must be scalable in application and effect, from lethal to nonlethal, to address everything from individual actions by small groups of terrorists to enduring operations as part of a campaign to dismantle large terrorist networks. Nonlethal weapons provide precision in terms of accuracy and the type, magnitude, and duration of effect; nonlethal weapons can resolve uncertain situations and isolate targets, thereby facilitating scalability to lethal weapons while limiting the risk of collateral damage including civilian casualties. Additionally, many capabilities can produce nonlethal effects to support the commander's objectives. Precision helps preserve legitimacy by limiting unnecessary collateral damage.

3. National Strategy for Counterterrorism

a. The *National Strategy for CT* outlines how the United States will combat terrorism at home and abroad. The objectives shown in Figure III-1 support the following CT end states:

(1) The terrorist threat to the United States is eliminated;

(2) US borders and all ports of entry into the United States are secure against terrorist threats;

(3) Terrorism, radical Islamist ideologies, and other violent extremist ideologies do not undermine the American way of life; and

(4) Foreign partners address terrorist threats so they do not jeopardize the collective interests of the United States and its partners.

b. Terrorists are difficult to disrupt because they are highly adaptive and use any means to achieve their objectives. Within the United States, they exploit our open and free society to target civilians. They take advantage of technology, such as the Internet and encrypted communications, to promote their malicious goals and spread their violent ideologies. Overseas, they thrive in countries with weak governments and where disenfranchised populations are vulnerable to terrorists' destructive and misinformed narratives, and they are

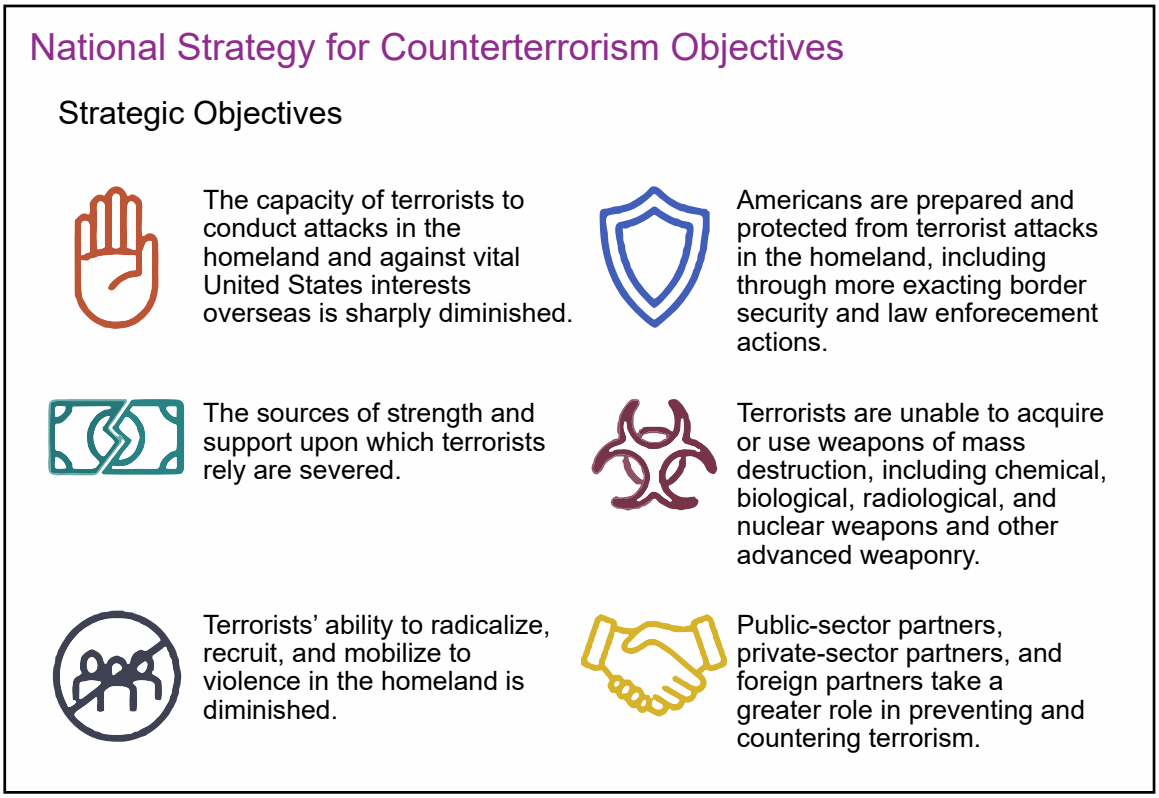


Figure III-1. National Strategy for Counterterrorism Objectives

adaptive in the face of pressure from countries with strong governments. Some are sheltered and supported by foreign governments or even do their bidding.

4. Counterterrorism Across the Competition Continuum

a. JFCs use capabilities in a wide variety of combat and noncombat situations to build a cohesive CT operation or support the combatant command campaign plans (CCPs). CT activities and operations are normally performed by forces with regional expertise, long-term relations, and specific CT equipment and training. Theater CT operations and campaigns may take place across the competition continuum from the activities of local forces and governments, developing indigenous CT security capabilities, and deterring terrorist threats; to crisis response operations; to counter terrorist incidents or limited CT contingencies; and, when required, CT operations in support of major operations and campaigns to counter local, regional, or global terrorist threats.

b. **Military Engagement, SC, and Deterrence Activities.** The primary purpose of military engagement and SC activities, which may include CT activities, is to enable the CCDR to build indigenous capabilities that deter terrorist acts and shape the OE to a desired set of conditions that facilitate stability activities and future operations. Shaping activities include development of PN and friendly military capabilities, information exchange and intelligence sharing, intelligence operations, identification and development of infrastructure and logistics capabilities, interagency coordination, and other efforts to ensure access to critical regions across the globe.

(1) CT, as a part of military engagement, is a noncombat activity conducted by specifically trained forces. CCDRs conduct routine military engagements to build trust and confidence, share information, coordinate mutual activities, maintain influence, build defense relationships, and develop allied and friendly military capabilities for self-defense and multinational operations. These US forces conduct military engagement with foreign military or civilian security forces and authorities.

(2) SC that involves interaction with PN or HN CT defense forces builds relationships that promote US CT interests and develops indigenous and PN CT capabilities and capacities. These activities provide US forces with peacetime and contingency access to critical regions around the world. SC includes activities such as FID, security force assistance, combined training and exercises, and similar noncombat activities.

(3) Deterrence prevents terrorist acts by presenting a credible threat of specific counteraction that would deny the success of an organization's use of terrorism and degrade its legitimacy or capabilities and influence over a population. Deterrence of an enemy who uses terrorism to achieve objectives is a difficult task, as often terrorists have no regard for their own safety or life and are only concerned with success of the attack. Military engagement and SC activities can help deter future terrorist acts by presenting a credible threat that US and regional partner CT action would render the organization ineffective. Deterrence in one region may force terrorists to move to another, which may deter or disrupt the organization temporarily.

5. Military Objectives Across the Competition Continuum

A more detailed example of CT across the competition continuum is shown in Figure III-2.

a. **Armed Conflict**

(1) **Defeat.** Create conditions to impose desired strategic objectives upon the enemy.

(2) **Deny.** Frustrate the strategic objectives of the enemy.

(3) **Degrade.** Reduce the enemy's ability and will to the greatest extent possible within resource constraints and acceptable risk.

(4) **Disrupt.** Temporarily interrupt the enemy's activities or the effectiveness of enemy organizations by interdiction, subversion, or coercion.

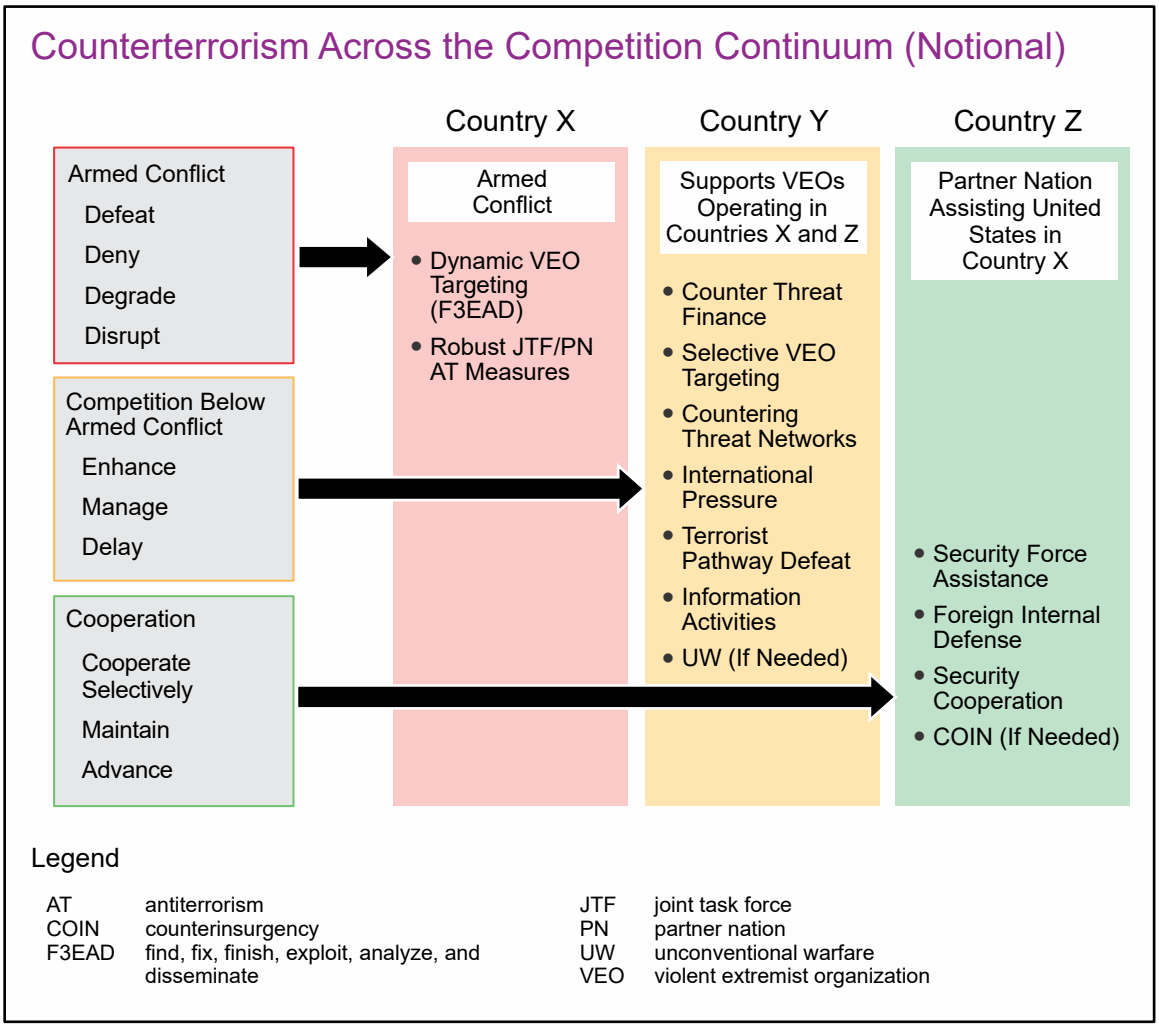


Figure III-2. Counterterrorism Across the Competition Continuum (Notional)

b. **Competition Below Armed Conflict**

(1) **Enhance.** Achieve strategic objectives, prevent the competitor from achieving incompatible objectives, and improve relative strategic or military advantage without causing an escalation to armed conflict.

(2) **Manage.** Maintain relative strategic or military advantage to ensure the competitor achieves no further gains; only seek to improve the US advantage when possible with existing resources and in a manner that does not jeopardize interests elsewhere.

(3) **Delay.** Achieve the best possible strategic objective within given resources or policy constraints, recognizing that this lesser objective entails risk that the competitor will achieve further gains.

c. **Cooperation**

(1) **Cooperate Selectively.** Transactional cooperation with a partner (who is often a competitor elsewhere) to achieve a specific policy objective. Cooperation with great power rivals to prevent terrorist acquisition of WMD is an example of this type of transactional cooperation.

(2) **Maintain.** Sustain an open-ended cooperative relationship with an ally or partner and secure bilateral advantage but without significant increase in resources or commitment.

(3) **Advance.** Establish and improve an open-ended cooperative relationship with an ally or partner by significantly increasing resources or commitment.

d. It is important to recognize that CT operations and activities can be executed simultaneously across the competition continuum during the same campaign. The operations and activities differ depending on the situation and relationship among participants.

6. Levels of Warfare and Counterterrorism

a. The three levels of warfare are strategic, operational, and tactical. At the strategic level, a nation articulates the national (or multinational in the case of an alliance or coalition) guidance that addresses strategic objectives in support of strategic end states and develops and uses national resources to achieve them (see Figure III-3). The President, aided by the NSC Staff, establishes CT policy and national strategic objectives in the *National Strategy for CT* that includes national objectives and end states, as well as establishing the interagency framework for achieving them. At the strategic level, SecDef translates national CT strategic objectives into military strategic objectives that facilitate theater planning. Theater planning links national strategic policy, strategy, objectives, and end states that address global and transregional adversaries to DOD global objectives and end states. DOD then develops global campaign plans to address inherently global and transregional threats that exceed the authority of a single CCDR. The CCDRs, along with

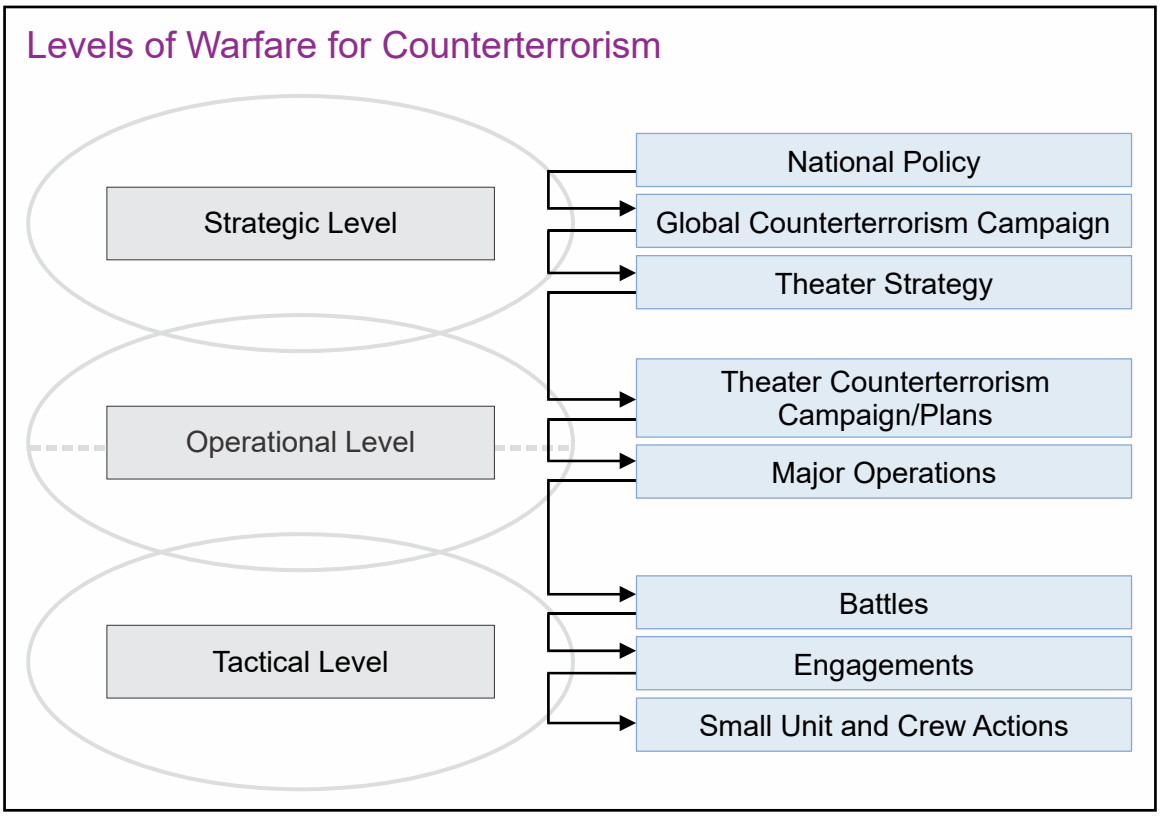


Figure III-3. Levels of Warfare for Counterterrorism

the combat support agencies, participate in development of global campaign plans that inform their regional efforts.

b. The operational level links the national and military CT strategic objectives and end states to the tactical level by the planning and execution of CCPs with day-to-day activities and contingency plans. The CT enterprise is where interagency capabilities and authorities coalesce into unified whole-of-government action. It operates across all levels of warfare but is centered between the strategic and operational levels close to national decision makers with the intelligence to make timely decisions. At this level, the CCDRs develop and execute CCPs in support of the *Global Campaign Plan to Counter Violent Extremist Organizations* and execute operations at the tactical level to achieve CCP military objectives.

c. The tactical level of warfare is where battles and engagements are planned and executed to achieve military objectives assigned to tactical units or task forces. SOF contain units dedicated to CT operations and should be a JFC's first choice. When SOF are not available, the most appropriate and available force may be used. CCDRs normally delegate OPCON to commanders of TSOCs to execute CT operations within their AOR, as applicable.

7. Command, Control, Plan, and Assess Counterterrorism Activities and Operations

Title 10, USC, Section 164, is the statutory authority for CCDRs. SecDef, CCDRs, subordinate JFCs, and tactical commanders delegate requisite authorities to subordinate

commanders at all levels by establishing command relationships. JP 1, Volume 2, *The Joint Force,* delineates and describes the types of command authority and contains a discussion of command authorities, relationships, transfer of forces, and C2.

a. **Command Relationships.** The nature of terrorist threats requires SecDef, CDRUSSOCOM, CCDRs, and JFCs to establish flexible and often complex command relationships to ensure the joint force has the required agility to coordinate with all DOD, interagency, and foreign partners and to pursue terrorists across military and governmental boundaries.

b. **SOF Command Relationships.** Special operations C2 have challenges similar to those of the joint force when establishing command relationships between the joint force, SOF components, and SOF units with different missions and responsibilities. The art of establishing a command relationship is the process for the commander to unify the effort between joint forces, SOF, and multinational forces. Besides command relationships, an SOF HQ can utilize mission command through coordinating procedures or direct liaison between units. When the CCDR establishes a JTF, whether from the joint forces or SOF, there will likely be a supported command relationship with other components, with forces attached or provided, and with a combination of OPCON or tactical control (TACON) relationships. CCDRs and other JFCs often exercise OPCON through subordinate JTF commanders, similar to a joint special operations task force having OPCON of other component SOF units. CDRUSSOCOM has COCOM of the TSOCs as subordinate unified commands, the CCDR has OPCON of the TSOCs (as applicable), and the commander of a TSOC has TACON of the SOF within the TSOC. Often, when a JTF and SOF HQ occupy the same operational area, SOF may be TACON to the JTF commander or have a supporting relationship. Commanders and their planning teams need to address what tasks must be accomplished and by whom, which informs the C2 structure for the mission and command relationships and is followed by an establishing directive. The establishing directive can be issued to specify the purpose of the support relationship, the effect desired, and the scope of the required action.

c. **COCOM.** Title 10, USC, Section 167, lists CT as a special operations activity of USSOCOM, which has forces specifically trained and equipped to conduct CT activities and operations. Special operations activities and missions are normally conducted under the OPCON of a specific CCDR.

(1) **OPCON.** Unless otherwise directed by SecDef, when USSOCOM forces are transferred to another CCDR, the gaining CCDR exercises OPCON over those forces. In addition to USSOCOM-provided forces, the gaining CCDR has OPCON over permanently forward-stationed forces.

(2) **TACON.** A CCDR or TSOC commander may delegate TACON to subordinate commanders to direct CT activities and operations and control assigned or attached forces or designated forces made available for tasking.

(3) **Support**

(a) Support is a command relationship especially useful for JFCs employing forces that must operate across multiple commands and operational areas because it creates flexibility for the JFC. A support relationship is established when a force must operate in another organization's operational area or across multiple AORs to effectively coordinate and pursue terrorists. Thus, a supporting force commander may be in support of two or more CCDRs/JFCs simultaneously to effectively address cross-boundary threats. The support relationship enables forces to address terrorist threats, thereby complementing forces conducting other offensive and defensive activities and operations such as stability activities, counterinsurgency operations, and FID operations.

(b) SecDef or a common superior commander assigns roles and responsibilities and grants authorities to the supporting and supported commanders in an establishing directive or order that creates the command relationship. An establishing directive is essential to ensure unity of effort. The support command relationship is used by SecDef to establish and prioritize CT support between and among CCDRs and to create command relationships for national joint forces with CCMDs and TSOCs to address terrorist threats within, and that transcend, AORs and/or functional areas.

(c) Effective employment of forces to conduct CT may require a JFC to be a supporting commander to two or more supported commanders simultaneously. When there is a conflict over prioritization between component commanders, SecDef or a common superior commander will have final adjudication. When the supporting commander cannot fulfill the needs of the supported commander, either the supported or supporting commander will notify the establishing authority. The establishing authority will provide a solution.

8. Organize for Counterterrorism Activities and Operations

a. **SOF C2 Organizations.** SOF provides an array of C2 options that enables effective CT mission command throughout the competition continuum, which spans daily activities supporting a CCP, competitive activities against adversaries, and conflict. Planning for SOF CT C2 requires an understanding of the differences of the SOF components and their C2 nodes, which contributes to the knowledge and ability to articulate the SOF C2 requirements for USSOCOM validation. TSOCs have the ability to project responsive SOF C2 from within their staffs for contingencies and when CCDRs and their staffs and TSOC commanders may need some clarity on the OE to support a plan development. All TSOCs are capable of deploying a small SOF C2 node, called a SOC-FWD, from their staffs, to support contingencies and emerging crises for limited-duration operations. Many TSOCs are included in CCDR war plans requiring larger C2 nodes, such as special operations JTFs. The SOF components provide small-to-medium C2 options, and United States Army Special Operations Command (USASOC) has organized a standing, large SOF C2 node with 1st Special Forces Command (Airborne), coupled with joint SOF and conventional components. SOF air and rotary-wing aviation elements, as well as special tactics team elements in Air Force Special Operations Command and USASOC, can provide supporting SOF air C2 nodes to coordinate, deconflict, and manage large and complex supporting air. The USASOC Special Forces, Rangers, Marine Forces Special Operations Command Raiders, and Naval Special Warfare Command can all

provide small-to-medium, self-contained C2 nodes with the accompanying operational forces. While planning for large SOF C2 nodes requires support from multiple SOF components, the Services, and possible multinational SOF, most large SOF C2 nodes have joint and multinational contributions. SOF C2 nodes are designed as modular nodes for agility, tailorable to integrate the right functions and capabilities and scalable for the right level of C2.

b. **SOF C2.** Figure III-4 displays various SOF C2 options that demonstrate the range of C2 from small-scale through to large-scale HQs. The figure does not represent a road to war or build-up over time but demonstrates how C2 can scale from small engagements, competition activities (including CT), and/or contingencies, to conflict or large-scale combat operations.

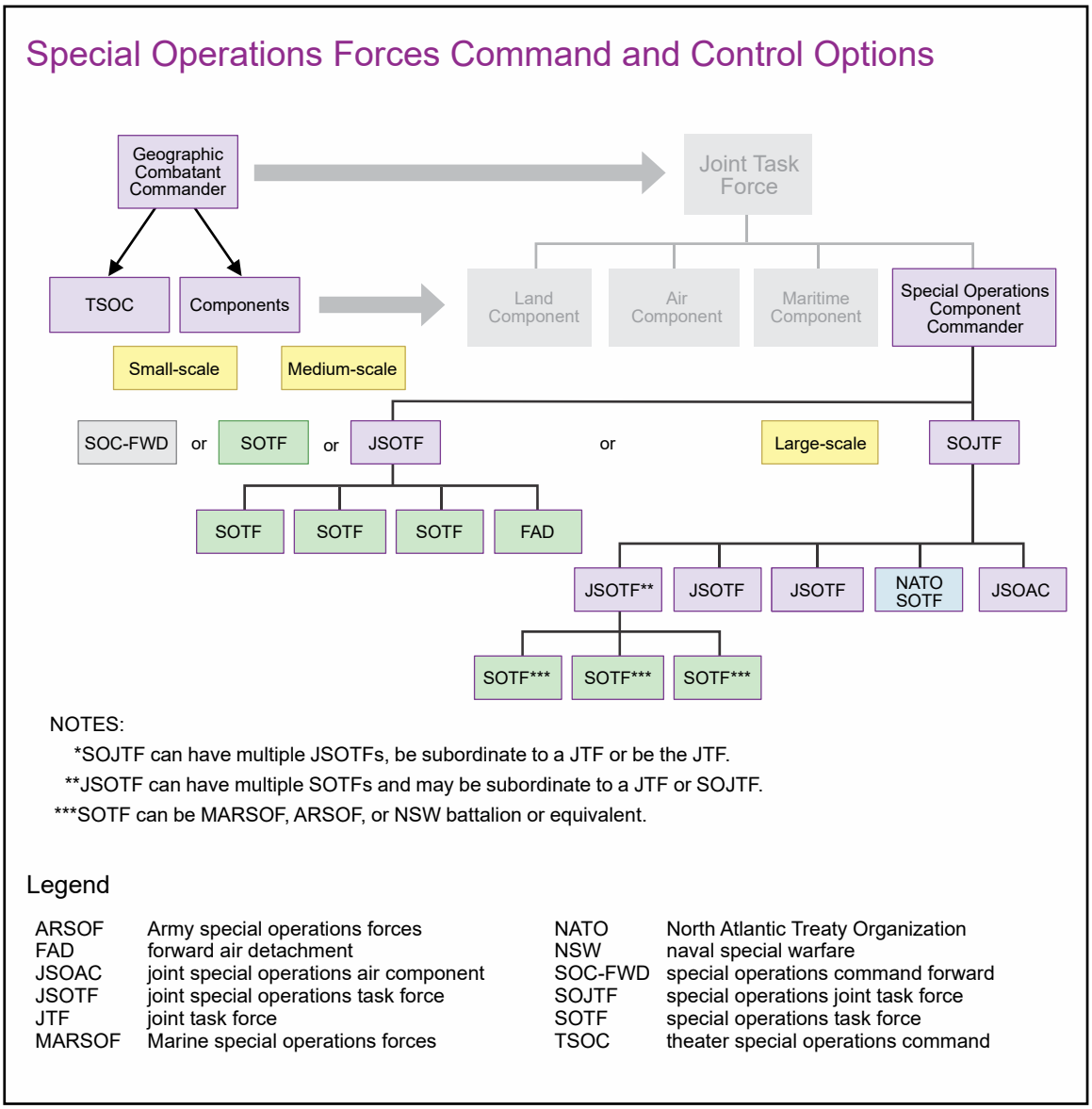


Figure III-4. Special Operations Forces Command and Control Options

For more information on special operations C2, see JP 3-05, Special Operations.

9. Execute Counterterrorism Activities and Decisive Operations

Executing CT activities and operations requires the formulation of approaches, lines of effort (LOEs), and decisive points that lead to an acceptable end state. Figure III-5 illustrates a notional CT operational approach, supporting LOEs, and decisive points. All CT operations and activities have measurable assessment criteria built into both planning and execution.

a. **Direct and Indirect Approaches and Decisive Points.** A direct approach attacks the enemy's COG by applying combat power directly against it. An indirect approach

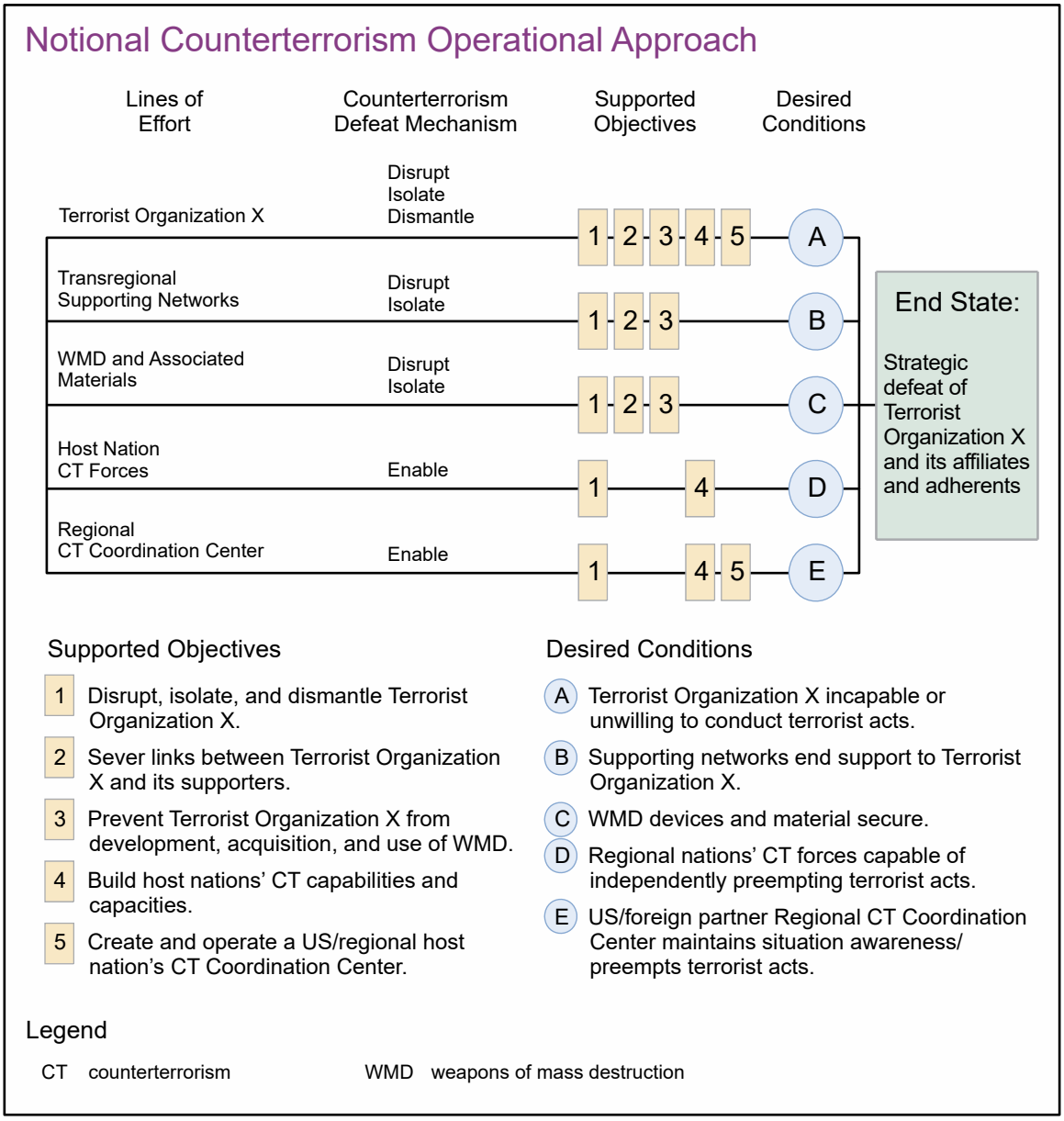


Figure III-5. Notional Counterterrorism Operational Approach

attacks the enemy's COG by applying combat power against a series of decisive points that lead to the defeat of the COG. Understanding the relationship among a COG's critical capabilities, requirements, and vulnerabilities can illuminate direct and indirect approaches to the COG. Most critical factors will be decisive points. When dealing with terrorists, the JFC must consider how actions against decisive points will affect not only the enemy but also the relevant population and their behavior and relationships with the terrorist and friendly forces. A CT campaign or operation is normally a sustained indirect approach to defeat a terrorist organization and its support networks. A JFC employing forces must selectively focus a series of actions against terrorists' critical vulnerabilities until the cumulative effects lead to achieving the objectives and attaining the end state determined by the President and SecDef. National policy does not always require defeat of terrorist organizations; it may direct the containment of the threat, monitoring it, and that forces be prepared to take action, if required.

b. **Lines of Operation (LOOs) and LOEs**

(1) **LOOs.** A LOO defines the interior or exterior orientation of a friendly force in relationship to an enemy force that connects actions on nodes and decisive points related in time and space to an objective(s). Interior lines refer to a force operating from a central position enabling it to mass combat power against a specific portion of an enemy force. Exterior lines mean a force converges on an enemy force, offering opportunities for encirclement. Major operations are typically designed using LOOs to tie offensive, defensive, and stability tasks to the geographic and opposing force-oriented objectives.

(2) **LOEs.** An LOE links multiple tasks and missions using the logic of purpose—cause and effect—to focus efforts toward establishing operational and strategic conditions. LOEs are used when COGs and decisive points do not involve friendly force orientation toward an enemy force as seen in LOOs. CT planning uses LOEs to link tasks, effects, and decisive points to achieve objectives and attain the end state and are particularly useful when CT force orientation at the operational and strategic levels has little relevance. CT force orientation at the tactical level may involve LOOs or a combination of LOOs and LOEs. Furthermore, the JFC planning CT operations may combine CT LOEs with those of corresponding DOS, FBI, and other interagency CT partners, which brings to bear capabilities, expertise, and authorities of multiple elements of the USG and facilitates unity of effort when addressing complex CT problems.

(3) **CT Defeat Mechanism.** The defeat mechanism complements the understanding achieved by a COG analysis of a problem by suggesting means to solve it. It is a useful tool to describe the main effects a commander wants to create along a LOO or LOE. The defeat mechanism is to identify, disrupt, isolate, and dismantle terrorist organizations, plus enable HN and PN forces that lead to the organization's defeat. Terrorists often reside in remote or inaccessible areas, avoid presenting their organizations to direct attack, blend with populations, and hide their activities until ready to take action. Defeating terrorist organizations requires the application of persistent pressure, eroding their ability to operate, and denying them the ability to instill fear or coerce populations and governments through violence. This requires enduring activities targeting both a terrorist organization's operational capability and its capacity to gain and employ

resources. Attacking terrorist organizations requires specifically trained and equipped forces, working with interagency partners and independently or with HNs and PNs.

(a) **Disrupt.** CT disruption is the direct attack of terrorist nodes that are identified during the joint intelligence preparation of the operational environment (JIPOE) process. All-source analysis conducted by specialized intelligence organizations, integrating intelligence provided by USG and PNs, facilitates the identification and targeting of key network nodes. Disruption contributes to degrading terrorist capabilities by eliminating or temporarily neutralizing organizational nodes. Terrorists do not normally mass their forces for engagement; thus, CT disruption attacks neutralize materiel required for terrorist acts. The effect of disruption is degradation of the organization's ability to commit acts of terrorism. For additional information, see JP 3-25, *Countering Threat Networks.*

(b) **Isolate.** Isolation limits a terrorist organization's ability to organize, train for, plan, or conduct operations effectively by denying communications, resources, recruits, and access to supporting population(s) and/or governments. The effect of isolation is a diminished organization, unable to grow or maintain its size, cutting off logistic support, and eliminating its ability to publicize its cause.

(c) **Dismantle.** Dismantling exploits the effects of disruption and isolation that further expose the organization to attack. Dismantling may include capturing or killing of remaining key personnel and neutralizing materiel essential to the organization's terrorist capabilities. The effect of dismantling may include dislocation, a shift of terrorist acts to another region or multiple dispersed locations, terrorists unable to acquire recruits or funding to maintain its organization, or members leaving the organization for other pursuits.

(d) **Enable.** Enabling is the advise-and-assist activities conducted by US forces to ensure HN and PN military and civilian forces have sufficient capabilities and capacities to contain or defeat organizations that commit acts of terrorism. In addition to providing equipment, training, and operational support, enabling may include sustained military engagement with HN and PN in regional CT coordination centers to maintain situational awareness and to preempt terrorists before they can strike.

For more information on the remaining elements of operations design (anticipation, operational reach, culmination, arranging operation, operational pause, and forces and functions), refer to JP 5-0, Joint Planning.

10. Assessment

a. Assessment is the process used to measure progress toward achieving objectives, attaining the desired end state and associated conditions, or performing tasks. The JFC assesses operations continuously to determine when to adjust operations—such as shifting priority of effort or transitioning to another phase—to ensure the joint force achieves its objectives and attains the military end state (see Figure III-6).

Examples of Counterterrorism End State, Objective, Measures of Effectiveness, and Indicators

End State: Strategic defeat of terrorist organization X.

Objective: Render terrorist organization X incapable of conducting in-country or external attacks against US persons, facilities, and interests.

Measure of Effectiveness (MOE) #1. Decrease in number and effectiveness of terrorist acts.

- Indicator #1. Number of terrorist acts attempted or executed.
- Indicator #2. Amount of military and civilian damage done.
- Indicator #3. Number of attempted attacks thwarted.

MOE #2. Degree to which links between terrorist organization X and administrative and logistic supporting organizations and individuals are severed.

- Indicator #1. Number of munitions found.
- Indicator #2. Number of media postings.
- Indicator #3. Amount of training conducted in training camps.
- Indicator #4. Number of materiel—weapons, funds, etc.—interdicted.

Figure III-6. Examples of Counterterrorism End State, Objective, Measures of Effectiveness, and Indicators

b. The assessment criteria of measures of effectiveness (MOEs) and measures of performance (MOPs) play key roles in determining a commander's critical information requirements (CCIRs). The CCIRs consist of priority intelligence requirements (PIRs) that focus on the threat and OE and friendly force information requirements (IRs), which address the status of friendly forces and supporting capabilities. Both may include MOEs and MOPs and assessment indicators associated with them in the form of IRs.

Refer to JP 5-0, Joint Planning, *for a complete discussion of the CCIR process, MOEs, MOPs, and assessment.*

11. Combat Terrorist Networks

a. The commander and staff must understand the desired condition of the threat network as it relates to the commander's objectives and desired end state as the first step of targeting any threat network.

b. An objective of CbT operations may be to influence neutral networks to establish conditions within the OE that make it more difficult for threat networks to conduct attacks.

c. Network engagement occurs through the simultaneous and continuous application of capabilities to generate desired lethal and nonlethal effects on selected networks or nodes. Effective network engagement occurs as part of a unified staff effort, not explicitly through separate or distinct working groups. The information gained from the analysis of networks is used to decide who and how to target to support achieving the commander's objectives.

d. Network engagement is particularly important in CbT, as those operations are intertwined with friendly, neutral, and threat networks. To effectively counter terrorist and other threat networks, the joint force should partner with friendly networks and conduct network engagement with neutral networks through the building of mutual trust and cooperation. Conducting network engagement with neutral actors or networks can help cut off potential support for a terrorist network. This enables the JFC to either solicit their assistance or prevent them from supporting a terrorist group and the ability to respond with pressure at multiple points of the terrorist network or other threat network. These integrated and combined activities are intended to establish conditions within the OE that align with the JFC's objectives.

For additional information regarding network engagement, see JP 3-25, Countering Threat Networks, *and Army Techniques Publication 5-0.6,* Network Engagement.

12. Network Targeting Considerations

Initial analysis provides the commander with the basic justification for targeting a particular network. Refined analysis, which happens continuously throughout staff processes, will provide the commander with a comprehensive targeting plan for specific nodes, links, or other network components. It also includes analysis of other networks, providing potential indicators of second- and third-order effects impacting mission accomplishment. Essentially, this refinement moves network analysis from a macro view of network components to a micro view of interrelated networks and network characteristics. If misinterpretation of the networks occurs, it has the potential to diminish the desired effects on a network or the ability to fully exploit potential targeting opportunities. Within an OE, there will be numerous networks (friendly, neutral, and threat). It is important the JFC gain and maintain visibility of these multiple networks and understand the interconnectivity among these networks. Threat networks also cross the boundaries between the strategic, operational, and tactical levels of warfare (see Figure III-7). JFCs gain and maintain awareness of these networks to better develop an accurate understanding of the OE.

13. Target Terrorists and Their Organizations

a. Using both military and nonmilitary capabilities, JFCs target terrorists and terrorist groups who pose the greatest threat to American citizens and interests. This includes terrorist leaders, operational planners, and individuals deploying their expertise in areas such as WMD, explosives, cyberspace operations, and propaganda. JFCs will apply persistent pressure to disrupt, degrade, and prevent the reconstitution of terrorist networks.

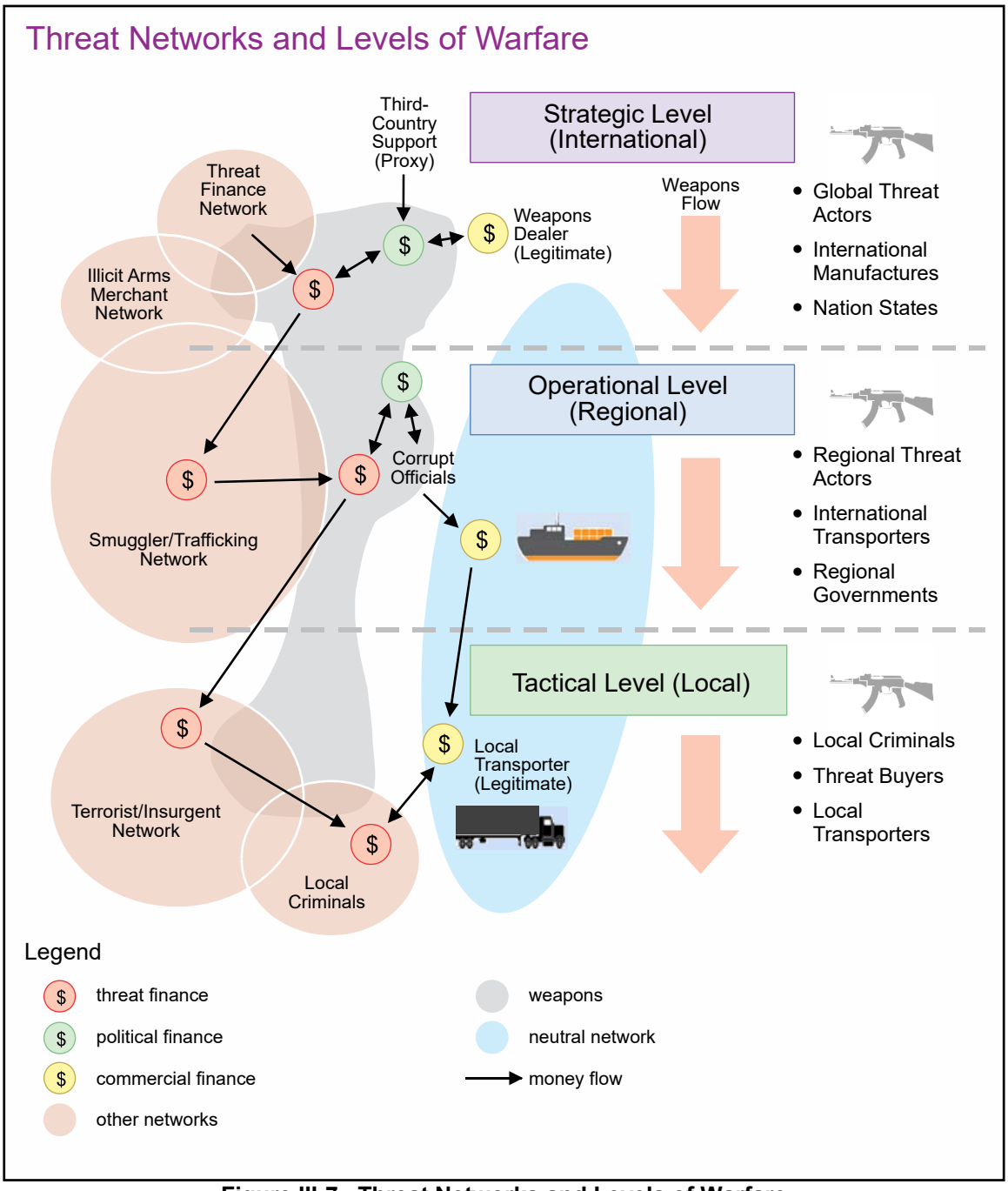


Figure III-7. Threat Networks and Levels of Warfare

b. Forces use the find, fix, finish, exploit, analyze, and disseminate (F3EAD) process to plan for and execute all CT operations against terrorists, terrorist organizations, and terrorist networks (see Figure III-8). The F3EAD process is a continuous analytical and operational process in which the analytical effort underpins all portions of the process and is conducted concurrently and continuously. This process analyzes a terrorist organization's structure, capabilities, and intentions to help develop courses of action to eliminate its capability to commit terrorist acts. CT planners identify COGs and decisive points where application of CT capabilities will produce desired effects. This process

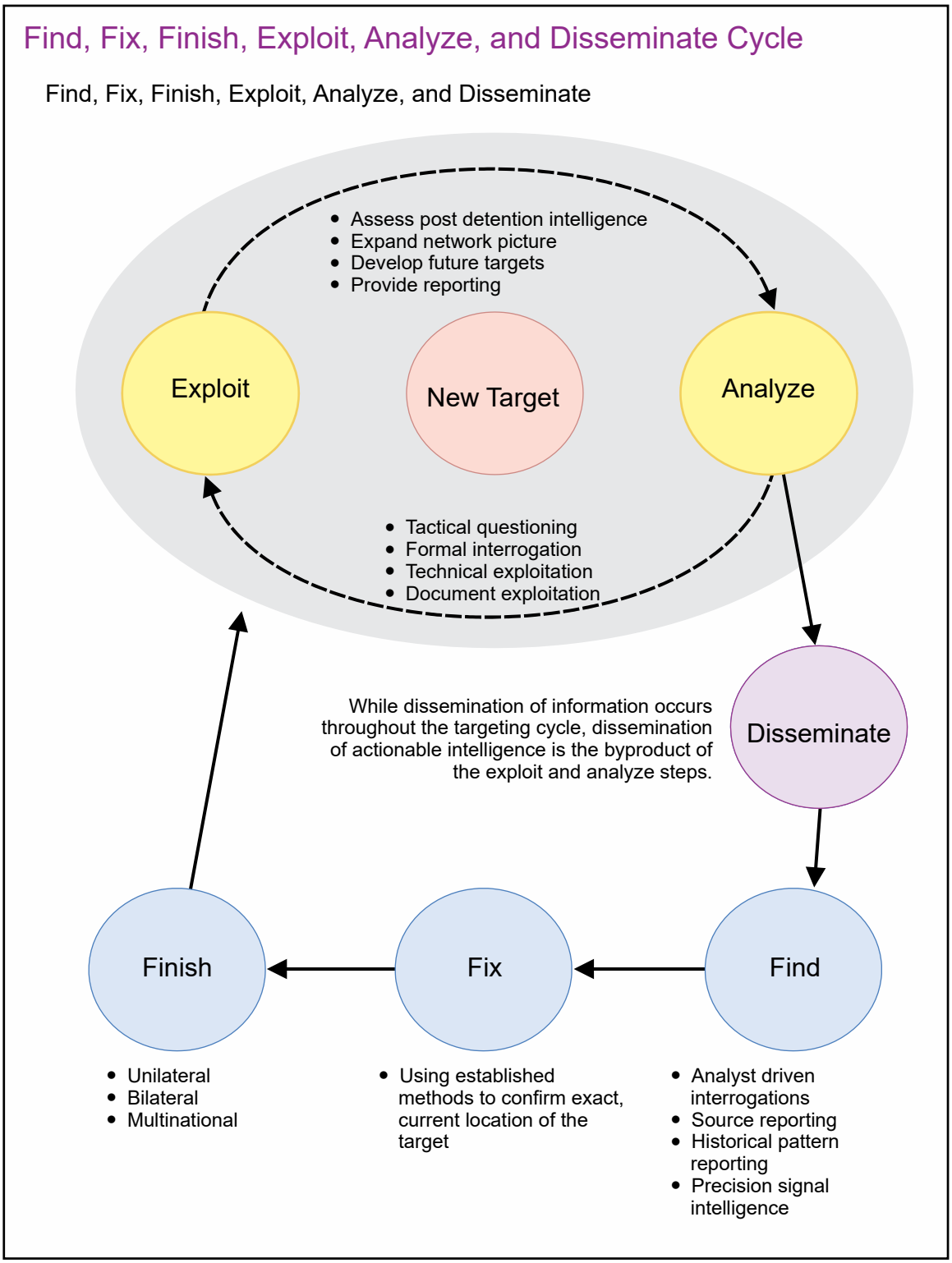


Figure III-8. Find, Fix, Finish, Exploit, Analyze, and Disseminate Cycle

involves all members of the CT enterprise. For those not in the CT enterprise, dissemination is required to inform those who may require the information. At the tactical and operational level, this process serves as a continuous cycle to prosecute known CT

targets and discover and identify future targets. The cycle also serves to focus resources on strategic CT priorities.

c. The F3EAD process relies on the close coordination between operational planners, intelligence collection, intelligence analysis, and tactical execution. Tactical forces should be augmented by a wide array of specialists to facilitate on-site exploitation and possible follow-on operations. Exploitation of captured materials and personnel will normally involve functional specialists from higher and even national resources. The objective is to quickly conduct exploitation and facilitate follow-on targeting of the network's critical nodes.

(1) **Find.** The purpose of "find" is to locate a specific node, preferably a COG or decisive point, in a terrorist organization that, if found and neutralized, would reduce its ability to commit terrorist acts. A node may be an individual, communications network, Website, weapon, destructive device, or other material used for, or that supports acts of, terrorism. Finding is a complex analytical effort that often requires the use of authorities unique to individual departments, agencies, or organizations and tenacity among a broad set of intelligence organizations at all levels of warfare. Find requires intelligence professionals to directly coordinate with operation planners and executors, as well as interagency cooperation and coordination.

(2) **Fix.** The purpose of "fix" is to definitively pinpoint a target in both time and space, with sufficient specificity to engage the target. When the find step culminates in sufficient intelligence, the analysts are augmented by operations personnel to produce actionable intelligence and operation plans. Fixing a target is a complex process that requires the rapid integration of information, intelligence, and assets in concert with partners. The information derived from the exploitation of a fix facilitates the selection of appropriate follow-on actions in the subsequent finish step.

(3) **Finish.** The purpose of "finish" is to neutralize a node in a terrorist organization by capturing, killing, or otherwise rendering the node ineffective and incapable of continuing its mission. US execution requires approval by a JFC, as authorized by the President and SecDef. HN military or civilian forces, partners, and LE or other agencies may also conduct operations to finish nodes or networks. During finishing operations, intelligence assets maintain focus on the node for situational awareness and involve commanders and staffs before, during, and after the operations.

(4) **Exploit.** The purpose of "exploit" is to optimize the value of the operation through questioning and screening individuals found at the site and collecting all material that may contain useful intelligence and information. During exploitation, detailed information is obtained from the technical and forensic examination of documents, cell phones, computers, biometrics, weapons, explosives, and other materials. The on-site screening and questioning of persons and analysis may lead to immediate follow-on finish operations, or at least contribute to the total intelligence and information picture obtained from the operation. Exploited information may assist in subsequent legal proceedings. Site exploitation teams normally conduct on-site collection and immediate analysis, including the questioning of persons found on site to determine the necessity for continued detention and further

interrogation. Exploitation is a continuous process; a steady build of information on the selected target(s) activities further refining the analysts' understanding of the network's operations, key nodes, and COGs. Successful exploitation requires a supporting dissemination architecture that provides the developed intelligence to the operations participants to facilitate planning and execution.

(5) **Analyze.** The purpose of "analyze" is to place the intelligence and information obtained from finish operations into the greater body of knowledge about the terrorist organization. DOD's multiple intelligence agencies cannot, by themselves, provide a complete intelligence context; all USG departments and agencies are required. The analyze step occurs across the levels of warfare and involves processing digital media, documents, clothing, weapons, and equipment on site and forwarding material beyond the analysts' capabilities to other members of the CT enterprises for timely analysis. The analyze step is the foundation of the F3EAD process. It continuously expands the understanding of terrorist organizations and informs all other steps of the F3EAD process. It is in the analyze process that the unique capabilities of the different USG departments and agencies come together.

(6) **Disseminate.** Dissemination of F3EAD information is a continuous process. It is critical that information gathered during all phases of terrorist targeting is shared with as broad an audience as possible, including partners and allies. JFCs recognize that partners have unique perspectives and, many times, can make better sense of data and information than a small group of nonindigenous analysts. Dissemination is not the end of the F3EAD process; rather, it is the beginning of a new cycle.

14. Cyberspace Operations in Support of Combating Terrorism

a. Cyberspace operations are used by insurgents, VEOs, and terrorist organizations as a tool for radicalization and recruitment; a method of propaganda distribution, operational communications, and financial transactions; and a platform for training. There are several methods for countering terrorists and insurgents operating in cyberspace. The USG has organizations that conduct communications and public diplomacy activities, offensive cyberspace operations, and defensive cyberspace operations. To assist in planning and execution, cyberspace can be described in terms of three interrelated layers: physical network, logical network, and cyber-persona. Each layer represents a different focus from which cyberspace operations may be planned, conducted, and assessed. The purpose of these operations is to collect intelligence, gain information on terrorist intentions and activities, and plan and conduct offensive and defensive operations. See Figure III-9 for a depiction of the following characteristics.

(1) The physical network layer consists of the IT devices and infrastructure in the physical domains that provide storage, transport, and processing of information within cyberspace, to include data repositories and the connections that transfer data between network components.

(2) The logical network layer consists of those network elements that relate to one another in a way that is abstracted from the physical network, based on the logic programming (code) that drives network components.

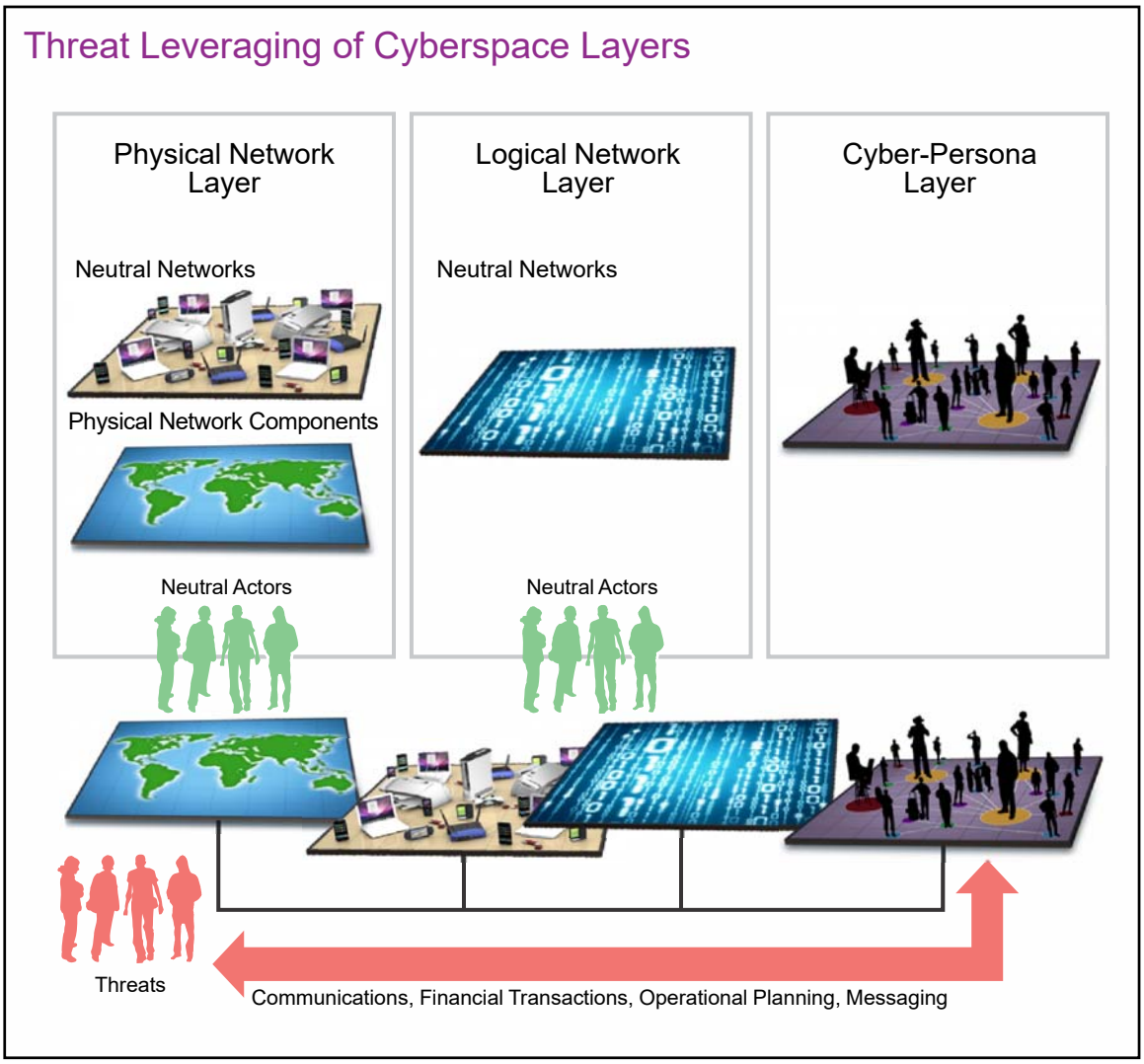


Figure III-9. Threat Leveraging of Cyberspace Layers

(3) The cyber-persona layer is a view of cyberspace created by abstracting data from the logical network layer using the rules that apply in the logical network layer to develop descriptions of digital representations of an actor or entity identity in cyberspace (cyber-persona).

See JP 3-12, Cyberspace Operations, *for a detailed discussion on these layers.*

b. State and non-state threats use a wide range of advanced technologies, which represent an inexpensive way for a small and materially disadvantaged adversary to pose a significant threat to the United States. The application of low-cost cyberspace capabilities can provide an advantage against a technology-dependent nation or organization. This can provide an asymmetric advantage to those who could not otherwise effectively oppose US military forces. Additionally, organized crime or other non-state, extralegal organizations often make sophisticated malware available for purchase or free, allowing even unsophisticated threats to acquire advanced capabilities at little to no cost. Because of the low barriers to entry and the potentially high payoff, the United States can expect an

increasing number of adversaries to use cyberspace threats to attempt to negate US advantages in military capability.

c. The pervasiveness of mobile IT is forcing governments and militaries to reevaluate the impact of the information environment on operations. The nature of global social interaction has been changed by the rapid flow of information from around-the-clock news, including from nontraditional and unverifiable sources such as social networking, media sharing and broadcast sites, online gaming networks, topical forums, and text messaging. The popularity of these information sources enables unprecedented interaction among global populations, much of which is increasingly relevant to military operations. The ability of social networks in cyberspace to incite popular support (whether factually based or not) and to spread ideology is not geographically limited, and the continued proliferation of IT has profound implications for the joint force and US national security.

15. Information Considerations for Combating Terrorism

> *"We must prevent terrorists from exploiting new technologies in today's dynamic information environment, and we must counter terrorists' ability to recruit and radicalize online and through other means."*
>
> ***National Strategy for Counterterrorism of the United States of America,* October 2018**

Information activities are key to influencing the target audience and bolstering the legitimacy of CbT. Integrated with US efforts, PNs and HNs conduct operations and information activities to effectively strengthen and defend support for CbT objectives. These operations and activities help isolate terrorists from the public.

a. Military information support operations are an essential part of the DOD psychological operations capabilities required for CbT, in particular in application of the indirect approach to shape, stabilize, and influence the environment in which terrorist organizations operate. Terrorist groups have gained sympathy and support of moderate audiences through disinformation, partly by activities focusing on miscues of the friendly forces. Within an operational area, there may be several threat assessments (TAs) and multiple synchronized actions, messages, and means of delivery required.

For more information, see DODI O-3607.02, Military Information Support Operations (MISO), *and Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3110.05,* Military Information Support Operations Supplement to the Joint Strategic Capabilities Plan.

(1) Terrorist organizations globally proliferate and grow by disseminating ideology through various means of communication to target audiences. Non-state actor terrorists, without governmental restrictions, may surpass national capabilities to create, produce, and disseminate messages to the public, especially in social media. CbT planners must anticipate and understand terrorist communication strategies to counter the effects of their messaging on local, regional, and global audiences.

(2) Terrorist organizations frequently attack targets not only for the purposes of physical destruction but also as a form of messaging. Examples include the US embassy bombings in Kenya and Tanzania; followed by the bombing attack on the USS [United States Ship] Cole (DDG 67) in Yemen; culminating with the attacks of September 11, 2001, on the World Trade Center and Pentagon. Each attack escalated in size and audacity to demonstrate Al-Qaeda's power and strategic reach.

(3) According to the 9/11 Commission Report, "The attack on the USS [United States Ship] Cole galvanized Al-Qaeda's recruitment efforts. Following the attack, [Osama] Bin Laden instructed the media committee to produce a propaganda video that included a reenactment of the attack." CbT planners should anticipate terrorist information capabilities and counter their efforts to recruit and radicalize new generations of fighters. In many instances, terrorist organizations will upload propaganda to the Internet and share propaganda on social media.

b. **Civil Affairs Operations (CAO).** Civil affairs typically do not participate in CT or direct action operations. Civil affairs contribute to CbT through activities to defeat the ideologies or motivations that spawn terrorism. CAO planning support to CT may include identifying TSOC, CCMD, and COM objectives and developing nonlethal activities that support them. CAO also supports CbT by gaining civil information through civil reconnaissance, civil engagement, and civil information management to develop the civil component of the supported commander's common operational picture.

See JP 3-57, Civil-Military Operations; *Field Manual 3-57,* Civil Affairs Operations; *and USSOCOM Directive 525-38,* Civil-Military Engagement, *for more information.*

CHAPTER IV
ANTITERRORISM ACTIVITIES

1. General Operational Context

a. AT is one of several requirements under a commander's overall responsibility to provide protection. Commanders routinely use a breadth of complementary programs to protect designated personnel, assets, processes, information, and interdependent networks and systems from a variety of threats, including terrorism. Certain programs focus on active defense measures that protect the joint force, its information, and its bases; necessary infrastructure; and lines of communications (LOCs) from an enemy's attack. Some involve both active and passive measures that make friendly forces, systems, and facilities difficult to locate and destroy. Other programs apply technology and procedures (e.g., biometrics) to reduce risk, while some focus on incident response, and emergency preparedness, to reduce the loss of personnel and capabilities due to accidents, health threats, and natural disasters.

b. As required or directed, the protection of forces, including the use of AT programs, may be extended to encompass protection of US civilians; the forces, systems, and civil infrastructure of friendly nations; and other USG departments and agencies, international organizations, and NGOs.

c. Although other protection efforts such as FP; COOP; critical infrastructure protection; cybersecurity policy procedures; chemical, biological, radiological, and nuclear (CBRN) defense; readiness; and installation preparedness, are inherently connected to AT, these programs also focus on other criminal and conventional threats. The overarching construct for these disparate activities is outlined in DODD 3020.40, *Mission Assurance (MA)*. AT is not only a sub-element of CbT, it is also a subset of the broader FP construct. FP consists of preventive measures to mitigate hostile actions against DOD personnel (to include DOD family members and DOD contractor personnel), resources, facilities, and critical information. FP does not include actions to defeat the enemy or protect against accidents, weather, or disease. While AT programs also integrate various FP-related programs to protect against terrorist attacks (e.g., physical security, CBRN passive defense, OPSEC, counterintelligence [CI], biometrics and forensics exploitation, and surveillance detection), it does not include all aspects of FP. That said, plans and capabilities developed for AT should be coordinated with other crisis management efforts to prevent or minimize redundant programs.

d. **FP and AT.** AT and FP are not synonymous (see Figure IV-1). AT is defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include rapid containment by local military and civilian forces. FP, on the other hand, is a broader construct that includes preventive measures taken to mitigate hostile actions against DOD personnel (to include family members), resources, facilities, and critical information.

e. **MA.** The *DOD Mission Assurance Strategy* provides a mission-centric framework to ensure resiliency for the capabilities and assets that support DOD mission-essential

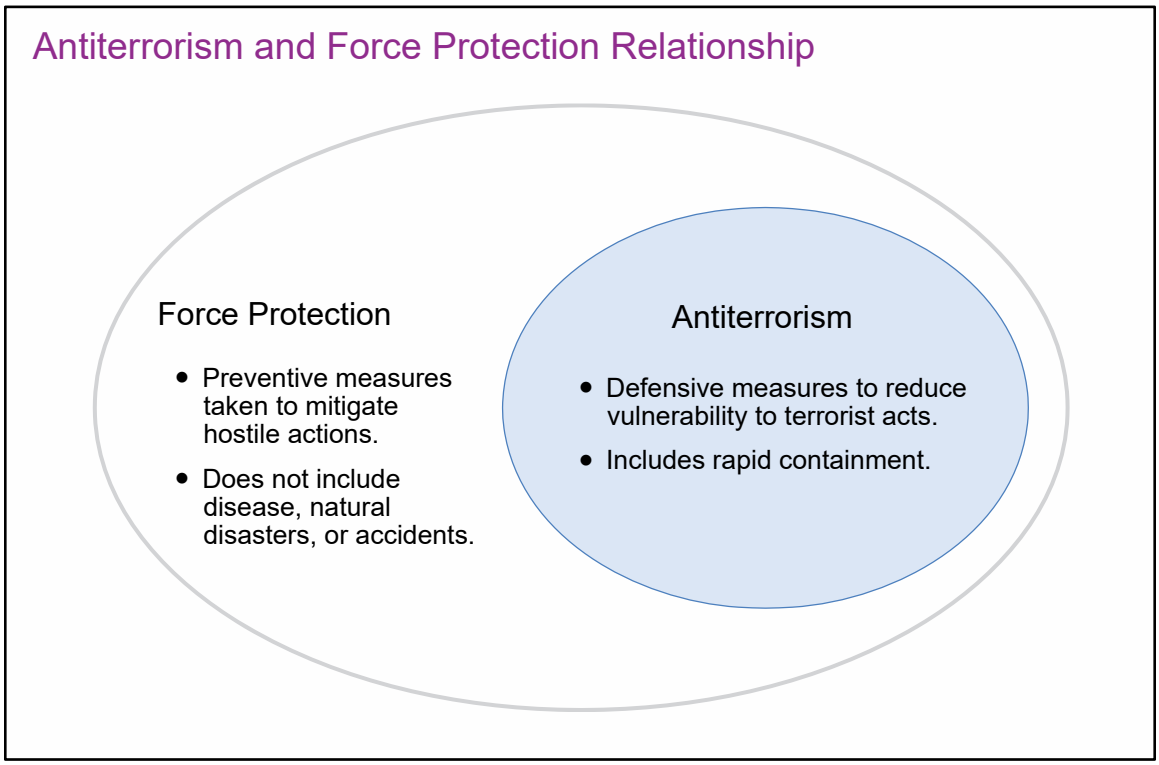


Figure IV-1. Antiterrorism and Force Protection Relationship

functions. The DOD AT program is one of the key components in that MA framework that also supports FP (see Figure IV-2). DODD 3020.40, *Mission Assurance (MA)*, provides the policy and responsibilities directly related to DOD mission execution as described in the *DOD Mission Assurance Strategy* and the MA implementation framework. DODI O-2000.16, Volume 1, *DOD Antiterrorism (AT) Program Implementation: DOD AT Standards,* implements the mandatory AT program elements as part of MA and provides standards for AT program elements. DOD uses MA as a process to protect or ensure the continued function and resilience of capabilities and assets by refining, integrating, and synchronizing the aspects of the DOD security, protection, and risk management programs that directly relate to mission execution. CCDRs synchronize MA through an integrated risk management methodology across CCMD missions, policies, plans, and programs mitigating risk from all threats and hazards to mission-critical capabilities, functions, and supporting assets.

f. **Assessments.** Commanders and component commanders may use higher HQ mission assurance assessments (MAAs) or joint mission assurance assessments (JMAAs) in lieu of annual comprehensive AT program reviews. An HQ MAA or JMAA will assess and evaluate the viability of the components' AT policies, the methodology for addressing resource shortfalls, interorganizational coordination, and synchronization of the AT program elements. An MAA is an assessment of the discipline under the MA umbrella (AT; DCI; chemical, biological, radiological, nuclear, and high-yield explosive preparedness; CBRN survivability; emergency management; cybersecurity; explosives safety; physical security; COOP; force health protection) to identify vulnerabilities and

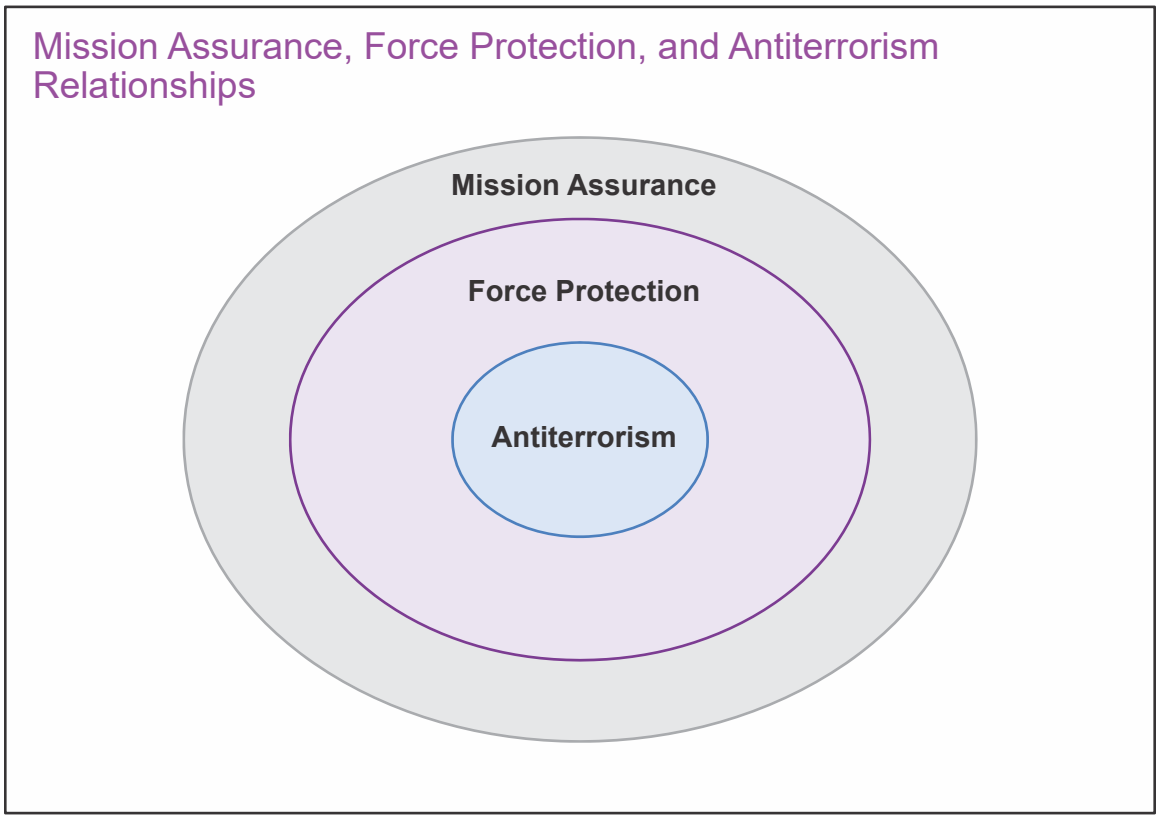


Figure IV-2. Mission Assurance, Force Protection, and Antiterrorism Relationships

gaps that could prevent accomplishment of a unit, installation, or higher-authority mission (see Figure IV-3 for a list of supporting MA-related programs).

2. Fundamentals of Antiterrorism

a. **Intelligence.** As with CT operations, accurate, timely, and relevant intelligence is critical in identifying and assessing terrorist capabilities, plans, intent, emerging trends, magnitude, probable courses of action, and possible targets. By integrating all available sources of intelligence, commanders have the basis for the development of an effective AT program. Intelligence provides the commander with a threat analysis of a terrorist group's operational capability, intentions, and activity, as well as the OE within which friendly forces operate. Commanders must carefully exercise judgment in estimating both the existing terrorist threat and the need for changes in AT measures. Accurate, timely, and relevant all-source intelligence provides decision makers with information and timely warnings upon which to recommend FP actions and build an effective AT program. An effective AT program contributes to disruption of threat incidents through preventive measures and includes proactive and reactive phases. There are numerous agencies and organizations within the IC, USG, and HN that have various responsibilities with regard to terrorist-related intelligence.

b. **Resilience.** Enemy capabilities have increased the need for a resilient joint force. The joint force achieves resiliency through professional military education and development, FP measures, depth, exchangeability, interoperability, and dispersal so that

Mission Assurance-Related Programs

Mission assurance-related programs and activities include, but are not limited to:

Programs/Activities	Supporting Guidance
Adaptive Planning	CJCS Instruction 3100.01
Antiterrorism	DODI O-2000.16
CBRN Survivability	DODI 3150.09
CBRNE Preparedness	DODI 3020.52
Continuity of Operations	DODD 3020.26
Cybersecurity	DODI 8500.01 and DODI 5205.13
Defense Critical Infrastructure	Contained in mission assurance policy.
Defense Security Enterprise. Composed of personnel, physical, industrial, information, and operational security programs; critical program information protection policy; and security training.	DODD 5200.43
Emergency Management	DODI 6055.17
Energy Resilience	DODI 4170.11
Fire Prevention and Protection	DODI 6055.06
Force Health Protection	DODD 6200.04
Insider Threat	DODD 5205.16
Law Enforcement. Suspicious activity reporting.	DODI 2000.26
Munitions Operations Risk Management	DODD 6055.09E
Operational Energy	DODD 4180.01
Readiness Reporting	DODD 7730.65

Legend

CBRN	chemical, biological, radiological, and nuclear	CJCS	Chairman of the Joint Chiefs of Staff
CBRNE	chemical, biological, radiological, nuclear, and high-yield explosives	DODD	Department of Defense directive
		DODI	Department of Defense instruction

Figure IV-3. Mission Assurance-Related Programs

a single attack cannot incapacitate it. Hardening includes not only physical barriers against attack but also virtual barriers to protect against cyberspace threats, electromagnetic pulse, and other disruptions. Depth provides the ability to replace capacity and capability with

reserves, as well as using the industrial base (the worldwide industrial complex with capabilities to perform research and development and design, produce, and maintain military weapon systems, subsystems, components, or parts to meet military requirements) to produce new assets. Exchangeability is the ability to substitute an asset for a lost one. The employment of multifunctional units and equipment that are both modular and scalable increases exchangeability and operational flexibility. Dispersal eliminates vulnerability to single-point failure. These considerations extend to the commercial infrastructure on which the joint force heavily depends, at both home and abroad.

c. **FP**

(1) **DOD Policy**

(a) DOD components, elements, and personnel shall be protected from terrorist acts through a high-priority, comprehensive AT program using an integrated systems approach.

(b) Commanders at all levels have the responsibility and authority to enforce appropriate security measures to ensure the protection of DOD elements and personnel subject to their control, including deployed DOD contractors authorized to accompany the force (CAAF) and other contractor personnel requiring access to military facilities, as referenced in DODI 3020.41, *Operational Contract Support (OCS).* Commanders should ensure the AT awareness and readiness of all DOD elements and personnel (including dependent family members) assigned or attached.

(c) The CCDR's AT policies take precedence over all AT policies or programs of any DOD component operating or existing in that CCDR's AOR (as applicable), except for those under the security responsibility of a COM. All DOD personnel traveling into or through a CCDR's AOR will familiarize themselves with all AOR and country-specific AT policies and comply with them.

(d) **Funding.** A funding source for emergent or emergency AT requirements is the Combatant Commander Initiative Fund (CCIF). For more information, refer to CJCSI 7401.01, *Combatant Commander Initiative Fund.*

(e) **Travel.** All personnel on DOD-related travel shall comply with theater, country, and special clearance requirements (DODD 4500.54E, *DOD Foreign Clearance Program [FCP]*) before overseas travel. Contractor personnel deploying with, or otherwise providing support to, the Armed Forces of the United States, in a theater of operations outside the United States, comply with DODI 3020.41, *Operational Contract Support (OCS).*

(f) **Contractor Personnel.** Protection of contractor personnel is a shared responsibility between the contractor and the government. For further information on FP and security of contractors, see DODI 3020.41, *Operational Contract Support (OCS),* and JP 4-10, *Operational Contract Support.*

For planning contractor personnel FP, see Chairman of the Joint Chiefs of Staff Manual 4301.01, Planning Operational Contract Support.

(2) **DOD Responsibilities.** The Assistant Secretary of Defense for Homeland Defense and Global Security (ASD[HD&GS]) provides overall supervision of AT, homeland defense (HD), DCI, and defense support of civil authorities (DSCA) activities within DOD. Specific to AT, ASD(HD&GS) has the following responsibilities:

(a) **Oversee High-Risk Personnel (HRP) Program.** For more information on HRP, refer to DODI O-2000.22, *Designation and Physical Protection of DOD High-Risk Personnel.*

(b) Monitor programs to reduce the vulnerability of DOD personnel and their family members, facilities, and other DOD materiel to terrorist attack with the CJCS and other DOD components.

(c) Provide policy and guidance for Defense Critical Infrastructure Program and oversee implementation of the activity.

(3) **Secretaries of the Military Departments**

(a) Institute and support AT programs in accordance with DODI 2000.12, *DOD Antiterrorism (AT) Program.*

(b) Provide AT resident training to personnel assigned to high-risk billets (HRBs) and others as appropriate.

(c) Ensure military construction programming policies include AT protective features for facilities and installations.

(d) Ensure all assigned military, DOD civilians, and their family members and DOD contractor personnel receive applicable AT training and briefings pursuant to DODI O-2000.16, Volume 1, *DOD Antiterrorism (AT) Program Implementation: DOD AT Standards.* Ensure personnel traveling to a CCMD AOR comply with DODD 4500.54E, *DOD Foreign Clearance Program (FCP*). Ensure personnel are aware of any DOS travel warnings and alerts in effect at the time of travel.

(4) **CJCS**

(a) Serve as the principal advisor to SecDef for all DOD AT issues.

(b) Prepare joint doctrine and assist ASD(HD&GS) in development and maintenance of the AT program, standards, and procedures. Review doctrine, policy, standards, and procedures of DOD components. Review, coordinate, and oversee AT training for all DOD personnel (including their dependent family members) in conjunction with DOD components.

(c) Assist ASD([HD&GS) with centralized policy and standard development for HRP programs, training, and support.

(d) Assess the DOD components' AT policies and programs for the protection of DOD elements and personnel, including DOD-owned, -leased, or -managed infrastructure and assets critical to mission accomplishment.

(e) Assess AT as an element of the overall force planning function of any force deployment decision. Periodically reassess the CCDR's AT posture of deployed forces.

(f) Assess the implementation of force protection conditions (FPCONs) for uniform implementation and dissemination as specified by DODI 2000.12, *DOD Antiterrorism (AT) Program,* and DODI O-2000.16, Volume 1, *DOD Antiterrorism (AT) Program Implementation: DOD AT Standards.*

(g) Coordinate with the Under Secretary of Defense for Intelligence and ASD(HD&GS) on sharing of intelligence on terrorism threats and CI data and information on AT.

(h) Assess the capability of the Military Departments, the CCMDs, and the DOD intelligence and security organizations to collect, receive, evaluate, analyze, and disseminate all relevant data on terrorist activities, trends, and indicators of imminent attack. Also assess the capability to fuse suspicious activity reports (SARs) from military security, LE, and CI organizations with national-level ISR collection activities.

(i) Manage and administer the CJCS CCIF.

(j) Maintain a centralized database of all vulnerability assessments (VAs). Prepare and disseminate analysis of DOD-wide vulnerability trends correlated to Military Department efforts within the process.

(k) Maintain the Antiterrorism Enterprise Portal.

(l) Review planned and ongoing activities and operations to leverage their inherent informational aspects to drive relevant actor behaviors in the context of AT.

(5) **CCDRs with applicable AORs.** As applicable, CCDRs have overall AT responsibility within their AOR, except for those DOD elements and personnel for whom a COM has security responsibility pursuant to law or a memorandum of agreement (MOA). Accordingly, CCDRs have the following AT responsibilities:

(a) Establish AT policies and programs for the protection of all DOD elements not under the authority of a COM within their AOR.

(b) Ensure AT policies and programs include specific prescriptive standards derived from DODI O-2000.16, Volume 1, *DOD Antiterrorism (AT) Program Implementation: DOD AT Standards*, to address specific terrorist capabilities and geographic settings, particularly regarding defense of critical infrastructure necessary for mission accomplishment (as defined in DODD 3020.40, *Mission Assurance [MA]*) and other DOD-owned, -leased, or -managed mission-essential assets.

(c) Exercise TACON authority for FP over all DOD personnel (including their family members) assigned, attached, transiting through, or training in the AOR, except for those for whom the COM retains security responsibility.

(d) Periodically assess and review the AT programs of all assigned and attached DOD components in their AOR. Assess the AT programs of all DOD components performing in their AOR, except for elements and personnel for whom the COM accepts or retains security responsibility (see Appendix D, "Policy, Jurisdiction, and Legal Considerations"). Component commands may be delegated responsibility to conduct these assessments. Ensure AT program reviews include a validation of the risk management methodology used to assess asset criticality, terrorist threat, and vulnerabilities. AT program reviews also evaluate installation and activity preparedness to respond to terrorist incidents (including CBRN incidents) and the plans for responding to terrorist incidents and maintaining continuity of essential military operations. Relocate forces as necessary and report to SecDef, through the CJCS, pertinent actions taken for protection.

(e) Consistent with DODI 5210.84, *Security of DOD Personnel at US Missions Abroad*; DODI 5240.22, *Counterintelligence Support to Force Protection;* and all appropriate memorandums of understanding (MOUs), serve as the DOD point of contact with HN officials on matters involving AT policies and programs.

(f) Provide updates to DODD 4500.54E, *DOD Foreign Clearance Program (FCP),* stating command travel requirements and theater entry requirements.

(g) Upon arrival in their AOR, ensure all assigned military, DOD civilians and their family members, and DOD contractor personnel receive applicable AT training and briefings pursuant to DODI O-2000.16, Volume 1, *DOD Antiterrorism (AT) Program Implementation: DOD AT Standards.* Ensure personnel traveling within or through their AOR comply with DODD 4500.54E, *DOD Foreign Clearance Program (FCP).* Ensure personnel are aware of any DOS travel warnings and alerts in effect at the time of travel. Provide information necessary to ensure all DOD personnel (including dependent family members) scheduled for permanent change of station to their AOR receive required AT training and briefings (e.g., AOR updates) in compliance with DODI O-2000.16, Volume 1, *DOD Antiterrorism (AT) Program Implementation: DOD AT Standards,* before departing their previous assignments. Identify and disseminate to deploying force providers specific AOR predeployment training requirements that all personnel, including CAAF, must complete before arrival in theater. All CAAF are required to comply with applicable CCDR and local commander FP policies.

(h) Identify, document, validate, prioritize, and submit to the Joint Staff the resource requirements necessary to achieve the AT program objectives for each activity under the CCDR or for which that commander has responsibility. Work with the Joint Staff and the Service component commands to ensure resource requirements to implement the AT programs are identified and programmed according to Planning, Programming, Budgeting, and Execution (PPBE) procedures.

(i) Establish command relationships and policies for subordinate commands, including JTFs, to ensure effective mechanisms are in place to maintain protective posture commensurate with the terrorist threat.

(j) Assess the terrorist threat for the AOR according to DODI 2000.12, *DOD Antiterrorism (AT) Program*, and provide TA information to DOD components and the COMs in the AOR. Develop risk mitigation measures and maintain a database of those measures and the issues that necessitated their implementation. On the basis of the TA, identify and designate incumbents of HRBs and dependent family members to receive AT resident training.

(k) Keep subordinate commanders informed of the nature and degree of the threat. Ensure commanders are prepared to respond to changes in threats and local security circumstances. Ensure the COMs are fully and currently informed of any threat information relating to the security of those DOD elements and personnel under their responsibility.

(l) Ensure compliance with the "no double standard" policy.

(m) Submit to the CJCS priority-emergent or emergency AT requirements that cannot be funded by the Military Departments for CCIF funding consideration (or through CbT Readiness Initiatives Fund when available).

(n) Ensure FPCONs are implemented and disseminated.

(o) Coordinate AT program issues with the functional CCDRs, COMs, DOD agencies and field activities, and Military Departments, as appropriate.

(p) Ensure a capability exists to collect, receive, evaluate, analyze, and disseminate all relevant data on terrorist activities, trends, and indicators of imminent attack. Develop and implement the capability to fuse biometrics-enabled intelligence, technical and forensics information, and SARs from military security, LE, and CI organizations with national-level ISR collection activities.

(q) Ensure subordinate commanders establish screening and access control policies and procedures for all personnel, to include contractor employees, requiring access to DOD installations consistent with DODI 5200.08, *Security of DOD Installations and Resources and the DOD Physical Security Review Board (PSRB)*, and DOD 5200.08-R, *Physical Security Program.* This requirement is especially pertinent to contractor personnel who have not been issued common access cards.

(6) **CCDRs without AORs**

(a) Establish AT policies and programs for assigned DOD elements and personnel, including assessment and protection of facilities and appropriate level of AT training and briefings. Coordinate programs with the appropriate CCDR and, in coordination with the CCDR, the COM.

(b) Coordinate with the CCDRs to ensure adequate AT measures are in place.

(c) Ensure subordinate elements that are tenant units on DOD installations and facilities coordinate their AT programs and requirements with their respective host installation commanders. Resolve differences through the applicable CCDR and the Service component command chain of command.

(d) Submit emergent or emergency AT fund requests to the CJCS.

(e) Identify, document, and submit to the Joint Staff the resource requirements necessary to achieve AT program objectives for each activity under the CCMD or for which the commander has responsibility. Work with the Service component commands to ensure resource requirements to implement the AT programs are identified and programmed according to PPBE procedures.

(7) **Directors of Other DOD Agencies and Components**

(a) Support CCDRs as they execute their AT programs. Institute AT programs of their own that include VAs and contingency response plans.

(b) Utilize DODI O-2000.16, Volume 1, *DOD Antiterrorism (AT) Program Implementation: DOD AT Standards*, for the AT planning and execution for their HQ and all activities under their cognizance; consider mission, characteristics of the activity, geographic location, threat level, and FPCON. Establish prescriptive AT standards for installations and facilities not located on US military installations. Coordinate with the applicable CCDR to ensure AT policies and programs are in concert with the CCDRs' overall responsibility for the AOR, as applicable.

(c) Comply with DODI O-2000.16, Volume 1, *DOD Antiterrorism (AT) Program Implementation: DOD AT Standards*, requirements to maintain an AT training and exercise program. Ensure all assigned personnel comply with DODD 4500.54E, *DOD Foreign Clearance Program (FCP).* Ensure personnel are aware of any travel security advisories in effect at the time of travel. Ensure all DOD personnel (including dependent family members) scheduled for permanent changes of station to foreign countries receive required AT training or briefing specified in DODI O-2000.16, Volume 1, *DOD Antiterrorism (AT) Program Implementation: DOD AT Standards,* before departing their current assignment.

(d) As part of the PPBE process, identify and document resource requirements necessary to implement and maintain AT programs. Submit AT requirements to SecDef with an information copy to the CJCS and the appropriate CCDRs. Include resource requirements in program and budget submissions. For emergent or emergency AT requirements that cannot be funded through other means, submit requests through the appropriate CCDR to the CJCS. Implement accounting procedures to enable precise reporting of data submitted to Congress in the Congressional Budget Justification Book, including the number and cost of personnel directly supporting the DOD's AT program.

(e) Identify and designate incumbents of billets that are potentially high-risk targets of terrorist attacks and dependent family members requiring AT resident training. Ensure AT resident training is provided to personnel assigned to HRBs and others, as applicable.

(f) Ensure current physical security technology and security requirements are incorporated into all new contracts, where appropriate.

(g) Ensure AT protective features for facilities and installations are included in the planning, design, and execution of military and minor construction projects to mitigate vulnerabilities and terrorist threats (Unified Facilities Criteria [UFC] 4-020-01, *DOD Security Engineering Facilities Planning Manual;* UFC 4-010-01, *DOD Minimum Antiterrorism Standards for Buildings;* UFC 4-022-01, *Security Engineering: Entry Control Facilities/Access Control Points;* UFC 4-010-02, *DOD Minimum Antiterrorism Standoff Distances for Buildings;* and UFC 4-021-01, *Design and O&M: Mass Notification Systems).*

d. **Agency Leads.** With respect to CbT and other HS concerns, DOD is not the lead agency, but it has significant supporting roles in several areas. In HD missions, DOD is the lead and is supported by other USG departments and agencies. Title 6, USC, Section 456, states, "Nothing in this chapter shall confer upon the Secretary [of Homeland Security] any authority to engage in warfighting, the military defense of the United States, or other military activities, nor shall anything in this chapter limit the existing authority of the Department of Defense or the Armed Forces to engage in warfighting, the military defense of the United States, or other military activities."

For more information on operations in the homeland, see JP 3-27, Homeland Defense, *and JP 3-28,* Defense Support of Civil Authorities.

3. Antiterrorism Intelligence Roles and Responsibilities

a. **National-Level AT Intelligence Roles and Responsibilities.** Within the United States, the FBI collects and processes terrorist information to protect the United States from terrorist attacks. Overseas, intelligence on terrorist threats is principally a Central Intelligence Agency (CIA) responsibility, but DOS, DIA, and the HN are also participants. Military intelligence activities are conducted in accordance with EOs, federal law, status-of-forces agreements (SOFAs), MOUs, and applicable Service regulations.

b. **DOD AT Intelligence Roles and Responsibilities**

(1) **DIA.** The Director, DIA, who is responsible to the Under Secretary of Defense for Intelligence, maintains an international, all-source, intelligence fusion center focusing on terrorism. The DCTC provides a wide range of intelligence on terrorist threats for DOD components, to include warning intelligence, current intelligence, assessments, in-depth analysis, DOD terrorism TAs/levels, and the maintenance of a CbT database. DIA's DCTC is responsible for setting DOD terrorism threat levels for all countries. Terrorism threat levels are country-wide assessments based on terrorists' intentions, capabilities, and operational activity and the OE. When determining a terrorism threat

level, DCTC focuses on terrorists' intent and operational activity and capability to conduct attacks when making the final decision on the threat level, as depicted in Figure IV-4. This decision is guided by the terrorism threat assessment factors in the *DOD Antiterrorism Officer's Guide*. DCTC coordinates terrorism threat level changes with the Defense Intelligence All-Source Analysis Enterprise.

(2) **CCDR.** CCDRs, through the intelligence directorate of a joint staff, joint intelligence operations center, command CI coordinating authority, and subordinate component command CI and AT organizations, and in consultation with DIA, the CIA, the US country team, and applicable HN authorities, collect intelligence and CI information specific to the operational area and issue intelligence and CI reports, advisories, and assessments. These relationships are the backbone for disseminating intelligence and CI

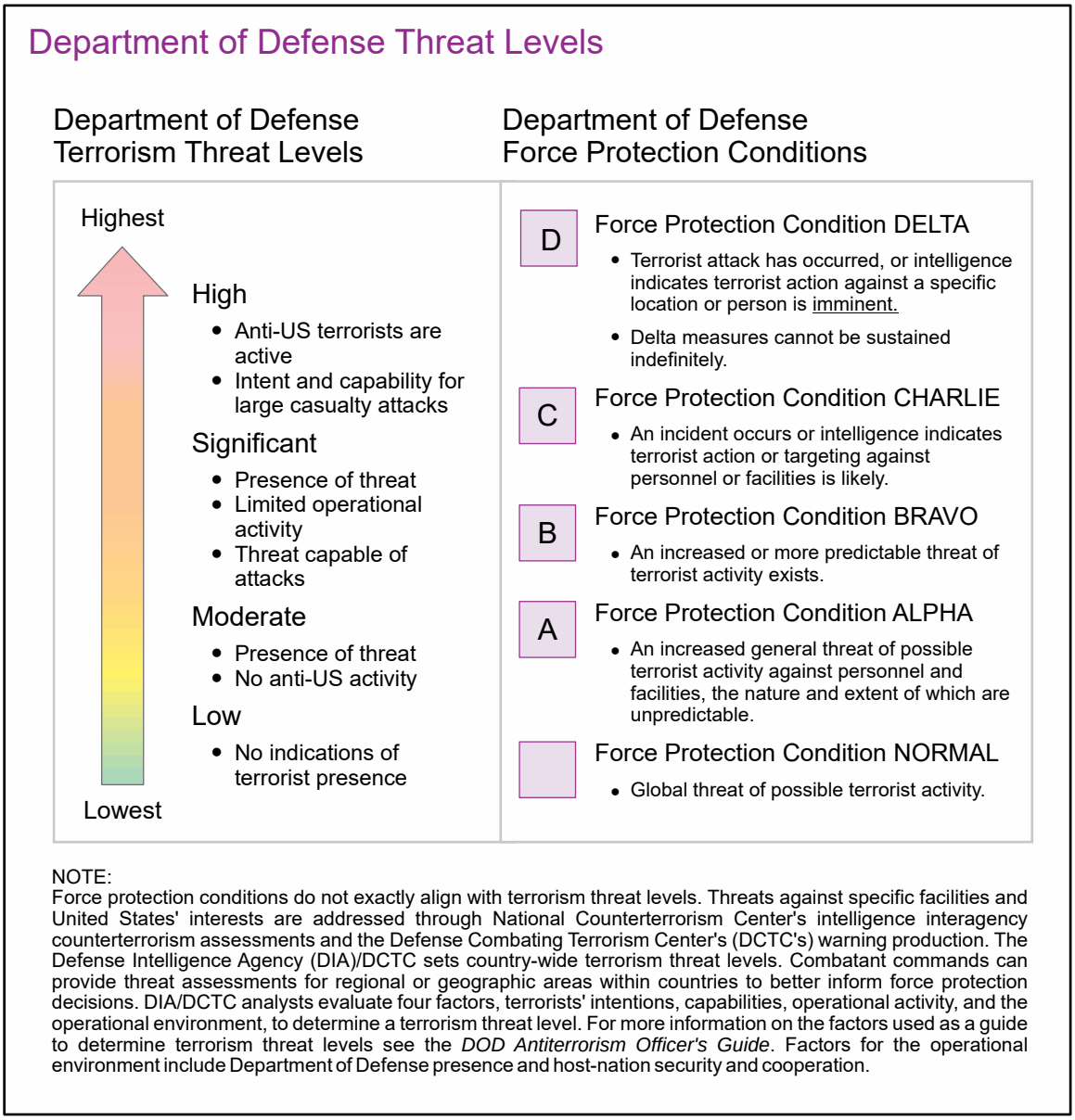


Figure IV-4. Department of Defense Threat Levels

information, advisories, and warnings of terrorist threats throughout the region. CCDRs may also set terrorism threat levels within their AOR (as applicable) in accordance with DODI O-2000.16, Volume 1, *DOD Antiterrorism (AT) Program Implementation: DOD AT Standards.*

(3) **Services.** DODI 2000.12, *DOD Antiterrorism (AT) Program*, and DODI 2000.26, *Suspicious Activity Reporting (SAR)*, task the Secretaries of the Military Departments to ensure Service component commands have the capability to collect, receive, evaluate, analyze, and disseminate all relevant data on terrorist activities, trends, and indicators of imminent attack and to develop the capability to fuse SARs from military security, LE, and CI organizations with national-level ISR collection activities. DODI 2000.26, *Suspicious Activity Reporting (SAR)*, establishes the eGuardian system to serve as the DOD LE SAR system. eGuardian is the FBI unclassified, LE-centric threat reporting system. Note: Although the CJCS has oversight of the responsibility and procedures for the documentation, storage, and exchange of SARs, SARs are applicable to all DOD components.

(a) Provide Service commanders with information on terrorist threats concerning their personnel, facilities, and operations.

(b) Investigate terrorist incidents with the FBI or HN authorities looking for intelligence, CI, and FP-relevant information.

(c) Provide terrorist threat information in threat briefings.

(d) Conduct liaison with representatives from federal, state, and local agencies (county, tribal, city) and, if applicable, HN agencies to exchange information on terrorists.

(e) Provide international terrorism summaries and other threat information to supported commanders. On request, provide current intelligence assessments and CI data on terrorist groups and disseminate time-sensitive and specific threat warnings to appropriate commands.

(4) **Investigative Agencies.** Service criminal investigative services (e.g., United States Army Criminal Investigation Command, Naval Criminal Investigative Service, Air Force Office of Special Investigations) collect and evaluate criminal information and disseminate terrorist-related information to supported installation and activity commanders, as well as to the Service lead agency. As appropriate, criminal investigative elements also conduct liaison with local military police or security personnel and civilian LE agencies.

(5) Intelligence staff elements at all echelons have the following responsibilities:

(a) Promptly report all actual or suspected terrorist incidents, activities, and indicators/early warnings of terrorist attack to supported and supporting activities, the local CI office, and through the chain of command to the Service lead agency.

(b) Adhere to the "no double standard" policy. The policy that no double standard exists regarding the availability of terrorist threat information and that terrorist threat information shall be disseminated as widely as possible within applicable law and regulations.

For more information on the policy, to include requirements, responsibilities, and procedures, see DODI 2000.12, DOD Antiterrorism (AT) Program.

(c) Initiate and maintain liaison with the security personnel or provost marshal's office; local military criminal investigative offices; local CI offices; security offices; HN agencies; and (as required or allowed by law or policy) other organizations, elements, and individuals.

(d) Develop and present terrorism threat awareness briefings to all personnel within their commands in cooperation with the local CI office.

(e) LE, military police, and security personnel staff elements will be responsible for the following:

1. Report all actual or suspected terrorist incidents or activities to their immediate commander, supported activities, and Service lead agency through established reporting channels.

2. Initiate and maintain liaison with local CI offices and military criminal investigative offices.

3. Maintain liaison with federal, HN, and local LE agencies or other civilian and military AT agencies as appropriate and as provided in Service or agency regulations.

(f) Installation, base, ship, unit, and port security officers will:

1. Report all actual or suspected terrorist incidents or activities to their immediate commander, supporting military LE office, other supported activities, local CI office, and local military criminal investigative office.

2. Conduct regular liaison visits with the supporting military LE office, CI office, and local criminal investigation office.

3. Coordinate with the supporting military LE office and CI offices on their preparation and continual updating of the TAs.

4. Assist in providing terrorism threat awareness training and briefings to all personnel and family members as required by local situations.

(g) Services, DOD agencies, and installations should submit SARs through their chain of command.

(h) Commanders will develop and implement proactive defensive techniques to detect, deter, and defeat terrorists, particularly in support of DOD elements and personnel or activities conducted in areas designated with "significant" or "high" threat levels. These activities include, but are not limited to, in-transit forces, HRP, special events, and high-value military cargo shipments.

(6) **IRs.** To focus threat analysis, the intelligence staff identifies significant gaps in what is known about the enemy and other relevant aspects of the OE and formulates intelligence requirements (general or specific subjects upon which there is a need for the collection of information or the production of intelligence). All staff sections may recommend intelligence requirements for designation as PIRs—a priority for intelligence support that the commander and staff need to understand the threat and other aspects of the OE. The JFC designates PIRs, which, together with friendly force IRs, constitute the CCIRs. Based on identified intelligence requirements (to include PIRs), the intelligence staff develops more-specific questions known as IRs (those items of information that must be collected and processed to develop the intelligence required by the commander). A subset of IRs that are related to and would answer a PIR are known as essential elements of information (see Figure IV-5).

4. Antiterrorism Programs

a. AT Program Overview

(1) Protection of DOD personnel and assets from acts of terrorism is one of the most complex challenges for commanders. AT programs consist of defensive measures to reduce the vulnerability of individuals and property to terrorist acts, including rapid containment by local military and civilian forces. An integrated and comprehensive AT program must be developed, implemented, and updated to effectively detect, defend, and respond to a terrorist threat.

(2) **AT Program Elements.** As a subset of the overarching FP program, the AT program is a collective, proactive effort focused on the prevention and detection of terrorist attacks against DOD personnel and their families, facilities, installations, and infrastructure critical to mission accomplishment, as well as the preparation to defend against and planning for the response to the consequences of terrorist incidents. Important adjuncts to an effective AT program include plans for the initial response to a terrorist incident, as well as plans for continuing essential military operations. The minimum elements of an AT program are AT risk management, planning, training and exercises, resource management, and a program review.

(3) The AT program contains command-specific guidance, as outlined in DODI O-2000.16, Volume 1, *DOD Antiterrorism (AT) Program Implementation: DOD AT Standards,* that includes measures designed to mitigate terrorist threats to off-installation DOD facilities, including assets that DOD identifies as critical to its operations in accordance with DODI 3020.45, *Mission Assurance (MA) Construct*. At a minimum, AT programs should be developed at the DOD-owned or DOD-leased, off-installation facilities

Information Requirements

Organization, Size, and Composition of Group

- Motivation, mission, vision
- Organization's long- and short-term goals
- Religious, political, academic, cultural, and ethnic affiliations
- International and national support (e.g., moral, physical, financial)
- Recruiting methods, locations, and targets (e.g., students)
- Identity of group leaders, opportunists, and idealists
- Group intelligence capabilities and connections with other terrorist groups
- Sources of supply and support
- Important dates
- Planning ability
- Internal discipline
- Preferred tactics and operations
- Willingness to kill
- Willingness for self-sacrifice
- Group skills (demonstrated or perceived) (e.g., sniping, demolitions, masquerade, industrial sabotage, airplane or boat operations, tunneling, underwater, electronic surveillance, poisons or contaminants)
- Equipment and weapons (on-hand and required)
- Transportation (on-hand and required)
- Medical support availability
- Means and methods of command and control
- Historical background, relations, operations, records, locations, and activities

NOTE:
List is not all-inclusive.

Figure IV-5. Information Requirements

and ships and also for operational deployments and training exercises or events. AT programs will include, but are not limited to, housing (including high-population housing), transportation services, child development and youth program facilities, medical facilities, recruiting centers, reserve centers, and other activities used by or involving a mass-gathering of DOD personnel and their family members and special events. AT programs and planning will:

(a) Synchronize AT programs with existing installation emergency management (IEM) plans. Incorporate AT tenants into all operation plans (OPLANs) and risk decisions to support the DOD components' unique roles, mission requirements, AT programs and planning, and activities to assist commanders with synchronizing more effective training and exercises for mitigating and remediating efforts at the local/installation level. Achieve the same objectives as other protection programs to manage risk through the

protection function. For example, coordinating with IEM in the execution of an installation AT and IEM exercise enables commanders to assess capabilities and the ability to respond to incidents (manmade and natural), including implementation of CBRN response. Exercising AT efforts assists in reducing task duplication (e.g., risk management) and enables better safety and security of DOD military personnel, civilians, family members, contractor personnel, facilities, infrastructure, and information.

(b) Establish mass warning and notification systems and recall procedures.

(c) Publish guidance for selection of off-installation housing, temporary billeting, and other soft targets.

(d) Establish chemical, biological, radiological, nuclear, and high-yield explosive measures in accordance with DODI 3020.52, *DOD Installation Chemical, Biological, Radiological, Nuclear, and High-Yield Explosive (CBRNE) Preparedness Standards,* and procedures for incident preparedness, physical security, lock down, shelter-in-place, relocation, and evacuation.

See DODI 2000.12, DOD Antiterrorism (AT) Program, *and DODI O-2000.16, Volume 1,* DOD Antiterrorism (AT) Program Implementation: DOD AT Standards, *for more information on these program elements.*

b. **Risk Management Process.** The risk management process is used to identify, assess, and mitigate risk arising from operational factors and make decisions that balance risk and cost with mission benefits. AT risk management allows the commander to decide how best to employ given resources and AT measures to deter, prevent, or mitigate a terrorist attack, balancing risk and cost while ensuring mission readiness. The risk management process consists of three key elements—TA, criticality assessment, and VA—which are used to produce a final risk assessment (RA). Commanders may use the MA objectives in the Enterprise Risk Management System to help complete the RA process.

(1) **TA.** The terrorism TA determines the capabilities, intentions, and activity of terrorist organizations. Each organization's doctrine, mindset, and objectives should be considered when evaluating its intentions. Red teams may be employed to use threat emulation to explore potential options available to the terrorist organization. Prescribed annual installation-level AT TAs are built by integrating threat information prepared by intelligence and LE communities. Tools, such as the Under Secretary of Defense for Intelligence Defense TA, are available as resources. The DCTC is the DOD focal point for the analysis of data and information pertaining to domestic and foreign terrorist threats to DOD personnel (excluding threats posed by US persons who have no discernable foreign control or connections). The DCTC also disseminates intelligence on foreign terrorist threats, including specific warning of threats against DOD personnel (including family members) and assets and is a starting point for any TA.

(2) **Criticality Assessment.** The criticality assessment provides the commander with a list of key assets and infrastructure based on the necessity for mission completion. An asset's criticality is determined by the impact of its loss on the mission. This can

include physical infrastructure and HRP, as well as the Internet and computer systems. Critical assets will be identified and prioritized in accordance with DODI, 3020.45, *Mission Assurance (MA) Construct.*

(3) **VA.** Vulnerability is determined by the level of susceptibility to attack by a broad range of terrorist threats against DOD personnel and assets. VAs for critical infrastructure should also address susceptibility to hazards (e.g., acts of nature, human error). Commanders are required to conduct a VA annually or more often as circumstances warrant.

c. **AT Training and Exercises.** An AT program should include training for development of individual, leader, and collective skills, and the conduct of comprehensive exercises to validate AT plans. AT training includes:

(1) Annual exercise of AT plans.

(2) Formal AT training (Levels I-IV for appropriate personnel).

(3) AOR-specific training.

(4) Training for HRP and personal security detachment personnel.

(5) Exercise documentation and process improvement/review.

d. **Resource Management.** The PPBE process is the resource mechanism used to identify baseline and supplemental needs. Unfunded requirements to support a commander's mission (e.g., priority emergent requirements) can be submitted via the CCIF process.

e. **Program Review.** A program review is required at least annually, during predeployment preparations and when significant changes occur regarding threat, asset criticality, or vulnerability. Commanders and component commands may use higher HQ assessment (e.g., MAA or JMAA) reports in lieu of annual AT program reviews.

5. Command, Control, Plan, and Assess Antiterrorism Activities and Operations

a. **AT Planning.** AT planning is the process of developing specific guidance, measures, and instructions to deter, mitigate, and prepare for a terrorist incident. The AT plan contains command-specific guidance to establish and maintain an AT program as outlined in DODI O-2000.16, Volume 1, *DOD Antiterrorism (AT) Program Implementation: DOD AT Standards.* At a minimum, AT plans should be developed at the installation, separate or leased facility or space, and ship levels and also for operational deployments, training exercises or events, and special events. If applicable, AT plans can be synchronized with any existing installation emergency management plan while incorporating the assessments from the risk management process. AT tenets should also be incorporated into all OPLANs and risk decisions to support the DOD components' unique roles and mission requirements. Additionally, stand-alone documents (e.g., standard operating procedures, local regulations, and operations orders articulating

requirements for these key elements) should be replicated and referenced in the AT plan. During the planning process, the JFC should consider the need for exploitation support to help fulfill the requirements for information about the OE (see Figure IV-6), identify potential threats to US forces, and understand the capabilities and capacity of adversary networks. The JFC can establish a joint force exploitation staff element (J-2E), in coordination with the operations directorate of a joint staff, to plan and manage exploitation resources. At the JTF level, the J-2E is established as necessary to integrate and synchronize disparate theater-level military, intelligence, LE, multinational, and HN collection and exploitation capabilities and processes. The J-2E (when organized) establishes policies and procedures for the coordination and synchronization of the exploitation of captured threat materials. The J-2E will evaluate and establish the commander's collection and exploitation requirements for deployed laboratory systems or material evacuation procedures based on the mission; its object and duration; threat-based, military geographic factors; and authorities granted to collect and process captured material.

(1) Enable broad discoverability, accessibility, and usability of exploitation information at all levels to support force protection; targeting; material sourcing; signature characterization of enemy activities; and the provision of materials collected, transported, and accounted for with the fidelity necessary to support prosecution of captured insurgents or terrorists.

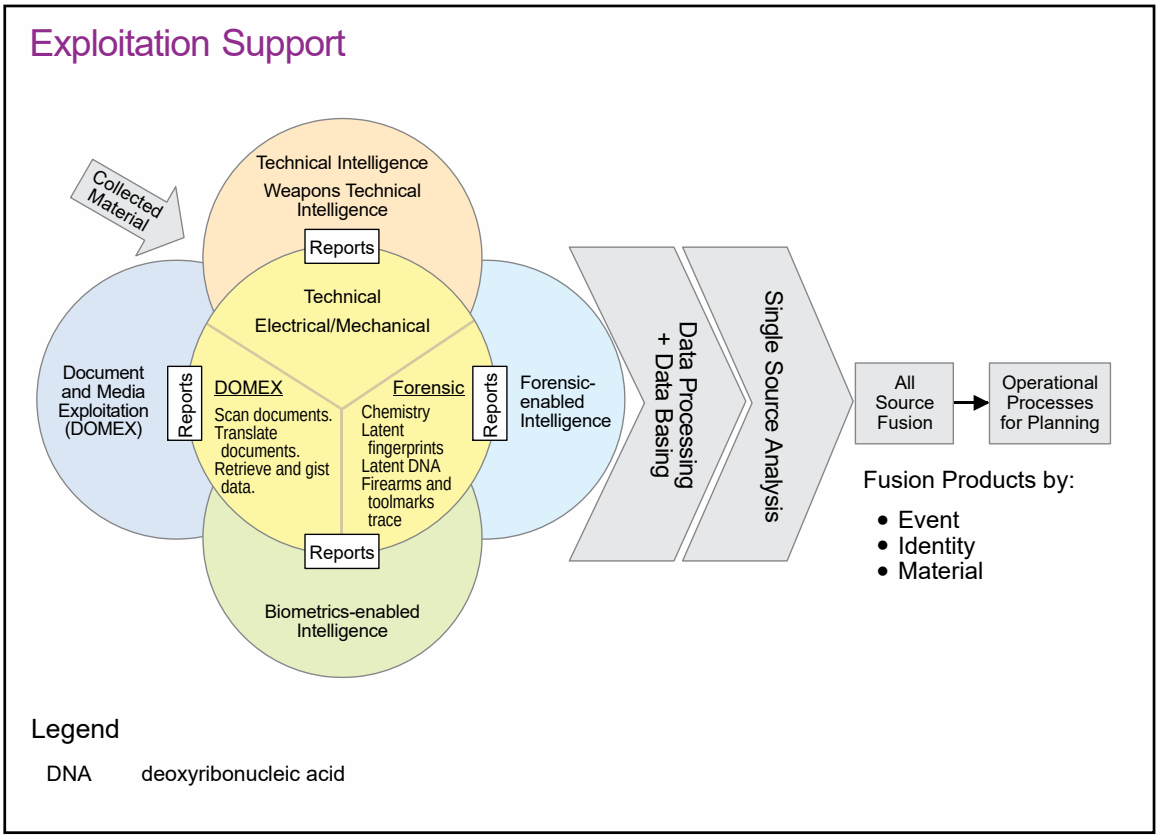


Figure IV-6. Exploitation Support

(2) Prepare collection plans for a subordinate exploitation task force responsible for finding and recovering battlefield materials.

(3) Provide direction to forces to ensure the initial site collection and exploitation activities are conducted to meet the commanders' requirements and address critical information and intelligence gaps.

(4) Ensure exploitation enablers are integrated and synchronized at all levels and their activities support collection on behalf of the commander's PIRs. Planning includes actions to:

(a) Identify units and responsibilities.

(b) Ensure exploitation requirements are included in the collection plan.

(c) Define priorities and standard operating procedures for materiel recovery and exploitation.

(d) Coordinate transportation for materiel.

(e) Establish technical intelligence points of contact at all levels to expedite dissemination.

(f) Identify required augmentation skill sets and additional enablers.

b. **AT Assessment.** Commanders and component commanders may use higher HQ MAAs or JMAAs in lieu of annual comprehensive AT program reviews. An HQ MAA or JMAA will assess and evaluate the viability of the components' AT policies, the methodology for addressing resource shortfalls, interorganizational coordination, and synchronization of the AT program elements.

6. Organize for Antiterrorism Activities and Operations

A JTF may have several elements supporting CbT (see Figure IV-7). Historically, the JTF provost marshal has been seen as the principal staff advisor to the JTF commander on AT and FP matters, as well as military police and criminal investigation division employment across the competition continuum. This consists of security support to promote stability within the joint security area (JSA). The provost marshal develops and issues policies, programs, and guidance to plan and conduct military police operations. JTF security elements will perform six functions: maneuver and mobility, area security, internment and resettlement, law and order, police intelligence, and AT. An additional special function includes air base defense. The JTF provost marshal is the principal command liaison with US civilian and military LE agencies, as well as the HN and US embassy security elements. While the provost marshal is a logical choice to provide overall AT matters, other staff sections and individuals play a critical role in establishing an expanded CbT fusion cell or group.

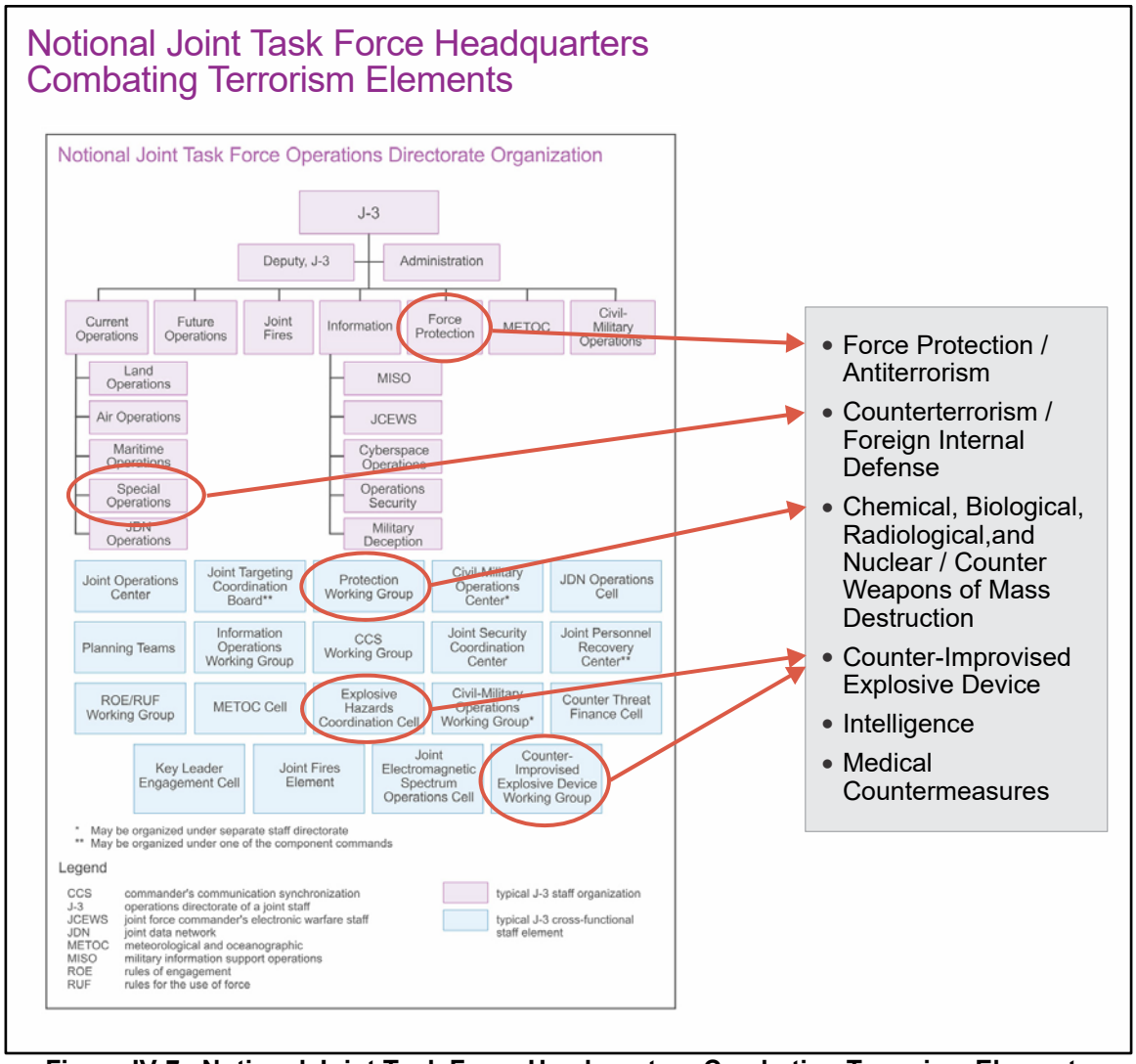


Figure IV-7. Notional Joint Task Force Headquarters Combating Terrorism Elements

7. Joint Security Area Antiterrorism Activities

a. **General.** A JSA is a specific surface area designated by the JFC to facilitate protection of joint bases and their connecting LOCs that support joint operations. Regional political considerations and sensitivities will influence whether a JSA is established. JSAs may be established in different countries in a CCDR's AOR, as applicable. The airspace above the JSA is normally not included in the JSA. This airspace is normally governed by procedures promulgated in the airspace control order (see JP 3-52, *Joint Airspace Control*). The JSA will typically evolve as the operational area changes in accordance with requirements to support and defend the joint force. An amphibious objective area may precede a JSA when establishing a lodgment. A lodgment would normally be expanded to an area including existing ports and airfields from which operations could be conducted and then eventually evolve to areas including multiple countries and sea bases. Joint planners should be aware that bases, base clusters, and forward operating bases may be referred to in higher-level guidance as contingency locations or contingency bases.

For more information on contingency locations and base classification, see DODD 3000.10, Contingency Basing Outside the United States; *JP 4-04,* Contingency Basing; *and JP 3-10,* Joint Security Area Operations in Theater.

b. The size of a JSA may vary considerably and is highly dependent on the size of the operational area, mission-essential assets, logistic support requirements, threat, or scope of the joint operation. The JSA may be used in both linear and nonlinear operations. In linear operations, the JSA may be included in, be separate from, or adjoin the rear areas of the joint force land component commander, joint force maritime component commander, or Service component commanders. JSAs may be designated where joint forces are engaged in combat operations or where stability activities are the primary focus. Providing security of units, activities, bases and base clusters, and LOCs located in noncontiguous areas presents unique challenges based on the location, distance between supporting bases, and the security environment.

c. **JSA AT Measures.** AT are a large part of the base security plan and consist of defensive measures to reduce the vulnerability of individuals and property to terrorist acts, including rapid containment by local military and civilian forces. Commanders use an "all hazards" approach to planning for terrorist response. The term "all hazards" means a threat or an incident, natural or manmade, that warrants action to protect life, property, the environment, and public health or safety and to minimize disruptions of government, social, or economic activities. It includes natural disasters, cyberspace threat incidents, industrial accidents, pandemics, acts of terrorism, sabotage, and destructive criminal activity targeting critical infrastructure. Figure IV-8 depicts a notional structure for JSAs in which all bases are located in a land component commander's area of operations.

d. **Protection.** The protection function focuses on preserving the joint force's fighting potential in four primary ways. One way uses active defensive measures that protect the joint force and its information, bases, necessary infrastructure, and LOCs from an enemy attack. Another way uses passive defensive measures that make friendly forces, systems, and facilities difficult to locate, strike, and destroy. What is important for both is the application of technology and procedures to reduce the risk of friendly fire incidents. Finally, emergency management and response reduce the loss of personnel and capabilities due to accidents, health threats, and natural disasters.

e. **Security.** The purpose of security is to prevent the enemy from acquiring unexpected advantage. Security enhances freedom of action by reducing friendly vulnerability to hostile acts, influence, or surprise. Security results from the measures taken by commanders to protect their forces. Staff planning and an understanding of enemy strategy, tactics, and doctrine enhance security. Risk is inherent in military operations. Application of this principle includes prudent risk management, not undue caution.

f. **Integration.** In a JSA, an integrated approach to security is critical to the protection of joint bases and their connecting LOCs that support joint operations. The integration of multiple security activities is a combination of protective measures, implemented by organizations throughout the joint force, to protect the force. Some essential, integrated security activities include:

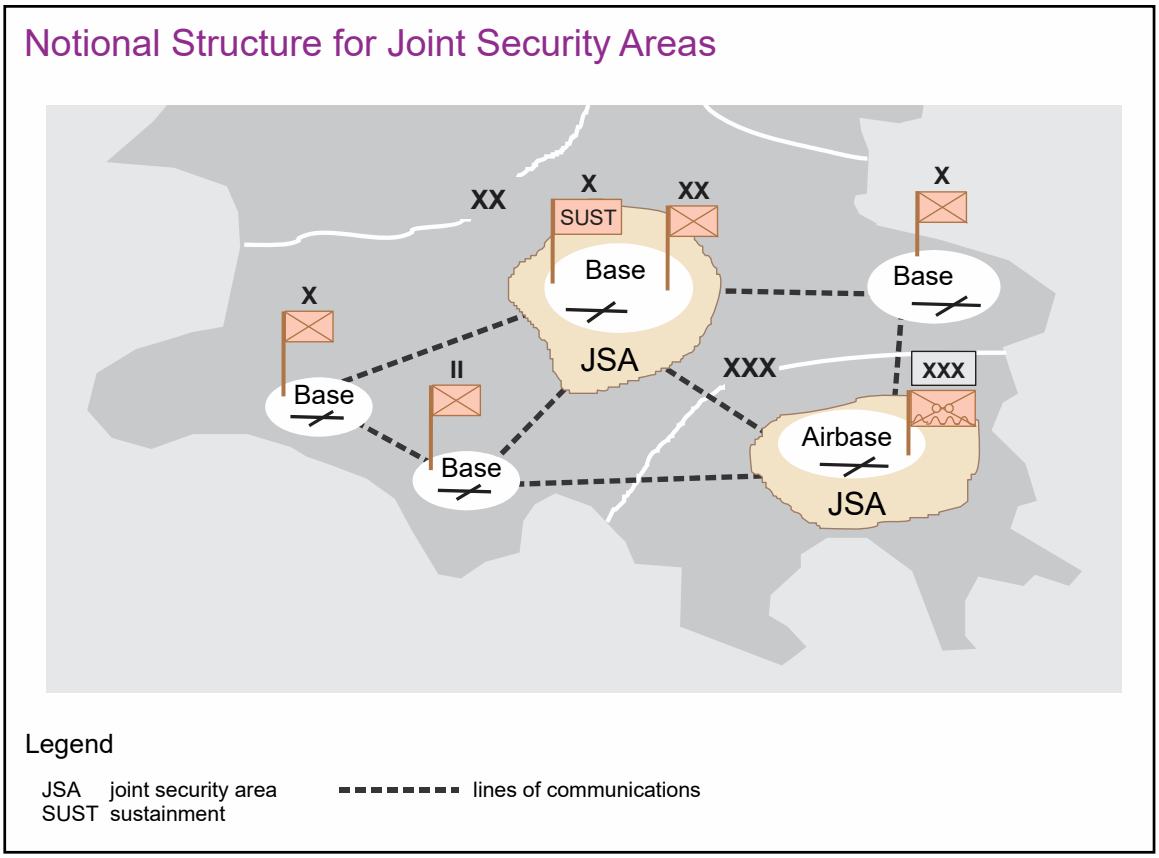


Figure IV-8. Notional Structure for Joint Security Areas

(1) **Communications Security.** Communication security is the result of all measures designed to deny unauthorized persons information of value that might be derived from the possession and study of telecommunications or to mislead unauthorized persons in their interpretation of the results of such possession and study. JP 6-0, *Joint Communications System,* provides additional information on communications security. For additional guidance on communications security, see Department of Defense Manual (DODM) 5105.21, Volume 1, *Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Information and Information Systems Security.*

(2) **Cybersecurity.** Cybersecurity policy requires measures to maintain the availability, integrity, authentication, confidentiality, and nonrepudiation of computers, communications systems, electronic communications services, wire communication, and electronic communication, to include the associated information. LOCs must be protected not only from destruction but also from sabotage and surreptitious access. Proper system configuration and approval to operate must be obtained to provide adequate protection of communications. Insider threat is of particular concern when dealing with information systems. Proper certification and accreditation of systems will assist with overall security.

8. Terrorist Incident Response

a. **Procedures.** The response to a terrorist incident includes procedures established to mitigate the effects of the incident. These procedures are designed to ensure the

commander is able to rapidly deploy a terrorist incident response team (i.e., the initial response force) to reduce further effects and damage, support emergency life-saving and rescue functions, provide protection of DOD personnel and property, and, when appropriate, conduct or support criminal investigations. An important objective of AT incident response is to mitigate the number and severity of casualties resulting from a terrorist attack. Well-developed response measures, to include intermediate force capabilities, employing the use of nonlethal weapons, can save lives, preserve health and safety, protect and secure property, and eliminate the hazard. A slow or uncoordinated response may result in additional loss of life, further damage to the installation, and the loss of public confidence in the organization's ability to respond to a terrorist incident. HSPD-5, *Management of Domestic Incidents,* mandates the use of National Incident Management System using the incident command system to facilitate a comprehensive and coordinated whole-of-government response at all levels.

b. **CBRN Response.** Commanders and joint security coordinators must be aware that CBRN weapons may be used at any level of threat by conventional, terrorist, or irregular forces.

For more information on CBRN response operations, see JP 3-41, Chemical, Biological, Radiological and Nuclear Response. *For information on CBRN passive defense and the relationship between CBRN response operations and CWMD, see JP 3-40,* Countering Weapons of Mass Destruction, *and JP 3-11,* Operations in Chemical, Biological, Radiological, and Nuclear Environments.

9. Cyberspace Operations in Support of Antiterrorism Operations

Cyberspace operations involve defending the nation against cyberspace attacks of significant consequence and protecting all US military-related networks or infrastructure. This includes finding and thwarting potential missile threats against US and allied forces. The Department of Defense Cyber Crime Center serves as DOD's operational focal point for the Defense Industrial Base Cybersecurity Program that incorporates a voluntary cyberspace threat information sharing and incident reporting program. The center operates under the executive agency of the Secretary of the Air Force. Its mission is to deliver digital forensics and multimedia lab services, cyberspace technical training, technical solutions development, and analytics for the following DOD mission areas: cybersecurity policy implementation and critical infrastructure protection, LE and CI, document and media exploitation, and CT.

For more information, see JP 3-12, Cyberspace Operations.

10. Space Operations in Support of Antiterrorism

Space operations depend upon gaining and maintaining space superiority to defend the nation against attacks on our space capabilities and to negate terrorist use of space capabilities. Space control operations include offensive measures to deceive, disrupt, degrade, deny, or destroy the space systems or services that terrorists may exploit to support their operations. Space control operations also include active and passive measures

taken to protect friendly space capabilities from a terrorist attack on any segment of a space system—space, link, or ground.

For more information, see JP 3-14, Space Operations.

11. Information Considerations for Antiterrorism Activities

a. Generally, installation commanders inform an internal and external public audience of AT activities. Internal audiences are military, civilians, and contractor personnel on installation; external audiences are the general public outside the installation. A terrorist event on installation may significantly impact the general public, depending on the magnitude of the event.

b. Installation commanders should have an information plan. The installation public affairs officer (PAO) supports the commander's AT plan. In case of an event, the PAO is the conduit from the commander to internal and external audiences. The installation PAO and AT planners work together to build an information plan. Additionally, by identifying and leveraging the inherent informational aspects of unit actions and activities, public affairs' efforts can disseminate accurate information to audiences.

c. **Internal Audiences.** The PAO develops a plan to inform the internal audience on the installation to support installation security. The PAO is prepared to disseminate the following information quickly:

(1) Situational awareness announcements.

(2) Threat advisories.

(3) Immediate actions to ensure personal safety.

(4) Situation and status updates.

(5) Post-threat advisories.

d. **External Audiences.** Civilian first responders will likely conduct their own media-relations activities to keep the general public informed in the event of a large-scale event impacting the general public. Police, fire, and local governments generally establish a joint information center off-installation to inform local media. The PAO develops a plan to share installation information with first-responder PAOs and are prepared to respond directly on-camera to civilian media requests for information and prepare the installation commander or other subject matter expert for on-camera interviews or press conference(s).

e. **Information Dissemination Methods.** Information dissemination strategies include push or pull strategies to inform audiences. Information push requires little effort from individuals to remain informed. Information pull requires audiences to seek information by going to a Website or making a phone call. Generally, information push works better in emergencies. Commanders should consider using the following methods for communicating with internal and external audiences:

Installation Alert Sign

(1) **Loudspeaker Systems.** Loudspeakers are an effective way for pushing short messages to internal and external audiences. "Take cover," "remain in place," and "evacuate immediately" are typical examples. The limitation to this method is that it is indiscreet, as both internal and external audiences will hear the messages. Another is that audiences outside the immediate broadcast range of speakers may not hear or understand the messages.

(2) **Electronic Signs.** Electronic signs enable installation commanders to push short advisories, threat levels, and messages to audiences, especially drivers in vehicles. The limitation to this method is that signs must be visible to the intended audience.

(3) **Internet Webpages.** Internet webpages require audiences to pull longer, more-detailed information. They require audiences go to a site to read or download updates and instructions. The limitation to this method is that audiences must actively pursue information using such web-enabled devices as a computer or smartphone.

(4) **Social Media.** Social media enables users to push, pull, and share detailed information with others very quickly, using text, photos, and video. Limitations to this method are that audiences must pursue information using such web-enabled devices as a computer or smartphone and, that since most social media platforms are hosted and operated by private entities, they are vulnerable to threat misinformation or exploitation. Additionally, audiences may not have access accounts to social media platforms, thereby restricting the dissemination of information on these platforms. Audiences must be technologically sophisticated and interested enough to voluntarily elect to receive alerts.

(5) **Text Messaging.** Texts communicate directly with individuals. The limitation to this method is that audiences must have smartphones to access information and, that generally, the installation must have individual phone numbers to broadcast

information. However, emerging technologies enable governments to broadcast warnings to the general public through cellular service providers. Amber/Silver Alerts and the Emergency Alert System are examples. The Federal Communications Commission, in coordination with the Federal Emergency Management Agency, recently tested a new text alert system. The Emergency Alert System sends wireless emergency alerts to most cellphones in the United States.

Intentionally Blank

APPENDIX A
COMMANDER'S ANTITERRORISM CHECKLIST

Commander's Antiterrorism Checklist
Assuming Command: • Does unit have an AT program and security posture appropriate for mission and potential threat? • AT officer appointed? • ATWG designated? • DIA and/or FBI TA current? • VA current? • AT plan complete? • Program review within past 12 months? • AT plan exercised within past 12 months? • AT level I training current? • Have you reviewed DODI O-2000.16 and appropriate combatant commander/Service AT guidance? • Is combatant commander/Service AT guidance implemented?
Organize for AT: • Does unit have adequate focus on AT? • Is unit ATO formally trained? • Are right functions represented in ATWG? • Is ATWG active? Meeting minutes? Accomplishments? • Next meeting? Next action?
TA: • Do TAs provided by DIA and/or FBI and/or the local TA process? • Identify specific terrorist capabilities, weapons, and tactics (to include CBRN). • Provide the necessary information for the commander to help tailor force protection conditions. • Have a review mechanism to provide up to date information. • Is unit aware of current and potential threats (conventional and CBRN)? • DIA and/or FBI (CONUS) assessed threat level for area? • CCDR-assigned higher local threat level? • Formal intelligence assessment on hand and current? • Relationship with supporting Intel activity? • Is CI or LE support needed? • Local information considered? • Local information network established? • Aggressive list of threat options identified?
VA: • Do VAs and the vulnerability process include? • The range of terrorist threat identified in the TA. • Recommendations for procedural enhancements and resource requirements. • Provided complete inventory of assets and areas. • Prioritization of assets/areas on criticality. • Catalog of known vulnerabilities. • Provide for annual revisions. • Has unit evaluated the vulnerability of all assets to potential threats to support risk management decisions? • When was the last VA? • Did last VA reveal significant vulnerabilities? • What is status of remedial actions?

Figure A-1. Commander's Antiterrorism Checklist

AT Exercises: • Has AT plan been validated by exercises and is unit ready to execute it? • Has AT plan been exercised within one year? • Have key organizations exercised their roles? • Unit response to increasing threat levels been exercised? • Unit response to incident/mass casualties been exercised? • AT plan been exercised in a manner to heighten awareness? Incorporated RAMs? • Has exercise identified discrepancies? Plan to correct them?
AT Resources: • Does AT resource program support the required long-term security posture? • Defined resource requirements to mitigate security deficiencies? • Requirements justified with risk analysis? • Alternative plans, policy, and procedural solutions considered or implemented? • Does the command have a formal process to track, document, and justify resource requirements and identify resource shortfalls to higher HQ? • Higher HQ approved these requirements? • Emergent and/or emergency needs submitted (e.g., CCIF)? • Does the command incorporate AT requirements into the program change proposal process? • Are program change proposal requirements submitted for out-year support of CCIF funded investments?
• Status of CCIF or program change proposal requirements in the program/budget process? • AT and security factors adequately weighed in acquisition and use of facilities (both temporary and permanent)? • Current facilities conform to DOD and component AT MILCON standards? • Do structural engineers and security personnel work together to incorporate AT consideration in building design and review? • Are DOD AT standards for buildings incorporated into new constructions? • How is technology, such as nonlethal weapons, being used to enhance security and human performance? • What technologies have been identified as recommended/required for higher threat levels/FPCONs? • Is the AT officer a member of the resource management committee?
AT Training: • Are personnel receiving the appropriate levels of AT training to include? • Level I-IV training. • High risk personnel. • AOR specific training prior to deployment. • A system to track and document training. • Is individual awareness of terrorism threat sufficient for threat environment/mission? • Annual level I training current? • AOR updates current and briefed? • Special local individual protective measures briefed and used?
Program Review: • Is AT program comprehensive, current, and effective? • Can unit do mission under FPCONs in use? • Are critical FPCONs compromised for unit morale or convenience? • Is AT a routine element of daily mission planning and execution? • Are operational patterns varied? • Is OPSEC included in mission planning? • Does unit continually monitor threat and corresponding security posture? • Does unit monitor and control access of visitors and employees in sensitive areas? • Has threat level changed since last VA? • Is TA current and valid? • Are RAMs having desired effect on unit awareness, readiness, and deterrence?

Figure A-1. Commander's Antiterrorism Checklist (continued)

MOU/MOA: • Is unit conforming to and employing MOU/MOA for local support? • Does unit or any detached personnel fall under DOS for force protection? • Are DOS's force protection instructions on hand for those individuals? • Identified organizations with jurisdiction for LE, health, safety, and welfare of assigned service members on and off duty? • Unit conforming to jurisdictional agreements in these areas (SOFA, interagency partners)? • Identified local community organizations with shared security interests (police, federal LE, hospitals, and public health)? • Mutual aid agreements in place with local community to leverage shared interests? • Mutual aid agreements been reviewed by higher HQ? • Mutual aid agreements executable (liability, jurisdiction, capabilities)?
Mitigate WMD Effects: • Has unit prepared for WMD attack? • Does AT plan consider terrorist use of WMD? • What are AT plan assumptions concerning the worst case threat options? • Procedures for detection of unconventional CBRN attacks? • Unit training include awareness of indicators of unconventional attacks? • Do all personnel have individual protective equipment available? • Are collective protective systems available? • What CBRN detection equipment is available? • What decontamination equipment is available? • Are decontamination procedures established?
• Are decontamination waste disposal procedures established in accordance with HN, federal, state, or local laws and regulations?
Off-Installation Housing: • Are personnel housed off-installation adequately secured? • Service members in moderate, significant, and high threat areas receive instruction and supervision in residential security measures? • In such areas, do unit AT response plans include current residence location information for all unit members residing off installation? • In such areas, do units coordinate with local LE authorities for protection of unit members residing off-installation (MOUs/MOAs/SOFAs)? • Incident response plans include measures for off-installation personnel (personnel warning system)?
ROE/ RUF: • Does unit have correct ROE/RUF guidance for the mission and environment? • Do plan/current procedures, such as the incorporation of nonlethal weapons, provide enough standoff to determine hostile intent and make proper decision to use force? • Are service members trained for making ROE/RUF decisions in realistic situations? • ROE/threat scenarios adequate and rigorous? • Is unit prepared to apply ROE/RUF for threat scenarios?

Figure A-1. Commander's Antiterrorism Checklist (continued)

Facility Antiterrorism Officer Questionnaire
Antiterrorism Checklist—ATOs
DODAT Policy: This standard does not apply.
Development of AT Standards • Do you have a copy of the applicable DOD, combatant commander, Service, and agency AT regulations, standards, and other guidance? • Combatant commander/Service and/or DOD agency standards should address: • Procedures to collect and analyze terrorist threat information, threat capabilities, and vulnerabilities to terrorist attacks. • Terrorism TA, VA, terrorism incident response measures, and measures to manage the consequences of AT incidents. • AT plans and procedures to enhance AT protection. • Procedures to identify AT requirements and to program for resources necessary to meet security requirements. • DOD military AT constructions considerations.
Assignment of AT Operational Responsibility • Does the facility understand which combatant commander, Service, or DOD agency has AT TACON for operational responsibility?
AT Coordination in Overseas Locations: This standard does not apply to facility AT plans.
Comprehensive AT Development, Implementation, and Assessment Does the installation AT program contain, as a minimum, the following elements: • TAs • Planning • Exercises • Program review • Training • VAs
• ATOs Assigned in Writing • Has the commander designated a Level II qualified/trained commissioned officer, non-commissioned officer, or civilian staff officer in writing as the ATO? • For deploying organizations (e.g., battalion, squadron, ship) have at least one Level II qualified individual designated in writing? • Has the ATO attended a Service approved Level II AT Training course?
Application of DOD Terrorism Threat Analysis Methodology • Does the unit use the DOD threat level methodology (Low, Moderate, Significant, High) in their local
TAs?
Threat Information Collection and Analysis • Has the commander tasked the appropriate organization under their command to gather, analyze, and disseminate terrorism threat information? • Are personnel in the command encouraged and trained to report information on individuals, events, or situations that could pose a threat to the security of DOD personnel, families, facilities, and resources? • Does the command have procedures to receive and process defense terrorism warning reports and/or higher HQ threat message?
Threat Information Flow • Does the command forward all information pertaining to suspected terrorist threats, or acts of terrorism involving DOD personnel or assets for which they have AT responsibility up and down the chain of command? • Does the command ensure there is intelligence sharing between all organizations? • Does the command provide tailored threat information for transiting units?

Figure A-2. Facility Antiterrorism Officer Questionnaire

Potential Threat of Terrorist Use of WMD • Does the command have the procedures to process immediately through the chain of command reports of significant information obtained identifying organizations with WMD capability in their AOR? • Is an estimate of terrorist potential use of WMD indicated in the local TA?
Adjustment of Force Protection Conditions • Does the command have a process, based on terrorism threat information and/or guidance from higher HQ, to raise or lower FPCONs?
FPCON Measures Implementation: This standard does not apply to facility AT plans.
FPCON Measures • Has the command developed site-specific measures or actions for each FPCON which supplement measures/actions enumerated for each FPCON? • Does the command have procedures to set and transition between FPCONs? • Does the command have procedures to establish a lower FPCON than Higher HQ? • Are site-specific AT measures linked to FPCONs classified, as a minimum, CONFIDENTIAL? • Site-specific AT measures separated from the AT plan can remain FOR OFFICIAL USE ONLY. • Do FPCONs permit sufficient time and space to determine hostile intent in accordance with standing ROE? • Has the command established procedures to expedite MOU/MOA assistance/response during elevated FPCONs?
Comprehensive AT plan • Does the command have a signed AT plan? • Is the plan site-specific and address the following key elements? • Terrorism TA (including WMD). • Vulnerability assessment. • RA. • AT physical security measures. • Terrorism incident response measures. • Measures to manage the consequences of AT incidents. • Does the installation incorporate AT planning into operations orders for temporary operations or exercises?
Terrorism Threat Assessment • Does the command have an annually updated terrorism TA? • Does the TA consider the following during the assessment process: • Capabilities of the terrorist threat. • Vulnerability of the facilities. • Criticality of the facilities. • Is the TA used as the basis and justification for recommendations on AT enhancements, program/budget requests, and establishment of FPCONs? • Does the command use an RA to integrate threat and VA information to make an informed decision to commit resources and/or enact policies and procedures to mitigate the threat or define the risk? • Does the RA analyze the following elements?
• Terrorist threat. • Criticality of the assets. • Vulnerability of facilities, programs, and systems to terrorist threats. • The ability to conduct activities to deter terrorist incidents, employ countermeasures, mitigate the effects of a terrorist incident, and recover from a terrorist incident.

Figure A-2. Facility Antiterrorism Officer Questionnaire (continued)

AT Physical Security Measures
- Does the installation commander coordinate and integrate subordinate unit physical security plans and measures into the AT plan?
- Are physical security measures considered, do they support, and are they referenced in the AT plan to ensure an integrated approach to terrorist threats?
- Do AT physical security measures include provisions for the use of:
- Physical structures.
- Physical security equipment.
- CBRN detection and protection equipment.
- Security procedures.
- RAMs.
- Response forces.
- Emergency measures sufficient to achieve the desired level of AT protection and preparedness to respond to terrorist attack.
- Are RAMs used for both in-place and transiting forces?

Terrorist Incident Response Measures (first response)
- Has the command prepared installation-wide and/or shipboard terrorist incident response measures which include:
- Procedures for determining the nature and scope of the terrorist incident and required response.
- Procedures for coordinating security, fire, and medical first responders.
- Steps to reconstitute the installation's ability to perform AT measures
- In moderate, significant, or high terrorist threat level areas, has the command included residential location information for all DOD personnel and their dependents in their incident response measures?

Manage the Consequences of AT Incidents
- Do measures provide for appropriate emergency response and disaster planning and/or preparedness to respond to a terrorist attack for the installation and/or base engineering, logistics, medical, mass casualty response, transportation, personnel administration, and local and/or host nation support?
- Do measures include guidelines for predeployment and garrison operations, pre-attack procedures, actions during attack, and post-attack actions?

Training and Exercises
- Has the command conducted field and staff training (annually) to exercise AT plans to include?
- AT physical security measures.
- Terrorist incident response measures.
- Measures to manage the consequences of AT incidents.
- Does the command maintain exercise AARs/lessons learned and document actions taken to remediate identified shortfalls for at least a year?
- Does command predeployment training include training and exercises?
- Credible deterrence/response.
- Deterrence-specific tactics, techniques, and procedures.
- Terrorist scenarios and hostile intent decision making.

Comprehensive AT Review
- Does the command review own and subordinate AT programs and plans at least annually to facilitate AT program enhancement?
- Does the command review the AT program when the terrorist threat level changes?

General Requirements for AT Training
- Does the command ensure all personnel records are updated to reflect AT training in accordance with DOD component policy?

Level I AT Awareness Training
- Does the command conduct Level I training in accordance with DOD and combatant commander/Service/agency Standards?

Figure A-2. Facility Antiterrorism Officer Questionnaire (continued)

• Does the installation ensure Service family members traveling beyond CONUS on official business receive Level I training (i.e., PCS move)?
AOR-Specific Training Requirements for all Department of Defense Personnel • Does the command ensure all individuals traveling outside CONUS for either permanent or temporary duty complete Level I AT awareness training? • Has the command provided combatant commander approved AOR specific AT protection information to individuals traveling outside CONUS within three months prior to travel? • Does the command ensure intra-theater transiting units receive detailed threat information covering travel routes and sites that will be visited by the unit?
Level II ATO Training • Does the installation and/or each deployed unit have at least one Level II trained ATO assigned? • Have O-5/O-6 commanders received Level III training prior to assumption of command?
Training for HRP and HRBs • Has the command identified HRBs and HRP to higher HQ annually? • Have personnel designated as "personnel at high-risk to terrorist attack" and "personnel assigned to HRBs" received appropriate AT training?
VAs of Installations • Has a local VA been conducted within the past year? • Did the VA identify vulnerabilities and means to eliminate or mitigation them? • Did the VA identify options for enhanced protection of DOD personnel and assets? • Does the AT VA assess the following functional areas at a minimum: • AT plans and programs. • CI, LE, liaison, and intelligence support. • AT physical security measures. • Vulnerability to a threat and terrorist incident response measures. • VA for terrorist use of WMD. • Availability of resources to support plans as written. • Frequency and extent to which plans have been exercised. • Level and adequacy of support from the host nation, local community, and, where appropriate, inter-Service and tenant organizations to enhance force protection measures or respond to a terrorist incident. • Status of formal and informal agreements to support AT functions. • Does the VA team contain expertise to meet the intent of providing comprehensive assessments? • Is there a process to track and identify vulnerabilities through the chain of command?
Predeployment AT VA • Has a predeployment AT VA been conducted for units prior to deployment? • Have appropriate AT measures been implemented to reduce risk and vulnerability? • Has the command received onboard and/or advance-site assessments prior to and during visits to higher-threat areas of significant or high threat Levels or where a geographically specific terrorism threat warning report is in effect? • Has the command requested funds from CCIF for emergent AT requirements prior to movement of forces? • Has the command explored the use of commercial-off-the-shelf or government-off-the-shelf products to meet near-term AT protection requirements?
Construction Considerations • Do DOD components adopt and adhere to common criteria and minimum construction (i.e., new construction, renovation, or rehabilitation) standards to mitigate AT vulnerabilities and terrorist attacks?

Figure A-2. Facility Antiterrorism Officer Questionnaire (continued)

Facility and Site Evaluation and/or Selection Criteria • Has the command developed a prioritized list of AT factors for site selection for facilities, either currently occupied or under consideration for occupancy by DOD personnel? AT factors should include, but not limited to, screening from direct fire weapons, building separation, perimeter standoff, window treatments, protection of entrances and exits, parking lots and roadways, standoff zone delineation,
Security lighting, external storage areas, mechanical and utility systems. • Has the command used these factors to determine if facilities can adequately protect occupants against terrorism attack?
AT Guidance for Off-Installation Housing • Does the command have procedures to ensure DOD personnel assigned to moderate, significant, and high terrorism threat Level areas, who are not provided on-installation or other government quarters, are furnished guidance on the selection of private residence to mitigate risk of terrorist attack? • Does the command have procedures to conduct physical security reviews of off-installation residences for permanently and temporary-duty DOD personnel in significant or high threat Level areas? • Based on these physical security reviews, does the command have procedures to provide AT recommendations to residents and facility owners? • As appropriate, does the command have procedures to recommend to appropriate authorities the construction or lease of housing on an installation or safer area? • Does the command have procedures to complete residential security reviews prior to personnel entering into formal contract negotiations for the lease or purchase of off-installation housing in significant or high threat areas? • Does the command have procedures to include coverage of private residential housing in AT plans where private residential housing must be used in moderate, significant, or high threat level areas? • In moderate, significant, or high threat areas, does the command incorporate family members and dependent vulnerabilities into AT assessment, mitigation, and reporting tools for: • Facilities used by DOD employees and their dependents. • Transportation services and routes used by DOD employees and their dependents.
Executive Protection and High Risk Personnel Security • Has the command annually reviewed and revalidated the protective services for executives? • Has the command taken necessary measures to provide appropriate protective services for designated individuals in high-risk billets and HRP? • Does the command review needs for supplemental security within 30 days of a change in the terrorism threat level?
Miscellaneous Issues • Does the command have technology to access critical terrorism intelligence e.g., SIPRNET? • Has the O-6 through O-8 commander been to Level IV training?

Figure A-2. Facility Antiterrorism Officer Questionnaire (continued)

APPENDIX B
FORCE PROTECTION MEASURES AND ACTIVITIES IN SUPPORT OF COMBATING TERRORISM

1. Countering Terrorist Attack Planning

Effective AT programs anticipate, detect, disrupt, and potentially defeat terrorist attack planning to ensure the safety of personnel and resources. AT plans should examine terrorist methods of surveillance, information gathering, and attack planning to determine the extent of training and resources needed to address the threat. In addition, AT plans must identify the most effective way to train personnel to counter terrorist attack planning with basic surveillance awareness procedures. This also requires identifying necessary surveillance detection requirements and promulgating incident reporting procedures. Most important, AT programs need to focus on building strong relationships with various LE and CI agencies. Indeed, this is a critical step in increasing the flow of information to neutralize the threat.

a. **Terrorist Methods of Surveillance and Information Gathering.** The typical terrorist attack planning process is best summarized in Figure B-1. Effective AT programs prevent or disrupt attacks by focusing on the initial stages in the terrorist attack planning process, where terrorists conduct initial surveillance and select targets for exploitation and suitability for attack. Terrorists examine security procedures, such as personnel and guard-force shift changes, access control procedures, frequency of roving security patrols, and the citizenship/nationalities of the guard forces. They also monitor installations or facilities to determine types of locks and access control devices, presence of closed-circuit security

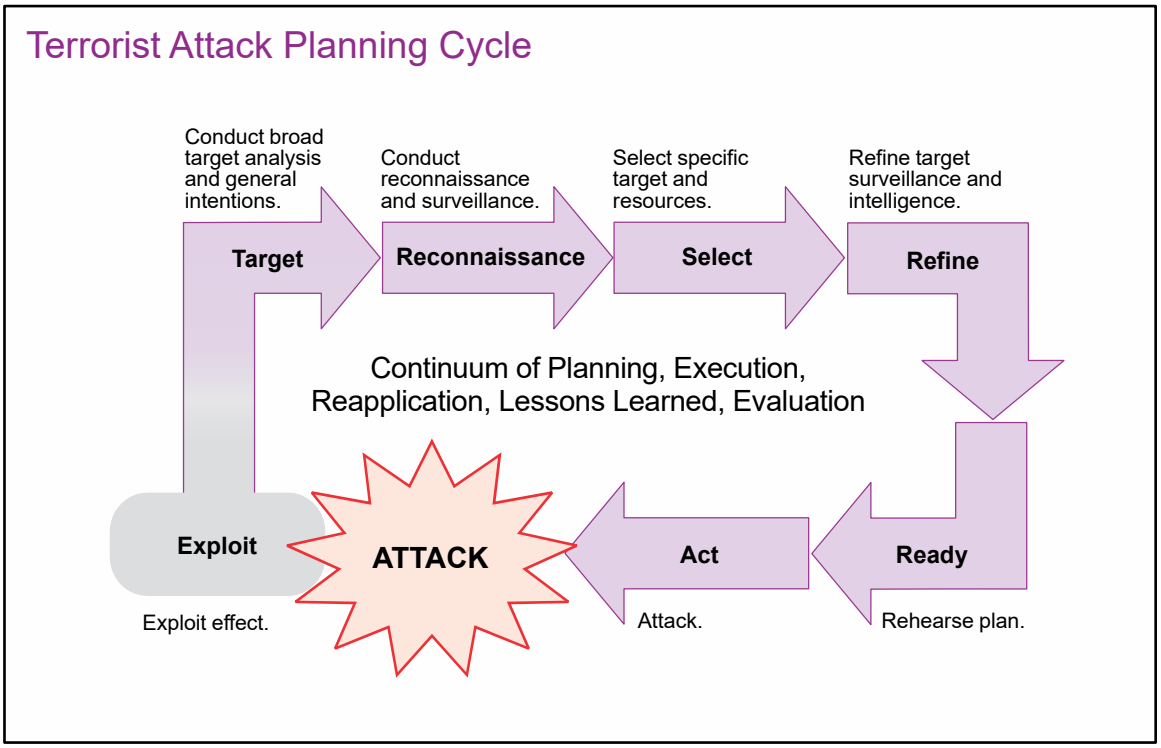


Figure B-1. Terrorist Attack Planning Cycle

cameras, and the use of military working dogs. Surveillance allows terrorists to assess gaps in physical security, as well as identify patterns in standard operations procedures, including reaction times to emergencies, which can be used to plan for subsequent attacks against heavily fortified areas or emergency responders. When terrorists assess personnel in particular, they seek to identify vulnerabilities in human patterns such as modes and times of travel, frequently traveled routes, and the target's overall security awareness. Five techniques in the methodology that contribute to the terrorist attack planning cycle are **fixed (static) surveillance, mobile surveillance, technical surveillance, casual questioning (elicitation), and probing.** Defense Threat Reduction Agency's DOD red team employs these threat techniques to safeguard US strategic assets through an all-source collection approach with the ability to emulate terrorist organizations spanning a single individual to well-funded, foreign intelligence entities and hostile-nation SOF providing methodologies to mitigate effects of threats while strengthening FP and national security. There is no universal model to reflect the terrorist planning process. Figure B-1 depicts a general cycle that terrorists would modify based on specific objectives, resources, and time available. Although terrorist activities may appear as random acts, they are typically purposeful and directed activities that are carried out by sophisticated groups who generally follow a deliberate planning cycle.

(1) **Fixed (Static) Surveillance.** Terrorists conduct fixed or static surveillance from one location to observe a target, whether a person, building, facility, or installation. Fixed surveillance often requires the use of an observation point to maintain constant, discreet observation of a specific location. Terrorists may attempt to establish observation posts near targets of interest in houses, apartments, offices, stores, restaurants, bars, bus stops, or on the street. A mobile surveillance platform, such as a parked car, truck, or recreational vehicle, can also serve as a semi-fixed observation post.

(2) **Mobile Surveillance.** Terrorists conduct mobile surveillance to follow targets. This can be done on foot (e.g., walking or jogging), in a vehicle, or a combination of the two. Mobile surveillance usually progresses from a fixed or static location to tailing the target, continuing until the target stops or arrives at its destination. At this point, terrorist operatives will position themselves to identify the target's departure. Meanwhile, other terrorist operatives will be positioned to cover the target's logical routes, thus enabling the surveillance to continue discreetly after the target moves again. Terrorists can also follow targets using parallel routes, especially with a highly visible target such as a military convoy.

(3) **Technical Surveillance.** Terrorists may use a variety of electronic means to assist in surveillance, to include the use of recording devices (e.g., cell phone cameras and camcorders). Terrorists have also used the Internet to obtain private information, security information, and open-source Internet mapping data to assist in attack planning.

(4) **Casual Questioning (Elicitation).** Terrorists can acquire useful information on a target by simply asking questions. Through friendly, casual conversations, terrorists are able to elicit security information, not necessarily from personnel willingly interested in divulging security procedures but rather those that seem more approachable to the

terrorist. Terrorists will exploit Internet chat rooms and other social networking media to acquire information needed for their attack planning.

(5) **Probing.** Terrorists may overtly approach secured areas carrying mock attack devices to determine firsthand the effectiveness of a facility's or installation's security procedures and to gauge the vigilance and reaction of the security personnel. They may also conduct routine activities to desensitize security personnel or to produce false alarms to dull the effectiveness of security personnel. Examples of probing include:

(a) Threats delivered via phone, e-mail, or mail meant to elicit a security response.

(b) Using some type of ruse to gain access or entry (e.g., approaching security checkpoints to ask for directions).

(c) "Accidentally" attempting to smuggle contraband through checkpoints.

(d) Leaving abandoned packages, vehicles, or other suspicious items near a target.

(e) Noticeably watching and recording security reaction drills and procedures.

b. **Surveillance Awareness.** DOD personnel and their families must understand the implications of hostile surveillance, to assume that it is occurring, how to discreetly detect or identify it, and what to do if they suspect it. In fact, personnel are often able to detect criminal or terrorist surveillance (i.e., targeting themselves or their installations) as a result of enhanced situational awareness orchestrated by aggressive AT programs. They may even make themselves less desirable targets by following the four fundamental tenets of surveillance awareness: **stay informed, keep a low profile, be unpredictable, and stay alert.**

(1) **Stay Informed.** This requires knowing the primary threats and terrorist elements operating in the immediate area. Commanders are responsible for keeping DOD personnel and their families informed of any changes in the local threat. More importantly, Service men and women have a personal responsibility to increase their own situational awareness on the local threat and the OE. Certainly, it helps to know one's neighbors (and their vehicles), the local vendors, and others who routinely operate near one's home or place of work.

(2) **Keep a Low Profile.** Terrorists may find it harder to monitor someone who blends in with the local population. Low-key appearance and behavior may force terrorists to work harder to identify a target, either forcing them to get closer to their target or moving on to another one. As the terrorist gets closer, it also becomes easier for a potential target to detect the surveillance. To be sure, any effort by DOD personnel to aggressively elude or "ditch" the terrorist will only reduce the opportunity to detect the terrorist. Thus, one should maintain a normal demeanor and report what they see (see paragraph 1.e., "Incident Reporting").

(3) **Be Unpredictable.** Through smart application of unpredictable behavior, routines, or travel, it is possible to greatly increase the time and resources required for terrorists to conduct surveillance. Deliberate variation of travel routes, for example, reduces the number of places a terrorist will select to plan an attack. This may frustrate them and force them to select more predictable locations or different targets. It is important, however, to avoid selecting alternate travel routes that transit sparsely-populated, less-secure, or dense traffic areas.

(4) **Stay Alert.** DOD personnel and their families need to know what to look for. Generally speaking, terrorists may look like they are trying to accomplish some "cover" task, but they will likely be paying more attention to their target, thus allowing themselves to be identified by an individual who has good situational awareness. Even more revealing is when a surveillance operative appears more than once in the vicinity of their target or behaves in a way that responds to what their target does. This is referred to as "correlation" and is considered one of the strongest indicators of hostile surveillance. (See Figure B-2 for a list of surveillance indicators.)

c. **Surveillance Detection.** The fundamental tenets of surveillance awareness discussed in paragraph 1.b., "Surveillance Awareness," if applied successfully, will directly contribute to detecting hostile surveillance by increasing the time, visibility, and efforts required to effectively target US personnel. Surveillance detection operations take it a step further by providing a commander the ability to move beyond ordinary FP measures and incident response to operations that will directly deter, detect, disrupt, and ultimately defeat the terrorist attack planning cycle. Simply stated, surveillance detection operations are used to detect and/or verify whether an individual, vehicle, or location is under surveillance. Surveillance detection teams, in particular, also identify specific locations where terrorists will most likely conduct surveillance or attack their targets and then provide recommendations to a commander for resource application. Surveillance detection should not be confused with countersurveillance operations which may involve more direct measures by trained security or intelligence professionals to counteract hostile surveillance, though surveillance detection and counter surveillance operations are often used in conjunction with each other (see JP 2-01.2, *[U] Counterintelligence and Human Intelligence in Joint Operations).* The following are examples of what surveillance detection professionals can provide a commander:

(1) **Route Analysis for Key Personnel.** This involves noting areas along a travel route where terrorists are more likely to conduct surveillance, profile a potential target, or launch an attack. An example of this is an area where routes overlap (including the beginning and end of a route which rarely changes) or where a route "channels" a target.

(2) **Likely Terrorist Attack or Surveillance Sites.** This entails determining the best locations for terrorist attacks and surveillance locations for profiling fixed or mobile targets. Potential surveillance and attack sites typically have the following characteristics: the site is routinely frequented by a mobile target at predictable times, has limited security or police presence, offers cover or camouflage for a hostile surveillance or attack team, offers a means to effectively control or limit the target's movement to ensure success during the attack, and has a variety of good escape routes for the terrorist operatives.

Surveillance Indicators

1. Multiple sightings of the same suspicious person, vehicle, or activity, separated by time, distance, or direction
2. Correlation (over time, distance, and direction) that involves actions by persons that relate to the target (for example, when someone in the vicinity of a facility looks at his watch when key personnel enter or exit the main gate, or when guard shifts change)
3. Paying undue attention to a facility, person, vehicle, or area; drawing pictures, taking notes, or photographing security cameras or guard locations in areas not normally of interest to tourists
4. Measuring distances and counting steps
5. Electronic audio and video devices in unusual places
6. Extended loitering near potential targets
   - Sitting in a parked vehicle for an extended period of time
   - Long telephone conversations
   - Observing vehicles as they enter or leave a designated entry control point, facility, or parking areas
7. Out-of-place attire or behavior
   - Joggers resting or stretching for an unreasonable period of time
   - Not eating or leaving table before ordered food arrives
8. Nervous behavior
   - Staring or quickly looking away from individuals or vehicles
   - Fidgeting or appearing uneasy
   - Excessive perspiration

Figure B-2. Surveillance Indicators

(3) **Determining What Is Normal.** Knowing what is normal enables security personnel to detect deviations from routine activity so that unusual or extraordinary behavior stands out. Surveillance detection teams can assist security personnel and military police in identifying anomalous activity.

Note: Skilled surveillance detection by ordinary DOD personnel involves formal training; however, the basic awareness techniques listed above should suffice for understanding suspicious behavior and evaluating daily routines. **It is important to emphasize that DOD personnel and their families should avoid confrontations with suspicious individuals whenever possible and allow security and LE professionals to take action.** It is never prudent to draw attention to oneself or to try to outrun or aggressively avoid surveillance, unless there is a threat of injury or death.

d. **CI and LE Resources.** Regardless of the AT capabilities, resources, and protective measures in place, close, working relationships with local, state, HN, and federal LE

agencies are essential to establishing timely and effective responses to terrorist activity. Commanders should coordinate and establish partnerships with local authorities (i.e., installation threat working groups) to develop intelligence and information sharing relationships to improve the overall security of their units and the military community at large. If indicators continue despite well-executed, overt security countermeasures and the trends clearly indicate preoperational terrorist attack planning, it may be necessary for commanders to implement more sophisticated, uniquely tailored CI assets. See JP 2-01.2, *(U) Counterintelligence and Human Intelligence in Joint Operations.*

e. **Incident Reporting.** Since terrorists frequently conduct extensive target surveillance—over a period of weeks, months, or years—their activities should be detectable. Moreover, terrorists will invariably commit mistakes, further increasing the chance of detection by ordinary individuals, security personnel, and trained surveillance detection teams. AT plans, therefore, require the most streamlined processes to expedite incident reporting of unusual activities so that information moves rapidly from the originator, through security and military police, and over to the required investigative and CI organizations. The best incident reports include detailed descriptions of the subject(s), time of day, locations, vehicles involved, and the circumstances of the sightings. Military police and security personnel need to report these incidents to their respective criminal investigative services or CI elements as soon as possible (see Figures B-3 and B-4). Indeed, these incident reports are important pieces of information that, over time and in combination with other reported sightings (i.e., correlation of place, time, people, or method), enable investigators to accurately assess the threat.

Notional Incident Report Format

Description of the activity:

- Fully identify all personnel, organizations, and locations in a narrative paragraph.
- Describe the details of the incident (date, time, and location).

Physical identifiers of the person(s) observed:

- Sex – male or female
- Race – white, black, Asian, Hispanic or other
- Age
- Height and weight
- Hair color and style
- Eye color – glasses
- Complexion – skin tone, imperfections
- Speech – accent, impediments (e.g., stutter, lisp)
- Scars – Tattoos, facial hair
- General appearance – clothing, shoes, jewelry

Vehicle descriptor information:

- Year, make and model
- Color
- License plate number and state
- Stickers (e.g., windshield, bumper), damage or dents
- Additional occupants

Where any suspicious persons may have gone:

- Mode of travel – on foot, bicycle, vehicle
- Direction of travel

Source point of contact information:

- Name
- Address
- Phone number(s)/e-mail address(es)

Figure B-3. Notional Incident Report Format

Antiterrorism Poster

Figure B-4. Antiterrorism Poster

APPENDIX C
INTELLIGENCE SUPPORT TO COMBATING TERRORISM

1. Joint Intelligence Preparation of the Operational Environment

a. **Process.** The JIPOE process is used to characterize the OE and provide a disciplined methodology for applying a holistic view to the analysis of the threat's capabilities and intentions. During CT operations, JIPOE places far greater emphasis on understanding the civil population and critical infrastructure. Additionally, JIPOE helps combat terrorism by supporting FP measures, CI, and other security-related activities. The JIPOE process consists of four basic steps that ensure the systematic analysis of all relevant aspects of the OE. The process is both continuous and cyclical in that JIPOE is conducted both prior to and during CT operations, as well as during planning for follow-on missions. All joint staff HQ sections, not just the intelligence section, are involved in the JIPOE process.

b. **Steps.** The four steps of the JIPOE process are to define the OE, describe the impact of the OE, evaluate the adversary and other relevant actors, and determine potential courses of action of the adversary and other relevant actors.

c. **Critical Factors Analysis.** Critical factors analysis for CT starts by analyzing the COGs of terrorist organizations and their networks and then determining their critical capabilities, requirements, and vulnerabilities. This enables the JIPOE team to recognize decisive points and what shaping operations are necessary to successfully execute CT operations. Figure C-1 graphically represents elements of the critical factors analysis.

For more information, see JP 2-01.3, Joint Intelligence Preparation of the Operational Environment.

2. Identity Intelligence

I2 is the intelligence production resulting from the processing of identity attributes concerning individuals, groups, networks, or populations of interest to deny anonymity to the adversary (especially terrorist threats) and to protect the assets, facilities, and forces. I2 supports the find, fix, exploit, analyze, and disseminate phases of the F3EAD process from the fusion of identity attributes (biologic, biographic, behavioral, and reputational information related to individuals) and other information and intelligence collected across all intelligence disciplines. I2 utilizes enabling intelligence activities such as biometrics-enabled intelligence, forensics-enabled intelligence, and document and media exploitation. I2 can discover the existence of unknown potential threats by connecting individuals to other known persons, places, events, or materials; analyzing patterns of life; and characterizing their level of potential threats to US interests. I2 enables the discovery of true identities; links identities to events, locations, ideology, and networks; and may reveal hostile intent.

For more information on I2, see JP 2-0, Joint Intelligence.

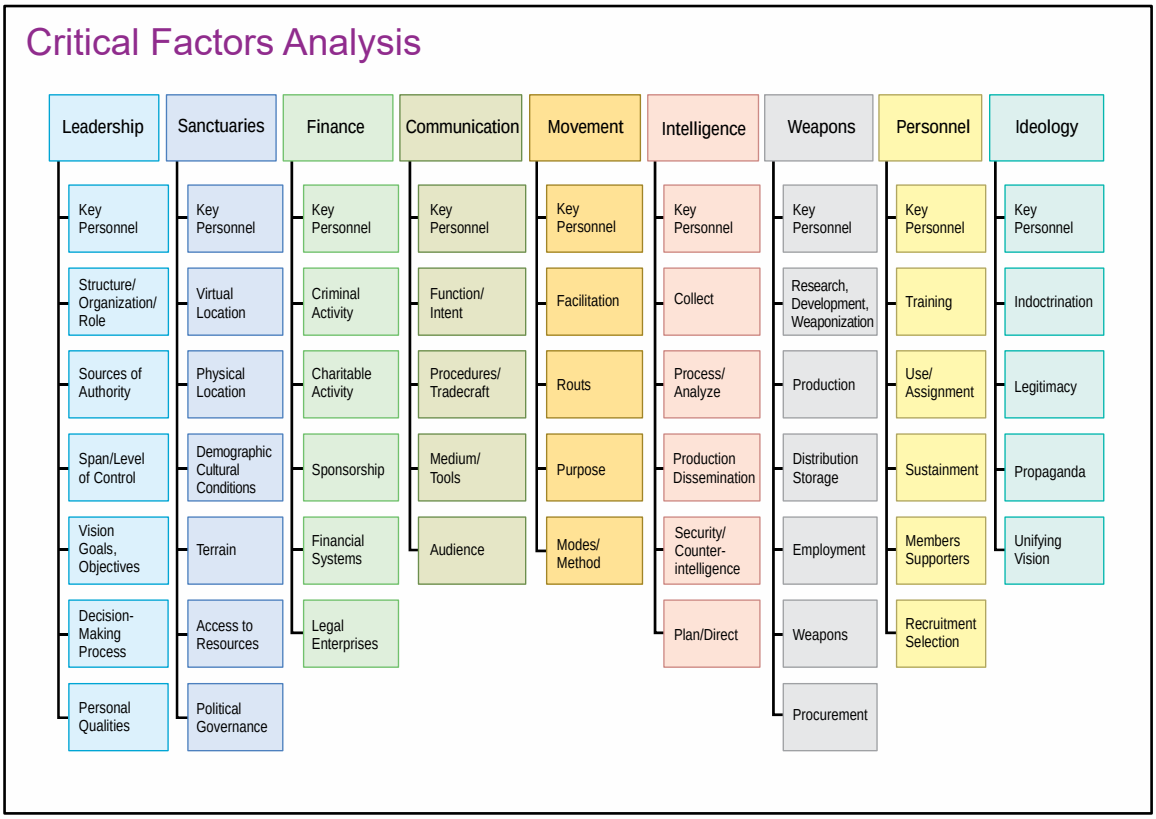


Figure C-1. Critical Factors Analysis

3. Biometrics and Identity Attribution

a. DOD's growing biometrics and forensic program capabilities enable appropriate authorities to collect, analyze, correlate, and disseminate a variety of biometric data (e.g., finger and palm prints and voice, facial, and iris images). Biometric data, combined with biographic, contextual, and other identity attributes, enables high-fidelity I2 for threat analysis and assessment. Biometric data is a key element leading to identity assurance or certitude and lifting the veil of anonymity surrounding terrorists and relevant actors.

b. Identity attribution is the planned and directed functions and actions that recognize and differentiate one person from another through collected exploitable material. Identity attribution includes the collection of identity attributes and physical materials and their processing and exploitation. They support all-source analytic efforts and production of I2 and DOD LE criminal intelligence products, and dissemination of those products, to inform policy and strategy development, operational planning and assessment, and appropriate action at the point of encounter. Identity attributes are the biometric, biographical, behavioral, and reputational data collected during encounters with an individual and across all intelligence disciplines that can be used alone or with other data to identify an individual. The processing and analysis of these identity attributes results in the identification of individuals, groups, networks, or populations of interest and facilitates the development of I2 products that allow an operational commander to:

(1) Identify previously unknown threat identities.

(2) Positively link identity information, with a high degree of certainty, to a specific person.

(3) Reveal the person's pattern of life and connect the person to other persons, places, materials, or events.

(4) Characterize the person's associates' potential level of threat to US interests.

(5) Support subsequent US or HN prosecution of detained individuals.

c. I2 fuses identity attributes and other information and intelligence associated with those attributes collected across all disciplines. I2 and DOD LE criminal intelligence products are crucial to the ability of commanders, staffs, and components to identify and select specific threat individuals as targets, associate them with the means to create desired effects, and support the JFC's operational objectives.

d. The maturation and increasing portability of biometric collection technologies and forensics science techniques provide the means to rapidly match individuals to a variety of biometric characteristics (e.g., facial images, iris images, fingerprints). This type of matching capability, when incorporated with all-source intelligence, has provided a powerful way to strip anonymity from our adversaries at the point of encounter. Collected, exploitable material obtained through imagery analysis and processed using biometric and forensic science techniques, and document and media exploitation capabilities, then integrated with the other intelligence disciplines, can be highly effective in CbT.

4. Identity and Exploitation Activities

Identity and exploitation activities leverage enabling intelligence activities to help identify threats; connect individuals to other persons, places, events, or materials; analyze patterns of life; and characterize capability and intent to harm US interests.

Intentionally Blank

APPENDIX D
POLICY, JURISDICTION, AND LEGAL CONSIDERATIONS

1. General

This appendix provides commanders with a basic understanding of relevant legal considerations in implementing an AT program. The policy and jurisdictional responsibilities generally applicable to the Armed Forces of the United States are outlined. However, commanders are encouraged to consult with their legal advisors for specific questions or concerns.

2. Commander's Authority

Commanders have both the inherent authority and the responsibility to enforce security measures and to protect persons and property under their control. Commanders should consult with their legal advisors regularly when establishing their AT programs.

3. Limits of Defense Support of Civil Authorities

a. **General.** DOD is the lead agency for conducting HD operations. However, against internal threats (e.g., domestic terrorism), DOD may be in support of DOJ or DHS and may conduct DSCA operations for declared emergencies.

b. **DSCA.** When providing DSCA, DOD will do so as directed by the President or SecDef and consistent with laws, presidential directives, EOs, and DOD policies and directives. DOD resources may be provided when requested by civil authorities and approved by SecDef. In most cases, assistance is provided on a cost-reimbursable basis. When imminently serious conditions resulting from any civil emergency or attack exist and time does not permit prior approval from higher HQs, local military commanders and responsible officials of other DOD components have immediate response authority to respond to requests from civil authorities to provide immediate assistance by temporarily employing resources under their control to save lives, prevent human suffering, or mitigate great property damage. This constitutes a policy of authority to act, where time does not permit obtaining express approval. In emergency response situations, support should not be delayed or denied because of the inability or unwillingness of the requester to make a commitment to reimburse DOD. See DODD 3025.18, *Defense Support of Civil Authorities (DSCA),* for proper implementation of immediate response authority.

c. Although statutory exceptions allow the use of military forces in some contexts, prior to committing forces, commanders should consult with their judge advocates or legal advisor and refer to applicable DOD and Service directives. Commanders retain responsibility for executing the FP mission but must recognize that the primary and most effective means of accomplishing the off-installation FP mission is via civilian LE. Commanders should develop and implement written, event-specific AT plans that are reviewed and approved by their higher HQ with FP responsibility. Commanders must understand that employment of joint forces, whether armed or unarmed, for the purpose of protecting DOD personnel and/or property outside a DOD installation may expose

commanders and individual security force members to significant personal liability under federal and state laws and raises concerns under the Posse Comitatus Act (PCA), unless other valid legislation is invoked that would remove restrictions of the PCA. CCDRs should establish planning guidance and tasking for their respective AORs.

For more information on legal considerations during domestic operations, see DODD 3025.18, Defense Support of Civil Authorities (DSCA); *JP 3-28,* Defense Support of Civil Authorities; *and JP 3-41,* Chemical, Biological, Radiological, and Nuclear Response.

4. Authority for Responding to Terrorist Incidents

a. Commanders' Responsibilities Inside the United States and Its Territories

(1) Although the FBI has primary LE responsibility for investigating terrorist incidents inside the United States (including its territories) and the DOD LE and the IC have a significant role within their departmental areas of jurisdiction, commanders remain responsible for maintaining law and order on DOD installations and vessels. The commander's AT plans should address the use of security personnel to isolate, contain, and neutralize a terrorist incident within the capability of the commander's resources. Terrorist attacks or incidents involving DOD personnel, facilities, or assets trigger the need for four separate, but related, activities:

(a) Immediate response, containment, and resolution of an incident.

(b) Cooperation with appropriate civilian LE authorities.

(c) Investigation of an incident for various purposes, to include protection of the crime scene.

(d) Prosecution of the alleged perpetrators.

(2) In the United States, installation and vessel commanders provide initial and immediate response to any incident occurring on military installations or vessels to isolate and contain the incident. This includes notifying the military criminal investigative organization and DOD Criminal Investigation Task Force regarding acts of terrorism and war crimes. Primary responsibility for investigating many of the most serious crimes on USG property normally rests with DOJ. On US military installations, the local commander retains primary responsibility, except for an identified terrorist incident.

For further information regarding use of force by DOD personnel, refer to CJCSI 3121.01, (U) Standing Rules of Engagement/Standing Rules for the Use of Force for US Forces. *For further information regarding the arming of DOD security and LE personnel, refer to DODD 5210.56,* Arming and the Use of Force.

(3) DOD may, under appropriate circumstances, provide support to state and/or federal LE agencies in response to civil disturbances or terrorist incidents occurring outside DOD installations or vessels. In addition to certain restrictions on direct DOD support to LE, commanders should also be mindful of applicable restrictions and DOD guidance

regarding the use of DOD intelligence components and non-intelligence components to support civil authorities in domestic activities. Relevant references include DODI 3025.21, *Defense Support of Civilian Law Enforcement Agencies;* DODD 5200.27, *Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense;* DODD 5240.01, *DOD Intelligence Activities;* DODI 5525.07, *Implementation of the Memorandum of Understanding (MOU) Between the Departments of Justice (DOJ) and Defense Relating to the Investigation and Prosecution of Certain Crimes;* and JP 3-28, *Defense Support of Civil Authorities.*

(4) In the event the FBI assumes jurisdiction, DOJ is the primary federal agency for the purpose of concluding the incident. If requested under pertinent statutes, the Attorney General may request SecDef approval for DOD commanders to provide support to the FBI. Military personnel, however, always remain under the C2 of the military chain of command. If military forces are employed during a tactical response to a terrorist incident, the military commander retains command responsibility of those forces. Command relationships and coordination of rules for the use of force (RUF) should be addressed as part of the request for assistance.

(5) Attacks on DOD personnel or assets within the United States and its territories that are not on DOD facilities or vessels are to be contained and resolved by state and federal LE. Limited exceptions to this rule may occur when incidents involve DOD units outside a DOD installation or vessel and immediate action is necessary to protect DOD personnel and property from immediate threat of injury before local LE or the FBI can respond. It is important to note that commanders should consult their legal advisors and US regulations before implementing any course of action off the installation.

For more information on RUF during DSCA, see DODD 5210.56, Arming and the Use of Force; *CJCSI 3121.01,* (U) Standing Rules of Engagement/Standing Rules for the Use of Force for US Forces; *and JP 3-28,* Defense Support of Civil Authorities.

b. **Commander's Responsibilities Outside the United States and Its Territories**

(1) Although DOS has the primary responsibility for dealing with terrorism involving Americans abroad, DOD commanders have the inherent right and obligation to defend their units and other US units in the vicinity from terrorist incidents wherever they occur, with the additional requirement to notify the cognizant CCDR for further reporting to DOS. The commander is responsible for incident response and containment to protect DOD personnel and property from immediate threat of injury. DOS has the primary responsibility for coordinating the political and diplomatic response to terrorism involving Americans abroad. The installation or vessel commander should also implement any provisions of any applicable SOFAs or any other agreements between the United States and the host government relevant to the incident.

(2) The host government may provide forces to further contain and resolve the incident in accordance with its obligations under international law, any applicable SOFA, and any other relevant agreements. If the USG asserts a prosecutorial interest, DOJ, in

coordination with DOS, assumes lead agency responsibilities for liaison and coordination with HN LE and prosecutorial agencies.

(3) The inherent right of unit commanders to exercise self-defense in response to a hostile act or demonstrated hostile intent, as reflected in CJCSI 3121.01, *(U) Standing Rules of Engagement/Standing Rules for the Use of Force for US Forces,* still applies in off-base situations or off vessel in foreign areas. Unless otherwise directed by the unit commander, in accordance with the specific guidelines of CJCSI 3121.01, military members may exercise individual self-defense in response to a hostile act or demonstrated hostile intent. If US forces are under attack, they retain the inherent right to respond with proportionate, necessary force until the threat is neutralized. The host government should take appropriate action to further contain and resolve the incident in accordance with its obligations under international law, as well as any applicable SOFA or other international agreement. In situations other than those triggering the inherent right of self-defense, US military assistance, if any, depends on the applicable SOFA and other international agreements. Such assistance is coordinated through the US embassy. Unless immediate action is necessary to protect DOD personnel and property from immediate threat of injury, or action is taken under immediate response authority to save lives, no US military assistance may be provided to assist a host government without direction from DOD and in coordination with DOS. The degree of the involvement of US military forces depends on the following:

(a) The incident site.

(b) The nature of the incident.

(c) The extent of foreign government involvement.

(d) The overall threat to US interests and security.

(e) The ability of US forces to sustain their capability to perform assigned missions.

c. **MOU and MOA**

(1) Title 22, USC, Section 4802, directs SECSTATE to assume responsibility for the security of all USG personnel on official duty abroad, except those under the command of CCDRs, and their accompanying dependents. SECSTATE discharges these responsibilities through the COMs. In December 1997, SecDef and SECSTATE signed the *Memorandum of Understanding on Security of Department of Defense Elements and Personnel in Foreign Areas* (also known as the "Universal MOU"). The MOU is based on the principle of assigning security responsibility to the party—CCDR or COM—in the most efficient and effective position to provide security for DOD elements and personnel. The MOU requires delineation of security responsibilities through nation-specific MOAs.

(2) Once security responsibility has been agreed upon through the universal MOU/MOA process, the COM and/or CCDR (and designated AT planning and response elements) may enter into mutual assistance agreements with HN authorities. These

MOAs/MOUs augment the installation's organic capabilities and/or are activated when a situation exceeds the installation's inherent capabilities, fulfilling requirements needed to respond to a terrorist incident. Therefore, each installation must prepare for the worst-case scenario by planning responses based on organic resources and local support available through MOAs/MOUs. These MOAs/MOUs must be a coordinated effort between the many AT planning and response elements of the installation.

(3) Installation-specific MOAs/MOUs and other special arrangements improve the resources and/or forces available to support any AT plan. These MOAs/MOUs may include, but are not limited to, HN and US military police forces; fire and emergency services; medical services; federal, state, and local agencies; SOF; engineers; CBRN units; and explosive ordnance disposal. Often through agreements with HN authorities, MOAs are adapted to grant the US installation commander responsibility within (or inside) the installation boundary, with the HN having responsibility outside this boundary. The wide dispersal of work areas, housing, support (medical; child care; exchange; and morale, welfare, and recreation), and utility nodes (power grids, water plants) may require US responsibility for certain fixed-site security outside the installation boundary. Although the installation commander may not have security responsibility "outside the wire," the commander still maintains a security interest. The installation commander must include exterior terrain, avenues of approach, threat capabilities (possession of standoff weapons such as man-portable air defense system or mortars), hazardous material storage in proximity to the US forces, and HN security processes when developing security plans for the installation, regardless of who provides exterior defense.

(4) In 2003, an MOU between DOS and DOD established force protection detachments (FPDs). The primary mission of an FPD is to support the in-transit FP requirements according to priorities established by the CCDRs when military criminal investigative and CI organizations are not present. FPD activities include, but are not limited to:

(a) Preparing TAs and informational documents;

(b) Coordinating with foreign LE and security officials;

(c) Producing AT surveys;

(d) Assessing route and travel threats;

(e) Briefing antiterrorist and CI threats;

(f) Assisting in investigations and operations, such as protective service operations; and

(g) Serving as a point of contact in embassies for DOD CI and LE organizations.

For further information, see DODI 5240.22, Counterintelligence Support to Force Protection, *and* Memorandum of Understanding (MOU) Between the Department of State,

Bureau of Diplomatic Security, and the Department of Defense Counterintelligence Field Activity Regarding Force Protection Detachments, *9May 2003.*

5. United States Coast Guard

The United States Coast Guard (USCG) is the lead federal agency for maritime homeland security (MHS) and operates, at all times, as both an Armed Force of the United States (Title 14, USC, Section 101) and an LE agency (Title 14, USC, Sections 102 and 522). One of the USCG's 11 statutory missions is to conduct MHS operations to protect the US maritime domain and Marine Transportation System and deny their use and exploitation by terrorists as a means for attacks on US territory, population, and maritime critical infrastructure. Additionally, the USCG prepares for and, in the event of attack, conducts emergency response operations either unilaterally or in support of DOJ or DOD or with other federal, state, or local government agencies. As a Service, the USCG regularly supports and/or complements DOD objectives globally. The USCG is especially qualified and/or uniquely suited for operations such as maritime interdiction, maritime interception, marine environmental response, port operations, SC, intelligence collection, support sea control, rotary-wing air intercept, and CbT operations. The USCG provides key support to the Maritime Operational Threat Response plan and, when directed, supports maritime HD operations.

For more information on USCG support to maritime HD, see JP 3-27, Homeland Defense.

6. Legal Considerations

a. **Application of the Law of War.** It is DOD policy that members of the DOD components comply with the law of war during all armed conflicts, however such conflicts are characterized, and in all other military operations. Law of war is that part of international law that regulates the conduct of armed hostilities. It encompasses all international law for the conduct of hostilities binding on the United States or its individual citizens, including treaties and international agreements to which the United States is a party, and applicable, customary international law. The law of war rests on fundamental principles of military necessity, unnecessary suffering, proportionality, and distinction (discrimination). JFCs must ensure CT operations in numerous locations across the globe comply with these legal requirements where an armed conflict exists.

b. **Legal Basis for Use of Force.** Nearly every military decision and action has potential legal considerations and implications. A legal basis must exist for every decision to use military force, including CT operations. In a general sense, under customary international law as reflected in the United Nations Charter and elsewhere, the United States has the inherent right of self-defense against hostile acts or demonstrations of hostile intent toward the United States or its citizens, including the use of force in anticipatory self-defense. Additionally, US forces may be acting under a United Nations Security Council resolution to take action to restore international peace and security in a particular area. Actions within the sovereign territory of another state should be based on either the consent of that state, a United Nations Security Council resolution, or a presidential determination that such action is necessary either in response to an armed attack or in anticipation of an imminent threat to

the security of the United States. Normally, for a given operation, the JFC has approved ROE for overseas operations or RUF for operations within the homeland or while conducting official DOD security functions outside US territory. These ROE/RUF govern the use of military force and were developed based on the legal and operational considerations for the situation.

For further guidance on the law of war, refer to CJCSI 5810.01, Implementation of the DOD Law of War Program. *For detailed information and guidance on legal support, refer to JP 3-84,* Legal Support.

c. **ROE and RUF.** For operations, the responsibility and authority for using military force is generally delegated from the President through SecDef to the supported CCDR/JFC in the form of approved plans/orders with either ROE for operations overseas or RUF for DSCA within the homeland or while conducting official DOD security functions outside US territory. When compared to major combat operations, ROE for some smaller-scale operations (i.e., some CT operations) may be more restrictive and detailed, especially in an urban environment, due to national policy concerns for the impact on civilians, their culture, values, and infrastructure. A JFC may begin operations with different ROE/RUF for each type of mission and especially for CT operations. The JFC responsible for CT should determine early in the planning stage what the required ROE/RUF should be, including anticipating the need for serial changes based on the need for escalation of force, changing phases of an operation, and branches/sequels to a plan. Dependent upon the required level of approval for any changes, that JFC must take anticipatory action if the serial changes are to be timely enough for effective operations. When conducting multinational CT operations, the use of military force may be influenced by the differences between US and HN or PN ROE/RUF. Commanders at all levels must take proactive steps to ensure an understanding of ROE by the individual Service member because a single errant act could cause significant adverse political consequences. Commanders are encouraged to leverage legal advisors and judge advocates in the effort to educate Service members on the relevant ROE/RUF for each operation.

For more detailed discussion on restraint and ROE/RUF, see JP 3-0, Joint Operations.

d. **Detainee Operations.** CT operations may result in detainees. Proper handling of detainees is essential, not only for possible exploitation purposes but also for prevention of violations of the law (civil or military). Improper handling of detainees may undermine the legitimacy of US CT operations. However, regardless of the detainees' legal status, US forces must treat all detainees humanely and be prepared to properly control, maintain, protect, and account for detainees in accordance with applicable US law, the law of war, and applicable US policy. Inhumane treatment of detainees is prohibited by the Uniform Code of Military Justice, domestic and international law, and DOD policy. Accordingly, the stress of combat operations, the need for intelligence, or provocations by captured or detained personnel does not justify deviation from this obligation. The challenges of today's security environment and the nature of the enemy require clear operational and strategic guidance for detainee operations during CT operations.

For more, detailed information regarding detainee operations, see JP 3-63, Detainee Operations.

e. **HS CT Operations.** HS CT operations are under the lead of DHS. DHS is considered the primary for coordinating executive branch efforts to detect, prepare for, prevent, protect against, respond to, and recover from terrorist attacks within the United States. DOJ supports DHS for CT but could also be the primary federal agency for some situations.

(1) If a CT situation should formally transcend into a matter of HD, then DOD is the lead for action and interagency coordination for HD. HD CT operations raise additional legal concerns due to the likely intersection with civil authorities and US persons. When participating in HD CT operations, JFCs must be particularly aware of the status of their forces; the legal basis for their use of force; the authority for conducting the operation and any specific limitations; and the characterization, treatment, and authorized activities regarding all persons and property encountered in their operations.

(2) SecDef retains the authority to approve use of DOD resources for DSCA where it is unlikely that use of military force will be required. The Joint Staff Joint Director of Military Support validates requests for assistance, determines what DOD capabilities are available to fulfill the requests, coordinates for SecDef approval to use DOD assets, and allocates forces to the CCDR with responsibility for that area of the United States.

(3) During HD and DSCA, the Constitution, federal law, and DOD policy limit the scope and nature of military actions. The President has the authority to direct the use of the military against terrorist groups and individuals in the United States for other than LE actions (i.e., national defense, emergency protection of life and property, and to restore order). The National Guard has a unique role. Under control of the respective states, National Guard units in Title 32, USC, and state active duty status can support a variety of tasks for HD and DSCA. National Guard forces in state active duty or Title 32, USC, status can perform direct LE tasks that Title 10, USC, forces cannot perform due to constraints in the PCA and DODI 3025.21, *Defense Support of Civilian Law Enforcement Agencies.* In its maritime LE role under DHS, the USCG, as a Service under DHS, has jurisdiction in both US territorial waters and on the high seas as prescribed in law.

(4) MOAs between DOD and DHS/USCG exist to facilitate the rapid transfer of forces between DOD and the USCG for support of HS, HD, and other defense operations. Therefore, the military response to extraordinary events that requires DSCA will likely be a coordinated effort between the National Guard (in state active duty or Title 32, USC, status) and the Armed Services (Title 10 and Title 14, USC).

(5) HS CT activities may involve other civil authorities, including state, territorial, local, or tribal governments.

For more information on HS, HD, and DSCA, and the coordination of associated interagency activities supporting those missions, see the National Strategy for Homeland

Security; *the* National Response Framework; *JP 3-27,* Homeland Defense*; and JP 3-28,* Defense Support of Civil Authorities.

7. Intelligence Activities and Oversight

Special Considerations for Intelligence Support to CbT Operations and Activities. During DSCA and HD, certain intelligence activities, military information support operations, ROE, and RUF have specific limitations, applications, and legal considerations. Further, ROE and RUF for DSCA and HD are often developed by less institutionalized processes and can, therefore, potentially be less thorough and subjected to less rigor.

a. **PCA.** The PCA prohibits the use of the United States Army (USA) and United States Air Force (USAF) from participating in civilian LE within the homeland. Title 10, USC, also directs SecDef to promulgate regulations prohibiting members of the USA, US Navy, USAF, and US Marine Corps from providing direct assistance to civilian LE, which was accomplished in DODI 3025.21, *Defense Support of Civilian Law Enforcement Agencies.* HD is a Constitutional exception to the PCA. Military operations conducted as HD are not LE activities, and thus, Title 10, USC, forces are not subject to the restriction of the PCA or DODI 3025.21, *Defense Support of Civilian Law Enforcement Agencies.* Additionally, several Act-of-Congress exceptions to the PCA permit the Armed Forces of the United States to support LE activities under other conditions. The PCA does not apply to National Guard forces under Title 32, USC, or state active duty status.

b. **Intelligence Activities.** Intelligence activities refer to all activities that DOD intelligence components are authorized to undertake in accordance with EO 12333, *United States Intelligence Activities* (as amended); DODD 5148.13, *Intelligence Oversight;* DODD 5240.01, *DOD Intelligence Activities;* DODM 5240.01, *Procedures Governing the Conduct of DOD Intelligence Activities;* DOD 5240.1-R, *Procedures Governing the Activities of DOD Intelligence Components that Affect United States Persons;* Chief, National Guard Bureau (CNGB) Instruction 2000.01, *National Guard Intelligence Activities;* and CNGB Manual 2000.01, *National Guard Intelligence Activities.* Intelligence activities include the collection, retention, and dissemination of intelligence by DOD intelligence components.

(1) Intelligence activities conducted by US intelligence organizations in the United States and its territories are strictly controlled. Several regulations and laws specifically govern the use of DOD intelligence assets and organizations during DSCA and HD. Figure D-1 lists several policy and guidance documents for the intelligence oversight program.

(2) **Acquisition of Open-Source Information.** Publicly available, open-source information can be used to obtain basic situational awareness and regional industrial knowledge on any part of the world; however, intelligence oversight still applies to information gathered on US persons or companies regardless of whether it is publicly available or not. Adherence to DODD 3115.18, *DOD Access to and Use of Publicly Available Information (PAI);* DODD 5240.01, *DOD Intelligence Activities;* DODM

Guidance and Policy for the Intelligence Oversight Program

- Executive Order 12333, *United States Intelligence Activities* (as amended)
- Department of Defense Directive (DODD) 5148.11, *Assistant to the Secretary of Defense for Intelligence Oversight (ATSD(IO))*
- DODD 5148.13*, Intelligence Oversight*
- DODD 5240.01, *DOD Intelligence Activities*
- Department of Defense (DOD) 5240.1-R, *Procedures Governing the Activities of DOD Intelligence Components that Affect United States Persons*
- National Geospatial-Intelligence Agency's National System for Geospatial Intelligence Manual FA 1806, *Domestic Imagery,* Revision 5, March 2009, Administrative Update: May 2011
- North American Aerospace Defense Command and United States Northern Command Instruction 14-3, *Domestic Imagery,* 29 July 2014 modified 23 June 2016
- DOD Manual 5240.01, *Procedures Governing the Conduct of DOD Intelligence Activities*
- DOD Instruction 3115.12, *Open Source Intelligence (OSINT)*
- Chief, National Guard Bureau Instruction, 2000.01, *National Guard Intelligence Activities*
- Chief, National Guard Bureau Manual, 2000.01, *National Guard Intelligence Activities*

Figure D-1. Guidance and Policy for the Intelligence Oversight Program

5240.01, *Procedures Governing the Conduct of DOD Intelligence Activities;* and DOD 5240.1-R, *Procedures Governing the Activities of DOD Intelligence Components That Affect United States Persons,* when performing such collections, is critical to the success of the effort and to avoid the appearance or conduct of questionable intelligence activities.

(3) **Acquisition of Information Concerning Persons and Organizations Not Affiliated with DOD.** Some restrictions on information gathering apply DOD-wide, not just to DOD intelligence elements. In accordance with DODD 5200.27, *Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense,* DOD policy prohibits collecting, reporting, processing, or storing information on individuals or organizations not affiliated with DOD, except in those limited circumstances where such information is essential to the accomplishment of certain DOD missions outlined within the directive. DOD intelligence elements are not governed by this directive and must look to DODM 5240.01, *Procedures Governing the Conduct of DOD Intelligence Activities;* DODI 3115.12, *Open Source Intelligence;* DODD 5240.01, *DOD Intelligence Activities;* and DOD 5240.1-R, *Procedures Governing the Activities of DOD Intelligence Components That Affect United States Persons,* for guidance.

(4) **Domestic Use of UASs.** In 2018, SecDef issued a memorandum titled *Guidance for the Domestic Use of Unmanned Aircraft Systems in US National Airspace*. Enclosure 2 of this memorandum details the levels of approval for various uses of UASs by DOD. Additionally, each Service has Service-specific guidance implementing lower-

level approval authorities for use of UASs. Each Service is responsible for coordinating with the Federal Aviation Administration for airspace use and the National Telecommunications and Information Administration for electromagnetic spectrum use.

(5) **Counter UAS.** Title 10, USC, Section 130i, authorizes DOD to detect, identify, track, defeat, and destroy a UAS determined to be a "threat" to covered installations located in the United States. Guidance regarding determination of whether a UAS is a "threat" is contained in SecDef Policy Memorandum17-00X, *(U) Supplemental Guidance for Countering Unmanned Aircraft (UA).* Non-covered installations and foreign installations apply the standing ROE and SecDef Policy Memorandum 16-003, *(U) Interim Guidance for Countering Unmanned Aircraft*. Each Service maintains a list of its covered and non-covered installations. For foreign installations, CCMDs must coordinate with the respective HN's airspace and spectrum authorities for authorization to operate counter UAS.

For more details regarding domestic use of UASs, refer to Secretary of Defense Policy Memorandum, Guidance for the Domestic Use of Unmanned Aircraft Systems in US National Airspace. *For additional details, refer to Title 10, USC, Section 130i; Deputy Secretary of Defense Memorandum 16-003,* (U) Countering Small Unmanned Aircraft Systems in the Homeland; *Policy Memorandum 16-003,* (U) Interim Guidance for Countering Unmanned Aircraft; *and Secretary of Defense Policy Memorandum 17-00X,* (U) Supplemental Guidance for Countering Unmanned Aircraft (UA).

Intentionally Blank

APPENDIX E
THREAT INFORMATION ORGANIZATION MATRIX

1. Introduction

The threat information organization matrix (see Figure E-1) is provided as a tool that could be used to categorize, organize, and analyze threat information relevant to an AT program. It is similar to an intelligence collection plan but is intended for use on installations. If an intelligence collection plan is already active on the installation or base, the antiterrorism officer (ATO) should endeavor to have AT efforts integrated with ongoing efforts.

2. Organization Matrix

a. The basic premise of this organization matrix is that there are several key questions—PIRs—the command needs to answer to keep the installation better protected or aware of potentially developing terrorist activity. These PIRs have supporting components or related questions—IRs. Individual indicators suggest when the IR is active. The indicators are then divided into their core elements (specific information requirements [SIRs]) that installation staff members or coordination agencies need to report or record. Similarly, for a given incident, such as a stolen identification card, that information can be traced back to a bigger question and suggests that someone is conducting surveillance on the base or nearby base.

b. The SIRs should be given to the staff members who would likely observe or see the types of information suggested. For instance, gate guards should be given the SIRs to report unauthorized access attempts (item 1.32a) (Column D row 28), but the installation IT office would be responsible for reporting computer viruses and unauthorized attempts to access the network (items 1.16a, 1.16b). The organization plan also assists the ATO in explaining to coordinating agencies exactly what information is expected.

c. There is no requirement to use this or another threat information organization model, but, if used, the model should be modified to fit specific commander and installation requirements, agreements, and efforts.

d. Similarly, AT threat analysis and reporting is conducted in accordance with the same intelligence oversight guidance. DOD intelligence oversight regulations and guidance remain in effect for all collection, analysis, and reporting on terrorist threats or suspicious activities within the United States.

Installation Threat Information Organization Plan																							
				Collection		Collection Agencies																	
Priority Intelligence Requirement	Information Requirement	Indicators	Specific Information Requirements	Date Info Needed	Date Info No Longer Needed	LET	CID, OSI, NCIS	CI	TWG	HHQ INT	CST	HS	FBI	ATF	Local LEA #1	Local LEA #2	Local LEA #3	State LEA	DOIM/IT	Installation	Near Base	Remarks
PIR #1	Installation																					
1. What local, regional, or international organizations pose a potential threat to XXXX or the surrounding community?				Always	Never	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	Reporting requirements 1. LEC 111-111-1111 2. IOC 111-111-1111 3. CID 111-111-1111 4. MI 111-111-1111 5. OSI 111-111-1111 6. FBI 111-111-1111 (After hrs 111-111-1111)
	1.1. What means do these organizations have to conduct attacks against XXXX and the surrounding community?			Always	Never	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
		1.11. Information on purchase or theft of material to make improvised devices	1.11a. Report unusual purchase or theft of explosives, weapons, ammunition, hazmat, fertilizers, chemicals, etc.	Always	Never																	
		1.12. Information on purchase of large quantity of weapons or theft of weapons	1.12a. Report unusual purchase or theft of vehicles capable of being configured with explosives or WMD	Always	Never																	
		1.13. Information on suspicious car, truck, van activity	1.13a. Report vehicles modified to handle heavier loads	Always	Never																	
		1.14. Information on suspicious activity dealing with military IDs, DOD decals, or other XXXX special access passes	1.14a. Report loss or theft of government vehicles or license plates	Always	Never																	
			1.14b. Report purchase or theft of vehicles with DOD decals																			
			1.14c. Report loss or theft of military IDs or special access passes																			

Figure E-1. Installation Threat Information Organization Plan

Installation Threat Information Organization Plan																							
				Collection		Collection Agencies																	
Priority Intelligence Requirement	Information Requirement	Indicators	Specific Information Requirements	Date Info Needed	Date Info No Longer Needed	LET	CID, OSI, NCIS	CI	TWG	HHQ INT	CST	HS	FBI	ATF	Local LEA #1	Local LEA #2	Local LEA #3	State LEA	DOIM/IT	Installation	Near Base	Remarks
PIR #1	Installation																					
		1.15. Information on unusual airborne activity on/vicinity XXXX	1.15a. Report unusual flight patterns of helicopters, single-engine aircraft, parachute/gliders, or parafoils																			
			1.15b. Report theft of airborne platforms																			
		1.16. Information on attempts to attack or access XXXX computer network	1.16a. Report any attempt to access XXXX computer network or reports of stolen or misused passwords																			
			1.16b. Report any ADP viruses immediately																			
			1.16c. Report any suspicious telephone calls or e-mails																			
	1.2. What historical patterns of attack has this group employed?			Always	Never																	
		1.21. Information on modus operandi of domestic dissident groups operating vicinity XXXX	1.21a. Report any suspicious activity associated with local domestic dissident groups	Always	Never																	
		1.22. Information on increased criminal activity on/vicinity XXXX	1.22a. Review records and report on previous activity of local domestic dissident groups	Always	Never																	
		1.23. Information on foreign terrorist groups, or groups sympathetic to foreign terrorist organizations, operating vicinity XXXX	1.23a. Report any suspicious activity associated with foreign terrorist groups	Always	Never																	
		1.24. Increase in SAEDA reporting	1.24a. Review foreign terrorist modus operandi and report any suspicious activity that is similar	Always	Never																	
			1.24b. Report any former dissident members recently arrested or detained vicinity XXXX																			

Figure E-1. Installation Threat Information Organization Plan (continued)

Installation Threat Information Organization Plan																						
				Collection		Collection Agencies																
Priority Intelligence Requirement	Information Requirement	Indicators	Specific Information Requirements	Date Info Needed	Date Info No Longer Needed	LET	CID, OSI, NCIS	CI	TWG	HHQ INT	CST	HS	FBI	ATF	Local LEA #1	Local LEA #2	Local LEA #3	State LEA	DOIM/IT	Installation	Near Base	Remarks
PIR #1	Installation																					
	1.3. What are the recent activities of this organization?			Always	Never																	
		1.31. Information on possible surveillance of XXXX	1.31a. Report all suspicious questions about XXXX or vicinity	Always	Never																	
		1.32. Information on possible unauthorized attempts to access XXXX	1.32a. Report all unauthorized attempts to access XXXX	Always	Never																	
		1.33. Queries about XXXX security measures	1.33a. Report all suspicious telephone calls or e-mails	Always	Never																	
		1.34. Requests for information on XXXX activities, missions, memoranda of agreement, memoranda of understanding	1.34a. Report all questions about sensitive locations																			
		1.35. Active dissident or terrorist groups recruiting vicinity XXXX	1.35a. Report all questions about working relationships with local, state, federal law enforcement agencies																			
		1.36. Active dissident or terrorist groups fund-raising vicinity XXXX	1.36a. Report all suspicious requests for job employment vicinity XXXX																			
		1.37. Active dissident or terrorist groups training vicinity XXX	1.37a. Report all suspicious fund-raising operations vicinity XXXX																			
			1.37b. Report all suspicious recruiting or training operations vicinity XXXX																			
			1.37c. Report what these groups collect against																			
		1.38. Recent arrests in vicinity XXXX	1.38a. Report any suspicious individuals arrested or detained vicinity XXXX																			

Figure E-1. Installation Threat Information Organization Plan (continued)

Installation Threat Information Organization Plan																						
				Collection		Collection Agencies																
Priority Intelligence Requirement	Information Requirement	Indicators	Specific Information Requirements	Date Info Needed	Date Info No Longer Needed	LET	CID, OSI, NCIS	CI	TWG	HHQ INT	CST	HS	FBI	ATF	Local LEA #1	Local LEA #2	Local LEA #3	State LEA	DOIM/IT	Installation	Near Base	Remarks
PIR #1	Installation																					
	1.4. What adjustments has this organization made in response to changes in XXXX threat conditions and force protection conditions?			Always	Never																	
		1.41. Information on new methods dissident groups or terrorist organizations are using to obtain information, surveil, recruit, fund-raise, or acquire weapons or equipment	1.41a. Report all suspicious questions about XXXX or vicinity	Always	Never																	
		1.42. Information on possible surveillance of XXXX	1.42a. Report all unauthorized attempts to access XXXX	Always	Never																	
		1.43. Information on possible unauthorized attempts to access XXXX	1.43a. Report all suspicious telephone calls or e-mails	Always	Never																	
		1.44. Queries about XXXX security measures	1.44a. Report all suspicious requests for job employment in vicinity XXXX																			
			1.44b. Report all suspicious recruiting or training operations vicinity XXXX																			
PIR #2	Installation																					
2. What patterns of activity, threats, or law enforcement advisories have there been that indicate an increased likelihood of attack on XXXX or the surrounding community?																						

Figure E-1. Installation Threat Information Organization Plan (continued)

Installation Threat Information Organization Plan																							
				Collection		Collection Agencies																	
Priority Intelligence Requirement	Information Requirement	Indicators	Specific Information Requirements	Date Info Needed	Date Info No Longer Needed	LET	CID, OSI, NCIS	CI	TWG	HHQ INT	CST	HS	FBI	ATF	Local LEA #1	Local LEA #2	Local LEA #3	State LEA	DOMI/T	Installation	Near Base	Remarks
PIR #2	Installation																					
	2.1. Have there been any suspicious surveillance activities on XXXX or against assigned personnel?																					
		2.11. Incidents of individuals videotaping, photographing, or sketching XXXX	2.11a. Report incidents of individuals videotaping, photographing, or sketching installation elements																			
		2.12. Incidents of unauthorized individuals attempting to access XXXX	2.12a. Report turnarounds at gates																			
			2.12b. Report loss or theft of military IDs or special access passes																			
		2.13. Incidents of XXXX personnel being surveilled by suspicious personnel	2.13a. Report any suspicious incidents in which base personnel suspect they were being surveilled																			
		2.14. Unusual attempts to obtain military uniforms, DOD decals, military IDs, or equipment in vicinity XXXX	2.14a. Report any attempts to obtain military uniforms or equipment																			
	2.2. Have there been any thefts or unusual circumstances involving the loss of personal ID cards, vehicle registrations, government license plates, or government vehicles?																					
		2.21. Incidents of stolen or lost personal ID cards	2.21a. Report loss or theft of government vehicles or license plates																			

Figure E-1. Installation Threat Information Organization Plan (continued)

Installation Threat Information Organization Plan																							
				Collection		Collection Agencies																	
Priority Intelligence Requirement	Information Requirement	Indicators	Specific Information Requirements	Date Info Needed	Date Info No Longer Needed	LET	CID, OSI, NCIS	CI	TWG	HHQ INT	CST	HS	FBI	ATF	Local LEA #1	Local LEA #2	Local LEA #3	State LEA	DOMI/T	Installation	Near Base	Remarks
PIR #2	Installation																					
		2.22. Incidents of stolen or lost DOD decals or special access passes for XXXX	2.22a. Report purchase or theft of vehicles with DOD decals																			
		2.23. Incidents of stolen or lost government license plates	2.23a. Report loss or theft of military IDs or special access passes																			
		2.24. Incidents of stolen government vehicles	2.24a. Report all unauthorized attempts to access XXXX																			
		2.25. Increase in vehicle break-ins or car theft vicinity XXXX	2.25a. Report all attempts at vehicle break-ins or car theft vicinity XXXX																			
		2.26. Queries of unauthorized personnel attempting to obtain XXXX access passes	2.26a. Report all suspicious requests for employment in vicinity XXXX																			
	2.3. Have there been thefts or unusual circumstances involving the loss of personal or government weapons, ammunition, or explosives?																					
		2.31. Increased reporting of theft of weapons, ammunition, or explosive materials in vicinity XXXX	2.31a. Report unusual purchase or theft of explosives, weapons, ammunition, hazmat, fertilizers, chemicals, etc.																			
		2.32. Attempts to illegally purchase weapons, ammunition, or explosive materials	2.32a. Report unusual purchase or theft of vehicles capable of being configured with explosives																			
		2.33. Unusual queries about location of storage of weapons on XXXX, especially by telephone or e-mail	2.33a. Report on vehicles modified to handle heavier loads																			

Figure E-1. Installation Threat Information Organization Plan (continued)

Installation Threat Information Organization Plan																							
				Collection		Collection Agencies																	
Priority Intelligence Requirement	Information Requirement	Indicators	Specific Information Requirements	Date Info Needed	Date Info No Longer Needed	LET	CID, OSI, NCIS	CI	TWG	HHQ INT	CST	HS	FBI	ATF	Local LEA #1	Local LEA #2	Local LEA #3	State LEA	DOM/IT	Installation	Near Base	Remarks
PIR #2	Installation																					
		2.34. Attempts by unauthorized individuals to observe military training sites where weapons are used	2.34a. Report loss or theft of government vehicles or license plates																			
	2.4. Have there been any perimeter violations, security breaches, unauthorized intrusions, or unauthorized overflights of XXXX?																					
		2.41. Incidents of physical signs of intrusion on XXXX	2.41a. Report loss or theft of government vehicles or license plates																			
		2.42. Incidents of unauthorized personnel attempting to access XXXX	2.42a. Report on purchase or theft of vehicles with DOD decals																			
		2.43. Incidents of unauthorized attempts to access XXXX	2.43a. Report loss or theft of military IDs or special access passes, refused entries, or turnarounds at gate																			
	2.5. Have there been receipts of any suspicious shipments of mail, packaged freight, truck inventory, containerized ship cargo, or special equipment?																					
		2.51. Increase in receipt of suspicious packages nationwide	2.51a. Report any suspicious mail, packages, or cargo received on/vicinity XXXX																			

Figure E-1. Installation Threat Information Organization Plan (continued)

Installation Threat Information Organization Plan																							
				Collection		Collection Agencies																	
Priority Intelligence Requirement	Information Requirement	Indicators	Specific Information Requirements	Date Info Needed	Date Info No Longer Needed	LET	CID, OSI, NCIS	CI	TWG	HHQ INT	CST	HS	FBI	ATF	Local LEA #1	Local LEA #2	Local LEA #3	State LEA	DOM/IT	Installation	Near Base	Remarks
PIR #2	Installation																					
		2.52. Increased reporting of potential threats to XXXX mail or cargo shipments, especially by telephone or e-mail	2.52a. Report unusual purchase or theft of explosives, weapons, ammunition, hazmat, fertilizers, chemicals, etc.																			
		2.53. Increase in stolen delivery, cargo, commercial trucks nationwide; focus on vicinity XXXX	2.53a. Report unusual purchase or theft of vehicles capable of being configured with explosives																			
			2.53b. Report vehicles modified to handle heavier loads																			
	2.6. Have there been any thefts from surrounding community of commercial or private aircraft, commercial or private helicopters, commercial vehicles, tanker trucks with tank capacity of more than 500 gallons of bulk chemical, or watercraft with a tank capacity of more than 1,000 gallons of bulk chemical?																					
		2.61. Increased reporting of threats against US facilities using aircraft	2.61a. Report any threats against US facilities																			
			2.61b. Report incidents of unauthorized individuals attempting to gain access to aircraft																			
		2.62. Incidents of surveillance of airports, aircraft, hangars, or flight lines	2.62a. Report any incidents at airports																			
		2.63. Incidents of theft of aircraft, watercraft, or large trucks	2.63a. Report thefts of aircraft, watercraft, or large trucks																			

Figure E-1. Installation Threat Information Organization Plan (continued)

Installation Threat Information Organization Plan																							
				Collection		Collection Agencies																	
Priority Intelligence Requirement	Information Requirement	Indicators	Specific Information Requirements	Date Info Needed	Date Info No Longer Needed	LET	CID, OSI, NCIS	CI	TWG	HHQ INT	CST	HS	FBI	ATF	Local LEA #1	Local LEA #2	Local LEA #3	State LEA	DOIM/IT	Installation	Near Base	Remarks
PIR #2	Installation																					
		2.64. Incidents of suspicious individuals trying to gain employment at businesses that have access to aircraft, commercial vehicles, tanker trucks, watercraft	2.64a. Report all suspicious attempts to gain employment with transportation industry in local area																			
PIR #3	Installation																					
3. What events are taking place on XXXX or in the surrounding community that may provide opportunity for threat or attack?																						
	3.1. What major sporting, cultural, industrial, political, military, or other symbolic events will take place at XXXX or in the community within the next 30 days that may trigger the targeting interests of threat organizations?																					
		3.11. Unusual number of queries concerning events taking place on/vicinity XXXX	3.11a. Report any unusual questions about events taking place on/vicinity XXXX																			
		3.12. Increased number of reports nationally about threat to major sporting, cultural, industrial, political, military, or other symbolic events	3.12a. Report increase in threat reporting nationwide concerning major sporting, cultural, industrial, political, military, or symbolic events																			
		3.13. Incidents of unauthorized individuals attempting to gain access to events on/vicinity XXXX	3.13a. Report all suspicious questions about XXXX or vicinity																			

Figure E-1. Installation Threat Information Organization Plan (continued)

Installation Threat Information Organization Plan																							
				Collection		Collection Agencies																	
Priority Intelligence Requirement	Information Requirement	Indicators	Specific Information Requirements	Date Info Needed	Date Info No Longer Needed	LET	CID, OSI, NCIS	CI	TWG	HHQ INT	CST	HS	FBI	ATF	Local LEA #1	Local LEA #2	Local LEA #3	State LEA	DOIM/IT	Installation	Near Base	Remarks
PIR #3	Installation																					
		3.14. Incidents of individuals making queries about security measures pertaining to events on/vicinity XXXX	3.14a. Report all suspicious telephone calls or e-mails																			
		3.15. Incidents of suspicious individuals attempting to gain employment to support specific events on/vicinity	3.15a. Report suspicious attempts to gain employment at special events																			
	3.2. What movements of hazmat take place on XXXX or in the community that may trigger the targeting interests of threat organizations?																					
		3.21. Incidents of individuals making queries about security measures pertaining to movements of hazmat on/vicinity XXXX	3.21a. Report unusual queries concerning movement of hazmat from XXXX																			
		3.22. Incidents of suspicious individuals trying to gain employment at businesses that have access to hazmat	3.22a. Report unauthorized individuals attempting to gain access to XXXX																			
		3.23. Incidents of stolen vehicles designed or that can be configured to haul hazmat	3.23a. Report thefts or individuals making queries about security measures pertaining to movement of hazmat on/vicinity XXXX																			
		3.24. Increased number of reports nationally about threat surrounding use of hazmat	3.24a. Report news concerning threat surrounding use of hazmat																			

Figure E-1. Installation Threat Information Organization Plan (continued)

Installation Threat Information Organization Plan																						
				Collection		Collection Agencies																
Priority Intelligence Requirement	Information Requirement	Indicators	Specific Information Requirements	Date Info Needed	Date Info No Longer Needed	LET	CID, OSI, NCIS	CI	TWG	HHQ INT	CST	HS	FBI	ATF	Local LEA #1	Local LEA #2	Local LEA #3	State LEA	DOIM/IT	Installation	Near Base	Remarks
PIR #4	Installation																					
4. Do indicators exist of a possible incident at XXXX or the surrounding community involving nuclear, biological, or chemical weapons?																						
	4.1. Do threat organizations have the means to conduct a CBRN attack or a hazmat attack at XXXX or in the surrounding community?																					
		4.11. Incidents of stolen CBRN material nationally and specifically in vicinity XXXX	4.11a. Report stolen CBRN material in vicinity XXXX																			
		4.12. Incidents of unusual purchase of explosives, weapons, ammunition, hazmat, fertilizers, chemicals, precursors, etc.	4.12a. Report excessive or unusual purchases of potential CBRN material																			
		4.13. Incidents of unusual purchase or theft of vehicles capable of being configured with explosives or adapted for agent dissemination	4.13a. Report purchases of protective or lab equipment for agent handling																			
		4.14. Incidents of individuals making queries about security measures pertaining to CBRN-related measures on/vicinity XXXX	4.14a. Report suspicious queries about the capability of CBRN materials																			
		4.15. Incidents of individuals making queries about security measures pertaining to CBRN-related measures on/vicinity XXXX	4.15a. Report queries about the security of chemicals used to train on XXXX																			

Figure E-1. Installation Threat Information Organization Plan (continued)

Installation Threat Information Organization Plan																						
				Collection		Collection Agencies																
Priority Intelligence Requirement	Information Requirement	Indicators	Specific Information Requirements	Date Info Needed	Date Info No Longer Needed	LET	CID, OSI, NCIS	CI	TWG	HHQ INT	CST	HS	FBI	ATF	Local LEA #1	Local LEA #2	Local LEA #3	State LEA	DOIM/IT	Installation	Near Base	Remarks
PIR #4	Installation																					
		4.16. Increased reporting of terrorist organization's ability and threat to CBRN material in the US	4.16a. Report unauthorized individuals attempting to gain access to XXXX																			
		4.17. Treatment of unusual illnesses or symptoms	4.17a. Report all medical cases seeking treatment for unusual illnesses or symptoms																			
		4.18. Purchase of CBRN antidotes	4.18a. Report purchases or attempted purchases of CBRN antidotes																			
			4.18b. Report any excess purchases of bleach																			
		4.19. Incidents of unusual odors or hazmat signs	4.19a. Report all cases of unusual odors or the appearance of hazmat signs																			
			4.19b. Report cases of unexplained animal deaths or lack of insect or plant life																			
	4.2. Do these threat organizations have a history of conducting CBRN attacks?																					
		4.22. Past reporting of a terrorist group in vicinity XXXX utilizing CBRN material to conduct attacks	4.22a. Review records and report previous CBRN activity of local domestic dissident groups																			
	4.3. What indicators suggest that a threat organization is about to conduct an attack?																					
		4.31. Incidents of threats to conduct CBRN attacks in vicinity XXXX	4.31a. Report all related threats																			
		4.32. Incidents of stolen CBRN materials in vicinity XXXX	4.32a. Report all stolen chemical agents																			
		4.33. Incidents of queries about XXXX's ability to respond to a CBRN attack	4.33a. Report all suspicious inquiries about CBRN defense capabilities																			

Figure E-1. Installation Threat Information Organization Plan (continued)

Installation Threat Information Organization Plan

				Collection		Collection Agencies															
Priority Intelligence Requirement	Information Requirement	Indicators	Specific Information Requirements	Date Info Needed	Date Info No Longer Needed	LET	CID, OSI, NCIS	CI	TWG	HHQ INT	CST	HS	FBI	ATF	Local LEA #1	Local LEA #2	Local LEA #3	State LEA	DOIM/IT	Installation	Near Base	Remarks
PIR #4	Installation																					
		4.34. Incidents of unusual purchases of CBRN protective gear	4.34a. Report thefts or purchases of CBRN protective gear																			
	4.4. Where are hazmat stored, transported, or used in bulk on XXXX or in the surrounding community, which could create mass casualties?																					
		4.41. Chemical or manufacturing industries, water treatment, waste treatment facilities	4.41a. Report all suspicious activity at these locations or with their transportation assets																			
			4.41b. Report what chemicals and quantities are stored at these locations																			
			4.41c. Report how these facilities store, receive, or ship chemicals																			
			4.41d. Report suspicious incidents related to storage or shipment of chemicals																			

Legend

ADP	automated data processing	HHQ	higher headquarters	LET	law enforcement team
ATF	Bureau of Alcohol, Tobacco, Firearms, and Explosives	hrs	hours	MI	military intelligence
CBRN	chemical, biological, radiological, and nuclear	HS	homeland security	NCIS	Naval Criminal Investigative Service
CI	counterintelligence	ID	identification	OSI	Office of Special Investigations
CID	Criminal Intelligence Division	INT	intelligence	PIR	priority intelligence requirement
CST	civil support team	IOC	installation operations center	SAEDA	subversion and espionage directed against the Army
DOD	Department of Defense	LEA	law enforcement agency	TWG	threat working group
DOIM/IT	Department of Information Management/Information Technology	LEC	law enforcement center	WMD	weapons of mass destruction
FBI	Federal Bureau of Investigation				

Figure E-1. Installation Threat Information Organization Plan (continued)

APPENDIX F
MULTINATIONAL CONSIDERATIONS

1. Overview

a. Military engagement with partners and advising and assisting them to develop CT/AT capabilities are key tools in US strategy and leverage DOD regional orientation and expertise that creates enduring partners in the region and often elsewhere. In the conduct of military engagement, the commander and staff should understand and account for variance in other nations' legal and cultural perspectives regarding terrorism and CbT principles and approaches.

b. The US's strategic network of allies and partners provides capacity, niche capabilities, intelligence, and forward access and basing that empowers the joint force when competing against global challenges. Maintaining this network is essential to the ability to deter and respond decisively throughout the competition continuum.

c. By assuring allies and partners in the fight against terrorism, the joint force also supports the mission to develop, strengthen, and sustain US security relationships.

d. The network of allies and partners enables assured force projection and freedom of maneuver, reducing the challenges associated with maintaining operational reach over expeditionary distances. Forward-deployed forces provide visible signs of US commitment to allies and partners while serving as a powerful deterrent to aggression by an adversary. Competitors, adversaries, and enemies also seek their own alliances and partnerships to offset US advantage in this mission area. Maintaining strong security relationships with allies and partners can deny access, basing, and overflight to competitors and adversaries. Where there are uncommitted entities, the joint force should seek to strengthen US security relationships to attract the uncommitted.

e. The joint force retains competitive advantage by reinforcing relationships with allies and partners, while seeking opportunities to expand the competitive space through new partnerships and relationships. Collectively, work on these relationships, to include multinational exercises and wider information sharing, bolsters allied and partner military capability, promotes interoperability, fosters resilience, and provides niche capabilities to mitigate joint force capacity shortfalls. Throughout competition, these activities build the confidence of allies and partners, gaining their commitment to share the burden of defense. Building resilience in the joint force includes training, advising, and assisting partners to counter malign influence by those who are seeking to undermine the rules-based order or create instability.

f. Commanders must understand that other nations do not necessarily execute FP in the same way as the Armed Forces of the United States. Some nations' armed forces may or may not be willing or able to assume the same risk as US forces. US commanders, whether under US control or under a command relationship to a multinational force, must continuously assess threats and vulnerabilities, while implementing appropriate FP countermeasures in accordance with published CCDR directives. Special consideration

must be given to personnel with duties that require interaction with local populations. Throughout multinational operations, risk management techniques and methodologies should be used to reduce or offset risk by systematically identifying, assessing, and controlling risk.

2. United Nations

The Counter-Terrorism Implementation Task Force (CTITF) was established by the United Nations to strengthen coordination and coherence of CT efforts of the United Nations system. The CTITF consists of multiple international entities that have a stake in multilateral CT efforts. Each entity makes contributions consistent with its own mandate. The primary goal of the CTITF is to maximize each entity's comparative advantage by delivering as one to help member states implement the following pillars:

a. Measures to address the conditions conducive to the spread of terrorism; measures to prevent and combat terrorism.

b. Measures to build states' capacity to prevent and combat terrorism and to strengthen the role of the United Nations system in that regard.

c. Measures to ensure respect for human rights for all and the rule of law as the fundamental basis for the fight against terrorism. For more information about the CTITF, visit the United Nations Website at https://www.un.org/counterterrorism/ctitf.

For more information, see JP 3-16, Multinational Operations.

APPENDIX G
COMBATING TERRORISM IN THE INFORMATION ENVIRONMENT

"The advent of the Internet, the expansion of information technology, the widespread availability of wireless communications, and the far-reaching impact of social media have dramatically impacted operations and changed the character of modern warfare."

Secretary of Defense James Mattis,
15 September 2017

1. Information Environment

The information environment is the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. This environment consists of three interrelated dimensions, which continuously interact with individuals, organizations, and systems. These dimensions are known as physical, informational, and cognitive. The physical dimension is composed of C2 systems, key decision makers, and supporting infrastructure that enable individuals and organizations to create effects. The informational dimension specifies where and how information is collected, processed, stored, disseminated, and protected. The cognitive dimension encompasses the minds of those who transmit, receive, and respond to or act on information.

a. **Physical Dimension.** In the physical dimension, terrorists and their organizations create C2 systems to transmit orders, gather targeting information, and transmit their influencing messaging (see Figure G-1). The physical dimension consists of terrorist key decision makers and supporting infrastructure that enable individuals and organizations to create effects. It is the dimension where physical platforms and the communications networks that connect them reside. The physical dimension includes, but is not limited to, human beings, C2 facilities, newspapers, books, microwave towers, computer servers, laptops, smart phones, tablet computers, or any other objects that are subject to empirical measurement. The physical dimension is not confined solely to military or even nation-based systems and processes; it is a diffuse network connected across national, economic, and geographical boundaries.

b. **Informational Dimension.** The informational dimension encompasses where and how information is collected, processed, stored, disseminated, and protected. It is the dimension where the C2 of military forces is exercised and where the commander's intent is conveyed. Actions in this dimension affect the content and flow of information.

c. **The Cognitive Dimension.** The cognitive dimension encompasses the minds of those who transmit, receive, and respond to or act on information. It refers to individuals' or groups' information processing, perception, judgment, and decision making. These elements are influenced by many factors, to include individual and cultural beliefs, norms, vulnerabilities, motivations, emotions, experiences, morals, education, mental health, identities, and ideologies. Determining these influencing factors in a given environment is critical for understanding how to best influence the mind of the decision maker and create

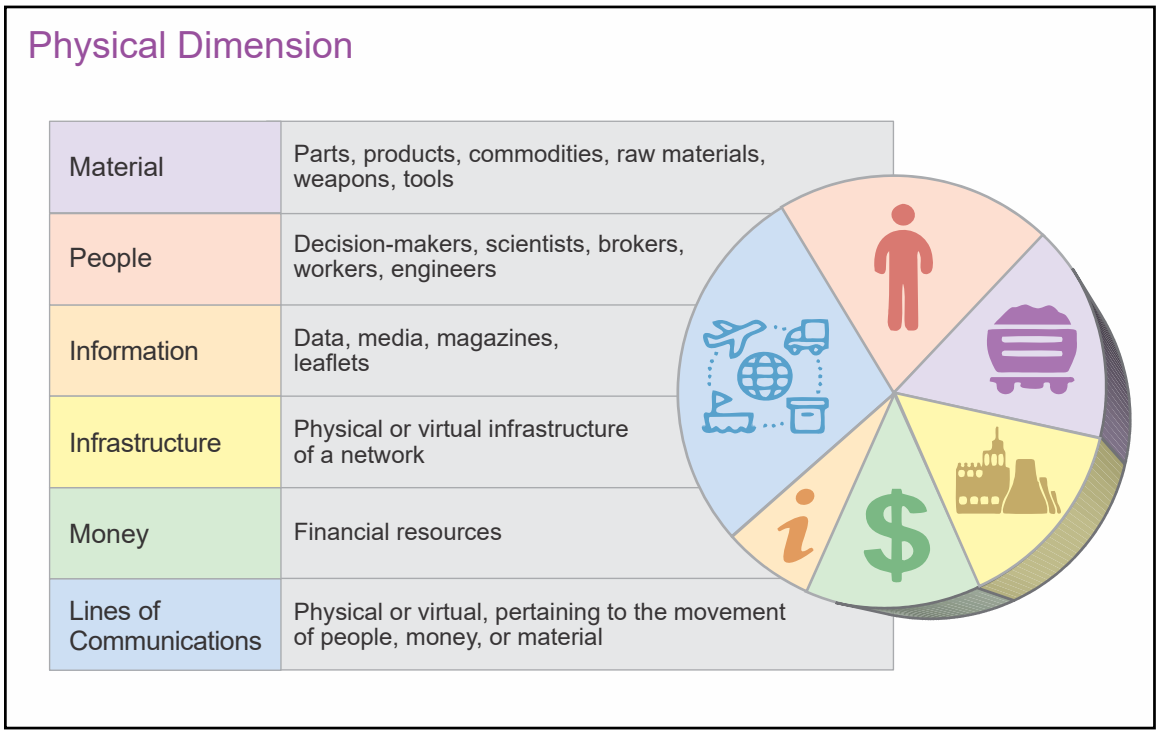


Figure G-1. Physical Dimension

the desired effects. As such, this dimension constitutes the most important component of the information environment.

2. Social Media Exploitation

Social networking sites attempt to inform, promote, influence, or modify social behaviors, sometimes while attempting to connect with and elicit information from users who are encouraged to share information while inherently trusting the information from those they are connected to within the network. Once information is posted or uploaded onto a social networking Website, it should no longer be considered private. Therefore, these sites present an OPSEC risk to military units and can raise the visibility of individual users and put them at greater risk for targeting.

For an example of social media protective measures, see the CJCS Guide 5260, A Self-Help Guide to Antiterrorism.

3. Cyberspace Threat Framework

The cyberspace threat framework was developed by the USG to enable consistent characterization and categorization of cyberspace threat events and to identify trends or changes in threat activities in cyberspace.

a. The cyberspace threat framework is applicable to anyone who works cyberspace-related activities, its principle benefit being that it provides a common language for describing and communicating information about cyberspace threat activity.

b. The framework and its associated lexicon provide a means for consistently describing cyberspace threat activity in a manner that enables efficient information sharing and cyberspace threat analysis that is useful to both senior policy/decision makers and detail-oriented intelligence analysts alike.

c. The framework captures the enemy life cycle from preparation of capabilities and targeting; to initial engagement with the targets or temporary nonintrusive disruptions by the adversary; to establishing and expanding the presence on target networks; to the creation of other effects, including theft, manipulation, or disruption. For more information, see the Office of the Director of National Intelligence, Cyber Threat Intelligence Integration Center Website at https://www.odni.gov/index.php/cyber-threat-framework.

Intentionally Blank

APPENDIX H
POINTS OF CONTACT

Joint Staff/J-7/Joint Doctrine Branch
Website: http://www.jcs.mil/doctrine/
E-mail: js.pentagon.j7.mbx.jedd-support@mail.mil
Phone number: 703-692-7273 (DSN 222)

Joint Staff Doctrine Sponsor
Joint Staff J-3, Operations Directorate
Phone number: 703-695-2994

Lead Agent
USSOCOM J59-D
7701 Tampa Point Blvd.
MacDill, AFB, FL 33621
E-mail: J59-CDI-D@socom.mil
Phone: 813-826-6829

Office of Coordinating Responsibility
USSOCOM J5/USSOCOM J5X
7701 Tampa Point Blvd.
MacDill, AFB, FL 33621

Intentionally Blank

APPENDIX J
REFERENCES

The development of JP 3-26 is based upon the following primary references:

1. General

a. Title 10, USC.

b. Title 14, USC.

c. Title 18, USC.

d. Title 22, USC.

e. *Homeland Security Act of 2002.*

f. *National Strategy for Counterterrorism of the United States.*

g. *2017 National Security Strategy of the United States of America.*

h. *National Strategy for Homeland Security.*

i. *(U) 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge.*

j. *Irregular Warfare Annex to National Defense Strategy.*

k. *(U) National Military Strategy of the United States of America, 2018.*

l. *Global Campaign Plan - Violent Extremist Organizations.*

m. *National Strategy for the Physical Protection of Critical Infrastructure and Key Assets.*

n. *National Strategy for Maritime Security.*

o. *National Strategy to Combat Terrorist Travel of the United States of America.*

p. HSPD-6, *Directive on Integration and Use of Screening Information to Protect Against Terrorism.*

q. NSPD-59/HSPD-24, *Biometrics for Identification of Screening to Enhance National Security.*

r. *Unified Command Plan.*

2. Department of Defense Publications

a. DODD 3000.03E, *DOD Executive Agent for Non-Lethal Weapons (NLW) and NLW Policy.*

b. DODD 3000.07, *Irregular Warfare (IW).*

c. DODD 3000.10, *Contingency Basing Outside the United States.*

d. DODD 3020.40, *Mission Assurance (MA).*

e. DODD 3025.18, *Defense Support of Civil Authorities (DSCA).*

f. DODD 4500.54E, *DOD Foreign Clearance Program (FCP).*

g. DODD 5105.62, *Defense Threat Reduction Agency (DTRA).*

h. DODD 5200.27, *Acquisition of Information Concerning Persons and Organizations Not Affiliated with the Department of Defense.*

i. DODD 5210.56, *Arming and The Use of Force.*

j. DODD 5240.01, *DOD Intelligence Activities.*

k. DODD 5240.06, *Counterintelligence Awareness and Reporting (CIAR).*

l. DODI 2000.12, *DOD Antiterrorism (AT) Program.*

m. DODI O-2000.16, *DOD Antiterrorism (AT) Program Implementation.*

n. DODI O-2000.22, *Designation and Physical Protection of DOD High Risk Personnel (HRP).*

o. DODI 2000.26, *Suspicious Activity Reporting (SAR).*

p. DODI 3000.11, *Management of DOD Irregular Warfare (IW) and Security Force Assistance (SFA) Capabilities.*

q. DODI 3020.41, *Operational Contract Support (OCS).*

r. DODI 3020.45, *Mission Assurance (MA) Construct.*

s. DODI 3020.52, *DOD Installation Chemical, Biological, Radiological, Nuclear, and High-Yield Explosive (CBRNE) Preparedness Standards.*

t. DODI 3025.21, *Defense Support of Civilian Law Enforcement Agencies.*

u. DODI 3115.12, *Open Source Intelligence*.

v. DODI O-3607.02, *Military Information Support Operations (MISO).*

w. DODI 5200.08, *Security of DOD Installations and Resources and the DOD Physical Security Review Board (PSRB).*

x. DODI 5210.84, *Security of DOD Personnel at US Missions Abroad.*

y. DODI 5240.19, *Counterintelligence Support to the Defense Critical Infrastructure Program.*

z. DODI 5240.22, *Counterintelligence Support to Force Protection.*

aa. DODI 5240.26, *Countering Espionage, International Terrorism, and the Counterintelligence (CI) Insider Threat.*

bb. DODI 5525.07, *Implementation of the Memorandum of Understanding (MOU) Between the Departments of Justice (DOJ) and Defense Relating to the Investigation and Prosecution of Certain Crimes.*

cc. DODI 6055.17, *DOD Emergency Management (EM) Program.*

dd. DODM 5105.21, Volume 1, *Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Information and Information Systems Security.*

ee. DODM 5240.01, *Procedures Governing the Conduct of DOD Intelligence Activities.*

ff. DOD 5240.1-R, *Procedures Governing the Activities of DOD Intelligence Components that Affect United States Persons.*

3. Chairman of the Joint Chiefs of Staff Publications

a. CJCSI 3110.05F, *Military Information Support Operations Supplement to the Joint Strategic Capabilities Plan.*

b. CJCSI 3121.01B, *(U) Standing Rules of Engagement/Standing Rules for the Use of Force for US Forces.*

c. CJCS 3150.25G, *Joint Lessons Learned Program.*

d. CJCSI 3210.06A, *Irregular Warfare (IW).*

e. CJCSI 5261.01G, *Combating Terrorism Readiness Initiatives Fund.*

f. CJCSI 7401.01G, *Combatant Commander Initiative Fund (CCIF).*

g. CJCSM 3130.03A, *Planning and Execution Formats and Guidance.*

h. CJCSM 4301.01, *Planning Operational Contract Support.*

i. CJCS Guide 5260, *A Self-Help Guide to Antiterrorism.*

j. JP 1, *Doctrine for the Armed Forces of the United States.*

k. JP 1-0, *Joint Personnel Support.*

l. JP 2-0, *Joint Intelligence.*

m. JP 2-01, *Joint and National Intelligence Support to Military Operations.*

n. JP 2-01.2, *(U) Counterintelligence and Human Intelligence in Joint Operations.*

o. JP 2-03, *Geospatial Intelligence in Joint Operations.*

p. JP 3-0, *Joint Operations.*

q. JP 3-05, *Special Operations.*

r. JP 3-08, *Interorganizational Cooperation.*

s. JP 3-10, *Joint Security Operations in Theater.*

t. JP 3-11, *Operations in Chemical, Biological, Radiological, and Nuclear Environments.*

u. JP 3-13, *Information Operations.*

v. JP 3-15.1, *Counter-Improvised Explosive Device Activities.*

w. JP 3-16, *Multinational Operations.*

x. JP 3-24, *Counterinsurgency.*

y. JP 3-25, *Countering Threat Networks.*

z. JP 3-27, *Homeland Defense.*

aa. JP 3-28, *Defense Support of Civil Authorities.*

bb. JP 3-40, *Countering Weapons of Mass Destruction.*

cc. JP 3-41, *Chemical, Biological, Radiological, and Nuclear Response.*

dd. JP 3-85, *Joint Electromagnetic Spectrum Operations.*

ee. JP 4-10, *Operational Contract Support.*

4. Service and Other Military Publications

a. Army Techniques Publication 3-37.2, *Antiterrorism.*

b. *Operational Law Handbook, The Judge Advocate General's Legal Center and School.*

5. Other Resources

a. Laura Clark and William E. Algaier, *Surveillance Detection: The Art of Prevention,(St. Louis: Cradle Press, 2007).*

b. Colonel Shannon D. Jurrens, USAF, *"Slashing the Enemy's Achilles Heel: Using*

Surveillance Detection to Prevent Terrorist Attacks," The Guardian, Winter 2010, Volume 12, Issue 3.

c. Donald J. Hanle, *Terrorism: The Newest Face of Warfare (Washington: Pergamon-Brassey's International Defense Publishers, Inc., 1989).*

Intentionally Blank

APPENDIX K
ADMINISTRATIVE INSTRUCTIONS

1. User Comments

Users in the field are highly encouraged to submit comments on this publication using the Joint Doctrine Feedback Form located at: https://jdeis.js.mil/jdeis/jel/jp_feedback_form.pdf and e-mail it to: js.pentagon.j7.mbx.jedd-support@mail.mil. These comments should address content (accuracy, usefulness, consistency, and organization), writing, and appearance.

2. Authorship

a. The lead agent for this publication is US Special Operations Command J59. The Joint Staff doctrine sponsor for this publication is Joint Staff, J-3.

b. The following staff, in conjunction with the joint doctrine development community, made a valuable contribution to the revision of this joint publication: lead agent, Mr. John Campbell, US Special Operations Command; Joint Staff doctrine sponsor, Mr. Donald Cantwell, Joint Staff J-3; and Lt Col Travis Ruhl, Joint Staff J-7, Joint Doctrine Branch.

3. Supersession and Cancellation

This publication supersedes JP 3-26, *Counterterrorism,* 24 October 2014, and cancels JP 3-07.2, *Antiterrorism,* 14 March 2014. Relevant material has been incorporated into the main body and appendices of this publication. Accordingly, JP 3-07.2, *Antiterrorism,* will be removed from the joint doctrine hierarchy.

4. Change Recommendations

a. To provide recommendations for urgent and/or routine changes to this publication, please complete the Joint Doctrine Feedback Form located at: https://jdeis.js.mil/jdeis/jel/jp_feedback_form.pdf and e-mail it to: js.pentagon.j7.mbx.jedd-support@mail.mil.

b. When a Joint Staff directorate submits a proposal to the CJCS 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. Lessons Learned

The Joint Lessons Learned Program (JLLP) primary objective is to enhance joint force readiness and effectiveness by contributing to improvements in doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy. The Joint Lessons Learned Information System (JLLIS) is the DOD system of record for lessons learned and facilitates the collection, tracking, management, sharing, collaborative resolution, and dissemination of lessons learned to improve the development and readiness

of the joint force. The JLLP integrates with joint doctrine through the joint doctrine development process by providing lessons and lessons learned derived from operations, events, and exercises. As these inputs are incorporated into joint doctrine, they become institutionalized for future use, a major goal of the JLLP. Lessons and lessons learned are routinely sought and incorporated into draft JPs throughout formal staffing of the development process. The JLLIS Web site can be found at https://www.jllis.mil (NIPRNET) or http://www.jllis.smil.mil (SIPRNET).

6. 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 IAW DOD Manual 5200.01, Volume 1, *DOD Information Security Program: Overview, Classification, and Declassification,* and DOD Manual 5200.01, Volume 3, *DOD Information Security Program: Protection of Classified Information.*

7. Distribution of Electronic Publications

a. Joint Staff J-7 will not print copies of JPs for distribution. Electronic versions are available on JDEIS Joint Electronic Library Plus (JEL+) at https://jdeis.js.mil/jdeis/index.jsp (NIPRNET) and https://jdeis.js.smil.mil/jdeis/generic.jsp (SIPRNET), and on the JEL at http://www.jcs.mil/doctrine (NIPRNET).

b. Only approved JPs are releasable outside the combatant commands, Services, and Joint Staff. Defense attachés may request classified JPs by sending written requests to Defense Intelligence Agency (DIA)/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 semiannually and when received can be locally reproduced for use within the combatant commands, Services, and combat support agencies.

GLOSSARY

PART I— ABBREVIATIONS, ACRONYMS, AND INITIALISMS

AOR	area of responsibility
ASD(HD&GS)	Assistant Secretary of Defense for Homeland Defense and Global Security
AT	antiterrorism
ATO	antiterrorism officer
C2	command and control
CAAF	contractors authorized to accompany the force
CAO	civil affairs operations
CBRN	chemical, biological, radiological, and nuclear
CbT	combating terrorism
CCDR	combatant commander
CCIF	Combatant Commander Initiative Fund
CCIR	commander's critical information requirement
CCMD	combatant command
CCP	combatant command campaign plan
CDRUSSOCOM	Commander, United States Special Operations Command
CF	conventional forces
CI	counterintelligence
CIA	Central Intelligence Agency
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman of the Joint Chiefs of Staff instruction
CJCSM	Chairman of the Joint Chiefs of Staff manual
CNGB	Chief, National Guard Bureau
COCOM	combatant command (command authority)
COG	center of gravity
COM	chief of mission
COOP	continuity of operations
CT	counterterrorism
CTF	counter threat finance
CTITF	Counter-Terrorism Implementation Task Force (UN)
CWMD	countering weapons of mass destruction
DCI	defense critical infrastructure
DCTC	Defense Combating Terrorism Center (DIA)
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DOD	Department of Defense
DODD	Department of Defense directive
DODI	Department of Defense instruction
DODM	Department of Defense manual
DOJ	Department of Justice
DOS	Department of State

DSCA	defense support of civil authorities
DVD	digital video disc
EO	executive order
F3EAD	find, fix, finish, exploit, analyze, and disseminate
FBI	Federal Bureau of Investigation (DOJ)
FID	foreign internal defense
FP	force protection
FPCON	force protection condition
FPD	force protection detachment
HD	homeland defense
HN	host nation
HQ	headquarters
HRB	high-risk billet
HRP	high-risk personnel
HS	homeland security
HSC	Homeland Security Council
HSPD	homeland security Presidential directive
HVE	homegrown violent extremist
I2	identity intelligence
IC	intelligence community
IED	improvised explosive device
IEM	installation emergency management
IR	information requirement
IRA	Provisional Irish Republican Army
ISR	intelligence, surveillance, and reconnaissance
IT	information technology
J-2E	joint force exploitation staff element
JFC	joint force commander
JIPOE	joint intelligence preparation of the operational environment
JMAA	joint mission assurance assessment
JP	joint publication
JSA	joint security area
JTF	joint task force
LE	law enforcement
LOC	line of communications
LOE	line of effort
LOO	line of operation
MA	mission assurance

MAA	mission assurance assessment
MHS	maritime homeland security
MOA	memorandum of agreement
MOE	measure of effectiveness
MOP	measure of performance
MOU	memorandum of understanding
NCTC	National Counterterrorism Center (DNI)
NGO	nongovernmental organization
NJTTF	National Joint Terrorism Task Force (FBI)
NSC	National Security Council
NSPD	national security Presidential directive
OE	operational environment
OPCON	operational control
OPLAN	operation plan
OPSEC	operations security
PAO	public affairs officer
PCA	Posse Comitatus Act
PE	preparation of the environment
PIR	priority intelligence requirement
PN	partner nation
PPBE	Planning, Programming, Budgeting, and Execution
RA	risk assessment
ROE	rules of engagement
RUF	rules for the use of force
SAR	suspicious activity report
SC	security cooperation
SecDef	Secretary of Defense
SECSTATE	Secretary of State
SIR	specific information requirement
SOC-FWD	special operations command-forward
SOF	special operations forces
SOFA	status-of-forces agreement
TA	threat assessment
TACON	tactical control
TSOC	theater special operations command
TTP	tactics, techniques, and procedures
UAS	unmanned aircraft system
UFC	Unified Facilities Criteria
USA	United States Army

USAF	United States Air Force
USASOC	United States Army Special Operations Command
USC	United States Code
USCG	United States Coast Guard
USG	United States Government
USSOCOM	United States Special Operations Command
VA	vulnerability assessment
VBIED	vehicle-borne improvised explosive device
VEO	violent extremist organization
WMD	weapons of mass destruction

PART II—TERMS AND DEFINITIONS

antiterrorism. Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include rapid containment by local military and civilian forces. Also called **AT.** (Approved for incorporation into the DOD Dictionary with JP 3-26 as the source JP.)

combating terrorism. Actions, including antiterrorism and counterterrorism, taken to oppose terrorism throughout the competition continuum. Also called **CbT.** (Approved for incorporation into the DOD Dictionary.)

countersurveillance. All measures, active or passive, taken to counteract hostile surveillance. (Approved for incorporation into the DOD Dictionary with JP 3-26 as the source JP.)

counterterrorism. Activities and operations taken to neutralize terrorists and their organizations and networks to render them incapable of using violence to instill fear and coerce governments or societies to achieve their goals. Also called **CT.** (Approved for incorporation into the DOD Dictionary.)

critical asset. A specific entity that is of such extraordinary importance that its incapacitation or destruction would have a very serious, debilitating effect on the ability of a nation to continue to function effectively. (Approved for incorporation into the DOD Dictionary with JP 3-26 as the source JP.)

criticality assessment. An assessment that identifies key assets and infrastructure that support Department of Defense missions, units, or activities and are deemed mission-critical by military commanders or civilian agency managers. (Approved for incorporation into the DOD Dictionary.)

force protection condition. A Chairman of the Joint Chiefs of Staff-approved standard for identification of and recommended responses to terrorist threats against United States personnel and facilities. Also called **FPCON.** (Approved for incorporation into the DOD Dictionary with JP 3-26 as the source JP.)

high-risk personnel. Personnel who, by their grade, assignment, symbolic value, or relative isolation, are likely to be attractive or accessible terrorist targets. Also called **HRP.** (Approved for incorporation into the DOD Dictionary with JP 3-26 as the source JP.)

mission assurance. A process to protect or ensure the continued function and resilience of capabilities and assets, including personnel, equipment, facilities, networks, information and information systems, infrastructure, and supply chains, critical to the execution of Department of Defense mission-essential functions. Also called **MA.** (Approved for inclusion in the DOD Dictionary.)

risk assessment. The identification and assessment of hazards (first two steps of risk management process). (Approved for incorporation into the DOD Dictionary.)

terrorism. The unlawful use of violence or threat of violence, often motivated by religious, political, or other ideological beliefs, to instill fear and coerce individuals, governments or societies in pursuit of terrorist goals. (Approved for incorporation into the DOD Dictionary.)

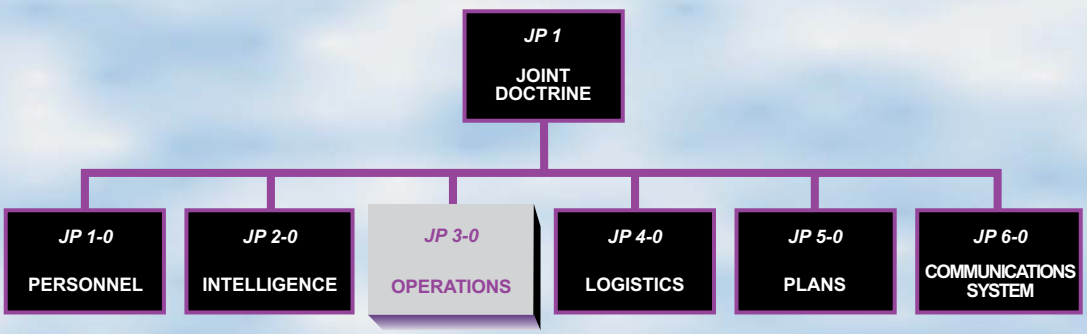
terrorism threat level. A Department of Defense intelligence threat assessment of the level of terrorist threat faced by United States personnel and interests in a foreign nation; the levels are expressed as **LOW, MODERATE, SIGNIFICANT,** and **HIGH.** (Approved for replacement of "terrorist threat level" and its definition in the DOD Dictionary.)

threat analysis. In antiterrorism, a continual process of compiling and examining all available information concerning activities by terrorist groups which could target a facility. (Approved for incorporation into the DOD Dictionary.)

threat assessment. In antiterrorism, examining the capabilities, intentions, and activities, past and present, of terrorist organizations, as well as the security environment within which friendly forces operate to determine the level of threat. (Approved for incorporation into the DOD Dictionary.)

vulnerability assessment. A Department of Defense, command, or unit-level evaluation to determine the vulnerability of an installation, unit, exercise, port, ship, residence, facility, or other site to a physical or cyberspace threat. (Approved for incorporation into the DOD Dictionary.)

JOINT DOCTRINE PUBLICATIONS HIERARCHY



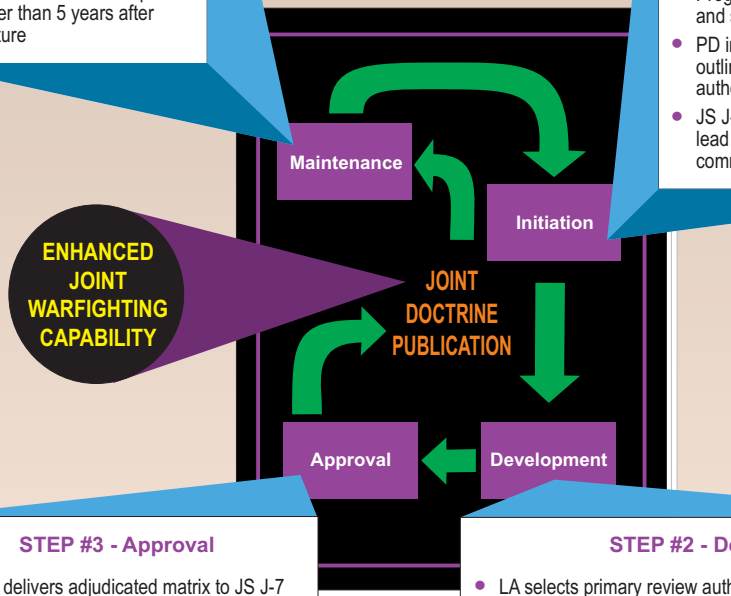
All joint publications are organized into a comprehensive hierarchy as shown in the chart above. **Joint Publication (JP) 3-26** is in the **Operations** series of joint doctrine publications. The diagram below illustrates an overview of the development process:

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