Joint Publication 3-25

Countering Threat Networks

21 December 2016

PREFACE

1. Scope

This publication provides joint doctrine for joint force commanders and their staffs to plan, execute, and assess operations to identify, neutralize, disrupt, or destroy threat networks.

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 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, and combat support agencies.

b. The guidance in this publication is authoritative; as such, this doctrine will be followed except when, in the judgment of the commander, exceptional circumstances dictate otherwise. If conflicts arise between the contents of this publication and the contents of Service publications, this publication will take precedence unless the 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 US, 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:

KEVIN D. SCOTT
Vice Admiral, USN
Director, Joint Force Development

Intentionally Blank

TABLE OF CONTENTS

Intentionally Blank

EXECUTIVE SUMMARY
COMMANDER'S OVERVIEW

- **Discusses the Importance of Unity of Effort in Levels of Warfare**
- **Reviews the Basic Construct of Networks, Nodes, Links, and Cells**
- **Looks at How Networks Function in the Operational Environment**
- **Addresses How to Analyze and Evaluate Networks**
- **Discusses How to Include Countering Threat Networks in Each Step of the Planning Process**
- **Reviews How to Target the Activities and Lines of Operation of Threat Networks Activities by Phase**
- **Discusses Countering Threat Finance and Maritime Threat Networks**
- **Discusses Clandestine Networks and Social Network Analysis**

Overview

Introduction

The worldwide emergence of adaptive threat networks introduces a wide array of challenges to joint forces in all phases of operations. Threat networks vary widely in motivation, structure, activities, operational areas, and composition. Threat networks may be adversarial to a joint force or may simply be criminally motivated, increasing instability in a given operational area. Countering threat networks (CTN) consists of activities to pressure threat networks or mitigate their adverse effects. Understanding a threat network's motivation and objectives is required to effectively counter its efforts.

Policy and Strategy

CTN planning and operations require extensive coordination as well as innovative, cross-cutting approaches that utilize all instruments of national power. The national military strategy describes the need of the joint force to operate in this complex environment.

Challenges of the Strategic Security Environment

Advances in technology and information have facilitated individual non-state actors and networks to move money, people, and resources, and spread violent ideology around the world.

CTN represents a significant planning and operational challenge because threat networks use asymmetric methods and weapons and often enjoy state cooperation, sponsorship, sympathy, sanctuary, or supply. The US military is one of the instruments of US national power that may be employed in concert with interagency, international, and regional security partners to counter threat networks. Compounding the challenge to planners is the threat of the use of weapons of mass destruction (WMD), which adds a significant dimension to violent extremist organizations' and other threat networks' capabilities not only to inflict harm on the US and its allies, but also to employ such weapons to catastrophically impede commerce and intimidate local populations.

The Strategic Approach

The groundwork for successful countering threat networks activities starts with information and intelligence to develop an understanding of the operational environment and the threat network.

Military engagement, security cooperation, and deterrence are just some of the activities that may be necessary to successfully counter threat networks without deployment of a joint task force. The military instrument of national power will support other United States Government departments and agencies and cooperate with international organizations and other partners and allies to protect and enhance national security interests, deter conflict, and set conditions for future contingency operations.

Joint Force and Interagency Coordination

Achieving synergy among diplomatic, political, security, economic, and information activities demands unity of effort between all participants. Once US assistance is committed, an operational approach must be devised, ideally in collaboration with the affected government and other partners, since their early inclusion can help mitigate the effects of operational-level differences in goals, capabilities, and culture.

Threat Network Fundamentals

Threat Network Construct

A **network** is a group of elements consisting of interconnected nodes and links representing relationships or associations. A **cell** is a subordinate organization formed around a specific process, capability, or activity within a designated larger

A threat network consists of interconnected nodes and links and may be organized using subordinate and associated networks and cells.

organization. A node is an element of a network that represents a person, place, or physical object. **Nodes** represent tangible elements within a network or operational environment (OE) that can be targeted for action. A link is a behavioral, physical, or functional relationship between nodes. **Links** establish the interconnectivity between nodes that allows 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 centers of gravity (COGs), networks, and cells the joint force commander (JFC) may wish to influence or change during an operation.

Network Analysis

Network analysis is a means of gaining understanding of a group, place, physical object, or system. It identifies relevant nodes, determines and analyzes links between nodes, and identifies key nodes. The political, military, economic, social, information, and infrastructure systems perspective is a useful starting point for analysis of threat networks. Networks are typically formed at the confluence of three conditions: the presence of a catalyst, a receptive audience, and an accommodating environment. As conditions within the OE change, the network must adapt in order to maintain a minimal capacity to function within these conditions.

Determining and Analyzing Node-Link Relationships

Social network analysis provides a method that helps the JFC and staff understand the relevance of nodes and links. The strength or intensity of a single link can be relevant to determining the importance of the functional relationship between nodes and the overall significance to the larger system. The number and strength of nodal links within a set of nodes can be indicators of key nodes and a potential COG.

Threat Networks and Cells

A network must perform a number of functions in order to survive and grow. These functions can be seen as cells that have their own internal organizational structure and communications. These cells work in concert to achieve the overall organization's goals. Examples of cells include: operational, logistical, training, communications, financial, and WMD proliferation cells.

Networks in the Operational Environment

Networked Threats and Their Impact on the Operational Environment

Networked threats are highly adaptable adversaries with the ability to select a variety of tactics, techniques, and technologies and blend them in unconventional ways to meet their strategic aims. Additionally, many threat networks supplant or even replace legitimate government functions such as health and social services, physical protection, or financial support in ungoverned or minimally governed areas. Once the JFC identifies the networks in the OE and understands their interrelationships, functions, motivations, and vulnerabilities, the commander tailors the force to apply the most effective tools against the threat.

Threat Network Characteristics

Threat networks manifest themselves and interact with neutral networks for protection, to perpetuate their goals, and to expand their influence. Networks take many forms and serve different purposes, but are all comprised of people, processes, places, material, or combinations.

Adaptive Networked Threats

For a threat network to survive political, economic, social, and military pressures, it must adapt to those pressures. Networks possess many characteristics important to their success and survival, such as flexible command and control structure; a shared identity; and the knowledge, skills, and abilities of group leaders and members to adapt.

Network Engagement

Network engagement is the interactions with friendly, neutral, and threat networks, conducted continuously and simultaneously at the tactical, operational, and strategic levels, to help achieve the commander's objectives within an OE. To effectively counter threat networks, the joint force must seek to support and link with friendly networks and engage neutral networks through the building of mutual trust and cooperation through network engagement. Network engagement consists of three components: partnering with friendly networks, engaging neutral networks, and CTN to support the commander's desired end state.

Networks, Links, and Identity Groups

All individuals are members of multiple, overlapping identity groups. These identity groups form links of affinity and shared understanding, which may be leveraged to form networks with shared purpose.

Types of Networks in an Operational Environment

There are three general types of networks found within an operational area: friendly, neutral, and hostile/threat networks. To successfully accomplish mission goals the JFC should equally consider the impact of actions on multinational and friendly forces, local population, criminal enterprises, as well as the adversary.

Identify a Threat Network

Threat networks often attempt to remain hidden. By understanding the basic, often masked sustainment functions of a given threat network, commanders may also identify individual networks within. A thorough joint intelligence preparation of the operational environment (JIPOE) product, coupled with "on-the-ground" assessment, observation, and all-source intelligence collection, will ultimately lead to an understanding of the OE and will allow the commander to visualize the network.

Planning to Counter Threat Networks

Joint Intelligence Preparation of the Operational Environment and Threat Networks

JIPOE is the first step in identifying the essential elements that constitute the OE and is used to plan and conduct operations against threat networks. The focus of the JIPOE analysis for threat networks is to help characterize aspects of the networks.

Understanding the Threat's Network

To neutralize or defeat a threat network, friendly forces must do more than understand how the threat network operates, its organization goals, and its place in the social order; they must also understand how the threat is shaping its environment to maintain popular support, recruit, and raise funds. Building a network function template is a method to organize known information about the network associated with structure and functions of the network. By developing a network function template, the information can be initially understood and then

used to facilitate critical factors analysis (CFA). CFA is an analytical framework to assist planners in analyzing and identifying a COG and to aid operational planning.

Targeting Evaluation Criteria

A useful tool in determining a target's suitability for attack is the criticality, accessibility, recuperability, vulnerability, effect, and recognizability (CARVER) analysis. The CARVER method as it applies to networks provides a graph-based numeric model for determining the importance of engaging an identified target, using qualitative analysis, based on seven factors: network affiliations, criticality, accessibility, recuperability, vulnerability, effect, and recognizability.

Countering Threat Networks Through the Planning of Phases

JFCs may plan and conduct CTN activities throughout all phases of a given operation. Upon gaining an understanding of the various threat networks in the OE through the joint planning process (JPP), JFCs and their staffs develop a series of prudent (feasible, suitable, and acceptable) CTN actions to be executed in conjunction with other phased activities.

Activities to Counter Threat Networks

Targeting Threat Networks

JIPOE is one of the critical inputs to support the development of these products, but must include a substantial amount of analysis on the threat network to adequately identify the critical nodes, critical capabilities (network's functions), and critical requirements for the network. Joint force targeting efforts should employ a comprehensive approach, leveraging military force and civil agency capabilities that keep continuous pressure on multiple nodes and links of the network's structure.

Desired Effects on Networks

When commanders decide to generate an effect on a network through engaging specific nodes, the intent may not be to cause damage, but to shape conditions of a mental or moral nature. The selection of effects desired on a network is conducted as part of target selection, which includes the consideration of capabilities to

employ that was identified during capability analysis of the joint targeting cycle.

Targeting

CTN targets can be characterized as targets that must be engaged immediately because of the significant threat they represent or the immediate impact they will make related to the JFC's intent, key nodes such as high-value individuals, or longer-term network infrastructure targets (caches, supply routes, safe houses) that are normally left in place for a period of time to exploit them. Resources to service/exploit these targets are allocated in accordance with the JFC's priorities, which are constantly reviewed and updated through the command's joint targeting process.

Lines of Effort by Phase

During each phase of an operation or campaign against a threat network, there are specific actions that the JFC can take to facilitate countering threats network. However, these actions are not unique to any particular phase, and must be adapted to the specific requirements of the mission and the OE.

Theater Concerns in Countering Threat Networks

Many threat networks are transnational, recruiting, financing, and operating on a global basis. Theater commanders need to be aware of the relationships among these networks and identify the basis for their particular connection to a geographic combatant commander's area of responsibility.

Operational Approaches to Countering Threat Networks

There are many ways to integrate CTN into the overall plan. In some operations, the threat network will be the primary focus of the operation. In others, a balanced approach through multiple line of operations and lines of effort may be necessary, ensuring that civilian concerns are met while protecting them from the threat networks' operators.

Assessments

Assessment of Operations to Counter Threat Networks

CTN assessments at the strategic, operational, and tactical levels and across the instruments of national power are vital since many networks have regional and international linkages as well as capabilities. Objectives must be developed during

the planning process so that progress toward objectives can be assessed. CTN assessments require staffs to conduct analysis more intuitively and consider both anecdotal and circumstantial evidence. Since networked threats operate among civilian populations, there is a greater need for human intelligence.

Operation Assessment

CTN activities may require assessing multiple measures of effectiveness (MOEs) and measures of performance (MOPs), depending on threat network activity. The assessment process provides a feedback mechanism to the JFC to provide guidance and direction for future operations and targeting efforts against threat networks.

Assessment Framework for Countering Threat Networks

The assessment framework broadly outlines three primary activities: organize, analyze, and communicate. In conducting each of these activities, assessors must be linked to JPP, understand the operation plan, and inform the intelligence process as to what information is required to support indicators, MOEs, and MOPs. In assessing CTN operations, quantitative data and analysis will inform assessors.

CONCLUSION

This publication provides joint doctrine for JFCs and their staffs to plan, execute, and assess operations to identify, neutralize, disrupt, or destroy threat networks.

CHAPTER I
OVERVIEW

"The emergence of amorphous, adaptable, and networked threats has far-reaching implications for the US national security community. These threats affect DOD [Department of Defense] priorities and war fighting strategies, driving greater integration with other departments and agencies performing national security missions, and create the need for new organizational concepts and decision-making paradigms. The impacts are likely to influence defense planning for years to come."

Department of Defense Counternarcotics and Global Threats Strategy, April 2011

1. Introduction

a. The worldwide emergence of adaptive threat networks introduces a wide array of challenges to joint forces in all phases of operations. Threat networks are those whose size, scope, or capabilities threaten US interests. These networks may include the underlying informational, economic, logistical, and political components to enable these networks to function. These threats create a high level of uncertainty and ambiguity in terms of intent, organization, linkages, size, scope, and capabilities. These threat networks jeopardize the stability and sovereignty of nation-states, including the US. They tend to operate among civilian populations and in the seams of society and may have components that are recognized locally as legitimate parts of society. Collecting information and intelligence on these networks, their nodes, links, and affiliations is challenging, and analysis of their strengths, weaknesses, and centers of gravity (COGs) differs greatly from traditional nation-state adversaries. Threat networks may traffic in licit or illicit goods and services or a combination of both using legal and illegal financial, transportation, and distribution networks.

For more information, see Appendix B, "The Convergence of Illicit Networks," and Appendix D, "Identity Activities Support to Countering Threat Network Operations."

b. Threat networks are part of the operational environment (OE). These networks utilize existing networks and may create new networks that seek to move money, people, information, and goods for the benefit of the network. Not all of these interactions create instability and not all networks are a threat to the joint force and its mission. While some societies may accept a certain degree of corruption and criminal behavior as normal, it is never acceptable for these elements to develop networks that begin to pose a threat to national and regional stability. When a network begins to pose a threat, action should be considered to counter the threat. The intelligence community maintains watch on those identified factors in the OE, while the Department of State (DOS), Department of Defense (DOD), and interagency partners consider their relative equities to determine if action is warranted. When they detect a change that can have potential adverse consequences to the US's interests, they begin planning tailored responses as part of the broader instruments of national power to prevent a threat network from fully developing. This doctrine will focus on those networks that do present a threat with an understanding that friendly, neutral, and

threat networks overlap and share nodes and links. Threat networks vary widely in motivation, structure, activities, operational areas, and composition. Threat networks may be adversarial to a joint force or may simply be criminally motivated, increasing instability in a given operational area. Some politically or ideologically based networks may avoid open confrontation with US forces; nevertheless, these networks may threaten mission success. Their activities may include spreading ideology, moving money, moving supplies (including weapons and fighters), human trafficking, drug smuggling, information relay, or acts of terrorism toward the population or local governments. Threat networks may be local, regional, or international and a threat to deployed joint forces and the US homeland.

c. Understanding a threat network's motivation and objectives is required to effectively counter its efforts. The issues that drive a network and its ideology should be clearly understood. For example, they may be driven by grievances, utopian ideals, power, revenge over perceived past wrongs, greed, or a combination of these. Understanding the needs and goals of these groups can increase the effectiveness of countering threat networks (CTN) activities by improving focus on the issues and identifying the resources best suited to reduce and/or neutralize the threats they pose. The Haqqani network, as an example, was born out of the need to defend its members' homeland and beliefs, and to date, it continues its struggle against its perceived adversaries.

d. CTN is one of three pillars of network engagement that includes partnering with friendly networks and engaging with neutral networks in order to attain the commander's desired military end state within a complex OE. It consists of activities to pressure threat networks or mitigate their adverse effects. These activities normally occur continuously and simultaneously at multiple levels (tactical, operational, and strategic) and may employ lethal and/or nonlethal capabilities in a direct or indirect manner. The most effective operations pressure and influence elements of these networks at multiple fronts and target multiple nodes and links. As part of the continuing analysis of the OE, planners learn that many networks and elements of those networks are shared by friendly, neutral, threat, and unknown groups. While the commander engages one portion of a network to achieve an objective related to a friendly group or to create an effect on that friendly group to achieve an objective, the commander may be simultaneously engaging another portion of the network to affect a threat group. The networks found in the OE may be simple or complex and must be identified and thoroughly analyzed. Neither all threats nor all elements of their supporting networks can be defeated, particularly if they have a regional or global presence. Certain elements of the network can be deterred, other parts neutralized, and some portions defeated. Engaging these threats through their supporting networks is not an adjunct or ad hoc set of operations and may be the primary mission of the joint force. It is not a stand-alone operation planned and conducted separately from other military operations. CTN should be fully integrated into the joint operational design, joint intelligence preparation of the operational environment (JIPOE), joint planning process (JPP), operational execution, joint targeting process, and joint assessments.

e. Threat networks are often the most complex adversaries that exist within the OEs and frequently employ asymmetric methods to achieve their objectives. Disrupting their global reach and ability to influence events far outside of a specific operational area requires unity of effort across combatant commands (CCMDs) and all instruments of national power. The

assistance of friendly nations and international organizations is vital to address threat network financing, recruiting, propaganda, and operational cells that cross multiple regions and exist in areas where US influence and presence is limited. Joint staffs must realize that effectively targeting threat networks must be done in a comprehensive manner. This is accomplished by leveraging the full spectrum of capabilities available within the joint force commander's (JFC's) organization, from intergovernmental agencies, and/or from partner nations (PNs).

2. Policy and Strategy

a. DOD strategic guidance recognizes the increasing interconnectedness of the international order and the corresponding complexity of the strategic security environment. Threat networks and their linkages transcend geographic and functional CCMD boundaries. CTN planning and operations require extensive coordination as well as innovative, cross-cutting approaches that utilize all instruments of national power. The national military strategy (NMS) describes the need of the joint force to operate in this complex environment.

b. The NMS and *Guidance for Employment of the Force* direct combatant commanders (CCDRs) to work with each other across regional and functional seams. CCDRs must be able to employ a joint force to work with interagency and interorganizational security partners in the operational area to shape, deter, and disrupt threat networks. They may employ a joint force with PNs to neutralize and defeat threat networks.

c. CCDRs develop their strategies by analyzing all aspects of the OE and developing options to set conditions to attain strategic end states. They translate these options into an integrated set of CCMD campaign activities described in CCMD campaign and associated subordinate and supporting plans. CCDRs must understand the OE, recognize nation-state use of proxies and surrogates, and be vigilant to the dangers posed by super-empowered threat networks. Super-empowered threat networks are networks that develop or obtain nation-state capabilities in terms of weapons, influence, funding, or lethal aid. The JFC and staff should plan to deter, neutralize, or defeat threat networks, as well as maintain capability to counter violent extremism and pay particular attention to the intersection between state and non-state actors in an array of threats. Those threats include proliferation of weapons of mass destruction (WMD) expertise, material, and technology. The proliferation of WMD is particularly important due to the existential threat WMD may pose to the US and its allies. In combination with US diplomatic, economic, and informational efforts, the joint force must leverage partners and regional allies to foster cooperation in addressing transnational challenges.

3. Challenges of the Strategic Security Environment

a. The strategic security environment is characterized by uncertainty, complexity, rapid change, and persistent conflict. Advances in technology and information have facilitated individual non-state actors and networks to move money, people, and resources, and spread violent ideology around the world. Non-state actors are able to conduct activities globally and nation-states leverage proxies to launch and maintain sustained campaigns in remote areas of the world. The problem is complicated by the participation of both witting and

unwitting facilitators who may provide products or services to both state and non-state actors. The security environment is fluid with local, national, regional, and transnational threats constantly changing, adapting, and intersecting. Alliances, partnerships, cooperative arrangements, and inter-network conflict may morph and shift week-to-week or even day-to-day. Threat networks or select components often operate clandestinely. The organizational construct, geographical location, linkages, and presence among neutral or friendly populations are difficult to detect during JIPOE, and once a rudimentary baseline is established, ongoing changes are difficult to track. This makes traditional intelligence collection and analysis, as well as operations and assessments, much more challenging than against traditional military threats.

b. Deterring threat networks is a complex and difficult challenge that is significantly different from classical notions of deterrence. Deterrence is most classically thought of as the threat to impose such high costs on an adversary that restraint is the only rational conclusion. When dealing with violent extremist organizations and other threat networks, deterrence is likely to be ineffective due to radical ideology, diffuse organization, and lack of ownership of territory. However, cost imposition may be useful against state sponsors or state-based threat networks. Therefore, due to the complexity of deterring violent extremist organizations, flexible approaches must be developed according to a network's ideology, organization, sponsorship, goals, and other key factors to clearly communicate that the targeted action will not achieve the network's objectives.

For more information on deterrence, see Joint Publication (JP) 3-0, Joint Operations, *and JP 5-0,* Joint Planning.

c. CTN represents a significant planning and operational challenge because threat networks use asymmetric methods and weapons and often enjoy state cooperation, sponsorship, sympathy, sanctuary, or supply. These networked threats transcend operational areas, areas of influence, areas of interest, and the information environment (to include cyberspace [network links and nodes essential to a particular friendly or adversary capability]). The US military is one of the instruments of US national power that may be employed in concert with interagency, international, and regional security partners to counter threat networks. Compounding the challenge to planners is the threat of the use of WMD, which adds a significant dimension to violent extremist organizations' and other threat networks' capabilities not only to inflict harm on the US and its allies, but also to employ such weapons to catastrophically impede commerce and intimidate local populations. Additionally, WMD possession by violent extremist organizations poses a particularly complex problem in preventing use of WMD, considering that cost imposition deterrence constructs may not apply.

For more information, see Appendix B, "The Convergence of Illicit Networks."

d. Threat networks have the ability to remotely plan, finance, and coordinate attacks through global communications (to include social media), transportation, and financial networks. These interlinked areas allow for the high-speed, high-volume exchange of ideas, people, goods, money, and weapons. The same means are also used by legitimate governments and businesses for legitimate transactions. For example, using the global

"Terrorists and insurgents increasingly are turning to TOC [transnational organized crime] to generate funding and acquire logistical support to carry out their violent acts. While the crime-terror[ist] nexus is still mostly opportunistic, this nexus is critical nonetheless, especially if it were to involve the successful criminal transfer of WMD [weapons of mass destruction] material to terrorists or their penetration of human smuggling networks as a means for terrorists to enter the United States."

Strategy to Combat Transnational Organized Crime, July 2011

communications network, threat networks have demonstrated their ability to recruit like-minded individuals from outside of their operational area and have been successful in recruiting even inside the US and PNs. Many threat networks have mastered social media and tapped into the proliferation of traditional and nontraditional news media outlets to create powerful narratives, which generate support and sympathy in other countries. Cyberspace is equally as important to the threat network as physical terrain. Future operations will require the ability to monitor and engage threat networks within cyberspace, since this provides them an opportunity to coordinate sophisticated operations that advance their interests.

4. Threat Networks and Levels of Warfare

a. The purpose of CTN activities is to shape the security environment, deter aggression, provide freedom of maneuver within the operational area and its approaches, and, when necessary, defeat threat networks. CTN activities can happen at any level of conflict and may include or be part of military engagement, security cooperation (includes security force assistance [SFA] and foreign internal defense [FID]), deterrence, antiterrorism, counterterrorism (CT), counterdrug (CD), enforcement of sanctions, no-fly zones, show of force, and counterinsurgency (COIN). Supporting activities may include training, use of military equipment, subject matter expertise, cyberspace operations, information operations (IO) (use of information-related capabilities [IRCs]), military information support operations (MISO), counter threat finance (CTF), interdiction operations, raids, or civil-military operations. In nearly all cases, diplomatic efforts, sanctions, financial pressure, criminal investigations, and intelligence community activities will complement military operations. The complexity of the OE may be increased due to the number of threat networks that may exist. The joint force staff should rely heavily on interorganizational cooperation to create more durable effects in the OE. The instruments of US national power and international power often operate under titles and authorities that are not available to the JFC and in fact may already be operating against threat networks prior to joint force deployment. (For more information on incorporating interorganizational elements into plans and operations, see JP 3-08, *Interorganizational Cooperation.*)

b. Threat networks and their supporting network capabilities (finance, logistics, smuggling, command and control [C2], etc.) will present challenges to the joint force at the tactical, operational, and strategic levels due to their adaptive nature to conditions in the OE. Figure I-1 depicts some of the threat networks that may be operating in the OE and their possible impact on the levels of warfare. These challenges will present themselves throughout the OE. Complex alliances between threat, neutral, and friendly networks may

vary at each level, by agency, and in different geographic areas in terms of their membership, composition, goals, resources, strengths, and weaknesses. Strategically they may be part of a larger ideological movement at odds with several regional governments, have regional aspirations for power, or oppose the policies of nations attempting to achieve military stability in a geographic region. This is the case of larger organizations like al-Qaida, Hizballah, the Islamic State of Iraq and the Levant (ISIL), and the Muslim Brotherhood. Operationally, these groups may employ networks directly or cooperate with like-minded

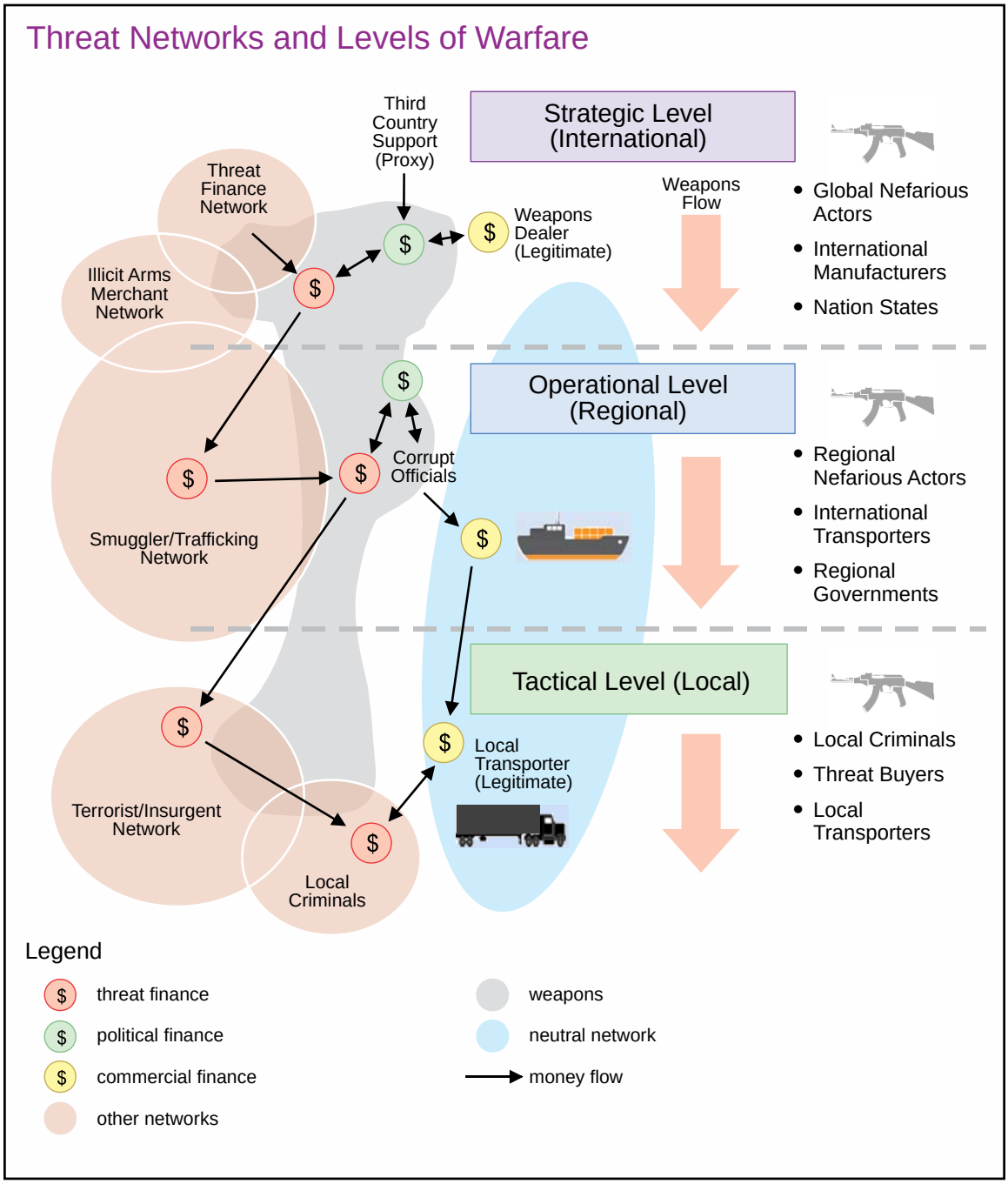


Figure I-1. Threat Networks and Levels of Warfare

groups to counter joint force operations. Tactically, there may be local alliances with criminal networks, tribes, or clans that may not be ideologically aligned with one another, but could find common cause in opposing joint force operations in their area or harboring grievances against the host nation (HN) government. Analysis will be required for each level of warfare and for each network throughout the operational area. This analysis should be aligned with analysis from intelligence community agencies and international partners that often inject critical information that may impact joint planning and operations.

5. The Strategic Approach

a. The groundwork for successful CTN activities starts with information and intelligence to develop an understanding of the OE and the threat network. Military engagement, security cooperation, and deterrence are just some of the activities that may be necessary to successfully counter threat networks without deployment of a joint task force (JTF). The military instrument of national power will support other United States Government (USG) departments and agencies and cooperate with international organizations and other partners and allies to protect and enhance national security interests, deter conflict, and set conditions for future contingency operations. Even when the US is not conducting limited contingency operations, major operations, or campaigns, numerous routine missions (such as security cooperation) and continuing operations or tasks are occurring under the general heading of military engagement. Some typical military engagement, security cooperation, and deterrence operations are emergency preparedness, arms control, nonproliferation, disarmament, combating terrorism, DOD support to CD operations, enforcement of sanctions, enforcing exclusion zones, ensuring freedom of navigation and overflight, FID, protection of shipping lanes, SFA, show of force operations, support to insurgency, and COIN operations. These operations also require detailed intelligence collection and analysis, which will lead to a deeper understanding of these networks once the decision is made to deploy a joint force. Ongoing daily activities should also include interagency partners, international organizations, nongovernmental organizations (NGOs) and HN coordination that includes information sharing and cultural awareness.

b. Current operational art and operational design as described within JPP is applicable to CTN. Threat networks tend to be difficult to collect intelligence on, analyze, and understand. Therefore, several steps within the operational approach methodology outlined in JP 5-0, *Joint Planning*, such as understanding the OE and defining the problem may require more resources and time. JP 2-01.3, *Joint Intelligence Preparation of the Operational Environment*, provides the template for this process used to analyze all relevant aspects of the OE. Within operational design, determining the strategic, operational, and tactical COGs and decisive points of multiple threat networks will be more challenging than analyzing a traditional military force, as illustrated in Figure I-2. The challenge in CTN activities is that there will not just be military objectives, but there may also be diplomatic, economic, and HN objectives. All these must be considered, along with military operations. Military, economic, diplomatic, and partner resources will be concentrated in a unified effort toward a sequence of actions to achieve objectives that will be constantly assessed and refocused as the OE, the threat network, and the populations' perceptions change. In many cases, the commander will still be the central figure in operational design, but must work with other instruments of national power to attain the overall national strategic end state.

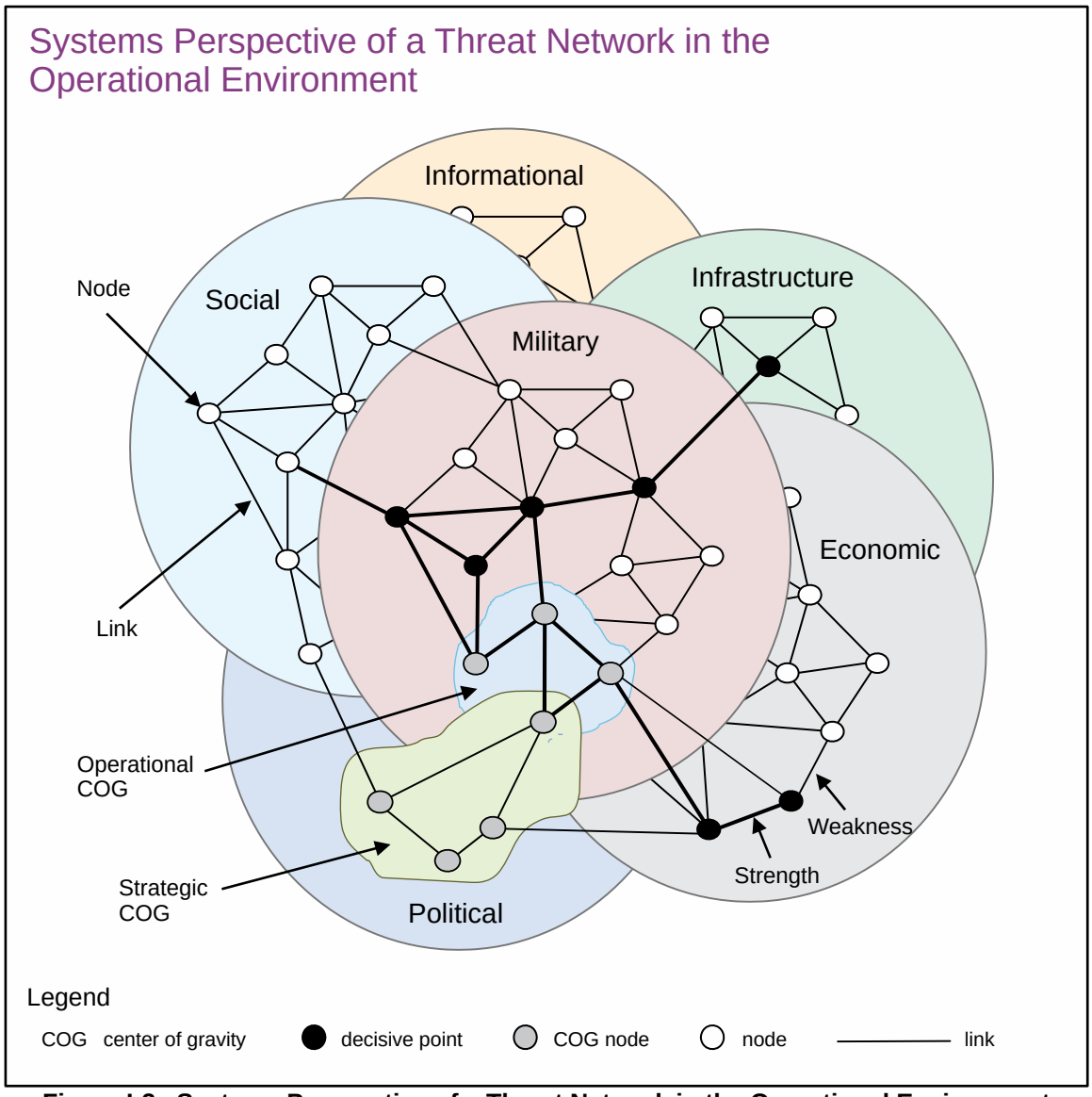


Figure I-2. Systems Perspective of a Threat Network in the Operational Environment

c. Strategic and operational approaches require greater interagency coordination. This is critical for achieving unity of effort against threat network critical vulnerabilities (CVs) (see Chapter II, "Threat Network Fundamentals"). When analyzing networks, there will never be a single COG. The identification of the factors that comprise the COG(s) for a network will still require greater analysis, since each individual of the network may be motivated by different aspects. For example, some members may join a network for ideological reasons, while others are motivated by monetary gain. This aspect must be understood when analyzing human networks.

d. Threat networks will adapt rapidly and sometimes "out of view" of intelligence collection efforts. Intelligence sharing between USG departments and agencies and PNs is vital. This must be complemented by integrated planning and execution to achieve the optimal operational tempo to defeat threats. Traditionally defined geographic operational

areas, roles, responsibilities, and authorities often require greater cross-area coordination and adaptation to counter threat networks. Unity of effort seeks to synchronize understanding of and actions against a group's or groups' political, military, economic, social, information,

STUDY: THE HAQQANI NETWORK—A CRIMINAL-TERRORIST INSURGENT CONVERGENCE

The Haqqani Network (HQN) from its beginnings as a subgroup in the Afghan insurgency fighting the Soviets in the 1980s has risen to become one of the most extensive criminal-terrorist-insurgent networks in the region composed of 10,000 to 15,000 effective, feared, and hard-core fighters. Its founder, Mawlawi Jalaluddin Haqqani transformed his network from a purely military organization fighting the Soviets into a political and economic franchise. The overall goal of HQN is to secure an Afghan state based on Shar'ia law and tie the region together in a financial web, using every aspect of both illicit and licit activities to benefit the HQN organization in ways not necessarily related to jihad.

The HQN has both conflicted with and worked cooperatively with the broader Afghan Taliban insurgency. The HQN's foreign fighter units, safe houses, facilitators, and infiltration routes from the Middle East into Pakistan and Central Asia all serve as valuable force multipliers for the Taliban in Afghanistan. Along with supporting the insurgency in Afghanistan, HQN also engages in terrorism, extortion, and assassinations using the Fedayeen model of high-profile coordinated attacks. HQN linked attacks include the Kabul Serena Hotel in 2008, the Afghanistan International Bank in 2009, the Hotel Inter-Continental Kabul in 2011, and the Spozhmai Hotel in 2012. By keeping significant pressure on Kabul with high profile terrorist attacks, the HQN helps to emphasize the Afghan government's lack of control over the country and diminishes the ability of the Afghan National Security Force to uphold the law and fight crime. The HQN produces a significant amount of propaganda from its operational successes. In keeping with its regional aspirations, propaganda is printed in Pashto, Dari, and Arabic to market the HQN and gain support and recruits.

The HQN financial empire consists of legal and illegal ventures throughout Asia, the Arabian Peninsula, Africa, and Europe. Legal businesses include the exporting of high-value minerals, construction, and real estate investment in Asia and the Middle East. HQN also smuggles pre-cursor chemicals, timber, and precious jewels through its complex logistical networks. Income is also derived from extortion of local and regional businesses, kidnaping for ransom and taxation of people in the border area. The HQN strengthens its power among the population by funding and running hospitals and madrassas in the border areas and providing essential services. Finally, sponsors in the Arabian Peninsula have a 30 year relationship with HQN and help raise money while at the same time rewarding the leadership for conducting high-profile attacks in Kabul. This external support diversifies the steady stream of money to the group.

HQN has a long history in the Central Asian and Middle East region and is the classic example of a criminal-terrorist insurgent network engaged in both licit and illicit activities and businesses. Its sub networks cross multiple international borders, and it is extra-regional in its reach. Understanding, analyzing, and countering these complex threat networks will continue to be a major challenge to future military operations.

Summary of the Haqqani Network:
Pursuing Feuds Under the Guise of Jihad?
***CTX Journal,* Vol. 3, No. 4, November 2013,**
Major Lars W. Lilleby, Norwegian Army
Source: https://globalecco.org/the-haqqani-network-pursuing-feuds-under-theguise-of-jihad

and infrastructure (PMESII) systems as well as the links and nodes that are part of the group's supporting networks.

6. Joint Force and Interagency Coordination

a. The USG and its partners face a wide range of local, national, and transnational irregular challenges to the stability of the international system. Successful deterrence of non-state actors is more complicated and less predictable than in the past, and non-state actors may derive significant capabilities from state sponsorship. Strategic success is increasingly dependent on the military's ability to operate in concert with the rest of the USG, allied and PN governments and their military and security forces, and NGOs.

b. Adapting to an increasingly complex world requires unity of effort to counter violent extremism and strengthen regional security. For CCMDs to work with other USG departments and agencies effectively, it is important to understand and respect that each department or agency approaches planning and strategy development differently. Some approaches are formal and structured, while others are informal. To improve understanding, USG departments and agencies should strive to develop strong relationships while learning to speak each other's language, or better yet, use a common lexicon.

c. At each echelon of command, the actions taken to achieve stability vary only in the amount of detail required to create an actionable picture of the enemy and the OE. Each echelon of command has unique functions that must be synchronized with the other echelons, as part of the overall operation to defeat the enemy. Achieving synergy among diplomatic, political, security, economic, and information activities demands unity of effort between all participants. This is best achieved through an integrated approach. A common interagency assessment of the OE establishes a deep and shared understanding of the cultural, ideological, religious, demographic, and geographical factors that affect the conditions in the OE. Once US assistance is committed, an operational approach must be devised, ideally in collaboration with the affected government and other partners, since their early inclusion can help mitigate the effects of operational-level differences in goals, capabilities, and culture. Detailed, integrated planning then follows and a process of continuous monitoring, evaluation, and assessment is used to measure progress and identify where changes in approach are necessary to achieve success.

d. Establishing a whole-of-government approach to achieve unity of effort should begin during planning. Achieving unity of effort is problematic due to challenges in information sharing, competing priorities, differences in lexicon, and uncoordinated activities. The unity of effort framework, contained in the *Unity of Effort Framework Solutions Guide,* is designed to improve unity of effort across the USG by setting the conditions for increased collaborative planning.

For further details, refer to the Joint Staff J-7's [Directorate for Joint Force Development's] Unity of Effort Framework Solutions Guide *and* Unity of Effort Framework Quick Reference *in the Joint Electronic Library at http://www.dtic.mil/doctrine/doctrine/jwfc_pam.htm.*

7. Responsibilities

a. Operations against threat networks require unity of effort across the USG and multiple authorities outside DOD. Multiple instruments of national power will be operating in close proximity and often conducting complementary activities across the strategic, operational, and tactical levels. In order to integrate, deconflict, and synchronize the activities of these multiple entities, the commander should form a joint interagency coordination group, with representatives from all participants operating in or around the operational area.

For a detailed discussion of interagency planning and coordination, see JP 3-08, Interorganizational Cooperation.

b. The military provides general support to a number of USG departments and agencies for their CTN activities ranging from CT to CD. A number of USG departments and agencies have highly specialized interests in threat networks, and their activities directly impact the military's own CTN activities. For example, the Department of the Treasury's CTF activities help to deny the threat network the funding needed to conduct operations.

Intentionally Blank

CHAPTER II
THREAT NETWORK FUNDAMENTALS

1. Threat Network Construct

a. **Network Basic Components.** All networks, regardless of size, share basic components and characteristics. Understanding common components and characteristics will help to develop and establish common joint terminology and standardize outcomes for network analysis, CTN planning, activities, and assessments across the joint force and CCMDs.

b. **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. (See Appendix G, "Social Network Analysis," for information on 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 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.

(1) **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, transportation system, etc.

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

(3) **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 PMESII categories.

(4) **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 allows 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.

2. Network Analysis

a. Network analysis is a means of gaining understanding of a group, place, physical object, or system. It identifies relevant nodes, determines and analyzes links between nodes, and identifies key nodes. The PMESII systems perspective is a useful starting point for analysis of threat networks. Network analysis facilitates identification of significant information about networks that might otherwise go unnoticed. For example, network analysis can uncover positions of power within a network, show the cells that account for its structure and organization, find individuals or cells whose removal would greatly alter the network, and facilitate measuring change over time.

b. All networks are influenced by and in turn influence the OEs in which they exist. Analysts must understand the underlying conditions; the frictions between individuals and groups; familial, business, and governmental relationships; and drivers of instability that are constantly subject to change and pressures. All of these factors evolve as the networks change shape, increase or decrease capacity, and strive to influence and control things within the OE, and they contribute to or hinder the networks' successes. Environmental framing is selecting, organizing, and interpreting and making sense of a complex reality; it serves as a guide for analyzing, understanding, and acting. Critical thinking requires analysts to develop a complete understanding of the OE and to solve the right problems and remain capable and willing to adapt to dynamic and even unpredictable conditions.

c. Networks are typically formed at the confluence of three conditions: the presence of a catalyst, a receptive audience, and an accommodating environment. As conditions within the OE change, the network must adapt in order to maintain a minimal capacity to function within these conditions. Elements of these conditions may be directly related to the factors that comprise the network's COG.

(1) **Catalyst.** A catalyst is a condition or variable within the OE that could motivate or bind a group of individuals together to take some type of action to meet their collective needs. These catalysts may be identified as critical variables as units conduct their evaluation of the OE and may consist of a person, idea, need, event, or some combination thereof. The potential exists for the catalyst to change based on the conditions of the OE.

(2) **Receptive Audience.** A receptive audience is a group of individuals that feel they have more to gain by engaging in the activities of the network than by not participating. Additionally, in order for a network to form, the members of the network must have the motivation and means to conduct actions that address the catalyst that generated the network. Depending on the type of network and how it is organized, leadership may or may not be necessary for the network to form, survive, or sustain collective action. The receptive audience originates from the human dimension of the OE.

(3) **Accommodating Environment.** An accommodating environment is the conditions within the OE that facilitate the organization and actions of a network. Proper conditions must exist within the OE for a network to form to fill a real or perceived need. Networks can exist for a time without an accommodating environment, but without it the network will ultimately fail.

d. Networks utilize the PMESII system structure within the OE to form, survive and function. Like the joint force, threat networks will also have desired end states and objectives. As analysis is being conducted of the OE, the joint staff should identify the critical variables within the OE for the network. A critical variable is a key resource or condition present within the OE that has a direct impact on the commander's objectives and may affect the formation and sustainment of networks. A critical variable is the focus for shaping, within the OE, to achieve the commander's objective or attain the military end state. Identifying critical variables is important because they affect COGs for key components and actors within the systems. Critical variables often serve to focus measures of effectiveness (MOEs) and indicators development. They become the focus for shaping and measuring, within the OE, to ascertain progress toward the end state.

For more information on developing a systems perspective, refer to JP 2-01.3, Joint Intelligence Preparation of the Operational Environment.

3. Determining and Analyzing Node-Link Relationships

Links are derived from data or extrapolations based on data. A benefit of graphically portraying node-link relationships is that the potential impact of actions against certain nodes can become more evident. Social network analysis (SNA) provides a method that helps the JFC and staff understand the relevance of nodes and links. Network mapping is essential to conducting SNA. For example, the number of links between nodes can indicate the importance of the node to the larger functional grouping. The strength or intensity of a single link can be relevant to determining the importance of the functional relationship between nodes and the overall significance to the larger system. Link strength or intensity is a qualitative assessment that indicates how much information, influence, and resource flows between nodes. There is no absolute scale for link strength since networks vary widely; it is a relative assignment as compared to other links in the network. Therefore, the number and strength of nodal links within a set of nodes can be indicators of key nodes and a potential COG. Due to the potential complexity of network relationships, graphic visualization techniques can facilitate network analysis.

a. **Link Analysis.** Link analysis identifies and analyzes relationships between nodes in a network. Network mapping provides a visualization of the links between nodes, but does not provide the qualitative data necessary to fully define the links. Analyzing interrelated networks requires clarity of the type and strength of each link in order to provide the commander with greater understanding of the network. Enhanced understanding of the relationships between network nodes provides the commander with information that will support the target selection process. During link analysis, the analyst examines the conditions of the relationship, strong or weak, informal or formal, formed by familial, social, cultural, political, virtual, professional, or any other condition. The qualitative data produced from link analysis is then used with other quantitative data to distinguish nodes lines of communications and hierarchies for disruption within the network.

b. **Nodal Analysis.** Individuals are associated with numerous networks due to their individual identities. A node's location within a network and in relation to other nodes carries identity, power, or belief and influences behavior. Examples of these types of

identities include locations of birth, family, religion, social groups, organizations, or a host of various characteristics that define an individual. These individual attributes are often collected during identity activities and fused with attributes from unrelated collection activities to form identity intelligence (I2) products. Some aspects used to help understand and define an individual are directly related to the conditions that supported the development of relationships to other nodes. Understanding this type of information about a specific node will help the commander throughout the targeting process. Chapter V, "Activities to Counter Threat Networks," explores how the information gained from understanding the network can be used to enhance the commander's targeting efforts. Figure II-1 illustrates some characteristics associated with networks that can be considered by the commander to help gain an understanding of a network to be targeted.

c. **Network Analysis.** Throughout the JIPOE process, at every echelon and production category, one of the most important, but least understood, aspects of analysis is sociocultural analysis (SCA). SCA is the study, evaluation, and interpretation of information about adversaries and relevant actors through the lens of group-level decision making to discern catalysts of behavior and the context that shapes behavior. SCA considers relationships and activities of the population, SNA (looking at the interpersonal, professional, and social networks tied to an individual), as well as small and large group dynamics. SNA not only

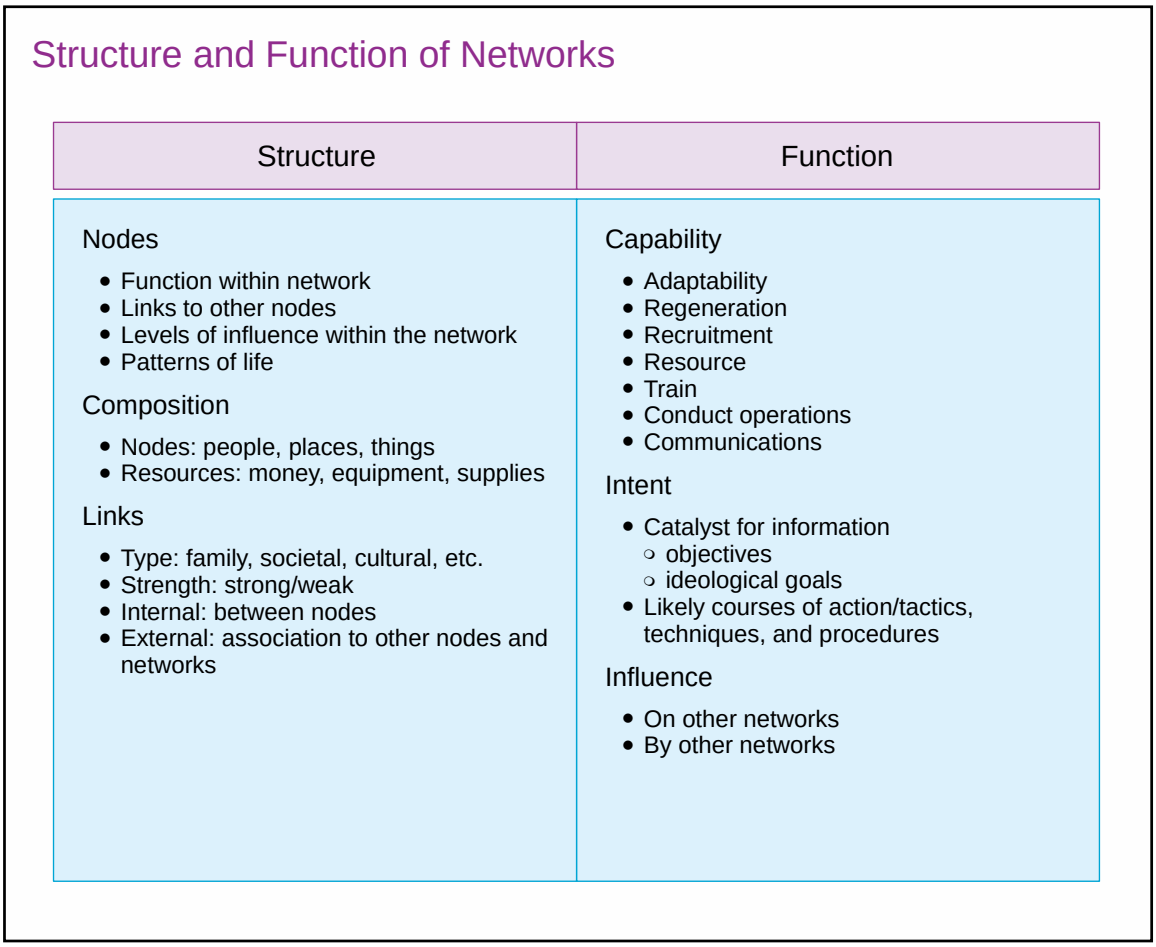


Figure II-1. Structure and Function of Networks

examines individuals and groups of individuals within a social structure such as a terrorist, criminal, or insurgent organization, but also examines how they interact. Interactions are often repetitive, enduring, and serve a greater purpose, and the interaction patterns affect behavior. If enough nodes and links information can be collected, behavior patterns can be observed and, to some extent, predicted. SNA differs from link analysis because it only analyzes similar objects (e.g., people or organizations), not the relationships between the objects. SNA provides objective analysis of current and predicted network structure and interaction of networks that have an impact on the OE. SNA computer software can save time, allow data to be manipulated, and produce graphical representation (matrices, etc.) of networks for the commander and staff.

For information on SCA and analysis matrices for use in CTN activities, see JP 2-01.3, Joint Intelligence Preparation of the Operational Environment.

For more information, see Appendix G, "Social Network Analysis."

4. Threat Networks and Cells

A network must perform a number of functions in order to survive and grow. These functions can be seen as cells that have their own internal organizational structure and communications. These cells work in concert to achieve the overall organization's goals. To survive, the network's internal structure has a high degree of flexibility, adapting to friendly pressure and the requirements of the OE. Networks do not exist in a vacuum. They normally share nodes and links with other networks. Each network may require a unique operational approach as they adapt to their OE or to achieve new objectives. They may form a greater number of cells if they are capable of independent operations consistent with the threat network's overall operational goals. They may move to a more hierarchical system due to lack of leadership, questions regarding loyalty of subordinates, or inexperienced lower-level personnel. Understanding these dimensions allows a commander to craft a more effective operational approach. These cells are examples only. The list is neither exclusive nor inclusive. Each network and cell will change, adapt, and morph over time.

a. **Operational Cells.** Operational cells carry out the day-to-day operations of the network and are typically people-based (e.g., terrorists, guerrilla fighters, drug dealers). It is extremely difficult to gather intelligence on and depict every single node and link within an operational network. However, understanding key nodes, links, and cells that are particularly effective allows for precision targeting and greater effectiveness.

b. **Logistical Cells.** Logistical cells provide threat networks the necessary supplies, weapons, ammunition, fuel, and military equipment to operate. Logistical cells are easier to observe and target than operational or communications cells since they move large amounts of material, which makes them more visible. These cells may include individuals who are not as ideologically motivated or committed as those in operational networks. Threat logistical cells often utilize legitimate logistics nodes and links to hide their activities "in the noise" of legitimate supplies destined for a local or regional economy. It is particularly important to determine which links extend into other countries or outside the operational area since this will require USG interagency and international cooperation. Interdiction

operations along international and regional boundaries may effectively target links and isolate threat networks.

c. **Training Cells.** Most network leaders desire to grow the organization for power, prestige, and advancement of their goals. Logistical cells may be used to move material, trainers, and trainees into a training area, or that portion of logistics may be a distinct part of the training cells. Once training is completed, logistical cells move new members to operational areas. These activities may be visible and provide insight to a network's activities and its topology. Training requires the aggregation of new personnel and often includes physical structures to support activities which may also be visible and provide additional information to better understand the network.

d. **Communications Cells.** Most threat networks have at minimum rudimentary communications cells for operational, logistical and financial purposes and another to communicate their strategic narrative to a target or neutral population. While it is quite difficult to completely neutralize any communications means, intelligence organizations can collect and analyze messages, track content trends, and identify the message originator. The use of Internet-based social media platforms by threat networks increases the likelihood of gathering information, including geospatial information.

e. **Financial Cells.** Threat networks require funding for every aspect of their activities, to maintain and expand membership, and to spread their message. Their financial cell moves money from legitimate and illegitimate business operations, foreign donors, and taxes collected or coerced from the population to the operational area. This movement may use the formally regulated financial networks that span the globe or informal regional networks such as hawalas (an informal regional transfer system that is based on trust and often portrayed as transferring money without actually moving the money). Funding may come from kidnapping, piracy, other criminal activity, state sponsors, or legitimate businesses controlled by the network.

f. **WMD Proliferation Cells.** Many of these cells are not organized specifically for the proliferation of WMD. In fact, many existing cells may be utilized out of convenience. Examples of existing cells include human trafficking, counterfeiting, and drug trafficking. As an additional consideration, some nodes within these networks may be unwitting partners. The threat is further complicated by the operations of multinational networks, potentially with the support of state resources. These global proliferation activities employ a combination of secrecy, dispersion, and fiscal resources that must be located, monitored, and ultimately targeted. The JFC should use a systems perspective to better understand the complexity of the OE and associated networks. This perspective looks across the PMESII systems to identify the nodes, links, COGs, and potential vulnerabilities within the network. The JFC understands that as these sub-networks expand in scope and area, the actions needed to adequately identify and affect them may reside outside DOD influence and may require interagency partner, NGO, PN, HN, or international organization efforts. Depending on joint force organization, the JFC may lack a full range of capabilities that can support unity of effort to proactively and comprehensively dissuade, deter, defeat, or deny these networks and cells.

For more information, see JP 3-40, Countering Weapons of Mass Destruction.

5. Analyze the Network

Key nodes exist in every major network and are critical to their function. Nodes may be people, places, or things. For example, a town that is the primary conduit for movement of illegal narcotics would be the key node in a drug trafficking network. Some may become decisive points for military operations since, when acted upon, they could allow the JFC to gain a marked advantage over the adversary or otherwise to contribute materially to achieving success. Weakening or eliminating a key node should cause its related group of nodes and links to function less effectively or not at all, while strengthening the key node could enhance the performance of the network as a whole. Key nodes often are linked to, resident in, or influence multiple networks. For example, a country's predominant religion could be central to the functioning of the country's social system, and the core group of religious leaders (or a single leader) could be a key node. Depending on the country's social and political structure, this same group of religious leaders also could be a key node in the political system when it is viewed as a network. Since each PMESII system and subsystem is composed of nodes and links, the capabilities of US instruments of national power can be employed against selected key nodes to create operational and strategic effects. Although largely influenced by subjective judgment, identifying a potential key node may be facilitated through an analysis of network density, degree of centrality, and node centrality (i.e., how individual entities fit in the systems network). Node centrality can highlight possible positions of importance, influence, or prominence and patterns of connections. A node's relative centrality is determined by analyzing measurable characteristics: degree, closeness, betweenness, and eigenvector.

For more information, see Appendix G, "Social Network Analysis."

Intentionally Blank

CHAPTER III
NETWORKS IN THE OPERATIONAL ENVIRONMENT

"How many times have we killed the number three in al-Qaida? In a network, everyone is number three."

Dr. John Arquilla, Naval Postgraduate School

1. Networked Threats and Their Impact on the Operational Environment

a. In a world increasingly characterized by volatility, uncertainty, complexity, and ambiguity, a wide range of local, national, and transnational irregular challenges to the stability of the international system have emerged. Traditional threats like insurgencies and criminal gangs have been exploiting weak or corrupt governments for years, but the rise of transnational extremists and their active cooperation with traditional threats has changed the global dynamic. Successful deterrence and elimination of these illicit networks is more complicated and less predictable than in the past.

b. All networks are vulnerable, and a JFC and staff armed with a comprehensive understanding of a threat network's structure, purpose, motivations, functions, interrelationships, and operations can determine the most effective means, methods, and timing to exploit that vulnerability. In order for the JIPOE process to produce understanding of threats and their networks, analysis must be conducted by intelligence analysts and operational planners familiar with the principles of network analysis. Network analysis and exploitation are not simple tasks. Networked threats are highly adaptable adversaries with the ability to select a variety of tactics, techniques, and technologies and blend them in unconventional ways to meet their strategic aims. Additionally, many threat networks supplant or even replace legitimate government functions such as health and social services, physical protection, or financial support in ungoverned or minimally governed areas. This de facto governance of an area by a threat network makes it more difficult for the joint force to simultaneously attack a threat and meet the needs of the population.

For more information, see Appendix E, "Exploitation in Support of Countering Threat Networks," and Appendix G, "Social Network Analysis."

c. Once the JFC identifies the networks in the OE and understands their interrelationships, functions, motivations, and vulnerabilities, the commander tailors the force to apply the most effective tools against the threat. Tailored task organizations and specialized teams are necessary to apply effective pressure across an entire network structure. For example, a traditional JTF does not normally have civilian financial experts on its staff to identify and assist in attacking threat financial network activities. Likewise, a JTF fires cell may require mainly MISO and/or IO specialists rather than field artillery and joint terminal attack controllers. Additionally, the JTF requires active support and participation by USG, HN, nongovernmental agencies, and partners, particularly when it comes to addressing cross-border sanctuary, arms flows, and the root causes of instability. This "team of teams" approach facilitates unified action, which is essential for organizing for operations against an adaptive threat.

2. Threat Network Characteristics

Threat networks do not differ much from non-threat networks in their functional organization and requirements. Threat networks manifest themselves and interact with neutral networks for protection, to perpetuate their goals, and to expand their influence. Networks involving people have been described as insurgent, criminal, terrorist, social, political, familial, tribal, religious, academic, ethnic, or demographic. Some non-human networks include communications, financial, business, electrical/power, water, natural resources, transportation, or informational. Networks take many forms and serve different purposes, but are all comprised of people, processes, places, material, or combinations. Individual network components are identifiable, targetable, and exploitable. Almost universally, humans are members of more than one network, and most networks rely on other networks for sustainment or survival. Because of the large number of networks, the problem is to find the given threats buried within and operating across multiple networks. Some threats, such as WMD proliferators, are particularly difficult to detect because legal networks may be used for illegal purposes. Organized threats leverage multiple networks within the OE based on mission requirements or to achieve objectives not unilaterally achievable. The following example shows some typical networks that a threat will use and/or exploit. This "network of networks" is always present and presents challenges to the JFC when planning operations to counter threats that nest within various friendly, neutral, and hostile networks (see Figure III-1).

3. Adaptive Networked Threats

For a threat network to survive political, economic, social, and military pressures, it must adapt to those pressures. Survival and success are directly connected to adaptability and the ability to access financial, logistical, and human resources. Networks possess many characteristics important to their success and survival, such as flexible C2 structure; a shared identity; and the knowledge, skills, and abilities of group leaders and members to adapt. They must also have a steady stream of resources and may require a sanctuary (safe haven) from which to regroup and plan.

a. **C2 Structure.** There are many potential designs for the threat network's internal organization. Some are hierarchical, some flat, and others may be a combination. The key is that to survive, networks adapt continuously to changes in the OE, especially in response to friendly actions. Commanders must be able to recognize changes in the threat's C2 structures brought about by friendly actions and maintain pressure to prevent a successful threat reconstitution.

b. **Shared Identity.** Shared identity among the membership is normally based on kinship, ideology, religion, and personal relationships that bind the network and facilitate recruitment. These identity attributes can be an important part of current and future identity activities efforts, and analysis can be initiated before hostilities are imminent. The relatively new ISIL draws much of its support from long-standing groups and populations in Iraq and Syria, just as disparate Palestinian organizations do in the Levant. Similarly, the Irish Republican Army drew much of its support and fund-raising from long-standing groups in the 1960s and 1970s within the Irish-American population.

A Network of Networks

Network	Function	Members	Threat Use	Nature/Scope
Information	Official communications, commerce, social communications, indoctrination/recruitment	Population, government, media	Continuous	Global
Cultural/Social	Shared Identity, sense of belonging	Population	Continuous	Global/regional/ local
Religious, Political, Ideological	Philosophical, moral, political power, cultural identity	Demographic groups	Threat dependent	Global/regional/ local
Transportation	Travel, commerce, migration	Population, government	Periodic	Global/regional
Financial	Commerce, means to power and influence	All	Continuous	Global/regional
Weapons, Munitions, Explosives	Military/law enforcement, militant/terrorist violence	Arms merchants, governments, business and criminal organizations	Periodic	Global/regional
Criminal	Criminal profit, threat financial support	Gangs, criminal organizations, corrupt government officials	Threat dependent	Global/regional/ local
Infrastructure (water, electric, government services, medical)	Sustainment	All	Continuous	Regional/local

Figure III-1. A Network of Networks

c. **Knowledge, Skills, and Abilities of Group Leaders and Members.** All threat networks have varying degrees of proficiency. In initial stages of development, a threat organization and its members may have limited capabilities. An organization's survival rests on the knowledge, skills, and abilities of its leadership and membership. By seeking out subject matter expertise, financial backing, or proxy support from third parties, an organization can increase their knowledge, skills, and abilities, making them more adaptable and increasing their chance for survival.

d. **Resources.** Resources in the form of arms, money, technology, social connectivity, and public recognition are used by threat networks. Identification and systematic

strangulation of threat resources is the fundamental principle for CTN. For example, money is one of the critical resources of adversary networks. Denying the adversary its finances makes it harder, and perhaps impossible to pay, train, arm, feed, and clothe forces or gather information and produce the propaganda. See Appendix A, "Department of Defense Counter Threat Finance," for more information. While ISIL has been able to use oil to help finance its operations, other threats will use various funding streams.

e. **Adaptability.** This includes the ability to learn and adjust behaviors; modify tactics, techniques, and procedures (TTP); improve communications security and operations security; successfully employ IRCs; and create solutions for safeguarding critical nodes and reconstituting expertise, equipment, funding, and logistics lines that are lost to friendly disruption efforts. Analysts conduct trend analysis and examine key indicators within the OE that might suggest how and why networks will change and adapt. Disruption efforts will often provoke a network's changing of its methods or practices, but often external influences, local relationships and internal friction, geographic and climate challenges, and global economic factors might also be some of the factors that motivate a threat network to change or adapt to survive.

f. **Sanctuary (Safe Havens).** Safe havens allow the threat networks to conduct planning, training, and logistic reconstitution. Threat networks require certain critical capabilities (CCs) to maintain their existence, not the least of which are safe havens from which to regenerate combat power and/or areas from which to launch attacks. The JFC and staff need to identify and deny access to threat safe havens. Safe havens outside the immediate operational area hosted by third parties, nation-states, or other criminal elements require a comprehensive analysis of the threat and will require an expanded whole-of-government approach.

4. Network Engagement

a. Network engagement is the interactions with friendly, neutral, and threat networks, conducted continuously and simultaneously at the tactical, operational, and strategic levels, to help achieve the commander's objectives within an OE. To effectively counter threat networks, the joint force must seek to support and link with friendly networks and engage neutral networks through the building of mutual trust and cooperation through network engagement. The joint force will coordinate and work cooperatively with interagency partners and PNs. Unified action provides the opportunity for the JFC to create powerful friendly networks with far-reaching capabilities and engage neutral networks to either solicit their assistance or prevent them from supporting our adversary. These integrated and synchronized activities are intended to establish conditions within the OE that align with the JFC's desired end state.

b. Network engagement consists of three components: partnering with friendly networks, engaging neutral networks, and CTN to support the commander's desired end state. Network engagement is not a stand-alone process, but rather lays out a number of methods that will support or amplify the JFC's processes (JPP, JIPOE, targeting, and assessment) to thrive and dominate in any OE. Network engagement utilizes both lethal and nonlethal actions against networks, nodes, and links.

c. Individuals may be associated with numerous networks due to their unique identities. Examples of these types of identities include location of birth, family, religion, social groups, organizations, or a host of various characteristics that define an individual. Therefore, it is not uncommon for an individual to be associated with more than one type of network (friendly, neutral, or threat). Individual identities provide the basis that allows for the interrelationship between friendly, neutral, and threat networks to exist. It is this interrelationship that makes categorizing networks a challenge. Classifying a network as friendly or neutral when in fact it is a threat may provide the network with too much freedom or access. Mislabeling a friendly or neutral network as a threat may cause actions to be taken against that network that can have unforeseen consequences.

d. Networks are comprised of individuals who are involved in a multitude of activities, including social, political, monetary, religious, and personal. These human networks exist in every OE, and therefore network engagement activities will be conducted throughout all phases of the conflict continuum and across the range of operations.

e. Figure III-2 depicts the effective results of utilizing lethal actions to counter threat networks and reduce their legitimacy in the OE. Figure III-2 also shows the effect of nonlethal actions against friendly and neutral networks to increase their legitimacy in the OE. It is important to remember that nonlethal actions can also have a desired effect when used against threat networks.

5. Networks, Links, and Identity Groups

All individuals are members of multiple, overlapping identity groups (see Figure III-3). These identity groups form links of affinity and shared understanding, which may be leveraged to form networks with shared purpose. These networks may form in response to perceived threats to the identity group, and existing networks may leverage overlaps between the core identity group and other groups in the operational area to broaden their support base or attract recruits. Networks with stronger and more numerous links will be more resilient to outside efforts seeking to divide the network and will have greater motivation among its membership. Many threat networks rely on family and tribal bonds when recruiting for the network's inner core. These members have been vetted for years and are almost impossible to turn. For analysts, identifying family and tribal affiliations assists in developing a targetable profile on key network personnel. Even criminal networks will tend to be densely populated by a small number of interrelated identity groups.

a. **Family Network.** Some members or associates have familial bonds. These bonds may be cross-generational.

b. **Cultural Network.** Network links can share affinities due to culture, which include language, religion, ideology, country of origin, and/or sense of identity. Networks may evolve over time from being culturally based to proximity based.

c. **Proximity Network.** The network shares links due to geographical ties of its members (e.g., past bonding in correctional or other institutions or living within specific regions or neighborhoods). Members may also form a network with proximity to an area

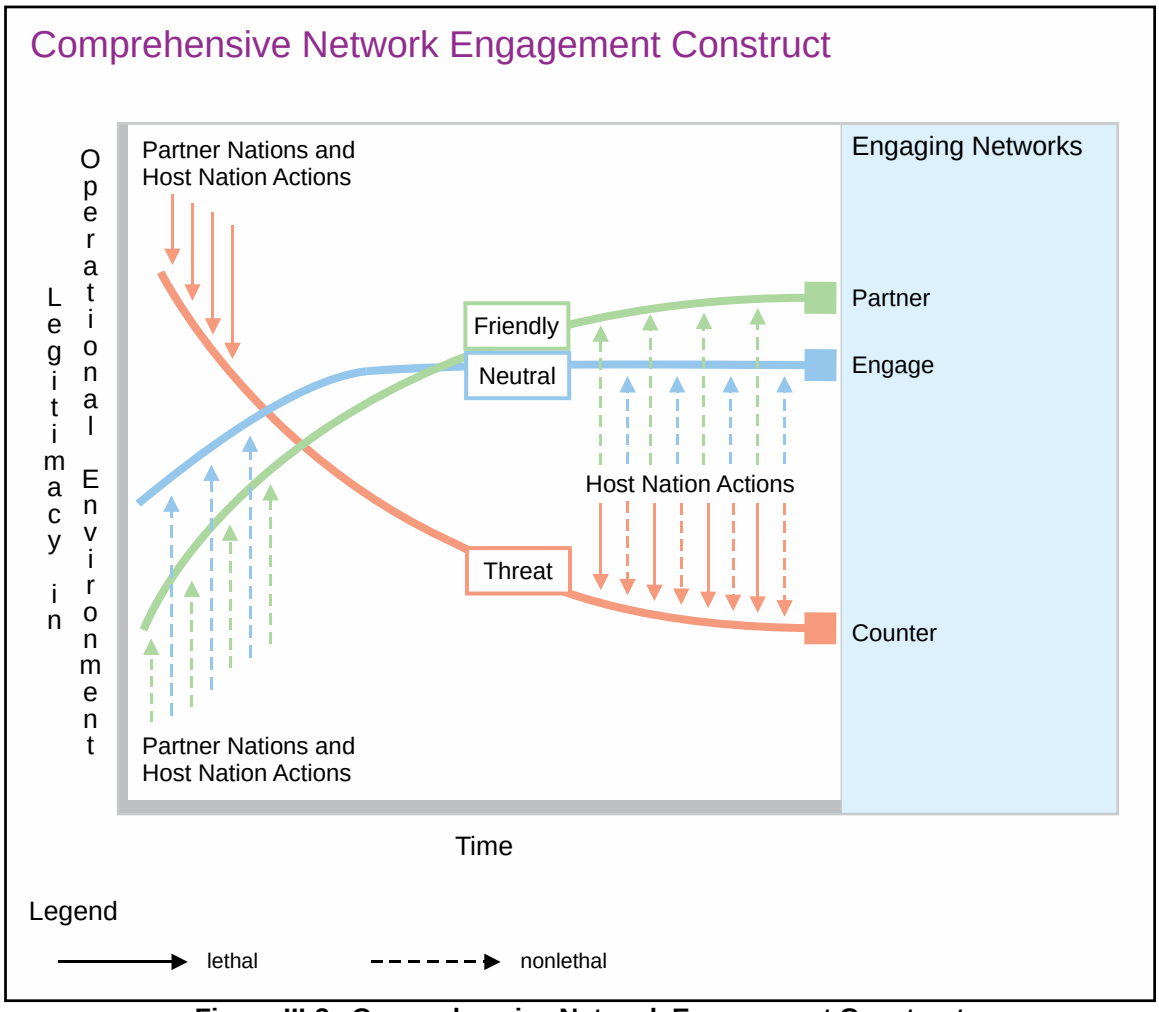


Figure III-2. Comprehensive Network Engagement Construct

strategic to their criminal interests (e.g., a neighborhood or key border entry point). There may be a dominant ethnicity within the group, but they are primarily together for reasons other than family, culture, or ethnicity.

d. **Virtual Network.** A network that may not physically meet but work together through the Internet or other means of communication, for legitimate or criminal purposes (e.g., online fraud, theft, or money laundering).

e. **Specialized Networks.** Individuals in this network come together to undertake specific activities based on the skills, expertise, or particular capabilities they offer. This may include criminal activities.

6. Types of Networks in an Operational Environment

There are three general types of networks found within an operational area: friendly, neutral, and hostile/threat networks. A network may also be in a state of transition and therefore difficult to classify. To successfully accomplish mission goals the JFC should equally consider the impact of actions on multinational and friendly forces, local population,

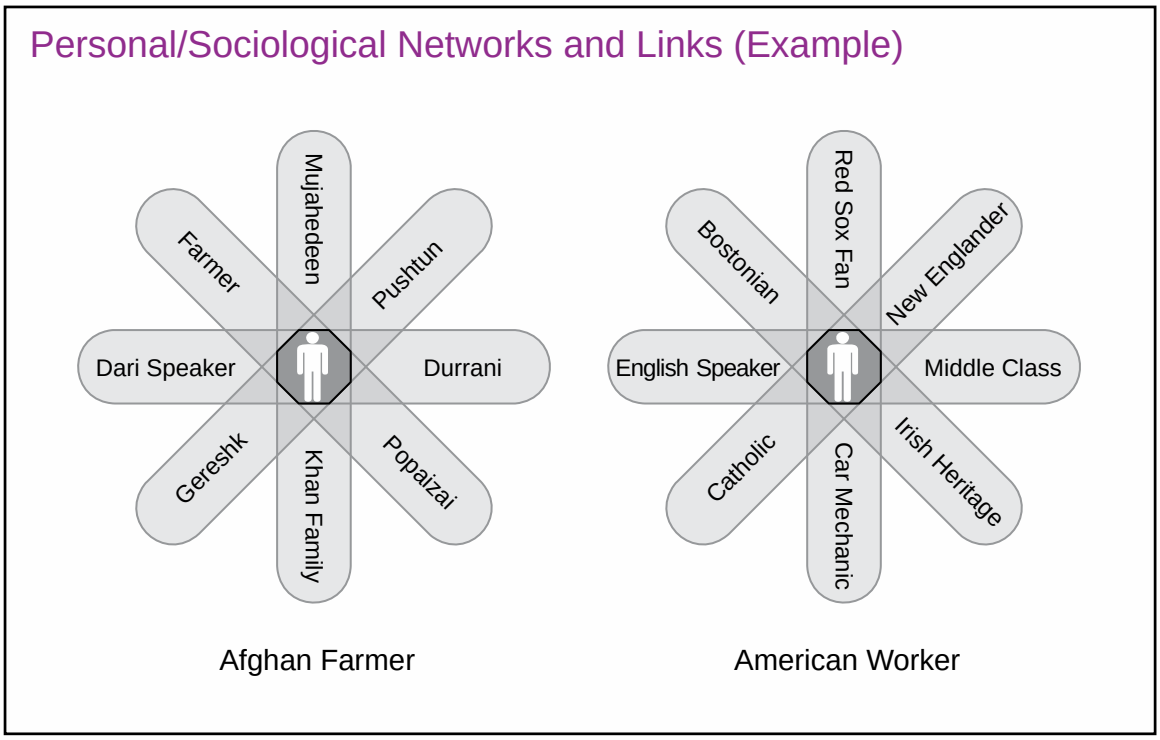


Figure III-3. Personal/Sociological Networks and Links (Example)

criminal enterprises, as well as the adversary. Intelligence may provide the commander with the location of the adversary, but if planning does not consider the impact of a strike on the local population, the adversary could gain twice the number of combatants lost during the attack. Additionally, a thorough and accurate understanding and template of the neutral networks, and how they are interrelated with threat networks, provides operating forces with greater opportunities to understand, penetrate, and target those threat networks. Providing the commander with an array of lethal and nonlethal capabilities (i.e., blunt impact munitions, acoustic/optical hail and warn devices, vehicle/vessel stoppers) to shape the OE allows for a variable response to the complex security environment.

a. **Friendly networks,** as notionally depicted in Figure III-4, can be divided into two groups: US and allied (PN) organizations, and those composed of the HN in which operations are being conducted.

b. **Neutral networks,** as notionally depicted in Figure III-5, are composed of generally benign groups, neither fully partnered with friendly units nor aligned with the threat. Many times, these networks will continue to operate largely unaffected by the activities of either threat or friendly operations. For example, before, during and after the fall of France in World War II, the Paris Metro, taxi service, telephone systems, nightclubs, bars, and restaurants all continued to operate. The JFC must keep in mind how operations may both positively and negatively affect these neutral networks.

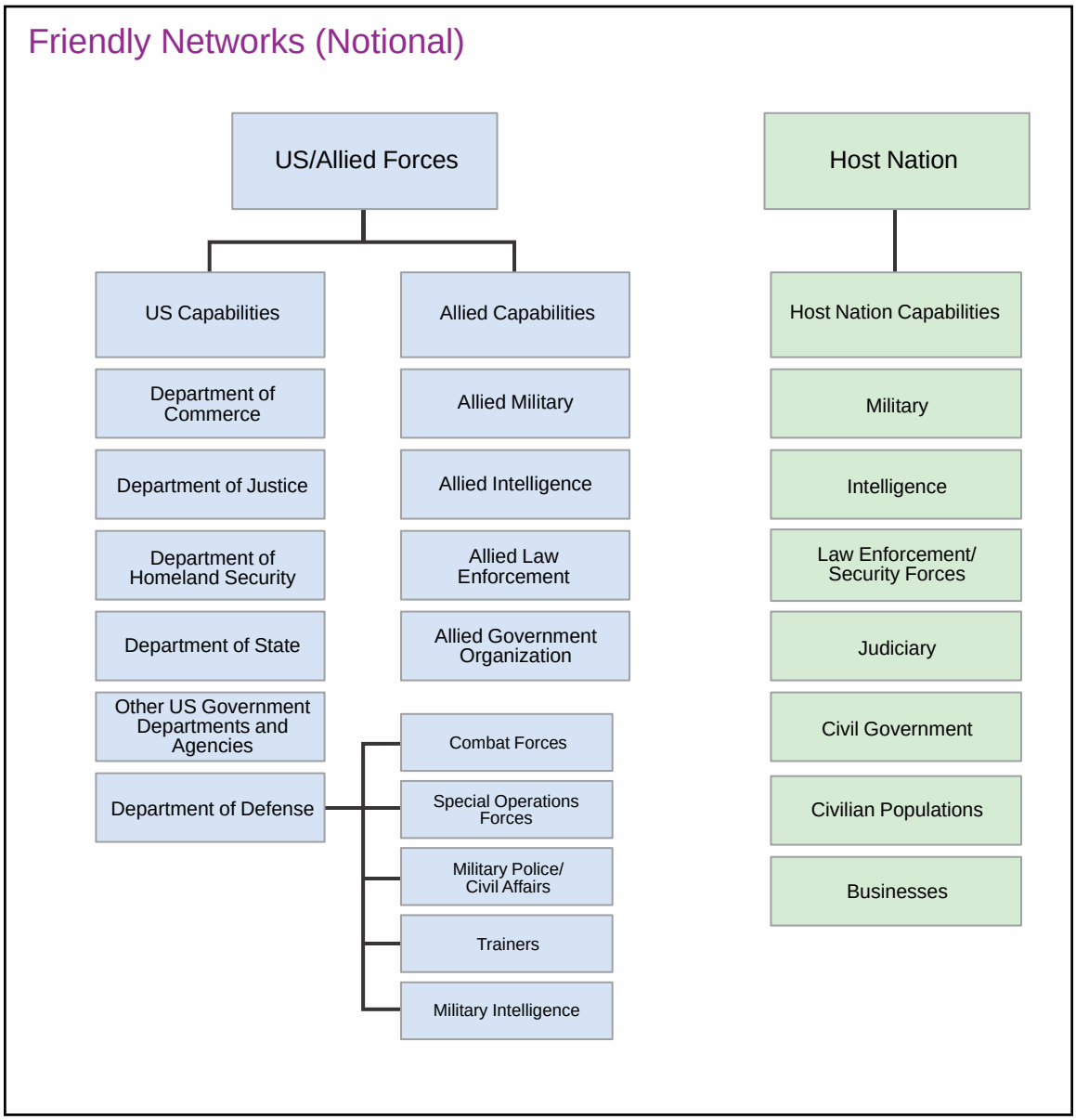


Figure III-4. Friendly Networks (Notional)

c. **Threat networks,** as notionally depicted in Figure III-6, can be composed of criminal, insurgent or terrorist organizations, each of which may have different motivations for operating outside of societal norms. They can also be government entities, legitimate legal organizations, or anyone who opposes the achievement of friendly objectives. Threat networks may be formally intertwined or come together when mutually beneficial. This convergence (or nexus) between threat networks has greatly strengthened regional instability and allowed threats and alliances to increase their operational reach and power to global proportions.

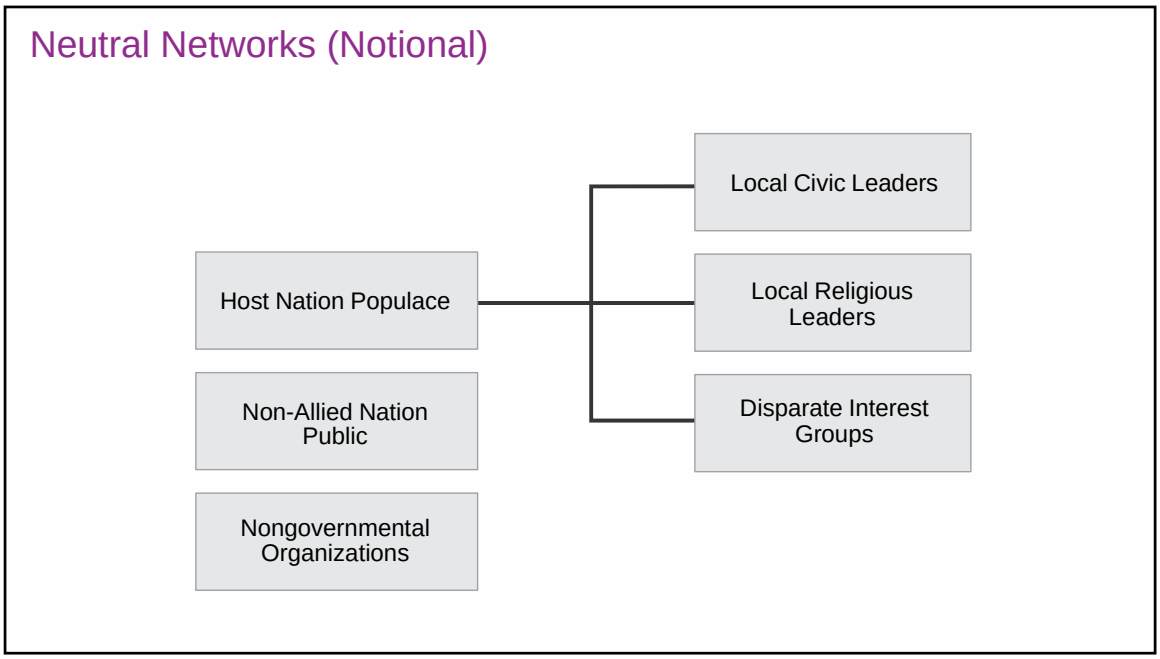


Figure III-5. Neutral Networks (Notional)

7. Identify a Threat Network

Threat networks often attempt to remain hidden. How can commanders determine not only which networks are within an operational area, but also which pose the greatest threat? By understanding the basic, often masked sustainment functions of a given threat network, commanders may also identify individual networks within. For example, all networks require communications, resources, and people. By understanding the functions of a network, commanders can make educated assumptions as to their makeup and determine not only where they are, but also when and how to engage them. As previously stated, there are many neutral networks that are used by both friendly and threat forces; the difficult part is determining what networks are a threat and what networks are not. The "find" aspect of the find, fix, finish, exploit, analyze, and disseminate (F3EAD) targeting methodology is initially used to discover and identify networks within the OE. The F3EAD methodology is not only used for identifying specific actionable targets; it is also used to uncover the nature, functions, structures, and numbers of networks within the OE. A thorough JIPOE product, coupled with "on-the-ground" assessment, observation, and all-source intelligence collection, will ultimately lead to an understanding of the OE and will allow the commander to visualize the network.

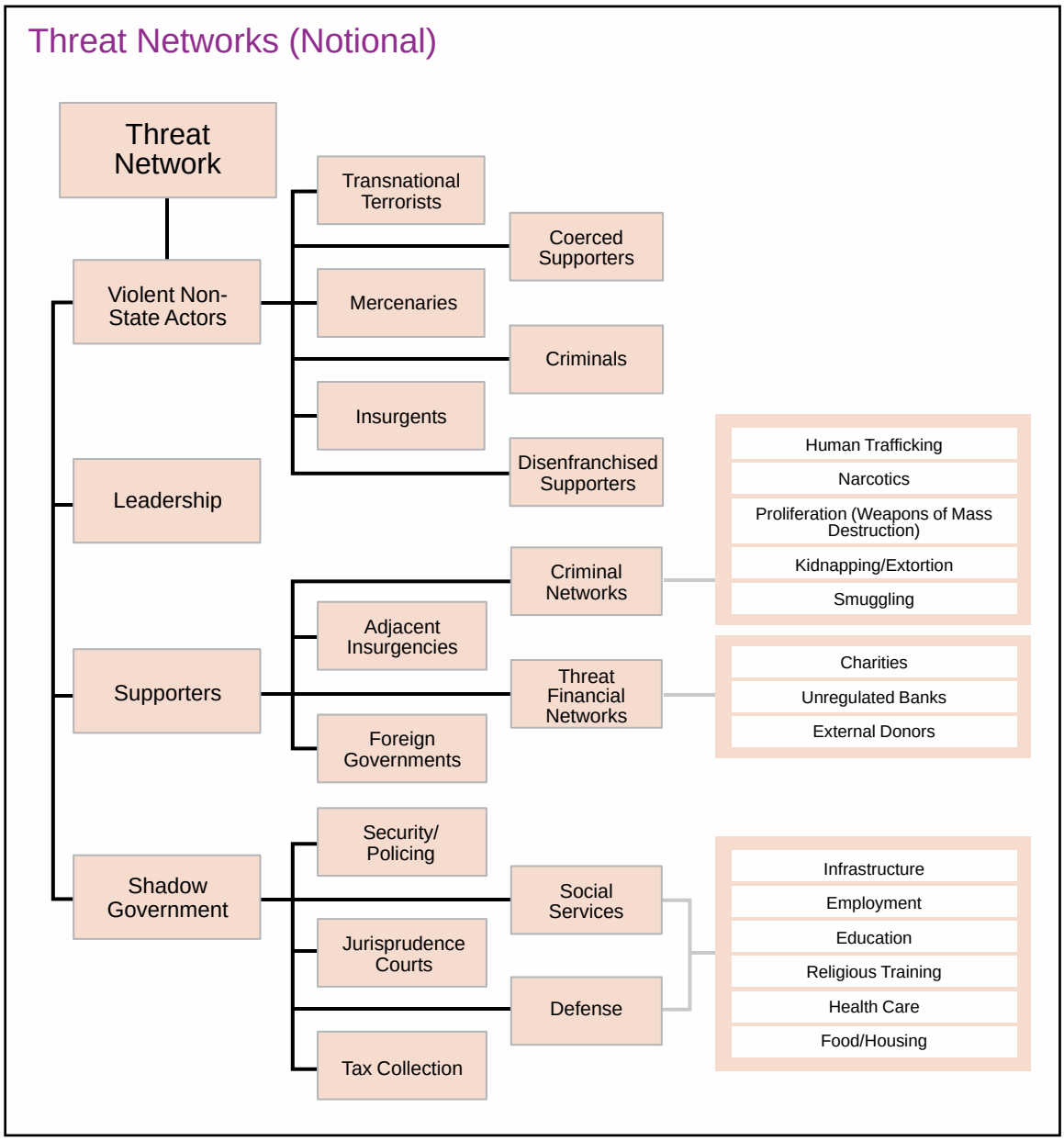


Figure III-6. Threat Networks (Notional)

CHAPTER IV
PLANNING TO COUNTER THREAT NETWORKS

"Analysts must realize that the structure of networks may feature much variety—from simple chain or line networks, to less simple hub or star designs, to complex all-channel designs, any and all of which may be blended into sprawling multi-hub and spider's-web networks."

Networks and Netwars: The Future of Terror[ism], Crime, and Militancy,
5 November 2001, Edited by John Arquilla, David Ronfeldt

1. Joint Intelligence Preparation of the Operational Environment and Threat Networks

a. A comprehensive, multidimensional assessment of the OE will assist commanders and staffs in uncovering threat network characteristics and activities, develop focused operations to attack vulnerabilities, better anticipate both the intended and unintended consequences of threat network activities and friendly countermeasures, and determine appropriate means to assess progress toward stated objectives. JIPOE is the first step in identifying the essential elements that constitute the OE and is used to plan and conduct operations against threat networks. The focus of the JIPOE analysis for threat networks is to help characterize aspects of the networks.

b. Joint force, component, and supporting commands and staffs use JIPOE products to prepare estimates used during mission analysis and selection of friendly courses of action (COAs). Commanders tailor the JIPOE analysis based on the mission. As previously discussed, the best COA may not be to destroy a threat's entire network or cells; friendly or neutral populations may use the same network or cells, and to destroy it would have a negative effect. A thorough JIPOE and network analysis will help commanders choose the most effective approach.

For more details on JIPOE, see JP 2.01-3, Joint Intelligence Preparation of the Operational Environment.

2. Understanding the Threat's Network

a. The threat has its own version of the OE that it seeks to shape to maintain support and attain its goals. In many instances, the challenge facing friendly forces is complicated by the simple fact that significant portions of a population might consider the threat as the "home team." To neutralize or defeat a threat network, friendly forces must do more than understand how the threat network operates, its organization goals, and its place in the social order; they must also understand how the threat is shaping its environment to maintain popular support, recruit, and raise funds. The first step in understanding a network is to develop a network profile through analysis of a network's critical factors.

b. **COG and Critical Factors Analysis (CFA).** One of the most important tasks confronting the JFC and staff during planning is to identify and analyze the threat's network, and in most cases the network's critical factors (see Figure IV-1) and COGs. An objective is

Network Critical Factors Analysis

Critical Factor	Composition	Outputs	Countering Threat Networks Countermeasures
Leaders/ Planners	Core threat leadership/ commanders, third country supporters, financiers	Guidance, ideological direction, attack plans, financing	Combat operations, high-value target interdiction, law enforcement
Fighters/ Operatives/ Followers	Internal (host nation) populace, foreign/ international fighters/ supporters, mercenaries, criminals	Violence, attacks, recruiting, subversion	Interdiction, military information support operations, combat operations, information operations
Intelligence	Spies, local supporters, media, cultural ties	Propaganda, mission planning, information operations	Counterintelligence operations, joint intelligence preparation of the operational environment
Finance	Criminal organizations, corrupt government, local supporters, international supporters	Logistics, personnel, weapons, equipment, bribes, sustainment	Counter threat finance operations, international pressure
Communications	Internet, telecom, couriers, print/radio/television media	Propaganda, mission orders, command and control	Space operations, information operations, military information support operations, electronic intelligence, signals intelligence, measurement and signature intelligence, cyberspace operations
Logistics	Transportation, food, weapons, ammunition, fuel, equipment	Sustainment, combat power	Interagency, multinational, law enforcement, interdiction
Freedom of Movement	Smuggling routes, local knowledge, covertness, anonymity	Survival, offensive capability, longevity, strategic “reach”	Combat operations, foreign internal defense/security force assistance counterintelligence
Safe Havens	Local supporters, foreign supporters, corrupt officials, denied areas, cyberspace	Reconstitution/regeneration, base of operations, forum for promulgating their “cause,” base for recruitment	Intelligence, counterintelligence, international pressure, cyberspace operations
Training	Recruit training, specialized (improvised explosive device, chemical, biological, radiological, and nuclear), foreign fighter support	Fighters, tactics, lessons learned, resiliency	Security cooperation/foreign internal defense/security forces assistance
Ideology*	Religious, political, anarchist	Recruitment, fear, international support	Information operations, foreign humanitarian assistance

* Normally found within terrorist and insurgent networks

Figure IV-1. Network Critical Factors Analysis

always linked to a COG. When analyzing the network and network COGs, it should be remembered that not only will there be different COGs at different levels, but they are likely to be nested. Determining the COG for a network or cell, such as finance or logistics, may

also be necessary for an overall understanding of the threat network. Complicating matters for the JFC is the potential convergence of criminal-terrorist-insurgent networks, all with different COGs.

c. **Network Function Template.** Building a network function template is a method to organize known information about the network associated with structure and functions of the network. By developing a network function template, the information can be initially understood and then used to facilitate CFA. Building a network function template is not a requirement for conducting CFA, but helps the staff to visualize the interactions between functions and supporting structure within a network. Network function templates would need to be developed for individual networks that have specific purposes, but still involve the same individuals since the functions associated with narcotics, as in the example, would be different if the same individuals were involved with improvised explosive devices (IEDs) or something else. See Figure IV-2 for an example of a network function template.

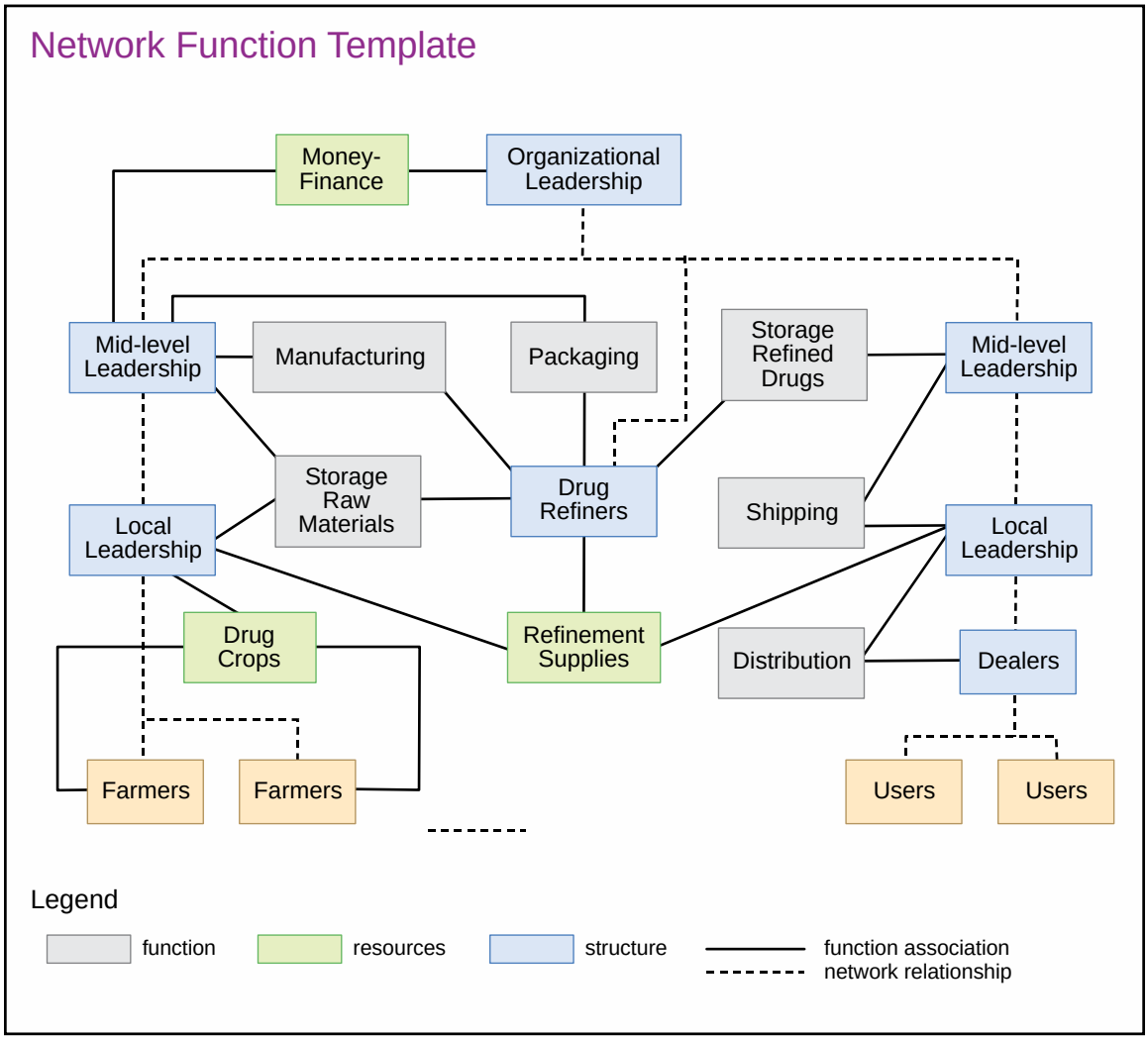


Figure IV-2. Network Function Template

3. Critical Factors Analysis

a. CFA is an analytical framework to assist planners in analyzing and identifying a COG and to aid operational planning. The critical factors are the CCs, critical requirements (CRs), and CVs. The CFA framework was developed to support analysis of adversaries, but has been adapted to support staffs in their analysis of any network within the OE. Since it is understood that networks comprise the human dimension of complex OEs, to gain a better comprehension of the impact of these factors on operation, we must correlate the factors with the analysis of the OE to determine the critical variables of the network to be analyzed (see Figure IV-1). Key terminology for CFA includes:

(1) **COG** for network analysis is a conglomeration of tangible items and/or intangible factors that not only motivates individuals to join a network, but also promotes their will to act to achieve the network's objectives and attain the desired end state. A COG for networks will often be difficult to target directly due to complexity and accessibility.

(2) **CCs** are the primary abilities essential to accomplishing the objective of the network within a given context. Analysis to identify CCs for a network is only possible with understanding the structure and functions of a network, which is supported by other network analysis methods.

(3) **CRs** are the essential conditions, resources, and means the network requires to perform the CC. These things are used or consumed to carry out action, enabling a CC to wholly function. Networks require resources to take action and function. These resources include personnel, equipment, money, and any other commodity that support the network's CCs.

(4) **CVs** are CRs or components thereof that are deficient or vulnerable to neutralization, interdiction, or attack in a manner that achieves decisive results. A network's CVs will change as networks adapt to conditions within the OE. Identification of CVs for a network should be considered during the targeting process, but may not necessarily be a focal point of operations without further analysis.

b. Building a network function template involves several steps:

(1) **Step 1: Identify the network's desired end state.** The network's desired end state is associated with the catalyst that supported the formation of the network. The primary question that the staff needs to answer is what are the network's goals? The following are examples of desired end states for various organizations:

(a) Replacing the government of country X with an Islamic caliphate.

(b) Liberating country X.

(c) Controlling the oil fields in region Y.

(d) Establishing regional hegemony.

(e) Imposing Sharia on village Z.

(f) Driving multinational forces out of the region.

(2) **Step 2: Identify possible ways or actions (COAs) that can attain the desired end state.** This step refers to ways a network can take actions to attain their desired end state through their COAs. Similar in nature to how staffs analyze a conventional force to determine the likely COA that force will take, this must also be done for the networks that are selected for engagement. It is important to note that each network will have a variety of options available to them and their likely COA will be associated with the intent of the members of the network. Examples of ways for some networks may include:

(a) Conducting an insurgency operation or campaign.

(b) Building PN capacity.

(c) Attacking with conventional military forces.

(d) Conducting acts of terrorism.

(e) Seizing the oil fields in Y.

(f) Destroying enemy forces.

(g) Defending village Z.

(h) Intimidating local leaders.

(i) Controlling smuggling routes.

(j) Bribing officials

(3) **Step 3: Identify the functions that the network possesses to take actions.** Using the network function template from previous analysis, the staff must refine this analysis to identify the functions within the network that could be used to support the potential ways or COAs for the network. The functions identified result in a list of CCs. Examples of items associated with the functions of a network that would support the example list of ways identified in the previous step are:

(a) Conducting an insurgency operation or campaign: insurgents are armed and can conduct attacks.

(b) Building PN capacity: forces and training capability available.

(c) Attacking with conventional military forces: military forces are at an operational level with C2 in place.

(d) Conducting acts of terrorism: network members possess the knowledge and assets to take action.

(e) Seizing the oil fields in Y: network possesses the capability to conduct coordinated attack.

(f) Destroying enemy forces: network has the assets to identify, locate, and destroy enemy personnel.

(g) Defending village Z: network possesses the capabilities and presence to conduct defense.

(h) Intimidating local leaders: network has freedom of maneuver and access to local leaders.

(i) Controlling smuggling routes: network's sphere of influence and capabilities allow for control.

(j) Bribing officials: network has access to officials and resources to facilitate bribes

(4) **Step 4: List the means or resources available or needed for the network to execute CCs.** The purpose of this step is to determine the CRs for the network. Again, this is support from the initial analysis conducted for the network, network mapping, link analysis, SNA, and network function template. Based upon the CCs identified for the network, the staff must answer the question what resources must the network possess to employ the CCs identified? The list of CRs can be extensive, depending on the capability being analyzed. The following are examples of CRs that may be identified for a network:

(a) A group of foreign fighters.

(b) A large conventional military.

(c) A large conventional military formation (e.g., an armored corps).

(d) IEDs.

(e) Local fighters.

(f) Arms and ammunition.

(g) Funds.

(h) Leadership.

(i) A local support network.

(5) **Step 5: Correlate CCs and CRs to OE evaluation to identify critical variables.**

(a) Understanding the CCs and CRs for various networks can be used alone in planning and targeting, but the potential to miss opportunities or accept additional risks are

not understood until the staff relates these items to the analysis of the OE. The analysis of the OE conducted as part of planning is used to support the identification of critical variables. During the OE analysis, the staff identifies the critical variables of the OE that are related to the commander's mission and objectives. These variables are used to describe the commander's desired end state and are used to support the assessment of operations. Knowing the critical variables for the networks with help the staff focus efforts on collection and targeting for the network, which is necessary to manage limited assets. The logic tree in Figure IV-3 provides a method to conduct this analysis.

(b) A critical variable may be a CC, CR, or CV for multiple networks. Gaining an understanding of this will occur in the next step of CFA. The following are examples of critical variables that may be identified for networks:

1. A group of foreign fighters is exposed for potential engagement.

2. A large conventional military formation (e.g., an armored corps) is located and likely COA is identified.

3. IED maker and resources are identified and can be neutralized.

4. Local fighters' routes of travel and recruitment are identifiable.

5. Arms and ammunition sources of supply are identifiable.

6. Funds are located and potential exists for seizure.

7. Leadership is identified and accessible for engagement.

8. A local support network is identified and understood through analysis.

(6) **Step 6: Compare and contrast the CRs for each network analyzed.** This step of CFA can only be accomplished after full network analysis has been completed for all selected networks within the OE. To compare and contrast, the information from the analysis of each network must be available. The intent of correlating the critical variables for each network allows for understanding:

(a) Potential desired first- and second-order effects of engagement.

(b) Potential undesired first- and second-order effects of engagement.

(c) Direct engagement opportunities.

(d) Indirect engagement opportunities.

(7) **Step 7: Identify CVs for the network.** Identifying CVs of a network is completed by analyzing each CR for the network with respect to criticality, accessibility, recuperability, and adaptability. This analysis is conducted from the perspective of the network with consideration of threats within the OE that may impact the network being

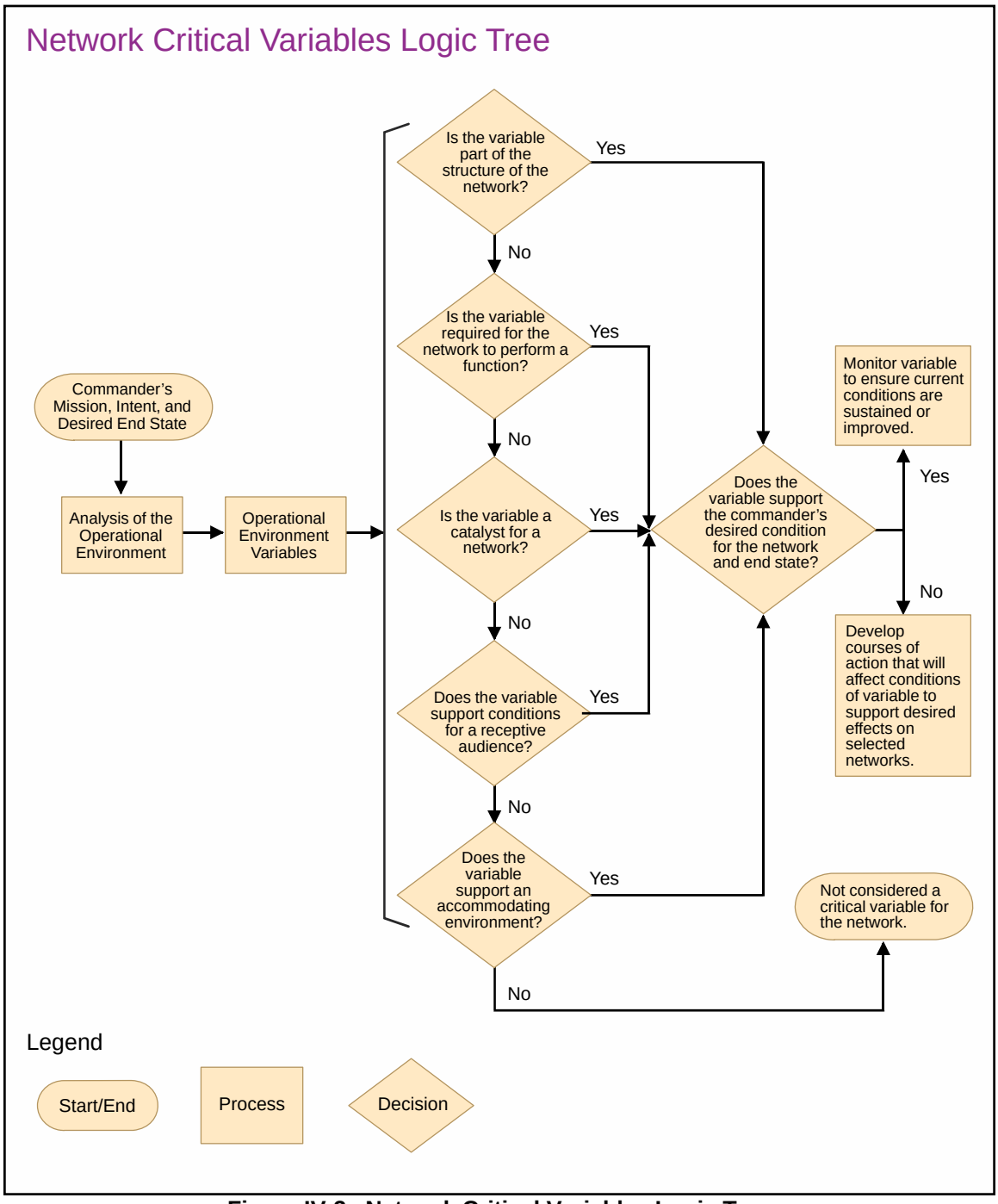


Figure IV-3. Network Critical Variables Logic Tree

analyzed. Conducting the analysis from this perspective allows staffs to identify CVs for any type of network (friendly, neutral, or threat).

(a) **Criticality.** A CR that when engaged by a threat results in a degradation of the network's structure, function or impact on its ability to sustain itself. Criticality considers the importance of the CR to the network and the following questions should be considered when conducting this analysis:

1. What impact will removing the CR have on the structure of the network?

2. What impact will removing the CR have on the functions of the network?

3. What function is affected by engaging the CR?

4. What effect does the CR have on other networks?

5. Is the CR a CR for other networks? If so, which ones?

6. How is the CR related to conditions of sustainment?

(b) **Accessibility.** A CR is accessible when capabilities of a threat to the network can be directly or indirectly employed to engage the CR. Accessibility of the CR in some cases is a limiting factor for the true vulnerability of a CR. There are many cases that a CR is not directly accessible due to battle space boundaries, international borders, or some level of hardened protection. Gaining this understanding as part of CFA will support the staff in deciding on targets to recommend to the commander. The following questions should be considered by the staff when analyzing a CR for accessibility:

1. Where is the CR?

2. Is the CR protected?

3. Is the CR static or mobile?

4. Who interacts with the CR? How often?

5. Is the CR in the operational area of the threat to the network?

6. Can the CR be engaged with threat capabilities?

7. If the CR is inaccessible, are there alternative CRs that if engaged by a threat result in a similar effect on the network?

(c) **Recuperability.** The amount of time that the network needs to repair or replace a CR that is engaged by a threat capability. Analyzing the CR in regard to recuperability is associated to the network's ability to regenerate when components of its structure have been removed or damaged. This plays a role in the adaptive nature of a network, but must not be confused with the last aspect of the analysis for CVs. The following questions should be considered by the staff when analyzing a CR for recuperability:

1. If CR is removed:

   a. Can the CR be replaced?

b. How long will it take to replace?

c. Does the replacement fulfill the network's structural and functional levels?

d. Will the network need to make adjustments to implement the replacement for the CR?

2. If CR is damaged:

a. Can the CR be repaired?

b. How long will it take to repair?

c. Will the repaired CR return the network to its previous structural and functional levels?

(d) **Adaptability.** The ability of a network (with which the CR is associated) to change in response to conditions in the OE brought about by the actions of a threat taken against it, while maintaining its structure and function. Analysis of the CR for adaptability is associated with conditions within the OE as the result of a threat to the network. Since CRs can be any type of resource or conditions necessary for the network to survive and function, this aspect allows the staff to analyze a CR of that nature with respect to its potential vulnerability. Adaptability considers the network's ability to change or modify their functions, modify their catalyst, shift focus on potential receptive audience(s), or make any other changes to adapt to the conditions in the OE. The following questions should be considered by the staff when analyzing a CR for recuperability:

1. Can the CR change its structure while maintaining its function?

2. Is the CR tied to a CC that could cause it to adapt as a normal response to a change in a CC (whether due to hostile engagement or a natural change brought about by a friendly network's adjustment to that CC)?

3. Can the CR be changed to fulfill an emerging CC or function for the network?

4. Visualizing Threat Networks

a. **Mapping the Network.** Mapping threat networks starts by detailing the primary threats (e.g., terrorist group, drug cartel, money-laundering group). Mapping routinely starts with people and places and then adds functions, resources, and activities. Mapping starts out as a simple link between two nodes and progresses to depict the organizational structure (see Figure IV-4). Individual network members themselves may not be aware of the organizational structure. It will be rare that enough intelligence and information is collected to portray an entire threat network and all its cells. Understanding the COGs and critical factors allows intelligence collection and analytic efforts to be optimized to support the planning needs of the JFC. Subsequent operations will generate additional intelligence and

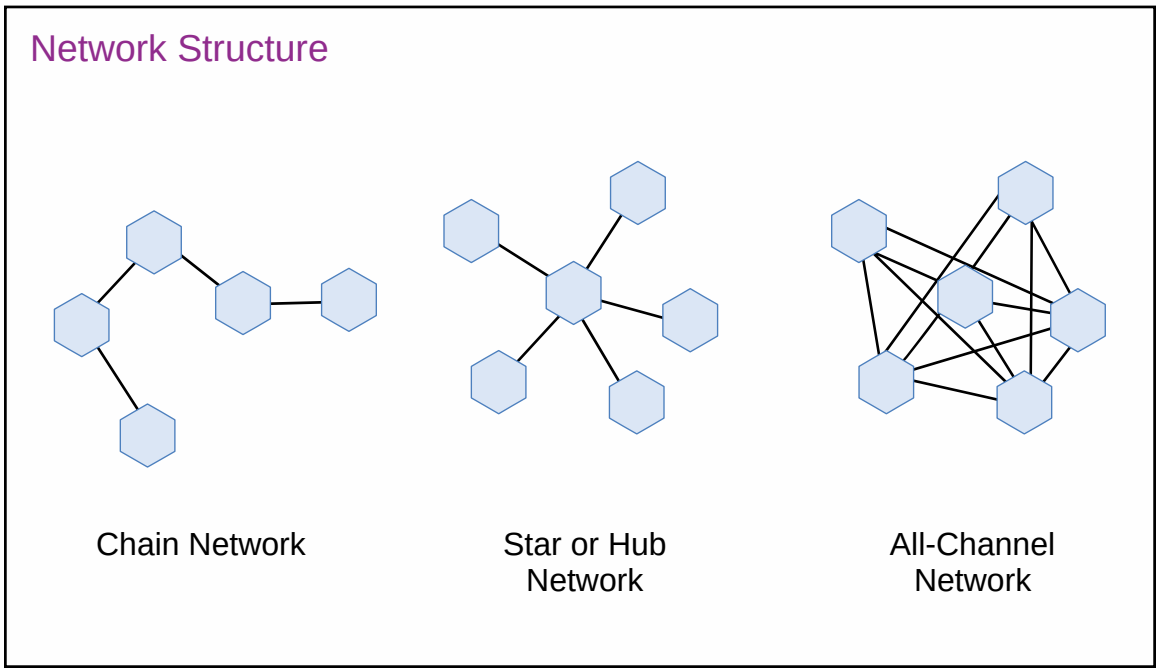


Figure IV-4. Network Structure

exploitation efforts that will yield valuable clues to support additional mapping of networks. This will be a continuous process as the networks themselves transform and adapt to their environment and the joint force operations. To develop and employ theater-strategic options, the commander must understand the series of complex, interconnected relationships at work within the OE. One way of developing solutions is to view these interrelated challenges from a systems perspective. In this systems analysis, consideration needs to be given to the relationship between all of the aspects of the system.

For more information, see Appendix E, "Exploitation in Support of Countering Threat Networks," and Appendix G, "Social Network Analysis."

(1) **Chain Network.** The chain or line network is characterized by people, goods, or information moving along a line of separated contacts with end-to-end communication traveling through intermediate nodes.

(2) **Star or Hub Network.** The hub, star, or wheel network, as in a franchise or a cartel, is characterized by a set of actors tied to a central (but not hierarchical) node or actor that must communicate and coordinate with network members through the central node.

(3) **All-Channel Network.** The all-channel, or full-matrix network, is characterized by a collaborative network of groups where everybody connects to everyone else.

b. **Mapping Multiple Networks.** Each network may be different in structure and purpose. Normally the network structure is fully mapped, and cells are shown as they relate to the larger network. It is time- and labor-intensive to map each network, so staffs should carefully consider the usefulness for how much time and effort they should allocate toward

mapping the supporting networks and where to focus their efforts so that they are both providing a timely response and accurately identifying relationships and critical nodes significant for disruption efforts.

c. **Identify the Influencing Factors of the Network.** Influencing factors of the network (or various networks) within an OE can be identified largely by the conditions created by the activities of the network. These conditions are what influence the behaviors, attitudes, and vulnerabilities of specific populations. Factors such as threat information activities (propaganda) may be one of the major influencers, but so are activities such as kidnapping, demanding protection payments, building places of worship, destroying historical sites, building schools, providing basic services, denying freedom of movement, harassment, illegal drug activities, prostitution, etc. To identify influencing factors, a proven method is to first look at the conditions of a specific population or group, determine how those conditions create/force behavior, and then determine the causes of the conditions. Once influence factors are identified, the next step is to determine if the conditions can be changed and/or if they cannot, determine if there is alternative, viable behavior available to the population or group.

d. To produce a holistic view of threat, neutral, and friendly networks as a whole within a larger OE requires analysis to describe how these networks interrelate. Most important to this analysis is describing the relationships within and between the various networks that directly or indirectly affect the mission. Although the intelligence directorate of a joint staff (J-2) manages the JIPOE process, other directorates and agencies can contribute valuable expertise to develop and assess the complexities of the OE.

e. **Collaboration.** Within most efforts to produce a comprehensive view of the networks, certain types of data or information may not be available to correctly explain or articulate with great detail the nature of relationships, capabilities, motives, vulnerabilities, or communications and movements. It is incumbent upon intelligence organizations to collaborate and share information, data, and analysis, and to work closely with interagency partners to respond to these intelligence gaps. Prior to developing or promoting COAs, decision makers should always be informed about the level of certainty and accuracy of intelligence data and sources; intelligence gaps and ambiguities for aspects of threat networks should be clearly identified and discussed often by interagency partners.

5. Targeting Evaluation Criteria

Once the network is mapped, the JFC and staff identify network nodes and determine their suitability for targeting. A useful tool in determining a target's suitability for attack is the criticality, accessibility, recuperability, vulnerability, effect, and recognizability (CARVER) analysis (see Figure IV-5). CARVER is a subjective and comparative system that weighs six target characteristic factors and ranks them for targeting and planning decisions. CARVER analysis can be used at all three levels of warfare: tactical, operational, and strategic. Once target evaluation criteria are established, target analysts use a numerical rating system (1 to 5) to rank the CARVER factors for each potential target. In a one to five numbering system, a score of five would indicate a very desirable rating while a score of one would reflect an undesirable rating. The analyst must tailor the criteria and rating scheme to

Notional Rating Scale for Part of a Network

Value	Network Affiliations	Criticality	Accessibility	Recuperability	Vulnerability	Effect	Recognizability
5	Key component and associated with several nodes of the network.	Loss would be catastrophic.	Easily accessible away from security.	Extremely difficult to recuperate (1 year).	Joint force definitely has the means and expertise to attack.	Favorable impact on structure, function, and sustainment of the network.	Easily recognizable.
4	Key component and associated with some nodes of the network.	Loss would considerably reduce mission performance.	Easily accessible outside.	Difficult to recuperate (< year).	Joint force probably has the means and expertise to attack.	Favorable impact, no adverse impact.	Easily recognizable with little confusion.
3	Key component and associated with one or two nodes of the network.	Loss would reduce mission performance.	Accessible.	Can recuperate in relatively short time (months).	Joint force may have the means and expertise to attack.	Generally favorable impact, some adverse impact.	Recognizable with some training.
2	Not a key component and associated with several nodes of the network.	Loss may reduce mission performance.	Difficult to gain access.	Easy to recuperate (weeks).	Joint force has little capability to attack.	Some adverse impact.	Hard to recognize with probable confusion.
1	Not a key component and associated with only some nodes of the network.	Loss would not reduce mission performance.	Very difficult to gain access.	Easy to recuperate (days).	Joint force has no capability to attack.	Unfavorable impact, assured adverse impact.	Extremely difficult to recognize without extensive orientation.

NOTE:
For specific targets, more specific target data may be added to each element of the matrix.

Figure IV-5. Notional Rating Scale for Part of a Network

suit the particular strategic, operational, or tactical situation. A notional network-related CARVER analysis is provided in paragraph 6, "Notional Network Evaluation." The CARVER method as it applies to networks provides a graph-based numeric model for determining the importance of engaging an identified target, using qualitative analysis, based on seven factors:

a. **Network Affiliations.** Network affiliations identify each network of interest associated with the CR being evaluated. The importance of understanding the network affiliations for a potential target stems from the interrelationships between networks. Evaluating a potential target from the perspective of each affiliated network will provide the joint staff with potential second- and third-order effects on both the targeted threat networks and other interrelated networks within the OE. For example, the elimination of a key piece of infrastructure will ultimately affect more than just the threat network.

b. **Criticality.** Criticality is a CR that when engaged by a threat results in a degradation of the network's structure, function, or impact on its ability to sustain itself. Evaluating the criticality of a potential target must be accomplished from the perspective of the target's direct association or need for a specific network. Depending on the functions and structure of the network, a potential target's criticality may differ between networks. Therefore, criticality must be evaluated and assigned a score for each network affiliation. If the analyst has completed CFA for the networks of interest, criticality should have been analyzed during the identification of CVs. The output from CFA would simply need to be applied to the CARVER (network) matrix for each potential target.

c. **Accessibility.** A CR is accessible when capabilities of a threat to the network can be directly or indirectly employed to engage the CR. Inaccessible CRs may require alternate target(s) to produce desired effects. The accessibility of a potential target will remain the same, regardless of network affiliation. This element of CARVER does not require a separate evaluation of the potential target for each network. Much like criticality, accessibility will have been evaluated if the analyst has conducted CFA for the network as part of the analysis for the network. The output from CFA would simply need to be applied to the CARVER (network) matrix for each potential target.

d. **Recuperability.** Recuperability is the amount of time that the network needs to repair or replace a CR that is engaged by a threat capability. Recuperability is analyzed during CFA to determine the vulnerability of a CR for the network. Since CARVER (network) is applied to evaluate the potential targets with each affiliated network, the evaluation for recuperability will differ for each network. What affects recuperability is the network's function of regenerating members or replacing necessary assets with suitable substitutes. The output from CFA can be used to complete this part of the CARVER (network) matrix.

e. **Vulnerability.** A target is vulnerable if the operational element has the means and expertise to successfully attack the target. When determining the vulnerability of a target, the scale of the critical component needs to be compared with the capability of the attacking element to destroy or damage it. The evaluation of a potential target's vulnerability is supported by the analysis conducted during CFA and can be used to complete this part of the CARVER (network) matrix. Vulnerability of a potential target will consist of only one value. Regardless of the network of affiliation, vulnerability is focused on evaluating available capabilities to effectively conduct actions on the target.

f. **Effect.** This evaluates the potential effect on the structure, function, and sustainment of a network of engaging the CR as it relates to each affiliated network. The level of effect should consider both the first-order effect on the target itself, as well as the second-order effect on the structure and function of the network. The joint staff should also consider the duration in which the effect will be sustained on the network from engaging the target. Consider the aspects identified in adaptability considerations for CV evaluation during CFA.

g. **Recognizability.** Recognizability is the degree to which a CR can be recognized by an operational element and/or intelligence collection under varying conditions. The recognizability of a potential target will remain the same, regardless of network of affiliation.

Recognizability must be evaluated based upon current information available about the potential target. As collections and analysis of information occurs, potential targets may become more recognizable.

6. Notional Network Evaluation

a. The purpose of conventional target analysis (and the use of CARVER) is to determine enemy critical systems or subsystems to attack to progressively destroy or degrade the adversary's warfighting capacity and will to fight. In operations against threat networks, the commander determines the desired effects on the network (neutralize, disrupt, or defeat, etc.) and whether the capability and opportunity to effectively attack are available.

b. Using network analysis, a commander identifies the critical threat nodes operating within the OE. A CARVER analysis determines the feasibility of attacking each node (ideally simultaneously). While each CARVER value is subjective, detailed analysis allows planners to assign a realistic value. For example, the commander determines that direct lethal strikes on the terrorist training camps are not an option to the JFC due to diplomatic or political constraints or restraints (see Figure IV-6). The commander and the staff then look at other aspects of the network and, for example, determine whether they can disrupt the material needed for training, prevent the movement of trainees or trainers to the training location, or influence other groups to deny access to the area.

c. The JFC and staff methodically analyze each identified network node and assign a numerical rating to each. In this notional example (see Figure IV-7), it is determined that the communications cells and those who finance threat operations provide the best targets to attack. The method in which, and to what extent, the joint force will attack these nodes depends on the desired end state of the CTN activities and the joint force's capabilities and authorities. In this particular case, the JFC will coordinate with other instruments of US national power and international partners to target the communications cell and banking channels and institutions.

d. Planning operations against threat networks does not differ from standard military planning. These operations still support the JFC's broader mission and rarely stand alone. Identifying threat networks requires detailed analysis and consideration for second- and third-order effects. It is important to remember that the threat organization itself is the ultimate target and their networks are merely a means to achieve that. Neutralizing a given network may prove more beneficial to the JFC's mission accomplishment than destroying a single multiuser network node. The most effective plans call for simultaneous operations against networks focused on multiple nodes and network functions. Simultaneity of multiple lines of operation (LOOs) and lines of effort (LOEs) puts a threat on the defensive and more efficiently disrupts plans than piecemeal efforts against individual nodes. CARVER analysis provides one method for network nodal analysis and target selection criteria.

Notional Network Nodes

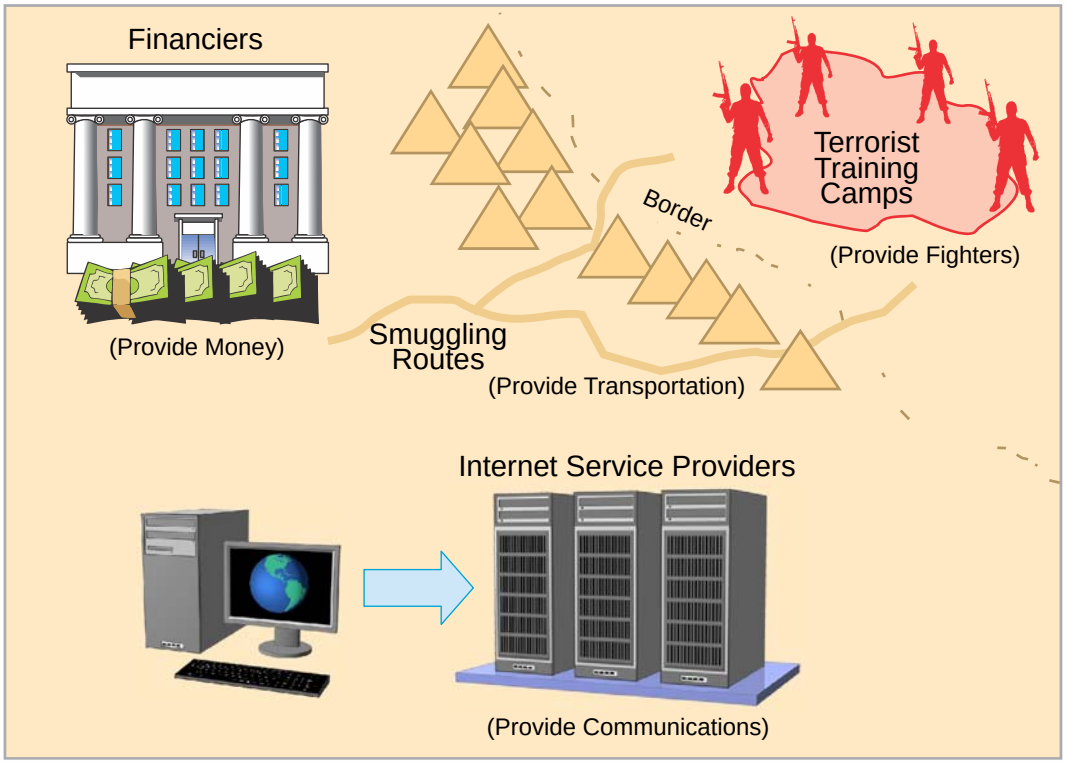


Figure IV-6. Notional Network Nodes

Sample Network Matrix Application

Network Node	N	C	A	R	V	E	R	Total
Smuggling Routes	1	3	3	1	2	3	2	15
Financiers	3	4	3	2	2	5	2	21*
Internet Service Providers	2	3	5	3	5	3	4	25*
Training Camps	1	4	2	2	2	4	3	18

* Based on the analysis, the financiers and Internet service providers have been selected for targeting.

Figure IV-7. Sample Network Matrix Application

7. Countering Threat Networks Through the Planning of Phases

As previously discussed, commanders execute CTN activities across all levels of warfare. JFCs may plan and conduct CTN activities throughout all phases of a given operation. Upon gaining an understanding of the various threat networks in the OE through JPP, JFCs and their staffs develop a series of prudent (feasible, suitable, and acceptable) CTN actions to be executed in conjunction with other phased activities. Given the rapid pace of operations, and constantly changing OE, commanders must be able to execute various CTN activities simultaneously rather than just sequentially. In that commanders may find themselves simultaneously conducting shaping operations in one area, dominating activities in another, and deterring operations in yet another, the JFC's CTN options must be adaptable to multiple situations and thoroughly synchronized. For example, over-allocating finite resources such as signals intelligence (SIGINT) platforms to only one phase of an operation may negatively impact the success in another phase. Threat networks can be countered using a variety of approaches and means. Early in the operation or campaign, the concept of operations will be based on a synchronized and integrated international effort (USG, PNs, and HN) to ensure that conditions in the OE do not empower a threat network and to deny the network the resources it requires to expand its operations and influence. As the threat increases and conditions deteriorate, the plan will adjust to include a broader range of actions, and an increase in the level and focus of targeting of identified critical network nodes: people and activities. Constant pressure must be maintained on the network's critical functions to deny them the initiative and disrupt their operating tempo. Figure IV-8 depicts the notional operation plan phase construct for joint operations. Some phases may not be used during CTN activities.

a. Shape (Phase 0)

(1) Unified action is the key to shaping the OE. The goal is to deny the threat network the resources needed to expand their operations and reduce it to a point where they no longer pose a direct threat to regional/local stability, while influencing the network to reduce or redirect its threatening objectives. Shaping operations against threat networks consist of efforts to influence their objectives, dissuade growth, state sponsorship, sanctuary, or access to resources through the unified efforts of interagency, regional, and international partners as well as HN civil authorities. Actions are taken to identify key elements in the OE that can be used to leverage support for the government or other friendly networks that must be controlled to deny the threat an operational advantage. The OE must be analyzed to identify support for the threat network, as well as that for the relevant friendly and neutral networks. Interagency/international partners help to identify the network's key components, deny access to resources (usually external to the country), and persuade other actors (legitimate and illicit) to discontinue support for the threat. SIGINT, open-source intelligence (OSINT), and human intelligence (HUMINT) are the primary intelligence sources of actionable information. The legitimacy of the government must be reinforced in the operational area. Efforts to reinforce the government seek to identify the sources of friction within the society that can be reduced through government intervention. DOD initiatives could include assisting the HN in conducting site exploitation and establishing a biometric database program for the known threat participants. Operations in phase 0 set conditions for follow-on phases; shape perceptions of threat, friendly, and neutral networks;

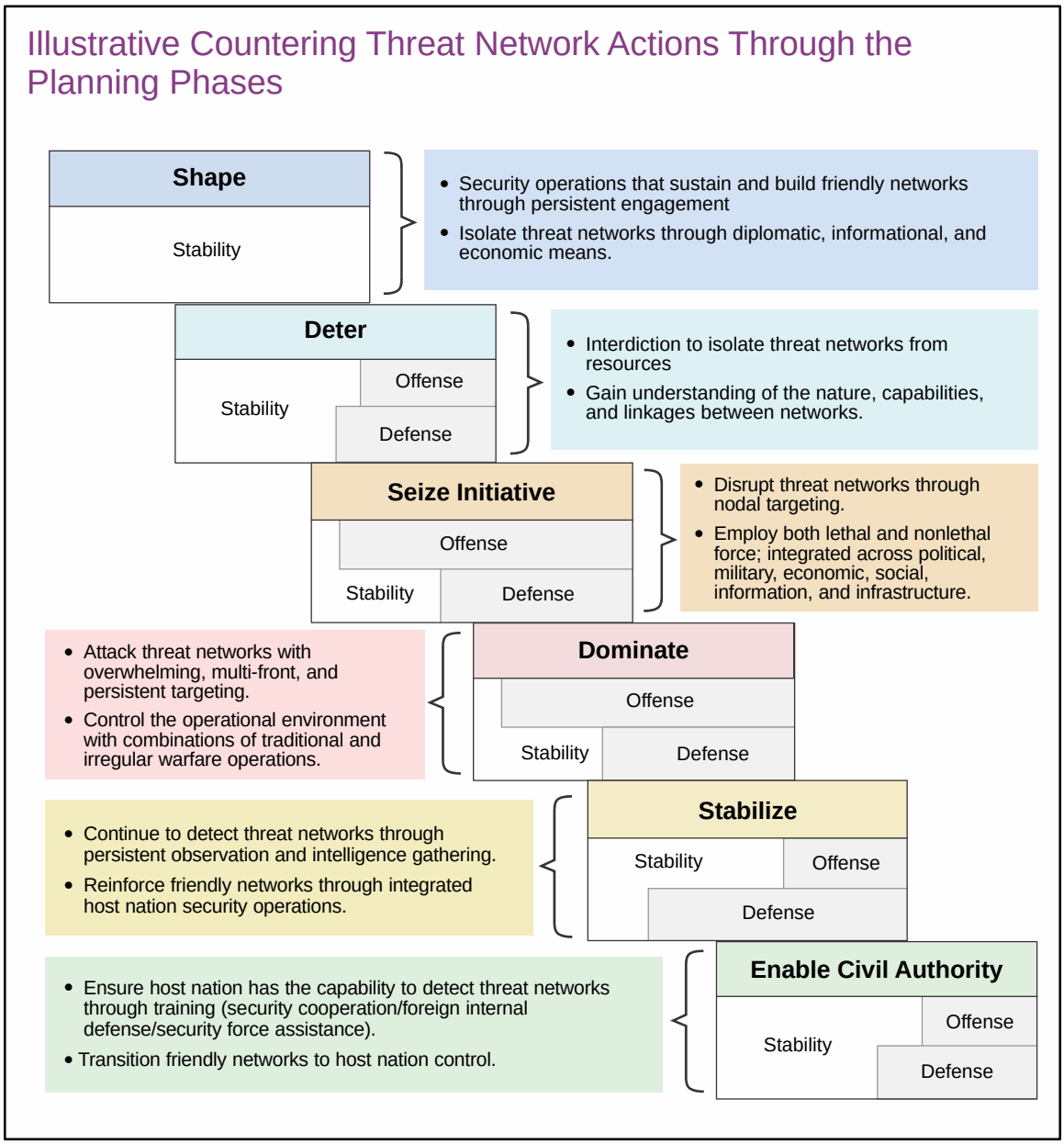


Figure IV-8. Illustrative Countering Threat Network Actions Through the Planning Phases

and attempt to isolate and influence threat networks through diplomatic, informational, military, and economic means. For example, the JFC can shape the OE by influencing the target audience perceptions (neutral network) on the benefits of opposing the threat network and supporting their own government and joint force (friendly network). Many phase I shaping activities need to be coordinated during phase 0 due to extensive legal and interagency requirements. Special technical operations, cyberspace operations, military deception, and MISO are effective IRCs used to shape adversary and potential adversary decision making. Due to competing resources and the potential lack of available IRCs, executing IO during phase 0 can be challenging. For this reason, consideration must be given on how IRCs can be integrated as part of the whole-of-government approach to effectively shape the information environment and to achieve the commander's information

objectives. Shaping operations may also include security cooperation activities designed to strengthen PN or regional capabilities and capacity that contribute to greater stability. Shaping operations should focus on changing the conditions that foster the development of adversaries and threats.

For more information, see Appendix E, "Exploitation in Support of Countering Threat Networks."

(2) During phase 0 (shaping), the J-2's threat network analysis initially provides a broad description of the structure of the underlying threat organization; identifies the critical functions, nodes, and the relationships between the threat's activities and the greater society; and paints a picture of the "on-average" relationships. It seeks to build detail on the network's internal structure and external relations. Some of the CTN actions require long-term and sustained efforts, such as addressing recruitment in targeted communities through development programming. It is essential that the threat is decoupled from support within the affected societies. Critical elements in the threat's operational networks must be identified and disrupted to affect their operating tempo. Even when forces are committed, the commander continues to shape the OE using various means to eliminate the threat and undertake actions, in cooperation with interagency and multinational partners, to reinforce the legitimate government in the eyes of the population.

(3) The J-2 seeks to identify and leverage information sources that can provide details on the threat network and its relationship to the regional/local political, economic, and social structures that can support and sustain it. These information sources include USG departments and agencies, HN (including civil authorities) and PN personnel and organizations, and special operations forces (SOF) with in-country experience. NGOs may serve as a source of information, although in some cases, they may be reluctant to coordinate with the USG because there may be a perception that coordination would compromise their neutrality, independence, and security.

(4) Sharing information and intelligence with partners is paramount since collection, exploitation, and analysis against threat networks requires much greater time than against traditional military adversaries. Information sharing with partners must be balanced with operations security and cannot be done in every instance. Intelligence sharing between CCDRs across regional and functional seams provides a global picture of threat networks not bound by geography. Intelligence efforts within the shaping phase show threat network linkages in terms of leadership, organization, size, scope, logistics, financing, alliances with other networks, and membership. This greatly assists a JFC in understanding threat networks and CTN.

b. **Deter (Phase I).** The intent of this phase is to deter threat network action, formation, or growth by demonstrating partner, allied, multinational, and joint force capabilities and resolve. Many actions in the deter phase include security cooperation activities and IRCs and/or build on security cooperation activities from phase 0. Increased cooperation with partners and allies, multinational forces, interagency and interorganizational partners, international organizations, and NGOs assist in increasing information sharing and provide greater understanding of the nature, capabilities, and linkages of threat networks. Phase I

begins with coordination activities to influence threat networks on multiple fronts. The JFC has the capability to enhance deterrence through unified action by collaborating with all friendly elements and by creating a friendly network of organizations and people with far-reaching capabilities and the ability to respond with pressure at multiple points against the threat network. Deterrent activities executed in phase I also prepare for phase II by conducting actions throughout the OE to isolate threat networks from sanctuary, resources, and information networks and increase their vulnerability to later joint force operations.

c. **Seize Initiative (Phase II).** JFCs seek to seize the initiative through the application of joint force capabilities across multiple LOOs. In traditional combat operations, this involves executing offensive operations at the earliest opportunity, forcing the adversary to offensive culmination, and setting the conditions for decisive operations. In CTN, direct offensive confrontation is often less effective or desirable than indirect approaches. Threat networks rarely present open targets. Destruction of a single node or cell might do little to impact network operations when assessed against the cost of operations and/or the potential for collateral damage. This does not mean that lethal power is never used, but it does mean that the application of force without the intent for death or gross physical destruction integrated across PMESII systems and against multiple threat network links and nodes often will constitute a majority of operations. As in traditional offensive operations against a traditional adversary, various operations create conditions for exploitation, pursuit, and ultimate destruction of those forces and their will to fight.

d. **Dominate (Phase III).** The dominate phase against threat networks focuses on creating and maintaining overwhelming pressure against network leadership, finances, resources, narrative, supplies, and motivation. This multi-front pressure should include diplomatic and economic pressure at the strategic level and informational pressure at all levels. They are then synchronized with military operations conducted throughout the OE and at all levels of warfare to achieve the same result as traditional operations, to shatter enemy cohesion and will. Operations against threat networks are characterized by dominating and controlling the OE through a combination of traditional warfare, irregular warfare, sustained employment of interagency capabilities, and IRCs. Stability activities are conducted in coordination with the HN and DOS as needed to ensure a smooth transition to the next phase and to relieve suffering. In noncombat missions, the joint force's activities seek to control the situation or OE. Phase III activities may establish the conditions for an early favorable conclusion of operations or set the conditions for transition to the next phase.

e. **Stabilize (Phase IV).** The stabilize phase is required when there is no fully functioning, legitimate civilian governing authority present or the threat networks have gained political control within a country or region. In cases where the threat network is government aligned, its defeat in phase III may leave that government intact, and stabilization or enablement of civil authority may not be required. After neutralizing or defeating the threat networks (which may have been functioning as a shadow government), the joint force may be required to unify the efforts of other supporting/contributing multinational, international organization, NGO, or USG department and agency participants into stability activities to provide local governance, until legitimate local entities are functioning. Stabilization efforts help move an HN from instability (and particularly the violent conflict that often accompanies it) to increased stability (and reduced violent conflict)

by maintaining or reestablishing a safe, secure environment and providing essential governmental services, emergency infrastructure reconstruction, or humanitarian relief. Stabilization efforts involve comprehensive efforts by the US and its partners to stabilize nation-states in crisis, build their capabilities and capacity to maintain law and order, protect economic activity, and mitigate the conditions enabling the power and influence of threat networks.

f. **Enable Civil Authority (Phase V).** This phase is predominantly characterized by joint force support to legitimate civil governance in the HN. Depending upon the level of HN capacity, joint force activities during phase V may be at the behest or direction of that authority. The goal is for the joint force to enable the viability of the civil authority and its provision of essential services to the largest number of people in the region. This includes coordinating joint force actions with supporting or supported multinational and HN agencies and continuing integrated finance operations and security cooperation activities to favorably influence the target population's attitude regarding local civil authority's objectives. Building the robust, responsive police forces and judicial and correction systems necessary to establish and maintain the rule of law is of particular importance to resisting the rise of threat networks. This is complemented by representative HN political institutions that can address the basic needs of the population. Ideally, the desired end state is an HN with functioning institutions sufficient to maintain rule of law and prevent the resurgence of threat networks. For more information on stability activities, refer to JP 3-07, *Stability*.

Intentionally Blank

CHAPTER V
ACTIVITIES TO COUNTER THREAT NETWORKS

"Regional players almost always understand their neighborhood's security challenges better than we do. To make capacity building more effective, we must leverage these countries' unique skills and knowledge to our collect[ive] advantage."

General Martin Dempsey, Chairman of the Joint Chiefs of Staff,
***Foreign Policy*, 25 July 2014, The Bend of Power**

1. The Challenge

A threat network can be operating for years in the background and suddenly explode on the scene. Identifying and countering potential and actual threat networks is a complex challenge.

a. Threat networks can take many forms and have many distinct participants from terrorists, to criminal organizations, to insurgents, locally or transnationally based, as shown in Figure V-1. CTN is not a localized fight within identifiable geographic boundaries. Many of our adversaries have spread transnationally to facilitate their operations and increase their survivability. Threat networks may leverage technologies, social media, global transportation and financial systems, and failing political systems to build a strong and highly redundant support system. Operating across a region provides the threat with a much broader array of resources, safe havens, and flexibility to react to attack and prosecute their attacks. To counter a transnational threat, the US and its partners must pursue multinational cooperation and joint operations to achieve disruption and cooperate with HNs within a specified region in order to fully identify, describe, and mitigate via multilateral operations the transnational networks that threaten an entire region and not just individual HNs. Defeating transnational threats requires the synchronization, coordination, and integration of all the instruments of US national power in cooperation with regional and multinational partners.

b. Successful operations are based on the ability of friendly forces to develop and apply a detailed understanding of the structure and interactions of the OE to the planning and execution of a wide array of capabilities to reinforce the HN's legitimacy and neutralize the threat's ability to threaten that society.

2. Targeting Threat 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. The joint targeting cycle outlined in JP 3-60, *Joint Targeting,* has been used to develop Figure V-2, and the phases of that cycle have been associated to steps of the planning and targeting processes.

b. The military end state that is desired is directly related to conditions of the OE. Interrelated human networks comprise the human aspect of the OE, which includes the threat

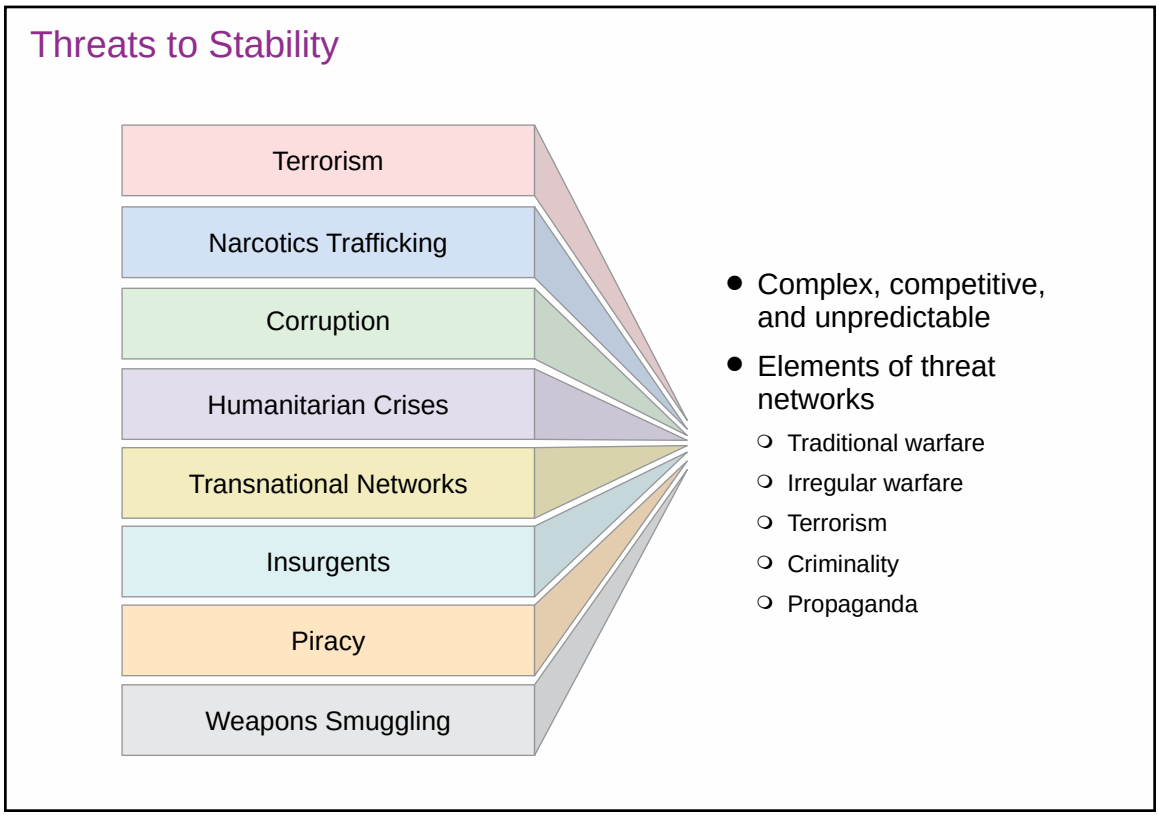


Figure V-1. Threats to Stability

networks that are to be countered. The actual targeting of threat networks begins early in the planning process, since all actions taken must be supportive in achieving the commander's objectives and attaining the end state. To feed the second phase of the targeting cycle, the threat network must be analyzed using network mapping, link analysis, SNA, CFA, and nodal analysis. One major difference that must be noted is that conventional targeting is usually done during military operations/conflict, where much of the threat network targeting is done by USG departments and agencies and PNs under US and international laws, respectively.

c. The second phase of the joint targeting cycle is intended to begin the development of target lists for potential engagement. JIPOE is one of the critical inputs to support the development of these products, but must include a substantial amount of analysis on the threat network to adequately identify the critical nodes, CCs (network's functions), and CRs for the network. This level of information must also be used by the staff to begin developing an assessment plan for the threat network. Similar to developing an assessment plan for operations as part of the planning process, the metrics for assessing networks must be developed early in the targeting cycle.

d. Networks operate as integrated entities—the whole is greater than the sum of its parts. Identifying and targeting the network and its functional components requires patience. A network will go to great lengths to protect its critical components. However, the interrelated nature of network functions means that an attack on one node may have a ripple effect as the network reconstitutes. Whenever a network reorganizes or adapts, it can expose

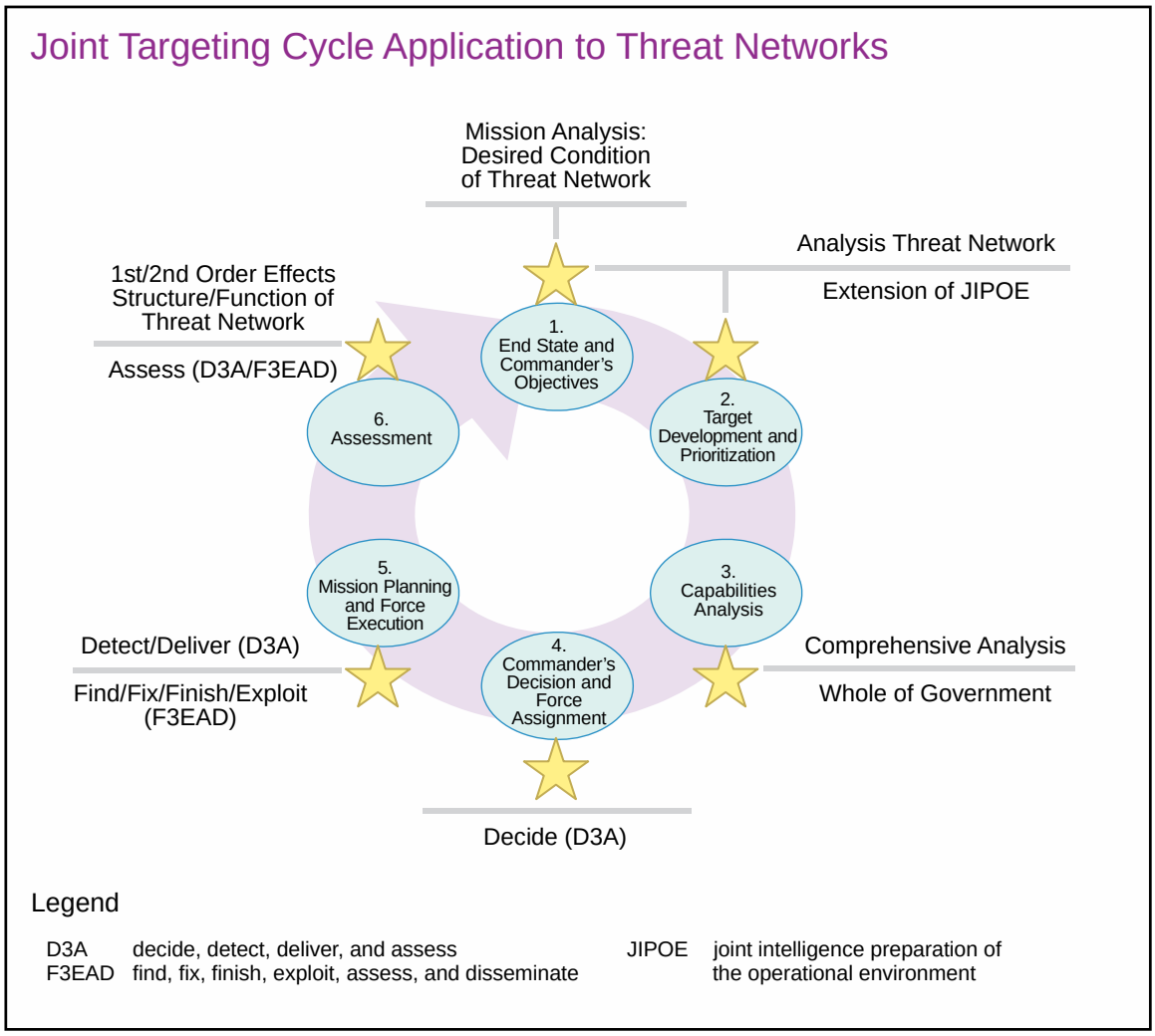


Figure V-2. Joint Targeting Cycle Application to Threat Networks

a larger portion of its members (nodes), relationships (links), and activities. Intelligence collection should be positioned to exploit any effects from the targeting effort, which in turn must be continuous and multi-nodal. Actions to attack CVs should be synchronized and integrated with the overall joint operation or campaign against the enemy. Joint force targeting efforts should employ a comprehensive approach, leveraging military force and civil agency capabilities that keep continuous pressure on multiple nodes and links of the network's structure. There are a few instances when specific CCs and requirements may be separated from the enemy's overall operational patterns and be subject to attack.

e. The analytical products for threat networks support the decision of targets to be added to or removed from the target list and specifics for the employment of capabilities against a target. The staff should consider the following questions when selecting targets to engage within a threat network:

(1) Who or what to target? Network analysis provides the commander and staff with the information to prioritize potential targets. Depending on the effect desired for a

network, the selected node for targeting may be a person, key resource, or other physical object that is critical in producing a specific effect on the network.

(2) What are the effects desired on the target and network? Understanding the conditions in the OE and the future conditions desired to achieve objectives supports a decision on what type of effects are desired on the target and the threat network as a whole. The desired effects on the threat network should be aligned with the commander's intent that support objectives or conditions of the threat network to meet a desired end state.

(3) How will those desired effects be produced? The array of lethal and nonlethal capabilities may be employed with the decision to engage a target, whether directly or indirectly. In addition to the ability to employ conventional weapons systems, staffs must consider nonlethal capabilities that are available.

3. Desired Effects on Networks

a. Damage effects on an enemy or adversary from lethal fires are classified as light, moderate, or severe. Network engagement takes into consideration the effects of both lethal and nonlethal capabilities. Figure V-3 illustrates the first-, second-, and third-order effects to be considered when selecting to engage targets within a network.

b. When commanders decide to generate an effect on a network through engaging specific nodes, the intent may not be to cause damage, but to shape conditions of a mental or moral nature. The intended result of shaping these conditions is to support achieving the commander's objectives. The desired effects selected are the result of the commander's vision on the future conditions for the threat networks and within the OE to achieve objectives. The selection of effects desired on a network is conducted as part of target

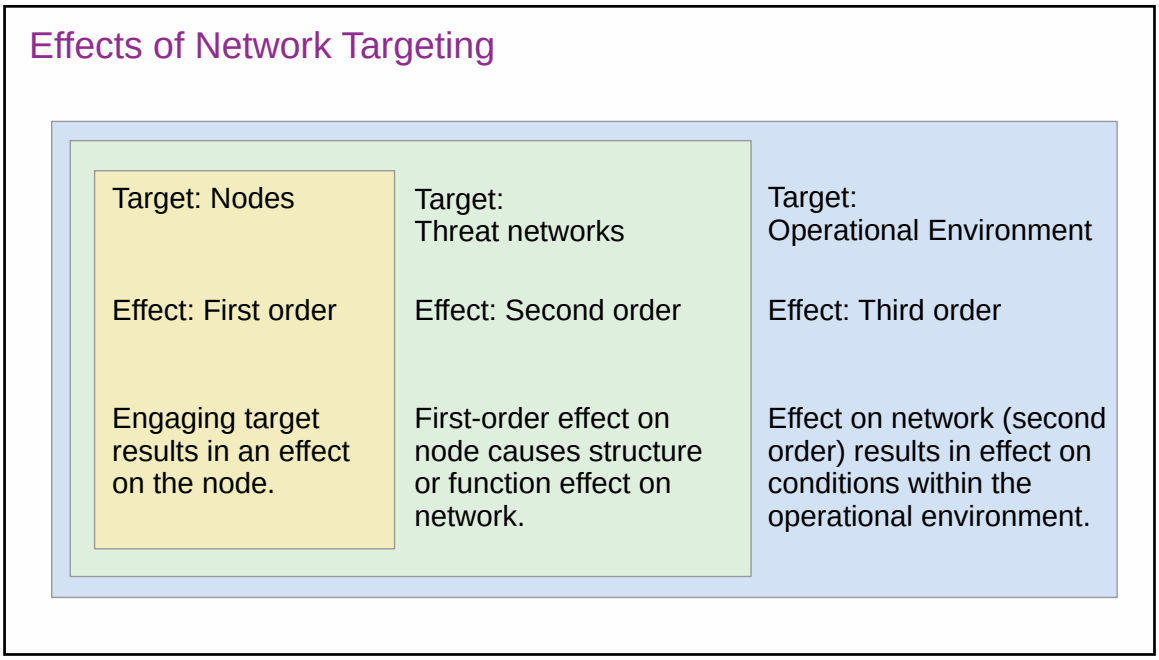


Figure V-3. Effects of Network Targeting

selection, which includes the consideration of capabilities to employ that was identified during capability analysis of the joint targeting cycle. The staff may consider the following effects for CTN. Terms that are used to describe the desired effects of CTN include:

(1) **Neutralize.** Neutralize is a tactical mission task that results in rendering enemy personnel or materiel incapable of interfering with a particular operation. The threat network's structure exists to facilitate its ability to perform functions that support achieving its objectives. Neutralization of an entire network may not be feasible, but through analysis, the staff has the ability to identify key parts of the threat network's structure to target that will result in the neutralization of specific functions that may interfere with a particular operation.

For example, the threat network has continued to influence the population in a geographical area through the means of intimidation and acts of terrorism that interfere with the commander's host nation partnering efforts. The JFC may elect to employ information-related capabilities to message the population for support of friendly forces efforts to counter the threat network. Simultaneously, diplomatic meetings may occur to solicit additional support from the host nation government in that area, while tactical commanders employ additional forces and lethal capabilities in accordance with the established rules of engagement. The balanced application of both lethal and nonlethal capabilities in a comprehensive and synchronized manner is focused to neutralize the function of the threat network in the area that is interfering with the commander's operation.

(2) **Degrade.** To degrade is to reduce the effectiveness or efficiency of a threat. The effectiveness of a threat network is associated with its ability to function as desired to achieve the threat's objectives. Countering the effectiveness of a network may be accomplished by eliminating CRs that the network requires to facilitate an identified CC, identified through the application of CFA for the network.

For example, if a threat network's main function is to pirate vessels near the coast of their operational area, the commander may elect to employ forces to engage the network with lethal capabilities to degrade the network's ability to pirate vessels. Through additional analysis, the staff may have identified that support of that network's enabling function is from the local population that receives benefits from pirated material. Degrading that type of support could be garnered with the application of information-related capabilities in the area and increase in civil affairs missions that undermine the threat network, with the intent of degrading support from the population to the threat network. Additionally, through diplomatic efforts, the HN government may establish laws that forbid the purchase of pirated material, which could be coordinated with an intergovernmental agency.

(3) **Disrupt.** Disrupt is a tactical mission task in which a commander integrates direct and indirect fires, terrain, and obstacles to upset an enemy's formation or tempo, interrupt the enemy's timetable, or cause enemy forces to commit prematurely or attack in a piecemeal fashion. From the perspective of disrupting a threat network, the staff should consider the type of operation being conducted, specific functions of the threat network, and conditions within the OE that can be leveraged and potential application of both lethal and nonlethal capabilities. Additionally, the staff should consider the potential impact and duration of time that disrupting the threat network will present in opportunities for friendly forces to exploit a potential opportunity. Should the disruption result in the elimination of key nodes from the network, the staff must also consider the network's means and time necessary to reconstitute.

For example, a threat network in an area has sustained extensive loses of fighters from operations conducted by tactical units. Analysis of the network and information received from numerous sources have identified that the threat network intends to launch an offensive to reestablish previously held positions. In order to accomplish this, they are actively recruiting and training within the operational area and adjacent countries acting as a safe haven. The commander may elect to locate and engage identified training areas within the operational area, while simultaneous coordination occurs for the employment of information-related capabilities with intergovernmental agencies to mitigate the threat networks recruiting efforts. Additional military engagements could also occur at the diplomatic level to coordinate with government and military leaders of the adjacent countries for potential identification and access to other training sites as part of the commander's area of interest. As the staff plans for operations to disrupt the threat network, they use known information to develop metrics to support an assessment on the effect of disrupting the network. Their primary focus is to understand how operations have disrupted the network and the duration in which the disruption is expected to affect the network.

(4) **Destroy.** Destroy is a tactical mission task that physically renders an enemy force combat ineffective until it is reconstituted. Alternatively, to destroy a combat system is to damage it so badly that it cannot perform any function or be restored to a usable condition without being entirely rebuilt. Destroying a threat network that is adaptive and transnationally established is an extreme challenge that requires the full collaboration of DOD and intergovernmental agencies, as well as coordination with partnered nations. Isolated destruction of cells may be more plausible and could be accomplished with the comprehensive application of lethal and nonlethal capabilities. Detailed analysis of the cell is necessary to establish a baseline (pre-operation conditions) in order to assess if operations have resulted in the destruction of the selected portion of a network.

For example, a threat network cell responsible for conducting improvised explosive device attacks in an area has been identified by analysts and geospatially associated. Through the support of biometrics, identities of all cell members have been confirmed. The commander has elected to employ information-related capabilities to offer rewards for information on the individuals, which is supported by host nation forces through close diplomatic coordination. Tactical units simultaneously plan to exit synchronized cordon and search operations for all known individuals of the cell and execute on a timeline established by the staff. The result of the operations was the killing or capture of all known cell members and is assessed as effectively destroying that portion of the network.

(5) **Defeat.** Defeat is a tactical mission task that occurs when a threat network or enemy force has temporarily or permanently lost the physical means or the will to fight. The defeated force's commander or leader is unwilling or unable to pursue that individual's adopted COA, thereby yielding to the friendly commander's will, and can no longer interfere to a significant degree with the actions of friendly forces. Defeat can result from the use of force or the threat of its use. Defeat manifests itself in some sort of physical action, such as mass surrenders, abandonment of positions, equipment and supplies, or retrograde operations. A commander or leader can create different effects against an enemy to defeat that force.

Identifying the defeat of a threat network is difficult due to the nature of how a threat network is organized and its ability to be located across a broad geographic area. An example of defeating a threat network is associated with Operation PHANTOM FURY, conducted by American, Iraqi, and British forces in November and December 2004. The success of this operation resulted in a defeat of the threat network in Fallujah and the insurgent's loss of physical means to fight. However, the threat network in Iraq was still capable in other geographical areas of Iraq, which resulted in friendly forces conducting subsequent operations. Analyzing if an entire threat network has been defeated will require an understanding of the network's structure and functions, which must consider physical locations of the threat network. Operation PHANTOM FURY was successful in defeating a portion of the threat network and was part of a larger campaign plan.

(6) **Deny.** Deny is an action to hinder or deny the enemy the use of territory, personnel, or facilities to include destruction, removal, contamination, or erection of obstructions. An example of deny is to destroy the threat's communications equipment as a means of denying his use of the electromagnetic spectrum. However, the duration of denial will depend on the enemy's ability to reconstitute.

(7) **Divert.** To divert is to turn aside or from a path or COA. A diversion is the act of drawing the attention and forces of a threat from the point of the principal operation; an attack, alarm, or feint diverts attention. Diversion causes threat networks or enemy forces to consume resources or capabilities critical to threat operations in a way that is advantageous to friendly operations. Diversions draw the attention of threat networks or enemy forces away from critical friendly operations and prevent threat forces and their support resources from being employed for their intended purpose. Diversions can also cause more circuitous routing along lines of communication, resulting in delays for enemy forces.

Threat networks within Somalia responsible for pirating vessels navigating within the region present a constant threat to international commerce. Although the networks realize that the cargo on these vessels provide a source of income, they have also taken advantage of holding the crew of pirated vessels as hostages to be traded for high ransoms. As the threat increased in the area, the US increased security by positioning naval assets within the area and have been successful in diverting the threat networks from pirating vessels in patrolled areas. The threat networks may elect to conduct their primary course of action by accepting additional risk of engagement by naval forces or divert to an alternative course of action to generate income for their network.

4. Engagement Strategies

a. **Counter Resource.** A counter-resource approach can progressively weaken the threat's ability to conduct operations in the OE and require the network to seek a suitable substitute to replace eliminated or constrained resources. Like a military organization, a threat's network or a threat's organization is more than its C2 structure. It must have an assured supply of recruits, food, weapons, and transportation to maintain its position and grow. While the leadership provides guidance to the network, it is the financial and logistical infrastructure that sustains the network. Most threat networks are transnational in nature, drawing financial support, material support, and recruits from a worldwide audience. While the joint force's intelligence apparatus may be able to target a reasonable portion of the threat's network's sustainment base and activities in the operational area, lasting results require active cooperation by interagency and international partners directed against the network's transnational activities. A counter resource approach focuses on friendly multi-nodal counter network actions that deprive the network of resources needed to consistently and freely conduct operations.

b. **Decapitation.** Decapitation is the removal of key nodes within the network that are functioning as leaders. Targeting leadership is designed to impact the C2 of the network. Detailed analysis of the network may provide the staff with an indication of how long the network will require to replace leadership once they are removed from the network. From a historical perspective, the removal of a single leader from an adaptive human network has resulted in short-term effects on the network. Capturing a member of the network that holds a leadership position may provide additional information and insights on the network. Staffs

should also consider the potential impact of individuals who will replace a leader that is removed. When targeting the nodes, links, and activities of threat networks, the JFC should consider the second- and third-order effects on friendly and neutral groups that share network and cell functions. Additionally, the ripple effects throughout the network and its cells should be considered. The effects of engaging a network must be analyzed and considered prior to making a decision to engage. An example of the depth and breadth of analysis necessary when targeting a threat network is illustrated in Figure V-4. It must be remembered that leadership is only one of many targets analyzed by DOD and interagency partners for lethal and nonlethal engagement and is often merely an entry point into discovering the entire network.

c. **Fragmentation.** A fragmentation strategy is the surgical removal of key nodes of the network that produces a fragmented effect on the network with the intent to disrupt the network's ability to function. Although fragmenting the network will result in immediate effects, the staff must consider when this type of strategy is appropriate. Elimination of nodes within the network may have impacts on collection efforts, depending on the node being targeted. The flow of information, as well as aspects of C2, are directly related to the understanding of the relationships that exist within the network. Visualizing the network's structure can be accomplished using products from network analysis. Figure V-5 is an example of a network analysis product that can be provided to the staff prior to and after targeting. As discussed earlier, staffs must develop an assessment plan to understand the effects of engaging networks to realize if the JFC's objectives are being achieved.

d. **Counter-Messaging.** Threat networks form around some type of catalyst that motivates individuals from a receptive audience to join a network. The challenging aspect of a catalyst is that individuals will interpret and relate to it in their own manner. There may be some trends among members of the network that relate to the catalyst in a similar manner; this perspective is not accurate for all members of the network. Threat networks have embraced the ability to project their own messages using a number of social media sites. These messages support their objectives and are used as a recruiting tool for new members. Countering the threat network's messages is one aspect of countering a threat network. IO planners will work with select intergovernmental agencies to develop the appropriate counter messages as part of the employment of IRCs. These messages are designed not only to counter the threat's message, but also to solicit support from neutral networks for friendly forces. Staffs should reference JP 3-13, *Information Operations,* for additional information.

5. Targeting

a. At the tactical level, the focus is on executing operations targeting nodes and links. Accurate, timely, and relevant intelligence supports this effort. Tactical units use this intelligence along with their procedures to conduct further analysis, template, and target networks. In a COIN operation, for example, friendly operations include efforts to secure the population, strengthen HN security forces, and counter the enemy's ideology and propaganda. These actions contribute to the overall CTN effort by serving to isolate the threat from its network supporters, suppliers, and sympathizers.

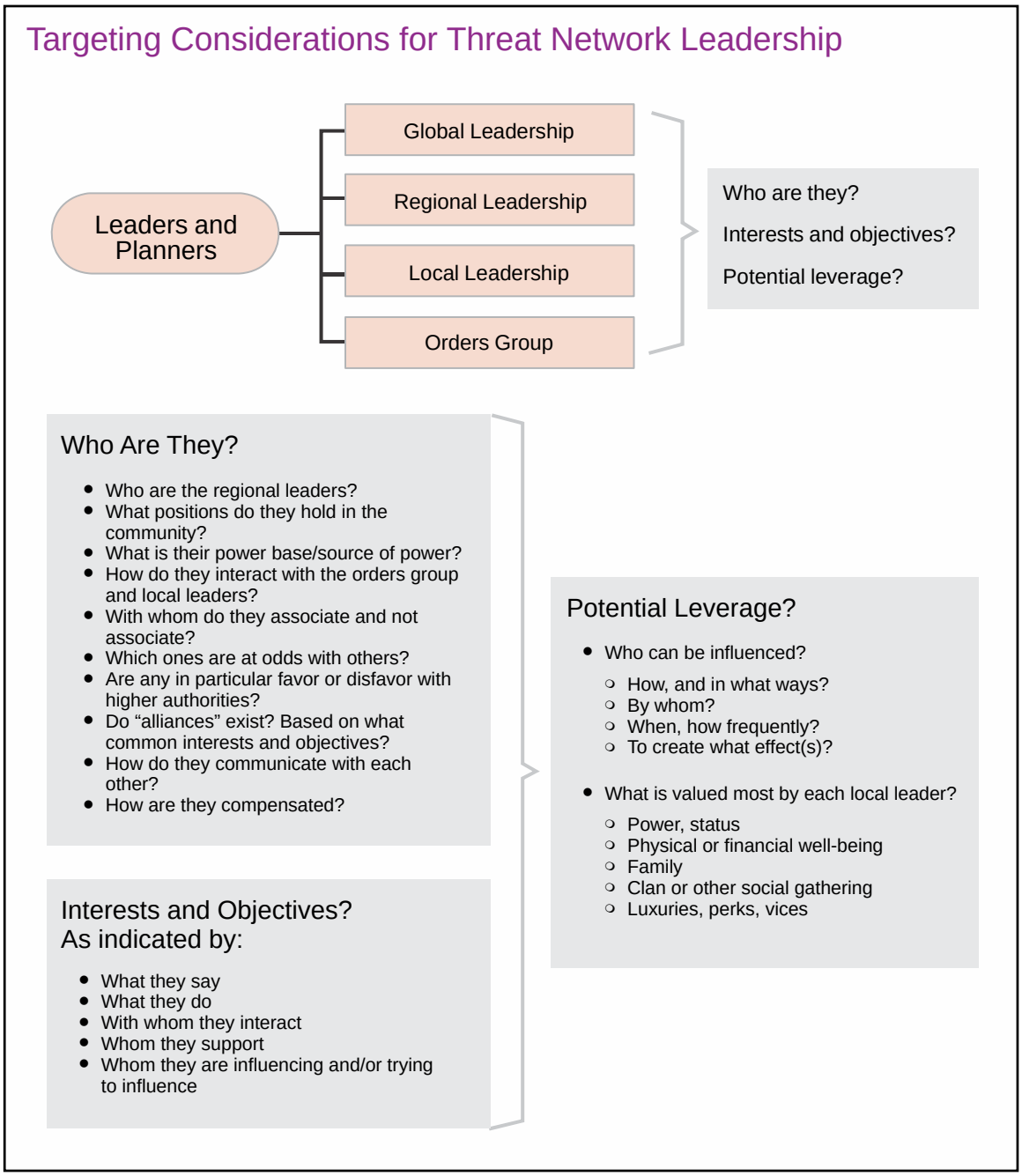


Figure V-4. Targeting Considerations for Threat Network Leadership

b. Targeting of threat network CVs is driven by the situation, the accuracy of intelligence, and the ability of the joint force to quickly execute various targeting options to create the desired effects. In COIN operations, high-priority targets may be individuals who perform tasks that are vulnerable to detection/exploitation and impact more than one CR. It may be more beneficial to analyze the next node up the financial network who is securing funds for the next payday. Timing is everything when attacking a network, as opportunities for attacking identified CVs may be limited.

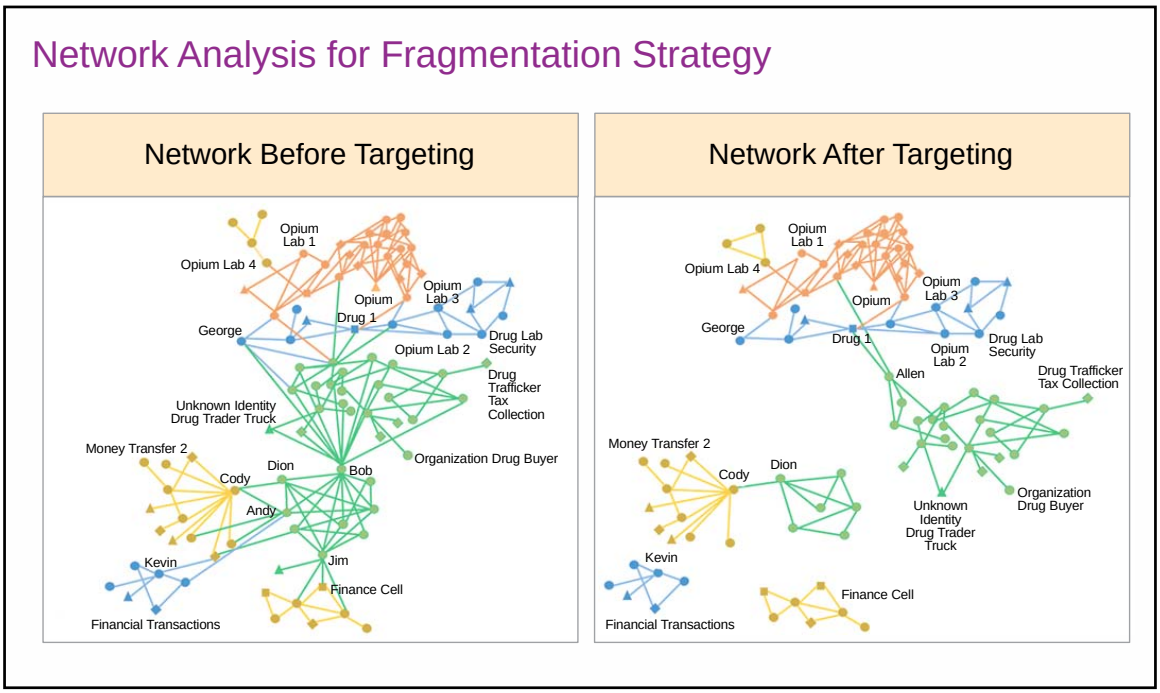


Figure V-5. Network Analysis for Fragmentation Strategy

For additional discussion on threat networks and their functions, see Appendix F, "The Clandestine Characteristics of Threat Networks."

c. CTN targets can be characterized as targets that must be engaged immediately because of the significant threat they represent or the immediate impact they will make related to the JFC's intent, key nodes such as high-value individuals, or longer-term network infrastructure targets (caches, supply routes, safe houses) that are normally left in place for a period of time to exploit them. Resources to service/exploit these targets are allocated in accordance with the JFC's priorities, which are constantly reviewed and updated through the command's joint targeting process. This allocation is validated through a daily asset synchronization meeting of the joint targeting coordination board. The targeting method used to engage these targets is either deliberate or dynamic.

(1) **Dynamic Targeting.** A time-sensitive targeting cell consisting of operations and intelligence personnel with direct access to engagement means and the authority to act on pre-approved targets is an essential part of any network targeting effort. Dynamic targeting facilitates the engagement of targets that have been identified too late or not selected in time to be included in deliberate targeting and that meet criteria specific to achieving the stated objectives.

(2) **Deliberate Targeting.** The joint fires cell is tasked to look at an extended timeline for threats and the overall working of threat networks. With this type of deliberate investigation into threat networks, the cell can identify catalysts to the threat network's operations and sustainment that had not traditionally been targeted on a large scale. With a constant flow of intelligence about individual actions and movements, the cell will examine what facilitated any number of events, such as terrorist, criminal, and narcotics activities;

failed public services; and governmental corruption. It will also focus on how these events ultimately impacted not only the JFC's operations in support of the overall joint operation/campaign plan, but also international development and aid efforts and the local government and population. This type of analysis will usually reveal a web of interconnected relationships and associations of which only a small percentage can be affected by lethal targeting and actions. When augmented with appropriate USG department and agency, special operations, and intelligence analysts, the joint fires cell can plan to exploit the threat network relationships and associations using all available means to reduce their contribution to the overall effectiveness of the network. The J-2, in conjunction with the joint targeting working group, completes target system analysis and target development to nominate CTN-related targets to the joint targeting coordination board for approval and subsequent execution on an on-call or deliberate basis.

d. The joint targeting cycle supports the development and prosecution of threat networks. Land and maritime force commanders normally use an interrelated process to enhance joint fire support planning and interface with the joint targeting cycle known as the decide, detect, deliver, and assess (D3A) methodology. D3A incorporates the same fundamental functions of the joint targeting cycle as the find, fix, track, target, engage, and assess (F2T2EA) process and functions within phase 5 of the joint targeting cycle. The D3A methodology facilitates synchronizing maneuver, intelligence, and fire support. The F2T2EA and F3EAD methodologies support dynamic targeting. While the F3EAD model was developed for personality-based targeting, it can only be applied once the JFC has approved the joint integrated prioritized target list. Depending on the situation, multiple methodologies may be required to create the desired effect.

e. **F3EAD.** F3EAD facilitates the targeting not only of individuals when timing is crucial, but also more importantly the generation of follow-on targets through timely exploitation and analysis. F3EAD facilitates synergy between operations and intelligence as it refines the targeting process. It is a continuous cycle in which intelligence and operations feed and support each other. It assists to:

(1) Analyze the threat network's ideology, methodology, and capabilities; helps template its inner workings: personnel, organization, and activities.

(2) Identify the links between enemy CCs and CRs and observable indicators of enemy action.

(3) Focus and prioritize dedicated intelligence collection assets.

(4) Provide the resulting intelligence and products to elements capable of rapidly conducting multiple, near-simultaneous attacks against the CVs.

(5) Provide an ability to visualize the OE and array and synchronize forces and capabilities.

f. The F3EAD process is optimized to facilitate targeting of key nodes and links tier I (enemy top-level leadership, for example) and tier II (enemy intermediaries who interact with the leaders and establish links with facilitators within the population). Tier III

individuals (the low-skilled foot soldiers who are part of the threat) may be easy to reach and provide an immediate result but are a distraction to success because they are easy to replace and their elimination is only a temporary inconvenience to the enemy. F3EAD can be used for any network function that is a time-sensitive target.

g. The F3EAD process relies on the close coordination between operational planners and intelligence collection 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 goal is to quickly conduct exploitation and facilitate follow-on targeting of the network's critical nodes.

For a detailed explanation of F3EAD targeting, see JP 3-15.1, Counter-Improvised Explosive Device Operations.

For more information, see Appendix E, "Exploitation in Support of Countering Threat Networks."

6. Targeting Considerations

a. There is no hard-and-fast rule for allocating network targets by echelon. The primary consideration is how to create the desired effect against the network as a whole. Generally network targets fall into one of three categories: individual targets, group targets, and organizational targets. The joint force staff and Service components, through the joint targeting process, determine and recommend network targets for JFC approval. These are complemented by the targeting of nodes and links by interagency partners, HN, and PNs.

b. An objective of network targeting may be to deny the threat its freedom of action and maneuver by maintaining constant pressure through unpredictable actions against the network's leadership and critical functional nodes. It is based on selecting the right means or combination thereof to neutralize the target while minimizing collateral effects.

c. While material targets can be disabled, denied, destroyed, or captured, humans and their interrelationships or links are open to a broader range of engagement options by friendly forces. For example, when the objective is to neutralize the influence of a specific group, it may require a combination of tasks to create the desired effect.

7. Lines of Effort by Phase

a. Targeting is a continuous and evolving process. As the threat adjusts to joint force activities, joint force intelligence collection and targeting must also adjust. Employing a counter-resource (logistical, financial, and recruiting) approach should increase the amount of time it will take for the organization to regroup. It may also force the threat to employ its hidden resources to fill the gaps, thus increasing the risk of detection and exploitation. During each phase of an operation or campaign against a threat network, there are specific actions that the JFC can take to facilitate countering threats network (see Figure V-6). However, these actions are not unique to any particular phase, and must be adapted to the

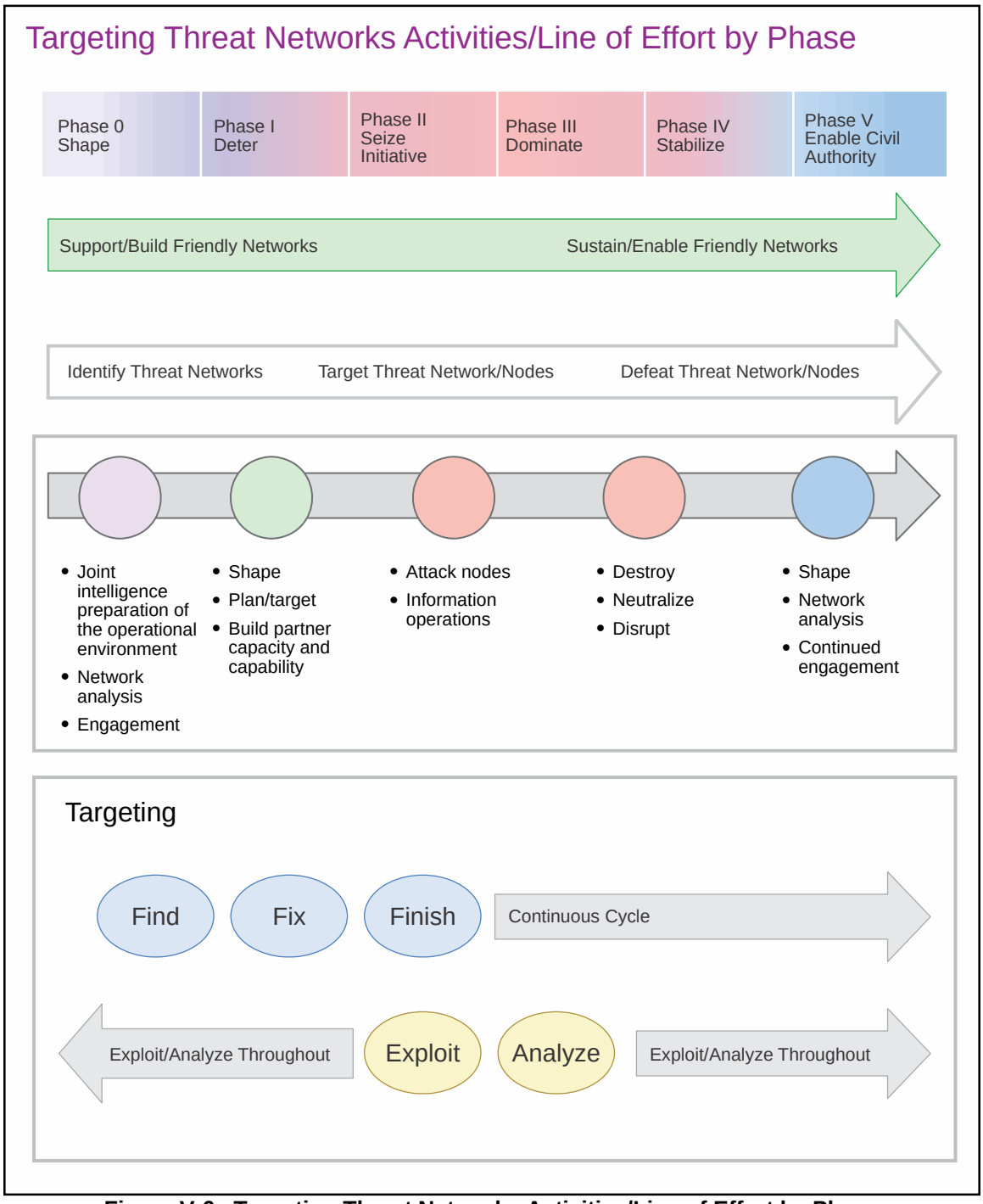


Figure V-6. Targeting Threat Networks Activities/Line of Effort by Phase

specific requirements of the mission and the OE. The simplified model in Figure V-6 is illustrative rather than a list of specific planning steps.

b. During phase 0, analysis provides a broad description of the structure of the underlying threat organization, identifies the critical functions and nodes, and identifies the relationships between the threat's activities and the greater society. US forces are commonly

deployed in support of theater security objectives. These forces provide a foundation of information about the region to include very specific information that falls into the categories of PMESII. Actions against the network may include targeting of the threat's transnational resources (money, supply, safe havens, recruiting); identifying key leadership; providing resources to facilitate PNs and regional efforts; shaping international and national populations' opinions of friendly, neutral, and threat groups; and isolating the threat from transnational allies.

c. During phase I, CTN activities seek to provide a more complete picture of the conditions in the OE. Forces already employed in theater may be leveraged as sources of information to help build a more detailed picture. New objectives may emerge as part of phase I, and forces deployed to help achieve those objectives contribute to the developing common operational picture. A network analysis is conducted to identify a target array that will keep the threat network off balance through multi-nodal attack operations. Actions against the threat network include targeting internal and external resources (money, supply, safe havens, recruiting) identifying key internal and external leadership; providing resources to facilitate PNs and regional efforts; and shaping international and national populations' opinions of the threat.

d. During phase II, CTN activities concentrate on developing previously identified targets, position intelligence collection to exploit effects, and continue to refine the description of the threat and its supporting network. Actions against the threat continue and include targeting of the organization's infrastructure using coordinated, preferably multimodal attacks, as well as IRCs directed to support government and persuade neutrals.

e. During phase III, CTN activities are characterized by increased physical contact and a sizable ramp-up in a variety of intelligence and information collection assets. The focus is on identifying, exploiting, and targeting the clandestine core of the network. Intelligence collection assets and specialized analytical capabilities provide around the clock support to committed forces. Actions against the network continue and feature a ramp-up in resource denial; key leaders and activities are targeted for elimination; and constant multi-nodal pressure is maintained. Activities continue to convince neutral networks of the benefits of supporting the government and dissuade threat sympathizers from providing continued support to threat networks. Ultimately, the network is isolated from support and its ability to conduct operations is severely diminished.

f. During phase IV, CTN activities focus on identifying, exploiting, and targeting the clandestine core of the network for elimination. Intelligence collection assets and specialized analytical capabilities continue to provide support to committed forces; the goal is to prevent the threat from recovering and regrouping. Phase III CTN activities continue.

g. During phase V, CTN activities continue to identify, exploit, and target the clandestine core of the network for elimination and to identify the threat network's attempts to regroup and reestablish control. CTN activities continue with a goal of ensuring that the network does not have the resources to reemerge. Phase III counter network activities continue.

8. Theater Concerns in Countering Threat Networks

a. Many threat networks are transnational, recruiting, financing, and operating on a global basis. These organizations cooperate on a global basis when necessary to further their respective goals. Theater commanders need to be aware of the relationships among these networks and identify the basis for their particular connection to a geographic combatant commander's (GCC's) area of responsibility (AOR). Actions taken in one AOR can impact networks in other AORs, for example, disrupting a heroin shipment at its source in another theater that a terrorist group had purchased to fund near-term operations.

b. In developing their CCMD campaign plans, CCDRs need to be aware of the complex relationships that characterize networks and leverage whole-of-government resources to identify and analyze networks to include their relationships with or part of known friendly, neutral, or threat networks. Militaries are interested in the activities of criminal organizations because these organizations provide material support to insurgent and terrorist organizations that also conduct criminal activities (e.g., kidnapping, smuggling, extortion). By tracking criminal organizations, the military may identify linkages (material and financial) to the threat network, which in turn might become a target. Figure V-7 is a notional example of how a seemingly innocent product can have connections in more than one AOR.

9. Countering Threat Networks Through Military Operations and Activities

Some threat networks may prefer to avoid direct confrontation with law enforcement and military forces. Activities associated with military operations at any level of conflict can have a direct or indirect impact on threats and their supporting networks. Even if not directly focusing on a threat, the military can be called upon to conduct a wide variety of activities that can directly or indirectly alter the OE to the detriment of a threat. For example, stability and foreign humanitarian assistance operations may address the root causes that facilitate threat recruiting and dissatisfaction with the government. Conversely, there are activities, such as CT and counter proliferation, that specifically focus on threat organization and are designed to destroy it. Commanders must be prepared to address threats, no matter what their primary mission, and take steps to ensure the success of the overall mission.

10. Operational Approaches to Countering Threat Networks

a. There are many ways to integrate CTN into the overall plan. In some operations, the threat network will be the primary focus of the operation. In others, a balanced approach through multiple LOOs and LOEs may be necessary, ensuring that civilian concerns are met while protecting them from the threat networks' operators. Figure V-8 is based on operating against an insurgent network but is adaptable to other threats. In all CTN activities, lethal actions directed against the network should also be combined with nonlethal actions to support the legitimate government and persuade neutrals to reject the adversary.

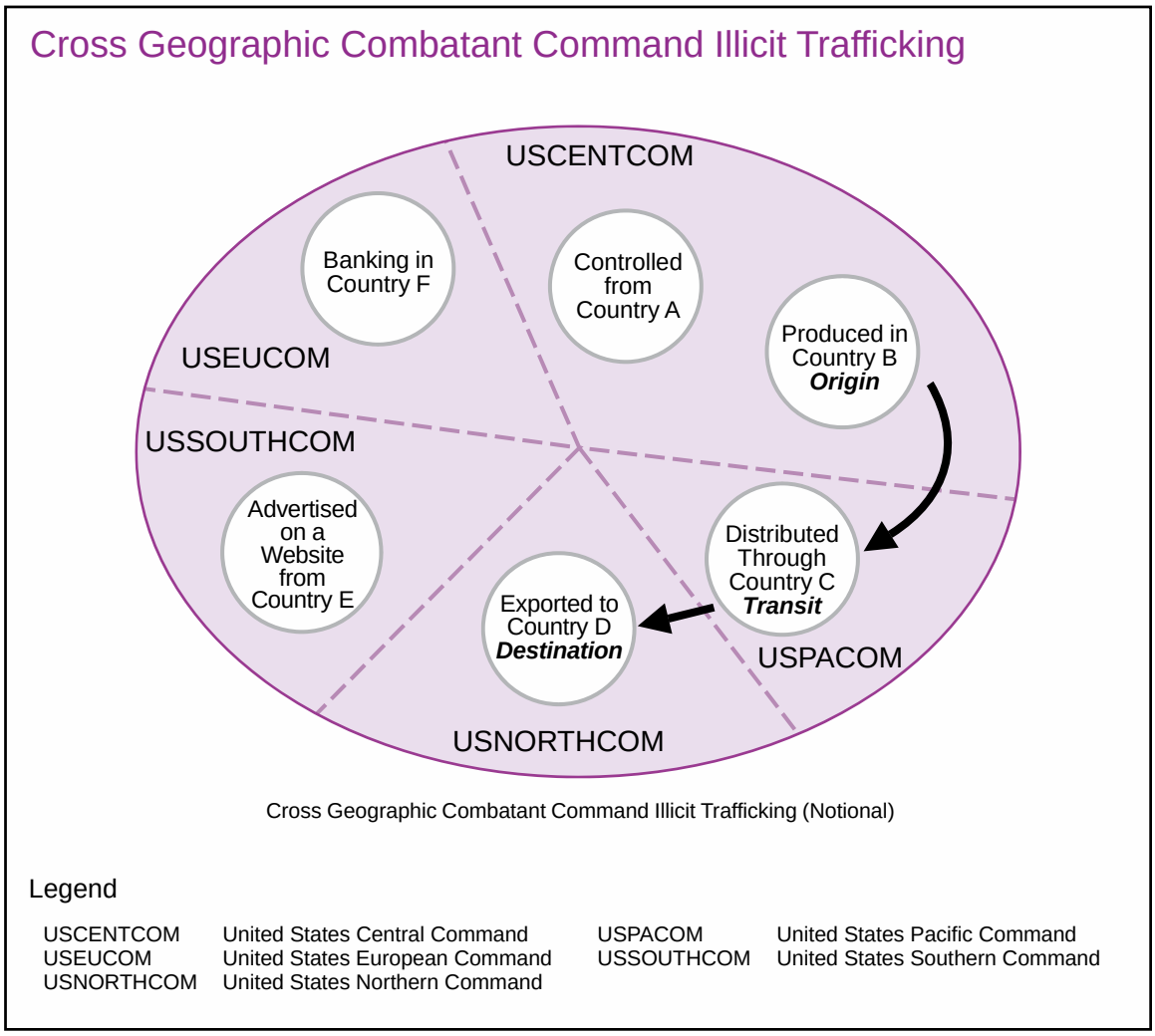


Figure V-7. Cross Geographic Combatant Command Illicit Trafficking

b. Effective CTN takes a deep understanding of the interrelationships between all the networks within an operational area, determining the desired effect(s) against each network, and nodes, and gathering and leveraging all available resources and capabilities to execute operations. CTN is generally a supporting effort, but can be the main focus of an operation, as in CT operations. Threat networks may cross international and theater boundaries, and CTN activities against a network within one area will affect many other networks. Joint forces need to coordinate operations to maximize positive effects against threat networks while limiting negative effects against friendly and neutral networks.

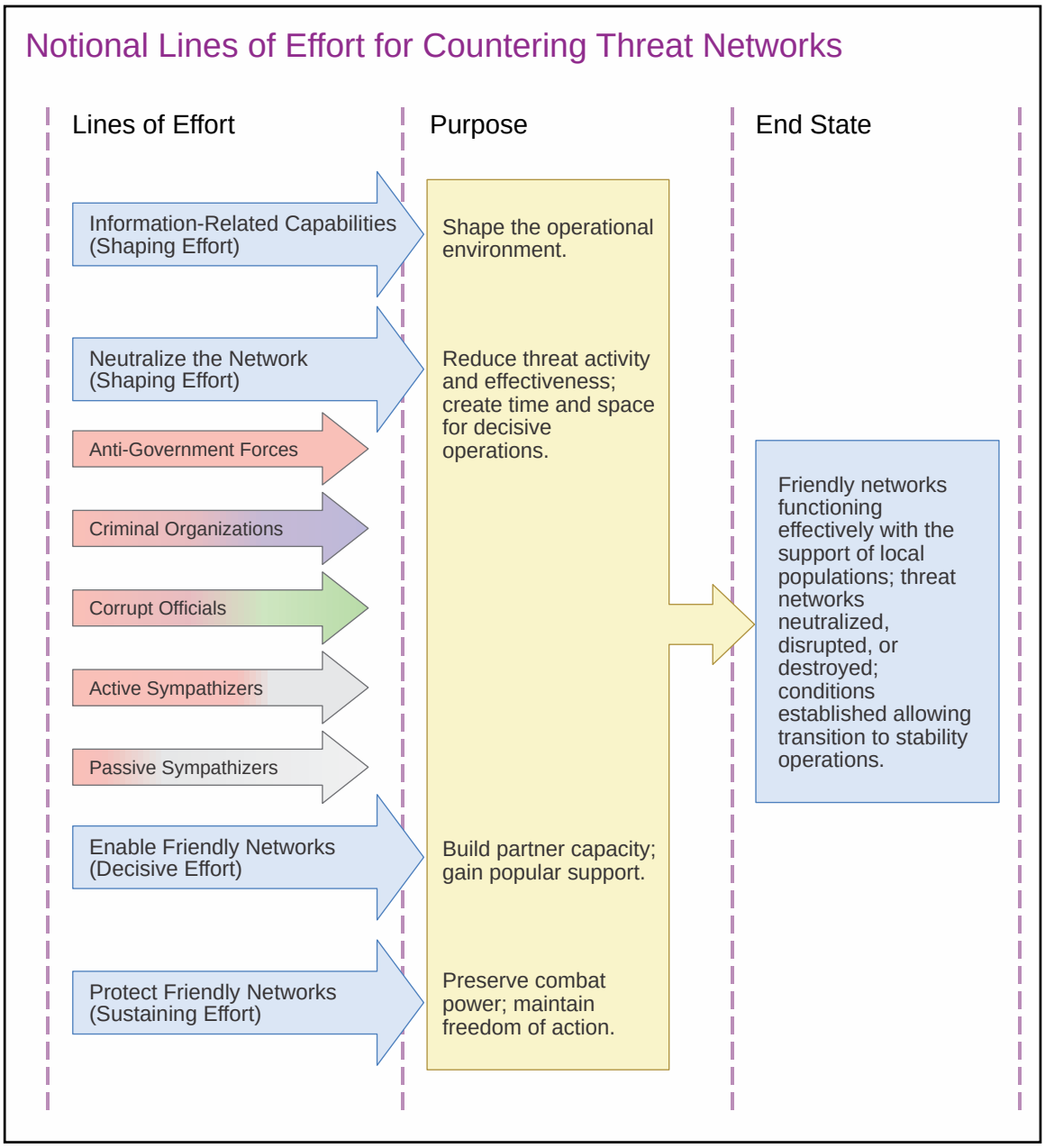


Figure V-8. Notional Lines of Effort for Countering Threat Networks

CASE STUDY: THE COMPLEXITY AND CHALLENGES OF COUNTERING THREAT NETWORKS

It has been stated many times, "it takes a network to defeat a network," and though those precise words may not have been used at the inception of the Joint Interagency Task Force-South (JIATF-S) two decades ago, the general premise driving its formation was exactly that—the creation of a US Government interagency and partner nation (PN) "friendly network" to interdict the flow of drugs from Central and South America and the Caribbean into the US from threat networks. From the onset, it became readily apparent that traditional approaches and processes used to address drug cartels and their associated threat networks were going to be ineffective. A strategic, concerted effort to reorganize along multiple lines—hierarchy and structure, legal, funding, and a host of others—was going to be absolutely essential in order to gain any real success against the sophisticated, international drug networks being encountered.

In response, JIATF-S built its own unparalleled network of law enforcement, intelligence, and military assets to focus on detecting the movements, and interdicting the shipments, of drug and narcoterrorist organizations. JIATF-S has gone past traditional boundaries of military focused joint operations to become a fully integrated interagency command. The command, operations, and intelligence structure include leaders and staff officers from the US Coast Guard, Customs and Border Protection, Department of Defense, Drug Enforcement Administration, and the Federal Bureau of Investigation. JIATF-S also incorporates a wide range of governmental and international organizations, allies and partners, to include the National Geospatial-Intelligence Agency, Defense Intelligence Agency, Central Intelligence Agency, and liaison officers from the United Kingdom, France, the Netherlands, Spain, and a host of Latin American countries, all playing an important role in intelligence, operations, and planning. Under a single command, JIATF-S epitomizes unity of effort.

Success has been achieved primarily in the international maritime and air domains since land operations involve complicated legal and diplomatic challenges. The task force also focuses on a discrete type of network, namely drug trafficking organizations and their distribution and transportation sub networks. Modifying the model so that it can effectively operate in the maritime, air, and land domains against all types of networks will be the next key step in its evolution. This evolution is critical since networks themselves are adapting and growing more powerful.

A CHANGING ENVIRONMENT—THE CONVERGENCE OF THREAT NETWORKS

In January 2010, the US completed a comprehensive assessment of transnational organized crime that concluded that transnational organized crime networks are proliferating, striking new and powerful alliances, and engaging in a range of illicit activities as never before. The result is a convergence of threats that have evolved to become more complex, volatile, and destabilizing. The President's Strategy to Combat Transnational Organized Crime warns that the threat of transnational organized crime is very real, particularly in the US Southern Command (USSOUTHCOM) area of responsibility. Transnational organized crime penetration of states is deepening, leading to co-option of government officers in some nations and weakening of governance in many others. Transnational organized crime networks insinuate themselves into the political process through bribery and in some cases have become alternate providers of governance, security, and livelihoods to win popular support. The nexus in some states among transnational organized crime groups and elements of government is so absolute that it threatens the rule of law. Furthermore, the Strategy to Combat Transnational Organized Crime goes on to highlight terrorists and insurgents are increasingly turning to crime and criminal networks for funding and logistics. In fiscal year 2010, 29 of the 63 top drug trafficking organizations identified by the Department of Justice had links to terrorist organizations. While many terrorist links to transnational organized crime are opportunistic, this nexus is dangerous, especially if it leads a transnational organized crime network to facilitate the transfer of weapons of mass destruction transportation of nefarious actors or materials into the US.

Funding and Legal Authority Challenges

As the Joint Interagency Task Force-South (JIATF-S) looks to expand its scope and operations it will encounter challenges in terms of authorities and funding. Years of experience and more complementary authorities have proven that success in the international air and maritime domains are achievable. But operations in the land domain, which constitutes sovereign nation-state rights and more complicated international issues will prove challenging. Operations on land will require JIATF's command structure to work very closely with the US country team and partner nation. Additionally, as JIATF-S looks to counter the nexus of criminal, terrorist, and insurgent networks, the authorities that provide the discrete basis for surveillance, targeting, and operations against drug trafficking organizations do not provide a sufficient legal basis for operations against all three.

Conclusion

USSOUTHCOM has been executing counter network operations against drug trafficking organizations for more than 20 years, and the JIATF-S interagency model has been at the forefront of these operational successes. JIATF-S is well known within the US Government as the "gold standard" for interagency collaboration. As the convergence of threat networks evolves to become more complex, volatile, and destabilizing, geographic combatant commanders will need to create a persistent unity of effort in order to fight threat networks with a friendly network.

Various Sources

Intentionally Blank

CHAPTER VI
ASSESSMENTS

1. General

Commanders and their staffs will conduct assessments to determine the impact CTN activities may have on the targeted networks. Other networks, including friendly and neutral networks, within the OE must also be considered during planning, operations, and assessments. The focus of this chapter is on assessing the impact on threat networks, to include identifying potential second- and third-order effects of operations relative to attaining the JFC's desired end state. Functional CCMDs with global synchronization responsibilities should also evaluate events and develop options for attaining their respective strategic goals. Threat networks will adapt visibly and invisibly even as collection, analysis, and assessments are being conducted, which is why assessments over time that show trends are much more valuable in CTN activities than a single snapshot over a short time frame. CCDRs develop theater and global strategies by analyzing the OE and developing mutually supporting objectives to best set conditions for attaining strategic end states. Over long periods of time, information can be compiled to describe changes in threat network organization, structure, composition, functions, and operational capabilities. This data can be used to support broad theater strategy, ongoing phase 0 and phase I operations, and as a baseline to support operations should joint force employment become necessary. Assessment of CTN activities will be part of the larger operation or campaign assessment.

2. Complex Operational Environments

Complex geopolitical environments, difficult causal associations, and the challenge of both quantitative and qualitative analysis to support decision making all complicate the assessment process. When only partially visible threat networks are spread over large geographic areas, among the people, and are woven into friendly and neutral networks, assessing the effects of joint force operations requires as much operational art as the planning process.

3. Assessment of Operations to Counter Threat Networks

a. CTN assessments at the strategic, operational, and tactical levels and across the instruments of national power are vital since many networks have regional and international linkages as well as capabilities. Objectives must be developed during the planning process so that progress toward objectives can be assessed. Assessments of threat networks will also be more challenging than against traditional adversaries since hard data on how CTN activities impact such things as number of weapons systems, troop strength, morale, and unit location will be difficult to measure. Dynamic interaction among friendly, threat, and neutral networks makes assessing many aspects of CTN activities difficult. As planners assess complex human behaviors, they draw on multiple sources across the OE, including analytical and subjective measures, which support an informed assessment.

b. Real-time network change detection is extremely challenging, and conclusions with high levels of confidence are rare. Since threat networks are rapidly adaptable, technological

systems used to support collection often struggle at monitoring change. Additionally, the large amounts of information collected require resources (people) and time for analysis. It is difficult to determine how networks change, and even more challenging to determine whether network changes are the result of joint force actions and, if so, which actions or combined actions are effective. A helpful indicator used in assessment comes when threat networks leverage social networks to coordinate and conduct operations, as it provides an opportunity to gain a greater understanding of the motivation and ideology of these networks. If intelligence analysts can tap into near real-time information from threat network entities, then that information can often be geospatially fused to create a better assessment. This is dependent on having access to accurate network data, the ability to analyze the data quickly, and the ability to detect deception.

c. CTN assessments require staffs to conduct analysis more intuitively and consider both anecdotal and circumstantial evidence. Since networked threats operate among civilian populations, there is a greater need for HUMINT. Collection of HUMINT is time-consuming and reliability of sources can be problematic, but if employed properly and cross-cued with other disciplines, it is extremely valuable in irregular warfare. Tactical unit reporting such as patrol debriefs and unit after action reports when assimilated across an OE may provide the most valuable information on assessing the impact of operations. There are challenges in collecting, analyzing, and assimilating information rapidly enough to inform the JFC for the next decision cycle. OSINT will often be more valuable in assessing operations against threat networks and be the single greatest source of intelligence. Information required to conduct assessments of CTN activities requires application of layered intelligence from multiple sources. The diversity of collection methods, types of information and intelligence collected, and analytic methodologies of these partners contributes to a holistic assessment in a complex OE.

4. Operation Assessment

a. The assessment process is a continuous cycle that seeks to observe and evaluate the ever-changing OE and inform decisions about the future, making operations more effective. Base-lining is critical in phase 0 and the initial JIPOE process for assessments to be effective. Assessments feed back into the JIPOE process to maintain tempo in the commander's decision cycle. This is a continuous process, and the baseline resets for each cycle. Change is constant within the complex OE and when operating against multiple, adaptive, interconnected threat networks.

b. Commanders establish priorities for assessment through their planning guidance, commander's critical information requirements (CCIRs), and decision points. Priority intelligence requirements, a component of CCIR, detail exactly what data the intelligence collection plan should be seeking to inform the commander regarding threat networks. The assessment process should measure the progress toward achieving the objectives and attaining the military end state. CTN activities may require assessing multiple MOEs and measures of performance (MOPs), depending on threat network activity. As an example, JFCs may choose to neutralize or disrupt one type of network while conducting direct operations against another network to destroy it.

c. Assessment precedes and guides every operation process activity and concludes each operation or phase of an operation. Like any cycle, assessment is continuous. The assessment process is not an end unto itself; it exists to inform the commander and improve the operation's progress. The assessment process provides a feedback mechanism to the JFC to provide guidance and direction for future operations and targeting efforts against threat networks.

d. Integrated successfully, assessment in CTN activities will:

(1) Depict progress toward achieving the commander's objectives and attaining the commander's end state.

(2) Help in understanding how the OE is changing due to the impact of CTN activities on threat network structures and functions.

(3) Inform the commander's decision making for operational design and planning, prioritization, resource allocation, and execution.

(4) Produce actionable recommendations that inform the commander where to devote resources along the most effective LOOs and LOEs.

5. Assessment Framework for Countering Threat Networks

The assessment framework broadly outlines three primary activities: organize, analyze, and communicate. In conducting each of these activities, assessors must be linked to JPP, understand the operation plan, and inform the intelligence process as to what information is required to support indicators, MOEs, and MOPs. In assessing CTN operations, quantitative data and analysis will inform assessors. Trends over time will have a higher level of confidence than short-term conclusions. The following is a general overview of assessment; for more information, refer to Army Techniques Publication (ATP) 5-0.3/Marine Corps Reference Publication (MCRP) 5-1C/Navy Tactics, Techniques, and Procedures (NTTP) 5-01.3/Air Force Tactics, Techniques, and Procedures (AFTTP) 3-2.87, *Multi-Service Tactics, Techniques, and Procedures for Operation Assessment.*

a. **Organize the Data**

(1) Based on the OE and the operation plan or campaign plan, the commander and staff develop objectives and assessment criteria to determine progress. The organize activity includes ensuring the indicators are included within the collection plan, information collected and then analyzed by the intelligence section is organized using an information management plan, and that information is readily available to the staff to conduct the assessment. Multiple threat networks within an OE may require multiple MOPs, MOEs, metrics, and branches to the plan. Threat networks operating collaboratively or against each other complicate the assessment process. If threat networks conduct operations or draw resources from outside the operational area, there will be a greater reliance on other CCDRs or interagency partners for data and information. Data associated within the OE may be organized by objective, phase, geography, network, LOEs, or LOOs.

Within the context of countering threat networks, example objective, measures of effectiveness (MOEs), and indicators could be:

Objective: Threat network resupply operations in "specific geographic area" are disrupted.

MOE: Suppliers to threat networks cease providing support.

Indicator 1: Fewer trucks leaving supply depots.

Indicator 2: Guerrillas/terrorists change the number of engagements or length of engagement times to conserve resources.

Indicator 3: Increased threat network raids on sites containing resources they require (grocery stores, lumber yards, etc.)

(2) Metrics must be collectable, relevant, measurable, timely, and complementary. The process uses assessment criteria to evaluate task performance at all levels of warfare to determine progress of operations toward achieving objectives. Both qualitative and quantitative analyses are required. With threat networks, direct impacts alone may not be enough, requiring indirect impacts for a holistic assessment. Operations against a network's financial resources may be best judged by analyzing the quality of equipment that they are able to deploy in the OE. Efforts against recruiting may require a detailed study of how well guerrillas are able to plan and carry out operations. Developing indicators for threat network changes over months may also be more valuable than attempting to determine day-to-day changes.

b. **Analyze the Data**

(1) Analyzing data is the heart of the assessment process for CTN activities. Baselining is critical to support analysis. Baselining should not only be rooted in the initial JIPOE, but should go back to GCC theater intelligence collection and shaping operations. Understanding how threat networks formed and adapted prior to joint force operations provides assessors a significantly better baseline and assists in developing indicators.

(2) Data analysis seeks to answer essential questions:

(a) What happened to the threat network(s) as a result of joint force operations? Specific examples may include the following: How have links changed? How have nodes been affected? How have relationships changed? What was the impact on structure and functions? Specifically, what was the impact on operations, logistics, recruiting, financing, and propaganda?

(b) What operations caused this effect directly or indirectly? (Why did it happen?) It is likely that multiple instruments of national power efforts across several LOOs and LOEs impacted the threat network(s), and it is equally unlikely that a direct cause and effect is discernible. Over time, however, and with critical thinking, trends regarding

operations and impacts will become evident. Analysts must be aware of the danger of searching for a trend that may not be evident. Events may sometimes have dramatic effects on threat networks, but not be visible to outside/foreign/US observers.

(c) What are the likely future opportunities to counter the threat network and what are the risks to neutral and friendly networks? CTN activities should target CVs. Interdiction operations, for example, may create future opportunities to disrupt finances. Cyberspace operations may target Internet propaganda and create opportunities to reduce the appeal of threat networks to neutral populations.

(d) What needs to be done to apply pressure at multiple points across the instruments of national power (diplomatic, informational, military, and economic) to the targeted threat networks to attain the JFC's desired military end state?

(3) Military units find stability tasks to be the most challenging to analyze since they are conducted among a civilian population. Adding a social dynamic complicates use of mathematical and deterministic formulas when human nature and social interactions play a major part in the OE. Overlaps between threat networks and neutral networks, such as the civilian population, complicate assessments and the second- and third-order effects analysis.

(4) The proximate cause of effects in complex situations can be difficult to determine. Even direct effects in these situations can be more difficult to create, predict, and measure, particularly when they relate to moral and cognitive issues (such as religion and the "mind of the adversary," respectively). Indirect effects in these situations often are difficult to foresee. Indirect effects often can be unintended and undesired since there will always be gaps in our understanding of the OE. Unpredictable third-party actions, unintended consequences of friendly operations, subordinate initiative and creativity, and the fog and friction of conflict will contribute to an uncertain OE. Simply determining undesired effects on threat networks requires a greater degree of critical thinking and qualitative analysis than traditional operations. Undesired effects on neutral and friendly networks cannot be ignored.

(5) Statistical analysis is necessary and allows large volumes of data to be analyzed, but critical thinking must precede its use and qualitative analysis must accompany any conclusions. SNA is a form of statistical analysis on human networks that has proven to be a particularly valuable tool in understanding network dynamics and in showing network changes over time but it must be complemented by other types of analysis and traditional intelligence analysis. It can support the JIPOE process as well as the planning, targeting, and assessment processes. SNA requires significant data collection and since threat networks are difficult to collect on and may adapt unseen, it must be used in conjunction with other tools.

For more information, see Appendix G, "Social Network Analysis."

c. **Communicate the Assessment**

(1) The assessment of CTN activities is only valuable to the commander and other participants if it is effectively communicated in a format that allows for rapid changes to LOOs/LOEs and operational and tactical actions for CTN activities.

(2) Communicating the CTN assessment clearly and concisely with sufficient information to support the staff's recommendations, but not too much trivial detail, is challenging.

(3) Well-designed CTN assessment products show changes in indicators describing the OE and the performance of organizations as it related to CTN activities.

For more information on communicating the assessment, refer to ATP 5-0.3/MCRP 5-1C/NTTP 5-01.3/AFTTP 3-2.87, Multi-Service Tactics, Techniques, and Procedures for Operation Assessment.

APPENDIX A
DEPARTMENT OF DEFENSE COUNTER THREAT FINANCE

1. Introduction

a. JFCs face adaptive networked threats that rapidly adjust their operations to offset friendly force advantages and pose a wide array of challenges across the range of military operations. CTN activities are a focused approach to understanding and operating against adaptive network threats such as terrorism, insurgency and organized crime. CTF refers to the activities and actions taken by the JFC to deny, disrupt, destroy, or defeat the generation, storage, movement, and use of assets to fund activities that support a threat network's ability to negatively affect the JFC's ability to attain the desired end state. Disrupting threat network finances decreases the threat network's ability to achieve their objectives. That can range from sophisticated communications systems to support international propaganda programs, to structures to facilitate obtaining funding from foreign based sources, to foreign based cell support, to more local objectives to pay, train, arm, feed, and equip fighters. Disrupting threat network finances decreases their ability to conduct operations that threaten US personnel, interests, and national security.

b. CTF activities against threat networks should be conducted with an understanding of the OE, in support of the JFC's objectives, and nested with other counter threat network operations, actions, and activities. CTF activities cause the threat network to adjust its financial operations by disrupting or degrading its methods, routes, movement, and source of revenue. Understanding that financial elements are present at all levels of a threat network, CTF activities should be considered when developing MOEs during planning with the intent of forecasting potential secondary and tertiary effects.

c. Effective CTF operations depend on developing an understanding of the functional organization of the threat network, the threat network's financial capabilities, methods of operation, methods of communication, and operational areas, and upon detecting how revenue is raised, moved, stored, and used.

2. Key Elements of Threat Finance

a. Threat finance is the manner in which adversarial groups raise, move, store, and use funds to support their activities. Following the money and analyzing threat finance networks is important to:

(1) Identify facilitators and gatekeepers.

(2) Estimate threat networks' scope of funding.

(3) Identify modus operandi.

(4) Understand the links between financial networks.

(5) Determine geographic movement and location of financial networks.

(6) Capture and prosecute members of threat networks.

b. **Raising Money.** Fund-raising through licit and illicit channels is the first step in being able to carry out or support operations. This includes raising funds to pay for such mundane items as food, lodging, transportation, training, and propaganda. Raising money can involve network activity across local and international levels. It is useful to look at each source of funding as separate nodes that fit into a much larger financial network. That network will have licit and illicit components.

(1) Funds can be raised through illicit means, such as drug and human trafficking, arms trading, smuggling, kidnapping, robbery, and arson. Whenever large amounts of money are generated in this way, such as in the sale of narcotics, the money must be laundered before it can enter the legitimate financial banking system. The laundering process is susceptible to being detected and is a vulnerability in the illicit fund-raising process.

(2) Alternatively, funds can be raised through ostensibly legal channels. Threat networks can receive funds from legitimate humanitarian and business organizations and individual donations. Charities raising funds for humanitarian relief in war-torn regions may or may not know their funds are supporting threat activities.

(3) Legitimate funds are commingled with illicit funds destined for threat networks, making it extremely difficult for governments to track threat finances in the formal financial system. Such transactions are perfectly legal until they can be linked to a criminal or terrorist act. Therefore, these transactions are extremely hard to detect in the absence of other indicators or through the identification of the persons involved.

c. **Moving Money.** Moving money is one of the most vulnerable aspects of the threat finance process. To make the illicit money usable to threat networks it must be laundered. This can be done through the use of front companies, legitimate businesses, cash couriers, or third parties that may be willing to take on the risks in exchange for a cut of the profits. These steps are called “placement” and “layering.”

(1) During the placement stage, the acquired funds or assets are placed into a local, national, or international financial system for future use. This is necessary if the generated funds or assets are not in a form useable by their recipient, e.g., converting cash to wire transfers or checks.

(2) During the layering stage, numerous transactions are conducted with the assets or proceeds to create distance between the origination of the funds or assets and their eventual destination. Distance is created by moving money through several accounts, businesses or people, or by repeatedly converting the money or asset into a different form.

d. **Storing Money.** Money or goods that have successfully been moved to a location that can be accessed by the threat network may need to be stored until it is ready to be spent. Money that has been cleaned through a laundering process may be stored in a bank or invested into stocks or real estate until it is needed, at which time those assets can be liquidated back into cash and dispersed. Another way to store money is bulk-cash storage.

e. **Using Money.** Once a threat network has raised, moved, and stored their money, they are able to spend it. This is called "integration." Roughly half of the money that was initially raised will go to operational expenses and the cost of laundering the money to convert it to useable funds. During integration, the funds or assets are placed at the disposal of the threat network for their utilization or re-investment into other licit and illicit operations.

3. Planning Considerations

a. CTF requires the integration of the efforts of disparate organizations in a whole-of-government approach in a complex environment. Joint operation/campaign plans and operation orders should be crafted to recognize that the core competencies of various agencies and military activities are coordinated and resources integrated, when and where appropriate, with those of others to achieve the operational objectives. The JFC and staff need to consider the nonmilitary options being developed, especially as they relate to CTF. Because the JFC will issue coordination instructions as part of initial guidance, identification of mission partners is a critically important part of initiation. The JFC and staff need to identify the end states and objectives of various mission partners (including their execution timelines and planning horizons). COA development should consider the unique capabilities and authorities of mission partners as well as any gaps they may have, as identified in mission analysis. The JFC should ensure the red cell understands and appreciates the impact CTF can have on an adversary. The JFC should consider if the COA places mission partners in the best posture for future operations/activities. The concept of operations needs to provide sufficient detail to outline coordination mechanisms with other mission partners.

b. The JFC and staff need to understand the impact that changes to the OE will have on CTF activities. The adaptive nature of threat networks will force changes to the network's business practices and operations based on the actions of friendly networks within the OE. This understanding can lead to the creation of a more comprehensive, feasible, and achievable plan.

c. CTF planning will identify the organizations and entities that will be required to conduct CTF action and activities. CTF organizations may include various combinations of three basic structures: organic CTF element established within a military staff at the CCMD or JTF level; CTF element comprised of DOD and interagency personnel operating at a foreign deployed location within a military operational area; and CTF element comprised of DOD and interagency personnel operating outside a military operational area, probably at a CCMD headquarters.

4. Intelligence Support Requirements

a. CTF activities require detailed, timely, and accurate intelligence of threat networks' financial activities to inform planning and decision making. Intelligence support to CTF includes intelligence collection and analysis activities to identify, understand, and evaluate a threat network's ability to generate, store, move, and use funds. Analysts can present the JFC with a reasonably accurate scope of the threat network's financial capabilities and impact probabilities if they have a thorough understanding of the threat network's financial

requirements and what the threat network is doing to meet those requirements. Analysts also support the joint force staff in the identification of CRs and CVs of a threat finance network. Financial system analysis focuses CTF efforts and is critical in prioritizing competing demands for intelligence collection resources. Much of the information related to the financial requirements for the threat network can be developed as a part of the JIPOE process.

For additional information, refer to JP 2-01.3, Joint Intelligence Preparation of the Operational Environment.

b. JFCs should identify intelligence requirements for threat finance-related activities to establish collection priorities prior to the onset of operations. Intelligence collection and analysis of threat network financial activities can provide insight into the threat network's business processes required to conduct operations and day-to-day activities from the strategic level down to the tactical level.

c. Intelligence support can focus on following the money by tracking the generation, storage, movement, and use of funds, which may provide additional insight into threat network leadership activities and other critical components of the threat network's financial business practices. Trusted individuals or facilitators within the network often handle the management of financial resources. These individuals and their activities may lead to the identification of CVs within the network and decisive points for the JFC to target the network.

5. Operation

a. DOD may not always be the lead agency for CTF. Frequently the efforts and products of CTF analysis will be used to support criminal investigations or regulatory sanction activities, either by the USG or one of its partners. This can prove advantageous as contributions from other components can expand and enhance an understanding of threat financial networks. Threat finance activities can have global reach and are generally not geographically constrained. At times much of the threat finance network, including potentially key nodes, may extend beyond the JFC's operational area. Therefore, establishing appropriate communications, information sharing, and coordinating relationships across the geographic boundaries will be essential for CTF activities. It is also important to understand the requirements of those with whom the JFC engages to ensure effective and efficient communication and coordination

b. Military support to CTF is not a distinct type of military operation; rather it represents military activities against a specific network capability of business and financial processes used by an adversary network. Additionally, CTF can support several types of military operations:

(1) **Major Operations.** CTF can reduce or eliminate the adversary's operational capability by reducing or eliminating their ability to pay troops and procure weapons, supplies, intelligence, recruitment, and propaganda capabilities. Cutting off funding that the adversary uses to pay troops may reduce the morale and effectiveness of the operational

force even if it is not able to prevent it being fielded altogether. However, adversaries with robust strategic and operational reserves will be better able to mitigate CTF efforts.

(2) **Arms Control and Disarmament.** CTF can be used to disrupt the financing of trafficking in small arms, IED or WMD proliferation and procurement, research to develop more lethal or destructive weapons, hiring technical expertise, or providing physical and operational security. Additionally, CTF can be used to disrupt the value remittances associated with transfers of small arms or chemical, biological, radiological, and nuclear (CBRN) materials that violate international agreements and conventions.

(3) **SFA.** CTF personnel can provide training to PN CTF and/or law enforcement personnel as well as provide CTF capabilities as a defense-related service under SFA and with specific authorities.

For additional information, refer to JP 3-20, Security Cooperation.

(4) **FID.** CTF personnel can provide training to HN CTF or law enforcement personnel as well as provide CTF capabilities to assist the nation in its fight against subversion, lawlessness, and insurgency.

For additional information, refer to JP 3-22, Foreign Internal Defense.

(5) **Combating Terrorism.** CTF activities can be used to disrupt financing to terrorist groups, thereby preventing, deterring, preempting, and responding to terrorism.

For additional information, refer to JP 3-26, Counterterrorism, *and JP 3-07.2,* Antiterrorism.

(6) **DOD Support to CD Operations.** The US military may conduct training of PN/HN security and law enforcement forces, assist in the gathering of intelligence, and participate in the targeting and interception of drug shipments. Disrupting the flow of drug profits via CTF directly impacts the primary motivator for narcotics trafficking, which is profit.

For additional information, refer to JP 3-07.4, Counterdrug Operations.

(7) **Enforcement of Sanctions.** CTF encompasses all forms of value transfer to the adversary, not just currency. DOD organizations can provide assistance to organizations that are interdicting the movement of goods and/or any associated value remittance as a means to enforce sanctions.

(8) **COIN.** CTF can be used to counter, disrupt, or interdict the flow of value to an insurgency. 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. In such cases, CTF is aimed at insurgent organizations as well as other malevolent actors in the environment.

For additional information, refer to JP 3-24, Counterinsurgency.

(9) **Peace Operations.** In peace operations, CTF can be used to stem the flow of external sources of support to conflicts to contain and reduce the conflict. Additionally, CTF can be used to bolster the legitimacy of the government by reducing crime and corruption and to build capable government institutions that are able to conduct their own CTF operations.

For additional information, refer to JP 3-07.3, Peace Operations.

c. Military support tasks to CTF can fall into four **broad** categories:

(1) Support civil agency and HN activities (including law enforcement):

(a) **Provide Protection.** US military forces may provide overwatch for law enforcement or PN/HN military CTF activities. This may include perimeter security for operations, aerial overwatch, intelligence warnings, and protection for civilian agencies or PN/HN military movements.

(b) **Provide Logistics.** US military forces may provide transportation, especially tactical movement-to-objective support, to law enforcement or PN/HN military CTF activities. This may include providing secure single vehicle movements of key individuals, providing convoys, and executing aerial lift for personnel, equipment, evidence, or prisoners. US military forces may provide supply services, including but not limited to food, equipment, medical materials and/or care, mortuary services, or contracting support for civil agency or PN/HN CTF activities. US military forces may provide basing, including housing, workspaces, engineering support, and physical security for civil agencies or PN/HN CTF personnel.

(c) **Provide Command, Control, and Communications Support.** US military forces may provide information technology and communications support to civilian agencies or PN/HN CTF personnel. This support may include provision of hardware and software, encryption, bandwidth, configuration support, networking, and account administration and cybersecurity.

(2) Direct military actions:

(a) **Capture/Kill.** US military forces may, with the support of mission partners as necessary, conduct operations to capture or kill key members of the threat finance network. Such operations may require the use of SOF, conventional ground forces, maritime forces, or strike/attack aircraft.

(b) **Interdiction of Value Transfers.** US military forces may, with the support of mission partners, conduct operations to interdict value transfers to the threat network as necessary. This may be a raid to seize cash from an adversary safe house, foreign exchange house, hawala or other type of informal remittance systems; seizure of electronic media including mobile banking systems commonly known as “red sims” and computer systems that contain data support payment and communication data in the form of cryptocurrency or exchanges in the virtual environment; interdiction to stop the smuggling of

goods used in trade-based money laundering; or command and control flights to provide aerial surveillance of drug-smuggling aircraft in support of law enforcement interdiction.

(c) **Training HN/PN Forces.** US military forces may provide training to PN/HN CTF personnel under specific authorities. Such training may include special operations training for tactical organizations, analytical training, and training for operations and planning staffs.

(3) **Intelligence Collection.** US military forces may conduct all-source intelligence operations, which will deal primarily with the collection, exploitation, analysis, and reporting of CTF information. These operations may involve deploying intelligence personnel to collect HUMINT and the operations of ships at sea and forces ashore to collect SIGINT, OSINT, and GEOINT.

(4) **Operations to Generate Information and Intelligence.** Occasionally, US military forces may conduct operations either with SOF or conventional forces designed to provoke a response by the adversary's threat finance network for the purpose of collecting information or intelligence on that network. These operations are pre-planned and carefully coordinated with the intelligence community to ensure the synchronization and posture of the collection assets as well as the operational forces. An example would be a show of force at a known drug and weapons bazaar to collect signals and imagery intelligence about the adversary's response.

d. **Threat Finance Cells**

(1) Threat finance cells can be established at any level based on available personnel resources. Expertise on adversary financial activities can be provided through the creation of threat finance cells at brigade headquarters and higher. The threat finance cell would include a mix of analysts and subject matter experts on law enforcement, regulatory matters, and financial institutions that would be drawn from DOD and civil USG agency resources. The threat finance cell's responsibilities vary by echelon. At division and brigade, the threat finance cell:

(a) Provides threat finance expertise and advice to the commander and staff.

(b) Assists the intelligence staff in the development of intelligence collection priorities focused on adversary financial and support systems that terminate in the unit's operational area.

(c) Consolidates information on persons providing direct or indirect financial, material and logistics support to adversary organizations in the unit's operational area.

(d) Provides information concerning adversary exploitation of US resources such as transportation, logistical, and construction contractors working in support of US facilities; exploitation of NGO resources; and exploitation of supporting HN personnel.

(e) Identifies adversary organizations coordinating or cooperating with local criminals, organized crime, or drug trafficking organizations.

(f) Provides assessments of the adversary's financial viability—ability to fund, maintain, and grow operations—and the implications for friendly operations.

(g) Develops targeting package recommendations for adversary financial and logistics support persons for engagement by lethal and nonlethal means.

(h) Notifies commanders when there are changes in the financial or support operations of the adversary organization, which could indicate changes in adversary operating tempo or support capability.

(i) Coordinates and shares information with other threat finance cells to build a comprehensive picture of the adversary's financial activities.

(2) At the operational level, the joint force J-2 develops and maintains an understanding of the OE, which includes economic and financial aspects. If established, the threat finance cell supports the J-2 to develop and maintain an understanding of the economic and financial environment of the HN and surrounding countries to assist in the detection and tracking of illicit financial activities, understanding where financial support is coming from, how that support is being moved into the area of operation and how that financial support is being used. The threat finance cell:

(a) Works with the J-2 to develop threat finance-related priority intelligence requirements and establish threat finance all-source intelligence collection priorities. The threat finance cell assists the J-2 in the detection, identification, tracking, analysis, and targeting of adversary personnel and networks associated with financial support across the operational area.

(b) The threat finance cell coordinates with tactical and theater threat finance cells and shares information with those entities as well as multinational forces, HN, and as appropriate and in coordination with the joint force J-2, the intelligence community.

(c) The threat finance cell, in coordination with the J-2, establishes a financial network picture for all known adversary organizations in the operational area; establishes individual portfolios or target packages for persons identified as providing financial or material support to the adversary's organizations in the operational area; identifies adversary financial TTP for fund-raising, transfer mechanisms, distribution, management and control, and disbursements; and identifies and distributes information on fund-raising methods that are being used by specific groups in the area of operations. The threat finance cell can also:

1. Identify specific financial institutions that are involved with or that are providing financial support to the adversary and how those institutions are being exploited by the adversary.

2. Provide CTF expertise on smuggling and cross border financial and logistics activities.

3. Establish and maintain information on adversary operating budgets in the area of operation to include revenue streams, operating costs, and potential additions, or depletions, to strategic or operational reserves.

4. Targets identified by the operational-level threat finance cell are shared with the tactical threat finance cells. This allows the tactical threat finance cells to support and coordinate tactical units to act as an action arm for targets identified by the operational-level CTF organization, and coordinate tactical intelligence assets and sources against adversary organizations identified by the operational-level CTF organization.

5. Multi-echelon information sharing is critical to unraveling the complexities of an adversary's financial infrastructure. Operational-level CTF organizations require the detailed financial intelligence that is typically obtained by resources controlled by the tactical organizations. Information obtained from tactical sources may require intelligence community or HN sources to gain access to the source of the documents or to financial accounts and communications accounts. Tactical-level CTF will require help in identifying and tracking financial support operations that initiate outside of their operational areas and terminate in their operational areas.

6. The operational-level threat finance cell facilitates the provision of support by USG and multinational organizations at the tactical level. This is especially true for USG department and agencies that have representation at the American Embassy.

(3) Tactical-level threat finance cells will require support from the operational level to obtain HN political support to deal with negative influencers that can only be influenced or removed by national-level political leaders, including governors, deputy governors, district leads, agency leadership, chiefs of police, shura leaders, elected officials and other persons serving in official positions; HN security forces; civilian institutions; and even NGOs/charities that may be providing the adversary with financial and logistical support.

(4) The threat finance cell should be integrated into the battle rhythm. Battle rhythm events should follow the following criteria:

(a) Name of board or cell: Descriptive and unique.

(b) Lead staff section: Who receives, compiles, and delivers information.

(c) When/where does it meet in battle rhythm: Allocation of resources (time and facilities), and any collaborative tool requirements.

(d) Purpose: Brief description of the requirement.

(e) Inputs required from: Staff sections, centers, groups, cells, offices, elements, boards, working groups, and planning teams required to provide products (once approved, these become specified tasks).

(f) When? Suspense for inputs.

(g) Output/process/product: Products and links to other staff sections, centers, groups, cells, offices, elements, boards, working groups, and planning teams.

(h) Time of delivery: When outputs will be available.

(i) Membership: Who has to attend (task to staff to provide participants and representatives).

6. Assessment

a. JFCs should know the importance and use of CTF capabilities within the context of measurable results for countering adversaries and should embed this knowledge within their staff. By assessing common elements found in adversaries' financial operations, such as composition, disposition, strength, personnel, tactics, and logistics, JFCs can gain an understanding of what they might encounter while executing an operation and identify vulnerabilities of the adversary. Preparing a consolidated, whole-of-government set of metrics for threat finance will be extremely challenging.

b. Metrics on threat finance may appear to be of little value because it is very difficult to obtain fast results or intelligence that can is immediately actionable. Actions against financial networks may take months to prepare, organize, and implement, due to the difficulty of collecting relevant detailed information and the time lags associated with processing, analysis, and reporting findings on threat financial networks.

c. The JFC's staff should assess the adversary's behaviors based on the JFC's desired end state and determine whether the adversary's behavior is moving closer to that end state.

d. The JFC and staff should consult with participating agencies and nations to establish a set of metrics which are appropriate to the mission or LOOs assigned to the CTF organization.

APPENDIX B
THE CONVERGENCE OF ILLICIT NETWORKS

1. Overview

a. The convergence of illicit networks (e.g., criminals, terrorists, and insurgents) incorporates the state or degree to which two or more organizations, elements, or individuals approach or interrelate. Conflict in Iraq and Afghanistan has seen a substantial increase in the cooperative arrangements of illicit networks to further their respective interests. From the Taliban renting their forces out to provide security for drug operations to al-Qaida using criminal organizations to smuggle resources, temporary cooperative arrangements are now a routine aspect of CTN operations. Similar to convergence, nexus describes a relationship or connection between people or things. Nexus is a refinement of convergence to a specific, targetable aspect of duration or location.

b. The US intelligence community has concluded that transnational organized crime has grown significantly in size, scope, and influence in recent years. A public summary of the assessment identified a convergence of terrorist, criminal, and insurgent networks as one of five key threats to US national security. Terrorists and insurgents increasingly have and will continue to turn to crime to generate funding and will acquire logistical support from criminals, in part because of successes by USG departments and agencies and PNs in attacking other sources of their funding, such as from state sponsors. In some instances, terrorists and insurgents prefer to conduct criminal activities themselves; when they cannot do so, they turn to outside individuals and facilitators. Some criminal organizations have adopted terrorist organizations' practice of extreme and widespread violence in an overt effort to intimidate governments and populations at various levels. USG documents characterize the confluence of transnational organized crime and international terrorism as a growing phenomenon. Department of Justice investigations suggest that international organized criminals are willing to provide logistical and other support to terrorists. Proceeds from the drug trade are critical to the continued funding of many criminal, terrorist, and insurgent groups. Over time not only has the number of DOS-designated foreign terrorist organizations (FTOs) grown, but the percentage of these FTOs involved in drug trafficking has also increased. The convergence between crime, terrorism, and insurgency will continue as the OE evolves.

c. 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 actors in shadow economies, distorting market forces. Indications are that although the operations and objectives of criminal groups, insurgents, and terrorists differ, these groups interact on a regular basis for mutually beneficial reasons. They each pose threats to state sovereignty. They share the common goals of ensuring that poorly governed and post-conflict countries have ineffective laws and law enforcement, porous borders, a culture of corruption, and lucrative criminal opportunities. Current strategies have largely defined these threats in narrow, separate, and often ambiguous terms. In most cases, the organized crime component has been artificially

separated from the activities of insurgents, jihadists, warlords, and terrorists. Organized crime has been traditionally treated as a law enforcement rather than national security concern. The convergence of organized criminal networks with the other non-state actors requires a more sophisticated, interactive, and comprehensive response that takes into account the dynamics of the relationships and adapts to the shifting tactics employed by the various threat networks. This response must be a unified action, which is the synchronization, coordination, and/or integration of the activities of governmental and nongovernmental entities with military operations to achieve unity of effort. International partners and HN governments must be included as necessary.

d. Mounting evidence suggests that the modus operandi of these entities often diverges and the interactions among them are on the rise. This spectrum of convergence (Figure B-1) has received increasing attention in law enforcement and national security policy-making circles. Until recently, the prevalent view was that terrorists and insurgents were clearly distinguishable from organized criminal groups by their motivations and the methods used to achieve their objectives. Terrorist and insurgent groups use or threaten to use extreme violence to attain political ends, while organized criminal groups are primarily motivated by profit. Today, these distinctions are no longer useful for developing effective diplomatic, law enforcement, and military strategies, simply because the lines between them have become blurred, and the security issues have become intertwined. The convergence of organized criminal networks and other illicit non-state actors, whether for short-term tactical partnerships or broader strategic imperatives, requires a much more sophisticated response or

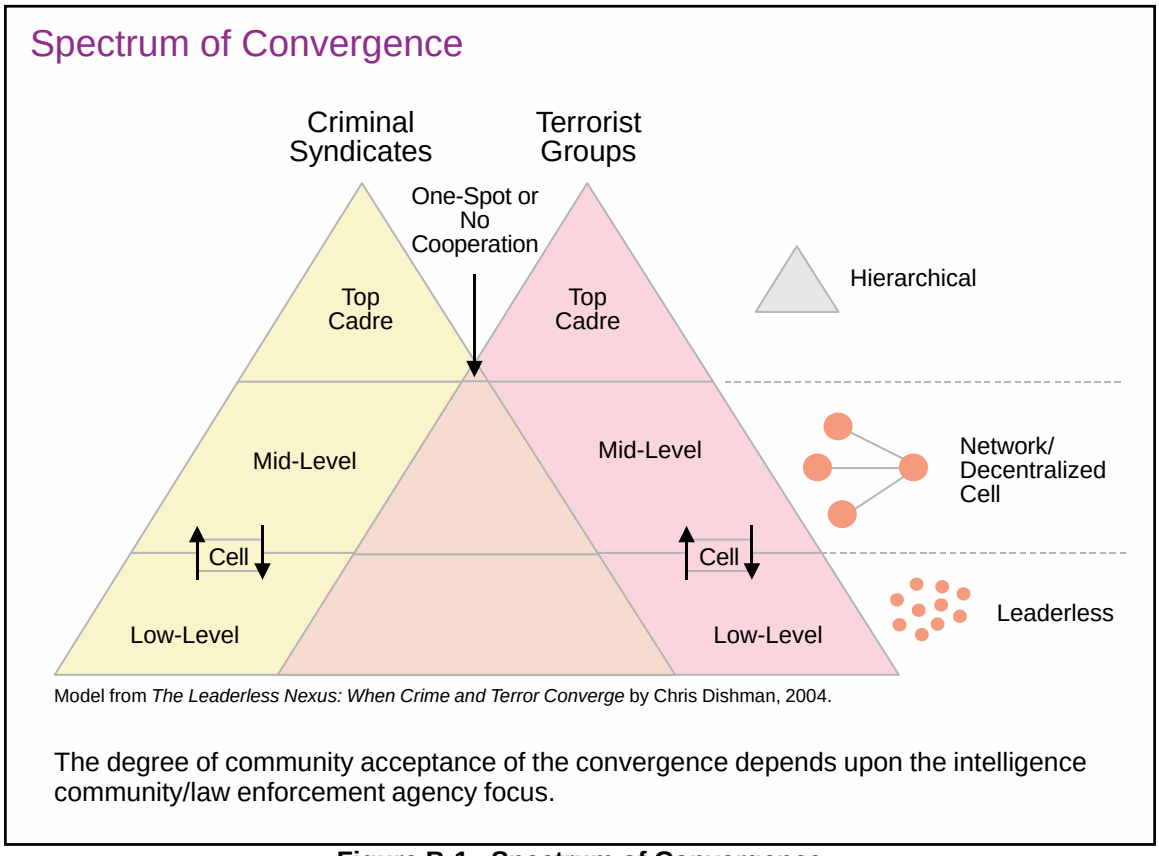


Figure B-1. Spectrum of Convergence

unified approach, one that takes into account the evolving nature of the relationships as well as the environmental conditions that draw them together.

e. The convergence of illicit networks has provided law enforcement agencies with a broader mandate to combat terrorism. Labeling terrorists as criminals undermines the reputation of terrorists as freedom fighters with principles and a clear political ideology, thereby hindering their ability to recruit members or raise funds. Likewise, participating in more diverse criminal acts increases their exposure to law enforcement investigations, thereby increasing the probability of interdicting and prosecuting them. Conversely, just as redefining terrorists as criminals damages their reputation, ironically it might prove to be useful at other times to redefine criminals as terrorists, such as in the case of the Haqqani network in Afghanistan. For instance, this change in term might make additional resources available to law enforcement agencies, such as those of the military or the intelligence services, thereby making law enforcement more effective.

f. However, there are some limitations associated with the latter approach. The adage that a terrorist to one is a freedom fighter to another holds true. This difference of opinion therefore renders it difficult for states to cooperate in joint CT operations. For instance, even though the US and the United Kingdom have a special relationship dating back to World War II, it does not mean that these two close allies see eye-to-eye on all matters. The US regards the entire Hizballah group as a terrorist organization; the United Kingdom regards only the organization's military wing as a terrorist organization.

g. The paradigm of fighting terrorism, insurgency, and transnational crime separately, utilizing distinct sets of authorities, tools, and methods, is not adequate to meet the challenges posed by the convergence of these networks into a criminal-terrorist-insurgency conglomeration. While the US has maintained substantial long-standing efforts to combat terrorism and transnational crime separately, the government has been challenged to evaluate whether the existing array of authorities, responsibilities, programs, and resources sufficiently responds to the combined criminal-terrorism threat. Common foreign policy options have centered on diplomacy, foreign assistance, financial actions, intelligence, military action, and investigations. At issue is how to conceptualize this complex illicit networks phenomenon and oversee the implementation of cross-cutting activities that span geographic regions, functional disciplines, and a multitude of policy tools that are largely dependent on effective interagency coordination and international cooperation.

2. Terrorist Organizations

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 has evolved as a preferred tactic for ideological extremists around the world, directly or indirectly affecting millions of people. DOS has an ever changing number of groups designated as FTOs; some of the more notable groups are Hamas, Hizballah, al-Qaida, al-Qaida in the Islamic Maghreb, Haqqani network, Boko Haram, and the Revolutionary Armed Forces of Colombia. Additionally, there are certain countries determined by the Secretary of State to have repeatedly provided support for acts of international terrorism, i.e., state sponsors of terrorism.

b. In addition to increasing law enforcement capabilities for CT, the US, like many nations, has developed specialized, but limited, military CT capabilities. CT actions are 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. However, defeating terrorist organizations usually requires maintaining the legitimacy and enhancing the credibility of a political authority to support and govern the relevant population. In addition to any diplomatic and law enforcement actions, the USG typically viewed CT missions as special operations by clandestine or low-visibility means. CT is one of the core activities of the US SOF, and their role and additive capability is to conduct offensive measures within DOD's overall combating terrorism efforts. Some significant policy and strategy adjustments were required because terrorism has evolved from a tactic of inducing fear in select populations/areas to a transnational threat of strategic proportion.

c. Commander, United States Special Operations Command (CDRUSSOCOM) is a global synchronizer for DOD CT efforts and is responsible for synchronizing planning, and as directed, executing operations against terrorist networks on a global basis in coordination with other CCMDs, the Services, and appropriate USG departments and agencies. CDRUSSOCOM has the authority to synchronize and lead a collaborative planning process, leveraging other CCMDs' capabilities and expertise that results in decentralized execution by both US Special Operations Command and other CCMDs against terrorist networks designated by the Secretary of Defense.

For more information, see JP 3-26, Counterterrorism, *and JP 3-07.2,* Antiterrorism.

3. Insurgencies

a. Insurgency is the organized use of subversion and violence to seize, nullify, or challenge political control of a region. Insurgency uses a mixture of subversion, sabotage, political, economic, psychological actions, and armed conflict to achieve its political aims. It is a protracted politico-military struggle designed to weaken the control and legitimacy of an established government, a military occupation government, an interim civil administration, or a peace process while increasing insurgent control and legitimacy.

b. COIN is a comprehensive civilian and military effort designed to simultaneously defeat and contain insurgency and address its root causes. COIN is primarily a political struggle and incorporates a wide range of activities by the HN government, of which security is only one element, albeit an important one. Unified action is required to successfully conduct COIN operations and should include all HN, US, and multinational partners.

For more information, see JP 3-24, Counterinsurgency.

c. Of the groups designated as FTOs by DOS, the vast majority possess the characteristics of an insurgency: an element of the larger group is conducting insurgent type operations, or the group is providing assistance in the form of funding, training, or fighters to another insurgency. Colombia's government and the Revolutionary Armed Forces of Colombia reached an agreement to enter into peace negotiations in 2012, taking another big

step toward ending the 50-year old insurgency. Hamas is an FTO, but conducts itself more as an insurgency in its battle with Israel. Hamas began as a Palestinian armed faction of the Egyptian Muslim Brotherhood in the early 1980s and developed into a multi-faceted organization with influential political, social, and military components and global reach; it was designated an FTO in 1997. Boko Haram was added to the DOS's FTO list in 2013, but has been waging an insurgency in Nigeria for the past five years. Boko Haram regularly engages the Nigerian military in bloody combat with the aim of destabilizing and ultimately overthrowing the government and establishing an Islamic caliphate in its place. In January 2012, US Africa Command assessed that Boko Haram had links to al-Qaida in the Islamic Maghreb and al-Shabaab and that Boko Haram and al-Qaida in the Islamic Maghreb were coordinating operations in Mali. Additionally, Boko Haram has pledged allegiance to the Islamic State in Iraq and Syria/ Islamic State in Iraq and the Levant.

d. The convergence of illicit networks contributes to the undermining of the fabric of society. Since the proper response to this kind of challenge is effective civil institutions, including uncorrupted and effective police, the US must be capable of deliberately applying unified action across all instruments of national power in assisting allies and PNs when asked.

4. Transnational Criminal Organizations

a. From the National Security Strategy, combating transnational criminal and trafficking networks requires a multidimensional strategy that safeguards citizens, breaks the financial strength of criminal and terrorist networks, disrupts illicit trafficking networks, defeats transnational criminal organizations, fights government corruption, strengthens the rule of law, bolsters judicial systems, and improves transparency. While these are major challenges, the JFC will be able to plan and execute operations with other nations facing the same threats.

b. Transnational criminal organizations are self-perpetuating associations of individuals that operate to obtain power, influence, monetary and/or commercial gains, wholly or in part by illegal means. These organizations protect their activities through a pattern of corruption and/or violence or protect their illegal activities through a transnational organizational structure and the exploitation of transnational commerce or communication mechanisms. Transnational criminal networks are not only expanding operations, but they are also diversifying activities, creating a convergence of threats that has become more complex, volatile, and destabilizing. These networks also threaten US interests by forging alliances with corrupt elements of national governments and using the power and influence of those elements to further their criminal activities. In some cases, national governments exploit these relationships to further their interests to the detriment of the US.

c. The convergence of illicit networks continues to grow as global sanctions affect the ability of terrorist organizations and insurgencies to raise funds to conduct their operations. The DOS's FTO list contains organizations that are not only considered terrorist, but participate in both illicit activities and insurgencies. The DOS's 2012 *Country Reports on Terrorism* described more than 20 FTOs as having financially profited from criminal activity to sustain their terrorist operations.

d. Although drug trafficking still represents the most lucrative illicit activity in the world, other criminal activity, particularly human and arms trafficking, have also expanded. As a consequence, international criminal organizations have gone global; drug trafficking organizations linked to the Revolutionary Armed Forces of Colombia, for example, have agents in West Africa, just as Lebanon's Hizballah has members, supporters and sympathizers throughout Latin America, and their licit and illicit activities span Asia, Europe, and Africa.

e. As the power and influence of these organizations has grown, their ability to undermine, corrode, and destabilize governments has increased. The links forged between these criminal groups, terrorist movements, and insurgencies have resulted in a new type of threat: ever-evolving networks that exploit permissive OEs and the seams and gaps in policy and application of unified action to conduct their criminal, violent, and politically motivated activities. Threat networks adapt their structures and activities faster than countries can combat their illicit activities. In some instances, illicit networks are now running criminalized states. These adversaries have become the new normal, compelling governments toward integrated, innovative approaches to countering the growing dangers posed by transnational organized crime.

THREAT NETWORK UNDERSTANDING

The burned skeleton of a Boeing 727 aircraft outbound from Venezuela in November 2009, but registered in Guinea-Bissau, lays on a makeshift landing strip near Sinkrebaka, some nine miles from Gao, in remote northeastern Mali. According to Alexandre Schmidt of the United Nations Office of Drugs and Crime, the plane 'unloaded cocaine and other illegal substances' and 'wanted to take off but crashed'. Investigators later determined, however, that the aircraft had been destroyed after its illicit cargo, estimated at between seven and 11 tons of cocaine, had been offloaded. In June 2011, in an action directly related to the above-mentioned aircraft, three individuals were arrested and charged with international trafficking in cocaine.

On January 19, 2012, one of the three, a Malian businessman was reportedly freed by Malian authorities 'following a demand from a group of young Arabs' whom the Malian government has called upon to assist the Malian armed forces in their fight against Tuareg rebels.

The incident was, and continues to be, cited by many as yet more 'evidence' of a growing nexus between radical Islamist elements active across the Sahel region of northern Africa, and particularly in northern Mali, and drug traffickers and other national and transnational criminal syndicates.

This nexus can be broadly grouped in three categories: coexistence (they occupy and operate in the same geographic space at the same time), cooperation (they decide their interests are served, or at not least severely threatened, by temporarily working together), and convergence (each begins to engage in behavior(s) more commonly associated with the other).

The Sahel is a densely layered and intricately fragmented sub-region, and the criminals and terrorists who have chosen to operate there do so as participants in existing social, political and economic environments; they are not necessarily considered exogenous actors nor are they necessarily seen as threats. Far too often every event in the sub-region is trumpeted as a terror[ist] threat, despite the fact that most of the 'events' were kidnappings for ransom. Resorting to antiterrorism tactics has led to an exaggerated response by US drone and support personnel in Niger and French forces intervening in Mali, which has dragged West Africa militaries in for the foreseeable future.

Drawing the necessary distinctions and differentiations [between coexistence, cooperation, and convergence] allows the necessary planning to begin in order to deal with the matter, not only in the Sahel, but across the globe:

By knowing your enemies, you can find out what it is they want. Once you know what they want, you can decide whether to deny it to them and thereby demonstrate the futility of their tactics, give it to them, or negotiate and give them a part of it in order to cause them to end their campaign. By knowing your enemies, you can make an assessment not just of their motives but also their capabilities and of the caliber of their leaders and their organizations.

It is often said that knowledge is power. However, in isolation knowledge does not enable us to understand the problem or situation. Situational awareness and analysis is required for comprehension, while comprehension and judgment is required for understanding. It is this understanding that equips decision makers with the insight and foresight required to make effective decisions.

Extract from Alda, E., and Sala, J. L., Links Between Terrorism, Organized Crime and Crime: The Case of the Sahel Region*. Stability: International Journal of Security and Development,* 10 September 2014.

Intentionally Blank

APPENDIX C
COUNTERING THREAT NETWORKS IN THE MARITIME DOMAIN

1. Overview

The maritime domain connects a myriad of geographically dispersed nodes of friendly, neutral, and threat networks, and serves as the primary conduit for nearly all global commerce. The immense size, dynamic environments, and legal complexities of this domain create significant challenges to establishing effective maritime governance in many regions of the world. Threat networks encountered in the maritime domain frequently include criminal, terrorist, and insurgent elements, all of which will seek to exploit areas of poor maritime governance to establish sea lines of communication for logistics and maneuver. As such, a comprehensive CTN plan often includes a significant maritime component.

2. Operational Environment

The maritime domain comprises the oceans, seas, bays, estuaries, islands, coastal areas, riverine areas, and the airspace above, including the littorals. Per JP 2-01.3, *Joint Intelligence Preparation of the Operational Environment*, the littoral comprises two segments of the OE. First, seaward: the area from the shore to the open ocean, which must be controlled to support operations ashore. Second, landward: the area inland from the shore that can be supported and defended directly from the sea. CTN activities occur in all facets of the maritime domain, resulting in a vast spectrum of possible conditions in the OEs. CTN activities in the maritime domain require close coordination with complementary activities on land, and the seam between land and sea is itself an important consideration. Maritime operations are generally classified as blue water (high seas and open oceans), green water (coastal waters, ports, and harbors), or brown water (navigable rivers, lakes, bays, and estuaries). Each region requires unique planning considerations. Blue water operations can target threat network supply lines where their distance from sanctuary renders them more vulnerable to detection and disruption, while remaining outside of other nation's territorial seas avoids many legal and diplomatic complications. However, providing effective coverage of a large threat vector for prolonged periods demands considerable resources. Green water operations can concentrate agile force packages closer to known threat network nodes, but they require special logistics considerations for sustained deployment, as well as the cooperation of one or more HNs. Brown water operations share many of the advantages and challenges inherent to green water, with additional considerations for the unique capabilities necessary for maneuvering in shallow and congested waterways.

3. Considerations for Countering Threat Networks in the Maritime Environment

As with land-based operations, CTN activities in the maritime domain require close coordination between the joint force, interagency partners, and PNs to bring the right mix of capabilities and authorities to bear. Maritime CTN activities often cross geographic seams such as GCCs' AORs, territorial water boundaries, and various federal, state, and local jurisdictions. Additionally, threat network convergence blurs legal distinctions between criminals, terrorists, and combatants, thereby exposing seams in the authorities required to counter them. Well-established international and interagency relationships and coordination

mechanisms are essential to achieving the unity of effort necessary to successfully execute maritime CTN activities.

a. **Maritime Legal Considerations.** CTN maritime activities will often overlap with geographic boundaries that affect what actions can be taken in accordance with US and international law. **The United Nations Convention on the Law of the Sea (UNCLOS)** codifies international law pertaining to many aspects of maritime operations, including navigational rights, territorial seas limits, and passage of ships through narrow straits. Although this is recognized internationally, the UNCLOS has not been ratified by the US. Figure C-1 and the accompanying descriptions illustrate the relevant regions defined by UNCLOS. The legal protections afforded to a sovereign nation over its waters by UNCLOS can be modified in certain situations, such as pursuant to a United Nations Security Council resolution. For example, the United Nations authorized international militaries and organizations to enter Somalia's territorial waters and exclusive economic zone (EEZ) to conduct counter-piracy operations.

(1) **Internal Waters.** Internal waters are waters landward of the baseline of the territorial sea. For the US, this includes waters on the US side of the international boundary of the Great Lakes.

(2) **Territorial Sea.** Territorial seas are the waters within the belt that is 12 nautical miles wide and adjacent to the coast measured seaward from the baseline. States

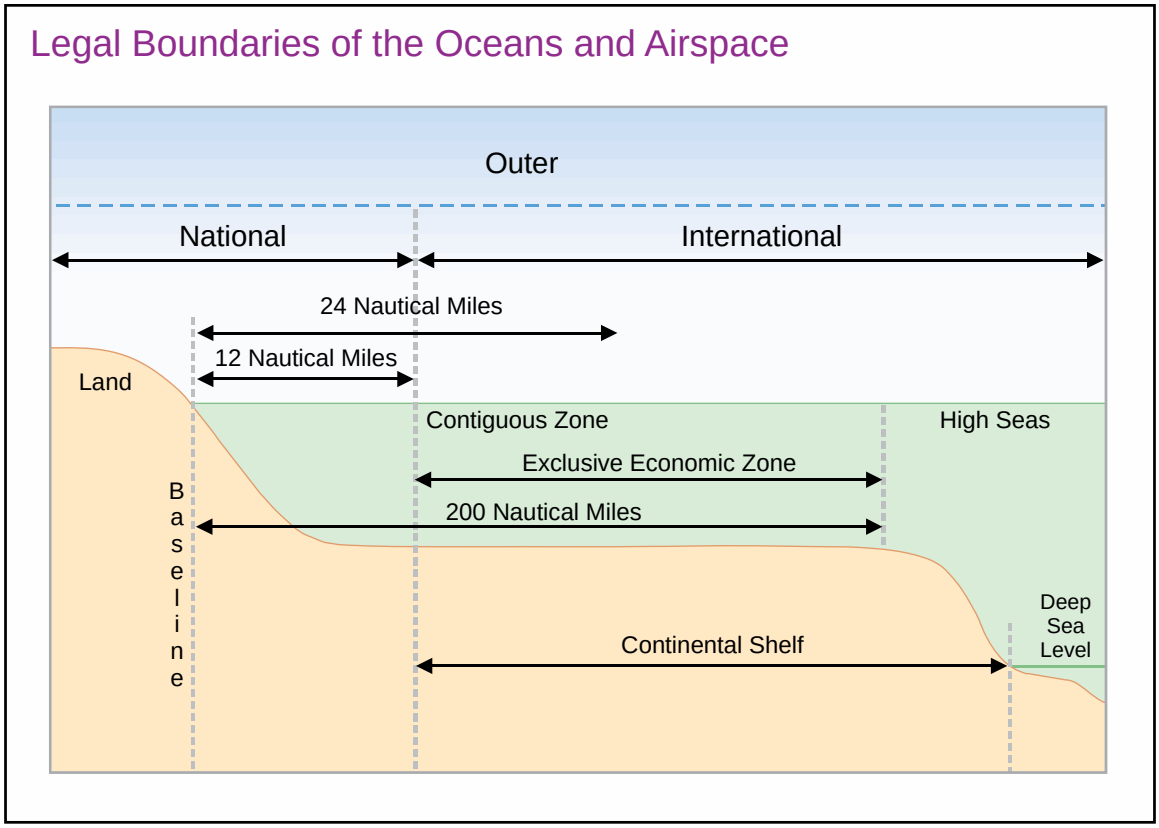


Figure C-1. Legal Boundaries of the Oceans and Airspace

have the right to establish the breadth of their territorial sea up to a limit not exceeding 12 nautical miles. For the purpose of enforcing some domestic US laws, the territorial sea extends only 3 miles seaward of the baseline.

(3) **Contiguous Zone.** Contiguous zones are the waters within the belt adjacent to and seaward of the territorial sea and extending to 24 nautical miles from the baseline.

(4) **Customs Waters.** Customs waters are generally described as US waters shoreward of a line drawn 12 nautical miles from the baseline (including territorial sea and inland waters with ready access to the sea).

(5) **EEZ.** An EEZ is the zone of waters beyond and adjacent to the territorial sea not extending beyond 200 miles from the baseline.

(6) **International Waters.** International waters are seaward of the outer limit of the territorial sea of any nation, but including the high seas, EEZ, and contiguous zones (when claimed seaward of the territorial sea).

(7) **High Seas.** High seas are all parts of the ocean seaward of the EEZ. If a nation has not proclaimed an EEZ, the high seas begin at the seaward edge of the territorial sea.

b. **Complementary Maritime Operations.** CTN LOEs in the maritime domain often correspond with other military operations. In cases where more than one mission is occurring simultaneously, the JFC should coordinate activities to avoid conflicting efforts. CTN activities will frequently overlap with one or more of the following:

(1) **CD Operations.** CD and CTN operations frequently share overlapping objectives because many threat networks, especially transnational criminal organizations, are tied directly or indirectly to the drug trade. Much of the illegal narcotics produced in source regions travels in bulk shipments along maritime routes before reaching its destination. At-sea interdictions deny millions of dollars in profits to transnational criminal organizations and can yield valuable intelligence. CD operations in the maritime domain will usually involve one or more law enforcement agencies in a primary role, with DOD forces in support. The United States Coast Guard (USCG) is the lead federal agency for maritime law enforcement, with broad law enforcement authorities in both domestic and international waters. Title 14, United States Code, gives the USCG statutory authority to make inquiries, examinations, inspections, searches, seizures, and arrests upon the high seas and waters over which the US has jurisdiction for the prevention, detection, and suppression of violations of the laws of the US. USCG vessels routinely conduct CD operations, and can embark law enforcement detachments onboard US and allied naval vessels to conduct boardings.

For additional information, refer to JP 3-07.4, Counterdrug Operations.

(2) **COIN.** Insurgents share the same vulnerability to maritime supply line targeting as other threat networks. However, detecting insurgent maritime activity in areas with dense coastal traffic often requires close inspection or boarding of numerous vessels, which can create force protection and resource availability challenges. One of the principal advantages to targeting insurgent networks from the maritime domain is that maritime forces

are often not subject to the same policy restrictions imposed by the US or HN government on military personnel allowed inside a particular country to support a COIN operation.

For additional information, refer to JP 3-24, Counterinsurgency.

(3) **Counter-Piracy.** Piracy occurs primarily in littoral areas with poor local governance and proximity to shipping lanes. Although piracy is by definition a maritime activity, applying the CTN methodology reveals that many of the root causes and critical network nodes exist on land. A successful counter-piracy campaign will usually combine operations to enhance maritime security with concurrent efforts to improve governance within the HN and the adoption of preventive measures by the maritime industry.

For additional information, refer to JP 3-16, Multinational Operations, *and Presidential Policy Directive-18,* Maritime Security.

(4) **CT.** Terrorist networks can be targeted directly or indirectly from the maritime domain. For CTN activities against narcoterrorist networks, the JFC must coordinate with PNs and interagency partners to establish a priority of objectives such as gathering of intelligence versus obtaining a criminal prosecution.

For additional information, refer to JP 3-26, Counterterrorism.

(5) **SFA and Security Cooperation.** Improving maritime governance in areas where threat networks operate is essential to eliminating the environments that allow illicit activity to thrive. SFA and security cooperation efforts designed to improve the capability of PNs to monitor and regulate their waters serve as an important enabler to that end.

c. **Maritime Operational Threat Response (MOTR).** The MOTR plan for the National Strategy for Maritime Security provides guidance for an integrated network of national-level maritime command centers to achieve coordinated, unified, timely, and effective planning and mission accomplishment by the USG. This integrated network consists of existing command or operations centers of the MOTR agencies, at the national level, to ensure a coordinated response consistent with desired national outcomes. MOTR addresses the full range of maritime security threats, including actionable knowledge of acts of terrorism, piracy, and other criminal or hostile acts committed by state and non-state actors. In the maritime domain, the MOTR plan:

(1) Directs the establishment of an integrated network of national-level maritime command centers to achieve coordinated, unified, timely, and effective planning and mission accomplishment.

(2) Sets forth lead and supporting federal agency roles and responsibilities for MOTR based on existing law, desired USG outcome, greatest potential magnitude of the threat, the response capabilities required, asset availability, and authority to act. Some of the applicable roles and responsibilities of the MOTR plan include:

(a) DOD is the pre-designated lead MOTR agency for tactical response and resolution of nation-state threats within the maritime domain.

(b) DOD is the pre-designated lead MOTR agency for maritime terrorist threats that occur in the forward maritime AORs. DOD will be prepared to take a lead or supporting role for response to maritime terrorist threats globally as part of the USG's active, layered defense of the US.

(c) The Department of Homeland Security (DHS) is the pre-designated lead MOTR agency for the interdiction of maritime threats in waters where DHS normally operates, except as otherwise noted in the plan.

(d) These pre-designated leads can shift to another MOTR agency dependent on changes in desired outcome or availability of assets.

(3) Directs clear coordination relationships and operational coordination requirements among the lead and supporting MOTR agencies. The MOTR coordination process is conducted through a virtual network of interagency national and operational command centers. This process includes protocols for interagency coordination, consultation, and assessment throughout MOTR execution. The MOTR protocols and procedures allow rapid response to short-notice (pop-up) threats and require interagency partners to begin coordination activities (i.e., MOTR conference calls) at the earliest possible opportunity when one of the following triggers is met:

(a) Any terrorist or foreign state threat exists and US agency response is anticipated.

(b) More than one federal department or agency has become or must become substantially involved in responding to the threat.

(c) A single agency or department lacks capability, capacity, or jurisdiction to address the threat.

(d) Upon resolving the threat, the initial responding federal department or agency cannot execute the disposition of cargo, people, or vessels acting under their own authority.

(e) The threat could have adverse effects on the foreign affairs of the US.

(4) This coordination process determines which department or agency is the right choice for leading the USG's response and what other agencies are needed to support the response effort. Additionally, this process includes protocols for transition of the lead from one agency to another and dispute resolution (i.e., if the USG's desired outcome cannot be resolved at the lower levels of government [e.g., operational level], the characterization of a particular threat could ultimately be elevated for Presidential resolution). At the tactical level, it is important to realize that the MOTR process exists not only to achieve the USG's desired outcome, but to coordinate and assist in bringing additional capabilities to bear on a threat.

CASE STUDY: COASTAL MARITIME INTERCEPTION OPERATIONS IN VIETNAM

During the Vietnam War, Viet Cong (VC) guerrillas exploited coastal and riverine shipping networks to transport weapons, troops, and supplies from North to South Vietnam. Initially, smuggling operations along the South China Sea provided the VC's main supply route into South Vietnam. Using small fishing vessels and other nondescript craft, VC supply vessels were nearly impossible to discern from normal maritime commerce. US commanders responded with a major coastal maritime interception operation called MARKET TIME. Operation MARKET TIME established Task Force 115, a large coastal maritime force comprised of Navy destroyers, mine sweepers, patrol craft, US Coast Guard cutters, and aircraft that patrolled the Mekong delta to identify and intercept clandestine VC vessels. To accomplish its mission, Task Force 115 units boarded up to 2,000 sampans and junks a day to check identification cards and search for contraband.

Operation MARKET TIME was the most successful US maritime operation during the Vietnam War. It had a major impact on the VC supply network, reducing the percentage of supplies the VC were able to obtain from South China Sea coastal routes from 70 to 10 percent between 1965 and 1966. Corresponding maritime operations such as GAME WARDEN and SEALORDS expanded patrols into rivers, canals, and lakes, and targeted other nodes such as VC installations and leadership.

Upon his departure as US Commander of American Forces in South Vietnam, General William Westmoreland stated, "MARKET TIME forces are a major element of my overall strategy without which we could not succeed. MARKET TIME forces have successfully blocked intrusions by sea, forcing the enemy to use the long tortuous Ho Chi Minh Trail, thus affecting significantly his ability to properly sustain his forces in the South."

Various Sources

APPENDIX D
IDENTITY ACTIVITIES SUPPORT TO COUNTERING THREAT NETWORK OPERATIONS

1. General

a. Identity activities are a collection of functions and actions that recognize and differentiate one person from another to support decision making. Identity activities include the collection of identity attributes and physical materials and their processing and exploitation. They support all-source analytic efforts; production of I2 and DOD law enforcement 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.

b. 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 human actor.

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

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

c. I2 fuses identity attributes and other information and intelligence associated with those attributes collected across all disciplines. I2 and DOD law enforcement criminal intelligence products are crucial to commanders', staffs', and components' ability 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 forensic capabilities 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. Biometric, forensic, and document and media exploitation (DOMEX) capabilities, when integrated with the traditional intelligence disciplines, can be highly effective in CTN.

2. Identity Activities Considerations

a. Identity activities leverage enabling intelligence activities to help identify threat actors by connecting individuals to other persons, places, events, or materials, analyzing patterns of life, and characterizing capability and intent to harm US interests.

b. The joint force J-2 is normally responsible for production of I2 within the CCMD.

(1) I2 products are normally developed through the JIPOE process and provide detailed information about threat activity identities in the OE. All-source analysis, coupled with identity information, significantly enhances understanding of the location of threat actors and provides detailed information about threat activity and potential high-threat areas within the OE. I2 products enable improved force protection, targeted operations, enhanced intelligence collection, and coordinated planning.

(2) The CCMD biometrics-enabled watch list (BEWL) is a subset of the DOD BEWL and is the authoritative watch list for a CCMD. The BEWL supports a broad array of missions to include targeting, vetting, control access, and CTN.

c. Development of I2 requires coordination throughout the USG and PNs, and may necessitate an intelligence federation agreement. During crises, joint forces may also garner support from the intelligence community through intelligence federation. Intelligence federation enables CCMDs to form support relationships with other theater joint intelligence operations centers, Service intelligence centers, joint reserve intelligence centers, or other DOD intelligence organizations to assist with the accomplishment of the joint force's mission. These support relationships, called federated partnerships, are preplanned agreements (formalized in operation plans, national intelligence support plans, or memorandums of agreement) intended to provide a rapid, flexible, surge capability enabling members of the intelligence community to assist the CCMD while remaining at their normal duty stations. Federated support can be provided in specific functional areas directly related to the crisis, or by assuming temporary responsibility for noncrisis-related areas within the GCCs' AORs, thereby freeing the supported command's organic assets to refocus on crisis support.

3. Identity Activities at the Strategic, Operational, and Tactical Levels

a. At the strategic level, identity activities are dependent on interagency and PN information and intelligence sharing, collaboration, and decentralized approaches to gain identity information and intelligence, provide analyses, and support the vetting the status (friendly, adversary, neutral, or unknown) of individuals outside the JFC's area of operations who could have an impact on the JFC's missions and objectives. Interagency partners and PNs also rely on the JFC for identity data developed at the tactical level to facilitate strategic-level decision making and actions.

b. At the operational level, identity activities employ collaborative and decentralized approaches blending technical capabilities and analytic abilities to provide identification and vetting of individuals within the AOR. Some CCDRs have established a dedicated office to manage identity activities and issued specific direction to guide operational employment.

CCMD-level identity activities inform all-source analysis. The resulting I2 product is disseminated through channels to inform all echelons about the potential adversary.

c. At the tactical level, identity information obtained via identity activities continues to support the unveiling of anonymities. Collection and analysis of identity-related data helps tactical commanders further understand the OE and to decide on the appropriate COAs with regards to individual(s) operating within it; as an example, identity information often forms the basis for targeting packages. In major combat operations, I2 products help provide the identities of individuals moving about the operational area who are conducting direct attacks on combat forces, providing intelligence for the enemy, and/or disrupting logistic operations. In COIN, identity information, as well as I2 products, can be integrated into mission sets such as cordon and search, checkpoints, population control and management, and other efforts to secure the population, strengthen HN security forces, and counter the threat's ideology and propaganda.

d. US Special Operations Command and partners currently deploy land-based exploitation analysis centers to rapidly process and exploit biometric data, documents, electronic media, and other material to support I2 operations and gain greater situational awareness of threats.

4. Policy and Legal Considerations for Identity Activities Support to Countering Threat Networks

a. The authorities to collect, store, share, and use identity data will vary depending upon the AOR and the PNs involved in the CTN activities. Different countries have strict legal restrictions on the collection and use of personally identifiable information, and the JFC may need separate bilateral and/or multinational agreements to alleviate partners' privacy concerns. Due to such legal complexities, one should consult with their staff judge advocate or legal advisor prior to the collection and use of personally identifiable information or biometric data.

b. Socio-cultural considerations also may vary depending upon the AOR. In some cultures, for example, a female subject's biometric data may need to be collected by a female. In other cultures, facial photography may be the preferred biometric collection methodology so as not to cross sociocultural boundaries.

c. Evidence-based operations and support to rule of law for providing identity data to HN law enforcement and judicial systems should be considered. The prosecution of individuals, networks, and criminals relies on identity data. However, prior to providing identity data to HN law enforcement and judicial systems, one should consult with their staff judge advocate or legal advisor.

For more information, refer to Joint Doctrine Note 1-16, Identity Activities.

Intentionally Blank

APPENDIX E
EXPLOITATION IN SUPPORT OF COUNTERING THREAT NETWORKS

1. Exploitation and the Joint Force

a. One of the major challenges confronting the joint force is the accurate identification of the threat network's key personnel, critical functions, and sources of supply. Threat networks often go to extraordinary lengths to protect critical information about the identity of their members and the physical signatures of their operations. These networks leave behind an extraordinary amount of potentially useful information in the form of equipment, documents, and even materials recovered from captured personnel. This information can lead to a deeper understanding of the threat network's nodes, links, and functions and assists in continuous analysis and mapping of the network. If the friendly force has the ability to collect and analyze the materials found in the OE, then they can gain the insights needed to cause significant damage to the threat network's operations. Exploitation provides a means to match individuals to events, places, devices, weapons, related paraphernalia, or contraband as part of a network attack.

b. Conflicts in Iraq and Afghanistan have witnessed a paradigm shift in how the US military's intelligence community supports the immediate intelligence needs of the deployed force and the type of information that can be derived from analysis of equipment, materials, documents, and personnel encountered on the battlefield. To meet the challenges posed by threat networks in an irregular warfare environment, the US military formed a deployable, multidisciplinary exploitation capability designed to provide immediate feedback on the tactical and operational relevance of threat equipment, materials, documents, and personnel encountered by the force. This expeditionary capability is modular, scalable, and includes collection, technical, and forensic exploitation and analytical capabilities linked to the national labs and the intelligence enterprise. It provides the joint force with the information and intelligence needed to answer CCIRs and enable subsequent operations; support force protection initiatives and refinement of friendly TTP; target key personnel and activities in a threat network including their supply chains; support interrogation and HN prosecution of detainees; and identify signatures associated with threat network activities.

c. Exploitation is accomplished through a combination of forward deployed and reachback resources to support the commander's operational requirements (see Figure E-1). The exact mix of resources will depend on the threats identified by JIPOE and the JFC's mission. Ideally, collection and exploitation capabilities should deploy early in the operation to assist in identifying the potential threats to friendly forces and prevent tactical surprise.

d. Exploitation employs a wide array of enabling capabilities and interagency resources, from forward deployed experts to small cells or teams providing scientific or technical support, or interagency or partner laboratories, and centers of excellence providing real-time support via reachback. Exploitation activities require detailed planning, flexible execution, and continuous assessment. Exploitation is designed to provide:

(1) Support to targeting, which occurs as a result of technical and forensic exploitation of recovered materials used to identify participants in the activity and provide

Exploitation Architecture

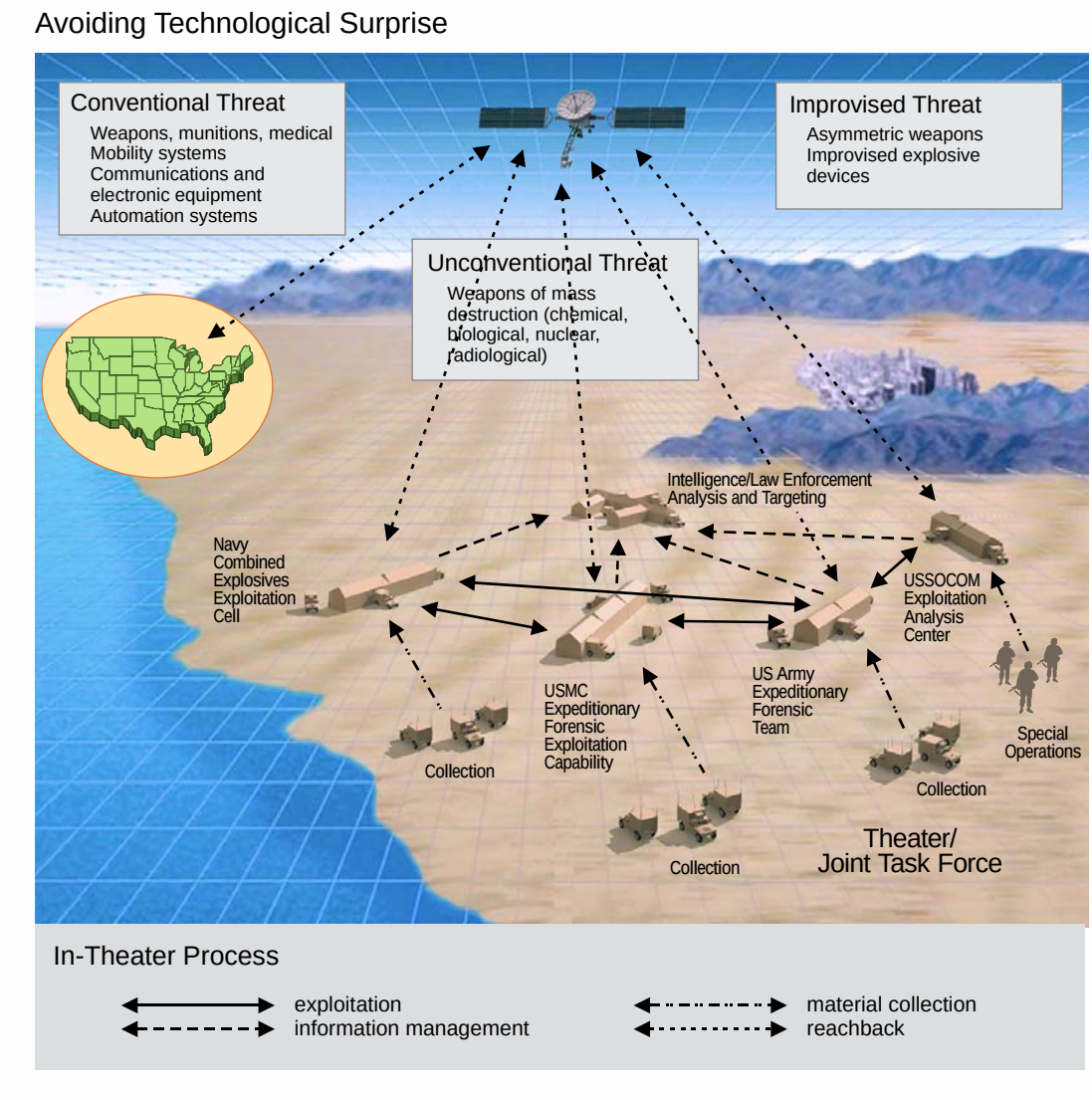


Figure E-1. Exploitation Architecture

organizational insights that are targetable. For example, when confronting an IED threat, technical exploitation and analysis of the IED can link a recovered device or materials to a particular bomb maker or insurgent cell through assembler patterns and components used.

(2) Support to component and material sourcing and tracking and supply chain interdiction uses exploitation techniques to determine origin, design, construction methods, components, and pre-cursors of threat weapons to identify where the materials originated, the activities of the threat's logistical networks, and the local supply sources. Once identified,

the threat network supply chain can be targeted for collection of additional information or for subsequent operations.

(3) Support to prosecution is accomplished when the results of the exploitation link individuals to illicit activities. When supporting law enforcement activities, recovered materials are handled with a chain of custody that tracks materials through the progressive stages of exploitation. The materials can be used to support detainment and prosecution of captured insurgents or to associate suspected perpetrators who are connected later with a hostile act.

(4) Support to force protection including identifying threat TTP and weapons' capabilities that defeat friendly countermeasures, including jamming devices and armor.

(5) Identification of signature characteristics derived from threat weapon fabrication and employment methods that can aid in cuing collection assets.

e. Tactical exploitation delivers preliminary assessments and information about the weapons employed and the people who employed them (see Figure E-2). Operational-level exploitation combines the outputs of tactical exploitation activities with more sophisticated exploitation results to inform all-source analysis. Operational-level exploitation can be conducted by deployed labs and provides detailed forensic and technical analysis of captured materials. When combined with all-source intelligence reporting, it supports detailed analysis of threat networks to inform subsequent targeting activities. In an irregular warfare environment, where the mission and time permit, commanders should routinely employ forensics-trained collection capabilities (explosive ordnance disposal [EOD] unit, weapons intelligence team [WIT], etc.) in their overall ground operations to take advantage of battlefield opportunities.

(1) Tactical exploitation begins at the point of collection. The point of collection includes turnover of material from HN government or civilian personnel, material and information discovered during a maritime interception operation, cache discovery, raid, IED incident, post-blast site, etc. These activities focus on gathering all relevant information and material and include limited field exploitation of that material as well as tactical questioning of any detained personnel to meet the immediate needs of tactical units. It informs recommendations for immediate adjustment to friendly TTP and can provide information to support immediate targeting of individuals or activities associated with local threat networks.

(2) Operational-level exploitation employs technical and forensic examination techniques of collected data and material and is conducted by highly trained examiners in expeditionary or reachback exploitation facilities. Information derived from operational exploitation supports operational activities, including but not limited to targeting, intelligence operations, force TTP enhancements, force protection initiatives, and regional activities to affect network supply sources/chains.

Levels of Exploitation

1. Tactical Collection and Exploitation	Collection, exploitation, and analysis conducted at the tactical level to provide timely and relevant information to help tactical commanders execute current operations or plan future ones.
2. In-Theater Operational Exploitation and Analysis	Occurring at the operational level and used primarily to identify associations between events, people, materials (improvised weapons; chemical, biological, radiological, and nuclear; conventional weapons).
3. Out of Theater Exploitation and Analysis Reachback	Provides strategic-theater support and leverages more advanced technical and forensic exploitation and analysis capabilities that usually exist outside of theater. Can deploy specialized teams to augment in-theater exploitation capabilities. Out of theater also applies to national-level exploitation capabilities that use advanced all-source analysis and scientific techniques to produce products that support national priorities.

Figure E-2. Levels of Exploitation

f. Strategic exploitation is designed to inform theater- and national-level decision makers. A commander's strategic exploitation assets may include forward deployed or reachback joint captured materiel exploitation centers and labs capable of conducting formally accredited and/or highly sophisticated exploitation techniques. These assets can respond to theater strategic intelligence requirements and, when very specialized capabilities are leveraged, provide support to national requirements. Strategic theater- and national-level exploitation capabilities facilitate the synthesis of multidisciplinary scientific, forensic, financial, and commercial intelligence information that exceeds the capabilities and time constraints characteristic of expeditionary capabilities. Strategic exploitation is designed to support national strategy and policy development. Strategic requirements usually involve targeting of high-value or high-priority actors, force protection design improvement programs, and source interdiction programs designed to deny the adversary externally furnished resources. An example of this level of exploitation is electronic exploitation of conventional or improvised weapon material to determine how electric components of a

STRATEGIC RELEVANCE OF EXPLOITATION

In October 2011, the Department of Justice unsealed an indictment describing the illegal export of electronic devices to Iran. Four men from Singapore had purchased 6,000 radio frequency (RF) modules through a Singapore front company, which were forwarded to Iran through third countries and ended up in improvised explosive devices (IEDs) in Iraq. Between 2008 and 2010, the US military recovered 16 of the RF modules from IEDs in Iraq. By locally exploiting the recovered IEDs, the US Government was able to trace the RF modules by serial number from the US to Iran and then to the IEDs in Iraq. This is an example of the strategic effects of technical exploitation—in this case, exposing third country support to an insurgency—and the importance of a continuum from collection through out-of-theater exploitation with connections to the broader intelligence community.

Various Sources

device or component function, including switches for arming and firing and their relationship to other features of the weapon system, including the mechanical components. For example, when dealing with radio-controlled IED, the analysis includes determining the radio frequency on which the device operates, which is critical to programming counter radio-controlled IED electronic warfare systems and equipment.

g. Exploitation activities are designed to provide a progressively detailed multidisciplinary analysis of materials recovered from the OE. From the initial tactical evaluation at the point of collection, to the operational forward deployed technical/forensic field laboratory and subsequent evaluation, the enterprise is designed to provide a timely, multidisciplinary analysis to support decision making at all echelons. Exploitation capabilities vary in scope and complexity, span peacetime to wartime activities, and can be applied during all military operations. Support ranges from providing exploitation advice and assistance to an HN during military engagement operations, to employing operational-level exploitation facilities during limited contingency and major operations, to supporting national-level requirements and activities.

2. Collection and Exploitation

a. An integrated and synchronized effort to detect, collect, process, and analyze information, materials, or people and disseminate the resulting facts provides the JFC with information or actionable intelligence. Collection involves gathering, preserving, and managing information and material taken from an incident site. Collection also includes the documentation of contextual information and material observed at the incident site or objective. All the activities vital to collection and exploitation are relevant to identity activities as many of the operations and efforts are capable of providing identity attributes used for developing I2 products. Specialized enablers, for example, EOD units, conduct collection, but other units, such as maritime visit, board, search, and seizure (VBSS) teams may also do so, if properly trained. Exploitation requires a team that possesses an appropriate level of competence in a broad range of scientific and technical disciplines and

that uses specialized equipment and automated information systems. While exploitation can occur at the incident site if required capabilities are available, more often it occurs at an off-site location where many of these capabilities can be established in a controlled environment.

(1) **Site Exploitation.** The JFC may employ hasty or deliberate site exploitation during operations to recognize, collect, process, preserve, and analyze information, personnel, and/or material found during the conduct of operations. Based on the type of operation, commanders and staffs assess the probability that forces will encounter a site capable of yielding information or intelligence and plan for the integration of various capabilities to conduct site exploitation. Commanders and staffs ensure subordinate elements are organized and equipped to effectively detect and collect information, materials, or people at an objective. A variety of organizations and resources are available to the JFC to conduct site exploitation.

(2) **Expeditionary Exploitation Capabilities.** Operational-level expeditionary labs are the focal point for the theater's exploitation and analysis activities that provide the commander with the time-sensitive information needed to shape the OE. The deployed laboratories conduct exploitation which includes technical exploitation and analysis, forensic and biometric exploitation/analysis, CBRN exploitation/analysis, DOMEX/analysis, and other functions as required. The information provided by these deployed labs may potentially influence force protection and training, network attack, and the defeat of asymmetric weaponry. Expeditionary labs generally evaluate materials in two broad categories: technical evaluation of captured weapons, including IEDs, and forensic examination of collected materials.

(a) **Technical Exploitation.** Technical exploitation includes electronic and mechanical examination and analysis of collected material. This process provides information regarding weapon design, material, and suitability of mechanical and electronic components of explosive devices, improvised weapons, and associated components. Technical exploitation results inform force protection activities, to include modification of friendly TTP, and efforts to detect and defeat asymmetric weapons. EOD and other specialized enablers will be required for technical evaluation of weapons, including IEDs.

1. **Electronic Exploitation.** Electronic exploitation at the operational level is limited and may require strategic-level exploitation available at reachback labs or forward deployed labs.

2. **Mechanical Exploitation.** Mechanical exploitation of material (mechanical components of conventional and improvised weapons and their associated platforms) focuses on devices incorporating manual mechanisms: combinations of physical parts that transmit forces, motion, or energy. In the case of IEDs, it can include things such as evaluation of munitions launch platforms and mechanical components that might be found in an IED, including alarm clock timers, pressure plates, or mechanical anti-tampering devices such as a trip wire.

(b) **Forensic Exploitation.** Forensic exploitation applies scientific techniques to link people with locations, events, and material that aid the development of targeting,

interrogation, and HN/PN prosecution support. Deployable exploitation assets include the forensic exploitation teams from the Army Defense Forensic Science Center, the US Marine Corps exploitation analysis cell-lite, and the US Special Operations Command exploitation analysis cell. These elements usually work with the combined explosives exploitation cell (CEXC) in operational areas where improvised weapons are a primary concern. These teams are scalable and can include latent print examiners, deoxyribonucleic acid (DNA) examiners, forensics chemists, firearms/tool marks examiners, and support personnel. Forensic exploitation includes:

1. **Latent Print Analysis.** Fingerprints recovered from weapons, bomb components, and other material enables biometric identification of people and their association with insurgent, terrorist, or criminal activities. It supports targeting, detainee interrogation, and HN/PN prosecution activities.

2. **DNA Analysis.** Comparison results of DNA samples collected from a variety of sources, including detainees, captured or recovered materials, and IED components. When fused with other information and intelligence, DNA results can be used to make associations between people, places, and things.

3. **Firearms and Tool Marks.** Examination of firearms and their associated components can determine whether a device was fabricated locally or by a foreign supplier and provides insights into the threat supply chains. Firearms exploitation also examines firearms, ammunition, ammunition components, gunshot residue, bullet trajectories, and other related material to determine the relationship of a firearm or other object to a person or event.

4. **Chemistry.** Chemistry is typically used to identify explosives, explosive precursors, and drugs. It is the basis for determining the components used in homemade explosives and informs friendly search teams on what to look for. Analysis of the chemical properties of an explosive sample provides information that can potentially influence force protection, sourcing, targeting, and prosecution.

(c) **DOMEX.** DOMEX consists of three exploitation techniques: document exploitation, cellular exploitation, and media exploitation. Documents, cell phones, and media recovered during collection activities, when properly processed and exploited, provide valuable information, such as adversary plans and intentions, force locations, equipment capabilities, and logistical status. Exploitable materials include paper documents such as maps, sketches, letters, cell phones, smart phones, and digitally recorded media such as hard drives and thumb drives.

b. **Expeditionary Laboratories**

(1) **Forensic Support.** The Army and Marine Corps have developed deployable forensic laboratories that are designed to provide a variety of forensic analysis for a joint force. These labs are modular and scalable to the needs of the supported command, depending on the type and level of threat. US Army labs, known as forensic exploitation teams, deploy from the Defense Forensic Science Center and are placed under the

operational control (OPCON) of the supported commander. The US Marine Corps expeditionary forensics cell-lite is assigned to the US Marine Corps law enforcement battalion and, when deployed, can also be placed under OPCON of the supported commander. Both organizations use reachback to the Defense Forensic Science Center for additional forensic analytical support. The supported commander's CCIRs and priority intelligence requirements set the priorities for these labs with the joint force exploitation staff element (J-2E) exercising staff supervision. When multiple labs are deployed, the supported commander may form a JTF for exploitation to provide administrative and logistical support to the deployed facilities.

(2) **Technical Support.** Unless subject matter experts from national resources have been deployed to assist in theater forensic facilities, the US Navy CEXC is the primary deployed laboratory for the technical exploitation of conventional and improvised weaponry. The CEXC is also placed under OPCON of the supported commander and usually collocates with the forensic labs to provide mutual support. In conventional warfare, the CEXC can expect to support the joint captured materiel exploitation center in exploiting captured enemy ordnance and associated systems. In irregular warfare, the CEXC will more likely support a counter-IED task force or other designated expeditionary forensic capability. The CEXC can provide C2 to other forensic activities.

(3) Forensic and technical facilities regularly cooperate on their cases, sharing capabilities as needed to provide seamless support to the joint force. See Figure E-3.

c. **Reachback to Theater-National-Specialized Exploitation Capabilities.** With reachback to additional specialized exploitation capabilities to support mission objectives, commanders have the ability to call upon a full range of national resources and multinational partners to assist forward deployed resources. The reachback capability improves the depth of the exploitation and provides analytical support that facilitates network targeting, force protection initiatives, and support to prosecution.

3. Supporting the Intelligence Process

a. Within their operational areas, commanders are concerned with identifying the members of and systematically targeting the threat network, addressing threats to force protection, denying the threat network access to resources, and supporting the rule of law. Information derived from exploitation can provide specific information and actionable intelligence to address these concerns. Exploitation reporting provides specific information to help answer the CCIRs. Exploitation analysis is also used to inform the intelligence process by identifying specific individuals, locations, and activities that are of interest to the commander (see Figure E-4).

b. Exploitation products may inform follow-on intelligence collection and analysis activities. Exploitation products can facilitate a more refined analysis of the threat network's likely activities and, when conducted during shape and deter phases, typically enabled by HN, interagency and/or international partners, can help identify threats and likely countermeasures in advance of any combat operations. For example, when facing an IED threat, exploitation capabilities assist in characterizing the OE by determining the types of

United States Army Expeditionary Forensic Facility in Afghanistan

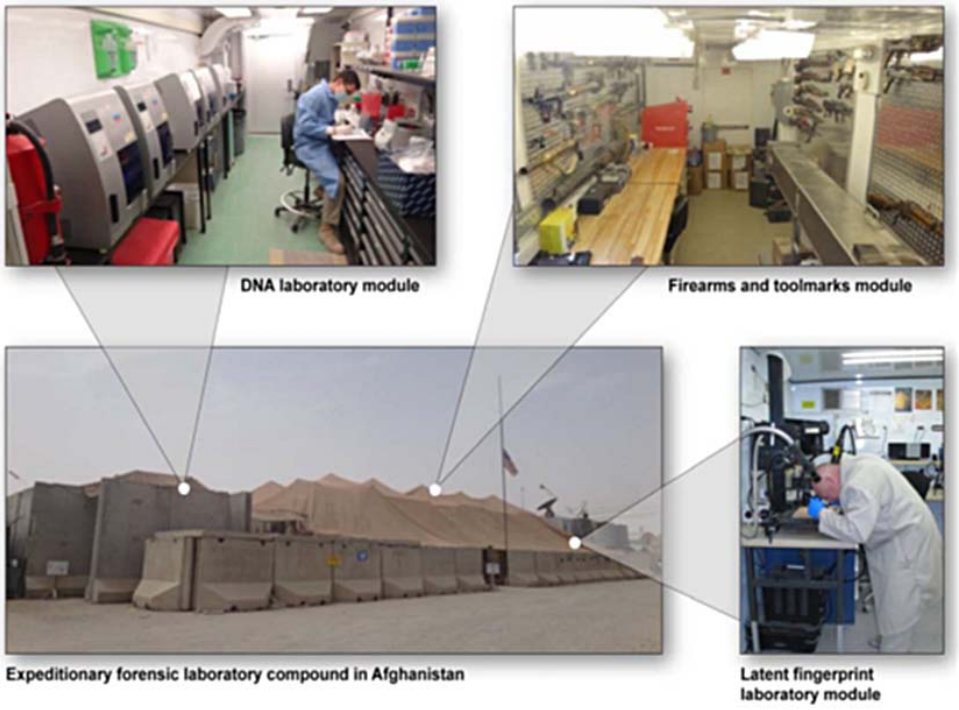


Figure E-3. United States Army Expeditionary Forensic Facility in Afghanistan

improvised weapons and IEDs used in the operational area and associating them to specific threat organizations.

4. Exploitation Organization and Planning

a. A wide variety of Service and national exploitation resources and capabilities are available to support forward deployed forces. These deployable resources are generally scalable and can make extensive use of reachback to provide analytical support. The JIPOE product will serve as a basis for determining the size and mix of capabilities that will be required to support initial operations. Managing these capabilities may initially be the responsibility of the J-2, the operations directorate of a joint staff (J-3), or a special staff section. A J-2E may be required for longer operations. Should the operation expand in size or intensity, the JFC may choose to establish an exploitation task force to manage exploitation activities in support of the joint force.

b. **J-2E.** 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 the adversary network. The JFC can establish a J-2E, in coordination with the J-3, 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, law enforcement, multinational, and HN

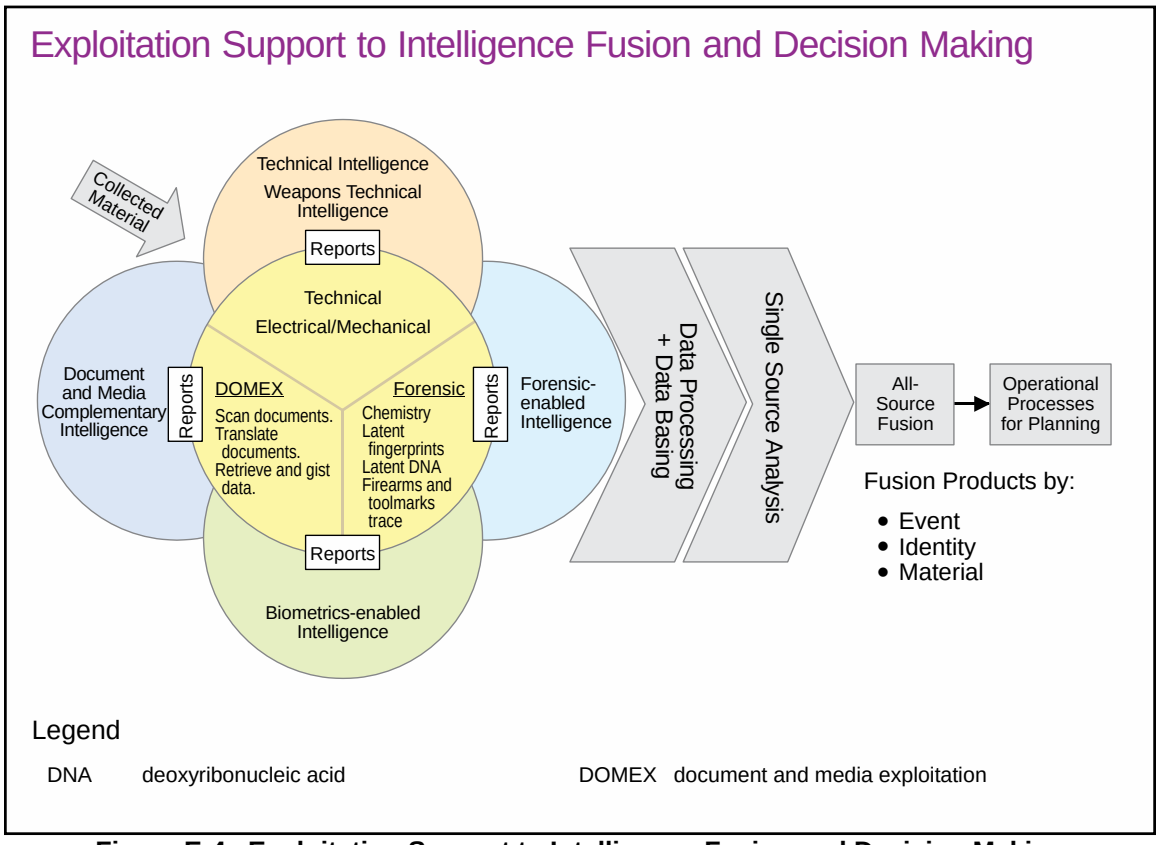


Figure E-4. Exploitation Support to Intelligence Fusion and Decision Making

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:

(1) 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 faced, military geographic factors, and authorities granted to collect and process captured material.

(2) Ensure 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.

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

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

(5) Ensure that exploitation enablers are integrated and synchronized at all levels and their activities support collection on behalf of the commander's priority intelligence requirements. 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.

c. **Exploitation Task Force**

(1) As an alternative to using the JFC's staff to manage exploitation activities, the JFC can establish an exploitation task force, integrating tactical-level and operational-level organizations and streamlining communications under a single headquarters whose total focus is on the exploitation effort. The task force construct is useful when a large number of exploitation assets have been deployed to support large-scale, long-duration operations. The organization and employment of the task force will depend on the mission, the threat, and the available enabling forces. The task force is normally built around an appropriately augmented brigade-level headquarters or its equivalent. In addition to controlling the subordinate organizations and battalions, the exploitation task force commander may exercise tactical control of the JFC's specialized collection and exploitation assets as necessary. The combination of collection assets with specialized exploitation enablers allows the task force to conduct focused threat network analysis and targeting, provide direct support packages of exploitation enablers to higher headquarters, and organize and conduct unit-level training programs.

(2) In establishing a task force to manage exploitation activities, the JFC will normally align supporting resources to provide the task force commander with the means necessary to accomplish the mission. Under the task force construct, the exploitation task force provides task-organized teams of exploitation resources in direct support of the components. The components provide sustainment to the assigned exploitation team. These teams may include specialized personnel from the following:

(a) **Site Exploitation Teams.** These units are task-organized teams specifically detailed and trained at the tactical level. The mission of site exploitation teams is to conduct systematic discovery activities and search operations, and properly identify, document, and preserve the point of collection and its material.

(b) **EOD Teams.** EOD personnel have special training and equipment to render safe explosive ordnance and IEDs, make intelligence reports on such items or components, and supervise the safe removal thereof. EOD personnel exploit an incident site, providing post-blast investigation expertise and site exploitation support, including a tactical characterization of the incident and a technical categorization of the device. They recognize, preserve, and collect items of exploitation value.

(c) **WITs.** WITs are task-organized teams, often with organic EOD support that exploit a site of intelligence value by collecting IED-related material, performing tactical questioning, collecting forensic materials, including latent fingerprints, preserving and documenting DOMEX, including cell phones and other electronic media, providing in-depth documentation of the site, including sketches and photographs, evaluating the effects of threat weapons systems, and preparing material for evacuation.

(d) **CBRN Response Teams.** When WMD or hazardous CBRN precursors may be present, CBRN response teams can be detailed to supervise the site exploitation. CBRN response team personnel are trained to properly recognize, preserve, neutralize, and collect hazardous CBRN or explosive materials. The teams may have an integrated EOD capability to enhance CBRN activities and mitigate threats.

(e) In a maritime environment, US Navy surface combatants employ VBSS teams to detect CBRN materials; collect biometrics; conduct tactical questioning; and preserve and document captured enemy documents and media, including cell phones and contextual and electronic data for DOMEX. Marine Corps units employ heliborne VBSS teams for the same purpose. Marine Corps and Navy VBSS teams can be augmented by intelligence exploitation teams to facilitate HUMINT and tactical site exploitation activities. Where IEDs or explosive hazards are likely, EOD and CEXC platoons can be assigned to support the VBSS missions.

(f) **DOMEX.** DOMEX support is scalable and ranges from a single liaison offer, utilizing reachback for full analysis, to a fully staffed joint document exploitation center for primary document exploitation.

APPENDIX F
THE CLANDESTINE CHARACTERISTICS OF THREAT NETWORKS

1. Introduction

a. Maintaining regional stability continues to pose a major challenge for the US and its PNs. The threat takes many forms from locally based to mutually supporting and regionally focused transnational criminal organizations, terrorist groups, and insurgencies that leverage global transportation and information networks to communicate and obtain and transfer resources (money, material, and personnel). In the long term, for the threat to win it must survive and to survive it must be organized and operate so that no one strike will cripple the organization. Today's threat networks are characterized by flexible organizational structures, adaptable and dynamic operational capabilities, a highly nuanced understanding of the OE, and a clear vision of their long-term goals.

b. While much has been made of the revolution brought about by technology and its impact on a threat network's organization and operational methods, the impacts have been evolutionary rather than revolutionary. The threat network is well aware that information technology, while increasing the rate and volume of information exchange, has also increased the risk to clandestine operations due to the increase in electromagnetic and cyberspace signatures, which puts these types of communications at risk of detection by governments, like the USG, that can apply technological advantage to identify, monitor, track, and exploit these signatures.

c. When it comes to designing a resilient and adaptable organizational structure, every successful threat network over time adopted the traditional clandestine cellular network architecture. This type of network architecture provides a means of survival in form through a cellular or compartmentalized structure; and in function through the use of clandestine arts or tradecraft to minimize the signature of the organization—all based on the logic that the primary concern is that the movement needs to survive to attain its political goals.

d. When faced with a major threat or the loss of a key leader, clandestine cellular networks contain the damage and simply morph and adapt to new leaders, just as they morph and adapt to new terrain and OEs. In some cases the networks are degraded, in others they are strengthened, but in both cases, they continue to fight on, winning by not losing. It is this "logic" of clandestine cellular networks—winning by not losing—that ensures their survival.

e. CTN activities that focus on high-value or highly connected individuals (organizational facilitators) may achieve short-term gains but the cellular nature of most threat networks allows them to quickly replace individual losses and contain the damage. Operations should isolate the threat network from the friendly or neutral populations, regularly deny them the resources required to operate, and eliminate leadership at all levels so friendly forces can deny them the freedom of movement and freedom of action the threat needs to survive.

2. Principles of Clandestine Cellular Networks

The survival of clandestine portions of a threat network organization rests on six principles: compartmentalization, resilience, low signature, purposeful growth, operational risk, and organizational learning. These six principles can help friendly forces to analyze current network theories, doctrine, and clandestine adversaries to identify strengths and weaknesses.

a. Compartmentalization comes both from form and function and protects the organization by reducing the number of individuals with direct knowledge of other members, plans, and operations. Compartmentalization provides the proverbial wall to counter friendly exploitation and intelligence-driven operations.

b. Resilience comes from organizational form and functional compartmentalization and not only minimizes damage due to counter network strikes on the network, but also provides a functional method for reconnecting the network around individuals (nodes) that have been killed or captured.

c. Low signature is a functional component based on the application of clandestine art or tradecraft that minimizes the signature of communications, movement, inter-network interaction, and operations of the network.

d. Purposeful growth highlights the fact that these types of networks do not grow in accordance with modern information network theories, but grow with purpose or aim: to gain access to a target, sanctuary, population, intelligence, or resources. Purposeful growth primarily relies on clandestine means of recruiting new members based on the overall purpose of the network, branch, or cell.

e. Operational risk balances the acceptable risk for conducting operations to gain or maintain influence, relevance, or reach to attain the political goals and long-term survival of the movement. Operations increase the observable signature of the organization, threatening its survival. Clandestine cellular networks of the underground develop overt fighting forces (rural and urban) to interact with the population, the government, the international community, and third-party countries conducting FID in support of the government forces. This interaction invariably leads to increased observable signature and counter-network operations against the network's overt elements. However, as long as the clandestine core is protected, these overt elements are considered expendable and quickly replaced.

f. Organizational learning is the fundamental need to learn and adapt the clandestine cellular network to the current situation, the threat environment, overall organizational goals, relationships with external support mechanisms, the changing TTP of the counter network forces, new technologies, and the physical dimension, human factors, and cyberspace.

3. Organization of Clandestine Cellular Networks

a. Clandestine elements of an insurgency use form—organization and structure—for compartmentalization, relying on the basic network building block, the compartmented cell, from which the term cellular is derived. The cell size can differ significantly from one to any

number of members, as well as the type of interaction within the cell, depending on the cell's function. There are generally three basic functions—operations, intelligence, and support. The cell members may not know each other, such as in an intelligence cell, with the cell leader being the only connection between the other members. In more active operational cells, such as a direct-action cell, all the members are connected, know each other, perhaps are friends or are related, and conduct military-style operations that require large amounts of communications. Two or more cells linked to a common leader are referred to as branches of a larger network. For example, operational cells may be supported by an intelligence cell or logistics cell. Building upon the branch is the network, which is made up of multiple compartmentalized branches, generally following a pattern of intelligence (and counterintelligence) branches, operational branches (direct action or urban guerrilla cells), support branches (logistics and other operational enablers like propaganda support), and overt political branches or shadow governments (see Figure F-1).

b. The key concept for organizational form is compartmentalization of the clandestine cellular network (i.e., each element is isolated or separated from the others). Structural compartmentalization is in two forms: the cut-out, which is a method ensuring that opponents are unable to directly link two individuals together, and through lack of knowledge; no personal information is known about other cell members, so capture of one does not put the others at risk. In any cell where the members must interact directly, such as in an operational or support cell, the entire cell may be detained, but if the structural compartmentalization is sound, then the counter-network forces will not be able to exploit the cell to target other cells, the leaders of the branch, or overall network.

c. The basic model for a cellular clandestine network consists of the underground, the auxiliary, and the fighters. The underground and auxiliary are the primary components that utilize clandestine cellular networks; the fighters are the more visible overt action arm of the insurgency (Figure F-2). The underground and auxiliary cannot be easily replaced, while the fighters can suffer devastating defeats (Fallujah in 2006) without threatening the existence of the organization.

d. The underground is responsible for the overall command, control, communications, information, subversion, intelligence, and covert direct action operations, such as terrorism, sabotage, and intimidation. The original members and core of the threat network generally operate as members of the underground. The underground cadres develop the organization, ideally building it from the start as a clandestine cellular network to ensure its secrecy, low-signature, and survivability. The underground members operate as the overarching leaders, leaders of the organization cells, training cadres, and/or subject matter experts for specialized skills, such as propaganda, bomb making, or communications.

Example of a Clandestine Network

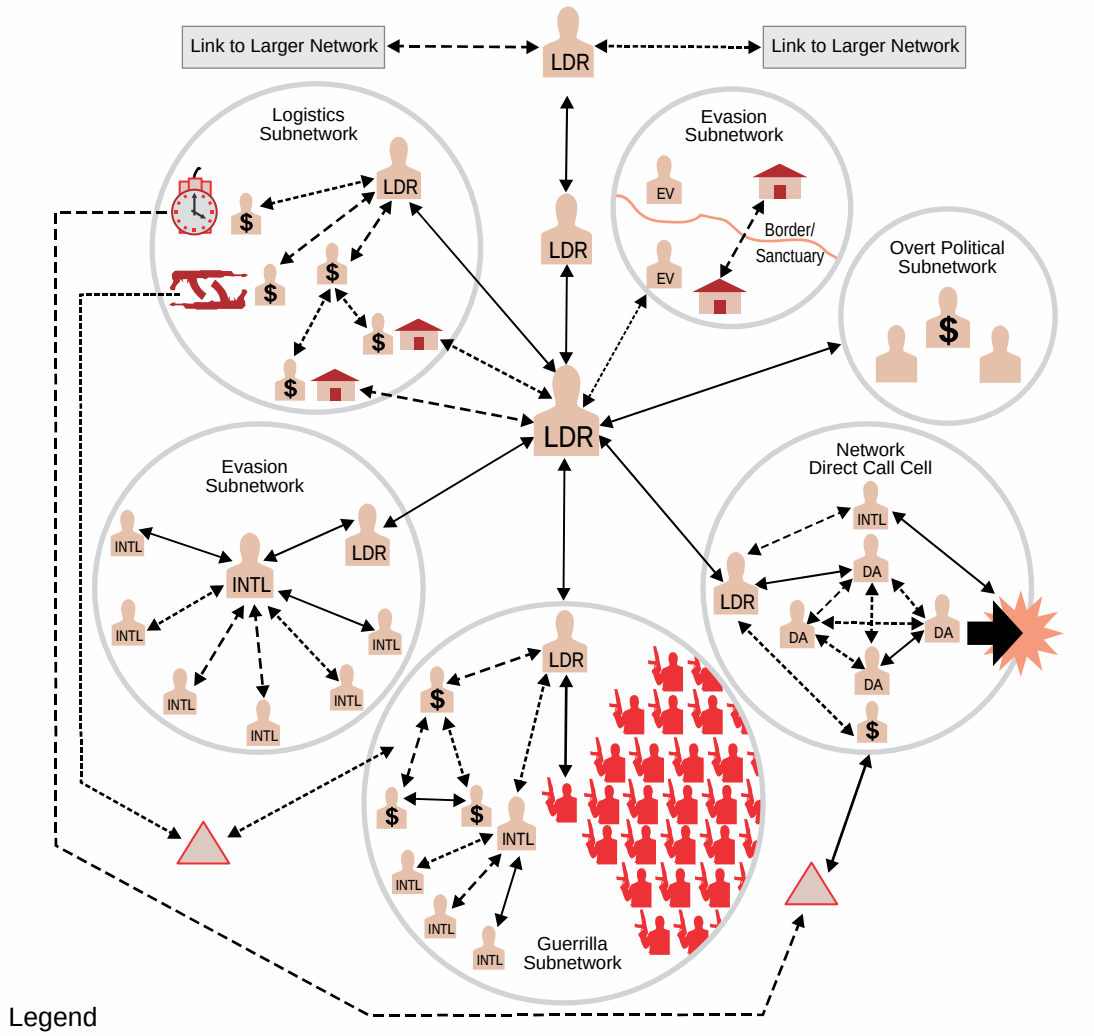


Figure F-1. Example of a Clandestine Network

Organization and Function

Underground	Auxiliary	Fighters
Command and control	Logistics	Low-level fighters
Communications	Operational support	Improvised explosive device employers
Information (media)	Intelligence collection	
Intelligence	Transportation	
Covert direct action	Specialized skills — improvised explosive device designers	

Figure F-2. Organization and Function

e. The auxiliary is the clandestine support personnel, directed by the underground, which provide logistics, operational support, and intelligence collection of the underground and the fighters. The auxiliary members use their normal daily routines to provide them cover for their activities in support of the threat, to include freedom of movement to transport materials and personnel, specialized skills (electricians, doctors, engineers, etc.), or specialized capabilities for operations. These individuals may hold jobs such as local security forces, doctors and nurses, shipping and transportation specialists, and businesspeople that provide them with a reason for security forces to allow them freedom of movement even in a crisis.

f. The fighters are the most visible and the most easily replaced members of the threat network. While their size and armament will vary, they use a more traditional hierarchical organizational structure. The fighters are normally used for the high-risk missions where casualties are expected and can be recovered from in short order.

4. The Elements of a Clandestine Cellular Network

a. A growing insurgency/terrorist/criminal movement is a complex undertaking that must be carefully managed if its critical functions are to be performed successfully. Using the clandestine cellular model, the organization's leader and staff will manage a number of subordinate functional networks (Figure F-3).

b. These functional networks will be organized into small cells, usually arranged so that only the cell leader knows the next connection in the organization. As the organization grows, the number of required interactions will increase, but the number of actively participating members in those multicellular interactions will remain limited. Unfortunately, the individual's increased activity also increases the risk of detection. The functional

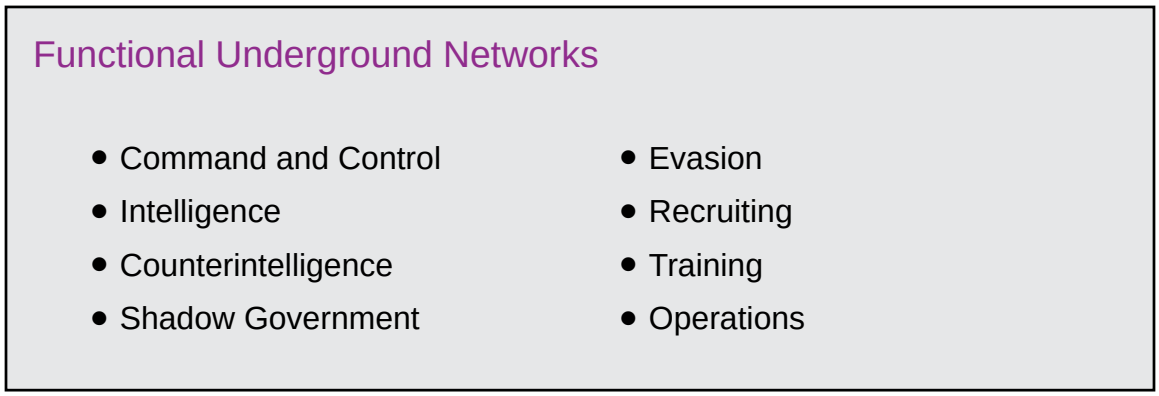


Figure F-3. Functional Underground Networks

network's managers ensure that critical functions are being performed, appropriately resourced, coordinated, and synchronized, and supporting organizational goals.

c. Clandestine cellular networks are largely decentralized for execution at the tactical level, but maintain a traditional or decentralized hierarchical form above the tactical level. The core leadership may be an individual, with numerous deputies, which can limit the success of decapitation strikes. Alternatively, the core leadership could be in the form of a centralized group of core individuals, which may act as a centralized committee. The core could also be a coordinating committee of like-minded threat leaders who coordinate their efforts, actions, and effects for an overall goal, while still maintaining their own agendas. Without centralized control, the organization would not be able to effectively develop a strategy based on ends, ways, and means, since each individual or group would not be bound to the common vision that a hierarchy provides.

d. To maintain a low signature necessary for survival, network leaders give maximum latitude for tactical decision making to cell leaders. This allows them to maintain tactical agility and freedom of action based on local conditions. The key consideration of the underground leader, with regard to risk versus maintaining influence, is to expose only the periphery tactical elements to direct contact with the counter-network forces. This allows

LASTING SUCCESS

For the counter-network operator, the goal is to conduct activities that are designed to break the compartmentalization and facilitate the need for direct communication with members of other cells in the same branch or members of other networks. By maintaining pressure and leveraging the effects of a multi-nodal attack, friendly forces could potentially cause a catastrophic "cascading failure" and the disruption, neutralization, or destruction of multiple cells, branches, or even the entire network. Defeat of a network's overt force is only a setback. Lasting success can only come with securing the relevant population, isolating the network from external support, and identifying and neutralizing the hard-core members of the network.

Various Sources

local adaptability to counter-network tactics, as well as agility to maintain pressure on the friendly force without getting decisively engaged or exposing the clandestine network.

e. Even with rigorous compartmentalization and internal discipline, there are structural weaknesses that can be detected and exploited. These structural points of weaknesses include the interaction between the underground and the auxiliary and between the auxiliary and the fighters and the interaction with external networks (transnational criminal, terrorist, other insurgents) who may not have the same level of compartmentalization.

5. Network Descriptors

a. Networks and cells can be described as open or closed. Understanding whether a network or cell is open or closed helps the intelligence analysts and planners to determine the scale, vulnerability, and purpose behind the network or cell. An open network is one that is growing purposefully, recruiting members to gain strength, access to targeted areas or support populations, or to replace losses. Given proper compartmentalization, open networks provide an extra security buffer for the core movement leaders by adding layers to the organization between the core and the periphery cells. Since the periphery cells on the outer edge of the network have higher signatures than the core, they draw the friendly force's attention and are more readily identified by the friendly force, protecting the core.

b. Closed cells or networks have limited or no growth, having been hand selected or directed to limit growth in order to minimize signature, chances of compromise, and to focus on a specific mission. While open networks are focused on purposeful growth, the opposite is true of the closed networks that are purposefully compartmentalized to a certain size based on their operational purpose. This is especially pertinent for use as terrorist cells, made up of generally closed, non-growing networks of specially selected or close-knit individuals. Closed networks have an advantage in operational security since the membership is fixed and consists of trusted individuals. Compartmentalizing a closed network protects the network from infiltration, but once penetrated, it can be defeated in detail.

Intentionally Blank

APPENDIX G
SOCIAL NETWORK ANALYSIS

1. Introduction

a. In military operations, maps have always played an important role as an invaluable tool to better understanding the OE. Understanding the physical terrain is often secondary to understanding the people. Identifying and understanding the human factors is critical. The ability to map, visualize, and measure threat, friendly, and neutral networks to identify key nodes enables commanders at the strategic, operational, and tactical levels to better optimize solutions and develop the plan.

b. Planners should understand the environment made up of human relationships and connections established by cultural, tribal, religious, and familial demographics and affiliations.

c. By using advanced analytical methodologies such as SNA, analysts can map out, visualize, and understand the human factors.

2. Social Network Analysis

a. **Overview**

(1) SNA is a method that provides the identification of key nodes in the network based on four types of centrality (i.e., degree, closeness, betweenness, and eigenvector) using network diagrams. SNA focuses on the relationships (links or ties) between people, groups, or organizations (called nodes or actors). SNA does this by providing tools and quantitative measures that help to map out, visualize, and understand networks and the relationships between people (the human factors) and how those networks and relationships may be influenced. Network diagrams, a graphical depiction of network analysis, used within SNA are referred to as sociograms that depict the social community structure as a network with ties between nodes (see Figure G-1). Like physical terrain maps of the earth, sociograms can have differing levels of detail.

(2) SNA provides a deeper understanding of the visualization of people within social networks and assists in ranking potential ability to influence or be influenced by those social networks. SNA provides an understanding of the organizational dynamics of a social network, which can be used for detailed analysis of a network to determine options on how to best influence, coerce, support, attack, or exploit them. In particular, it allows planners to identify and portray the details of a network structure, illuminate key players, highlight cohesive cells or subgroups within the network and identify individuals or groups that can or cannot be influenced, supported, manipulated, or coerced.

(3) SNA helps organize the informality of illusive and evolving networks. SNA techniques highlight the structure of a previously unobserved association by focusing on the preexisting relationships and ties that bind groups together. By focusing on roles, organizational positions, and prominent or influential actors, planners can analyze the

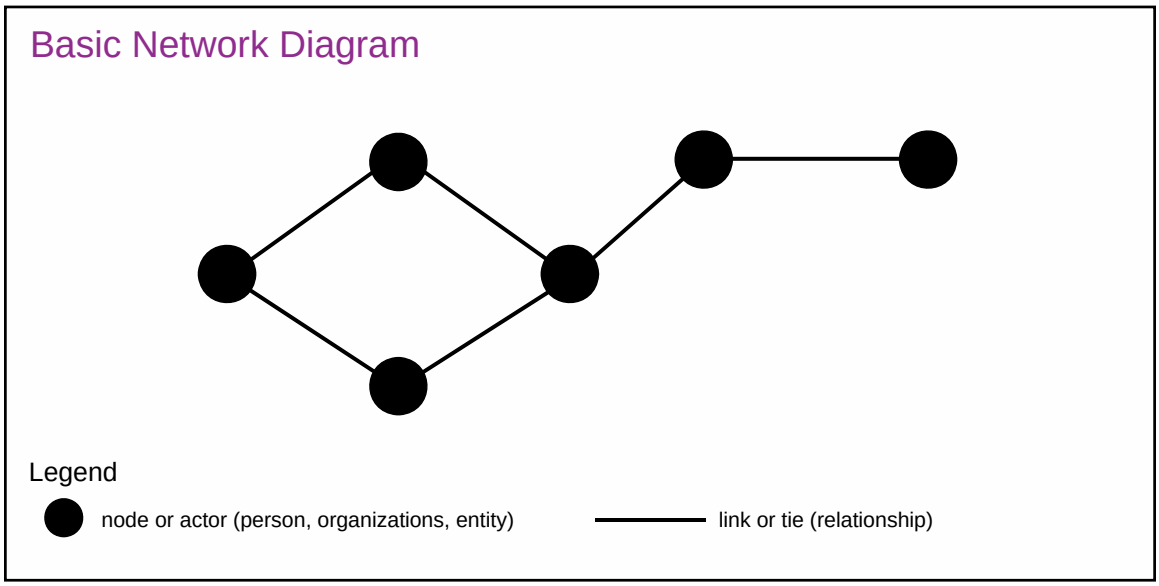


Figure G-1. Basic Network Diagram

structure of an organization, how the group functions, how members are influenced, how power is exerted, and how resources are exchanged. These factors allow the joint force to plan and execute operations that will result in desired effects on the targeted network.

(4) The physical, cultural, and social aspects of human factors involve complicated dynamics among people and organizations. These dynamics cannot be fully understood using traditional link analysis alone. SNA is distinguished from traditional, variable-based analysis that typically focuses on a person's attributes such as gender, race, age, height, income, and religious affiliation. While personal attributes remain fairly constant, social groups, affiliations or relationships constantly evolve. For example, a person can be a storeowner (business social network), a father (kinship social network), a member of the local government (political social network), a member of a church (religious social network), and be part of the insurgent underground (resistance social network). A person's position in each social network matters more than their unchanging personal attributes. Their behavior in each respective network changes according to their role, influence, and authority in the network.

b. **Analysis**

(1) **Metrics.** Analysts draw on a number of metrics and methods to better understand human networks. Common SNA metrics are broadly categorized into three metric families: network topology, actor centrality, and brokers and bridges.

(a) **Network Diagram.** Network topology is used to measure the overall network structure, such as its size, shape, density, cohesion, and levels of centralization and hierarchy (see Figure G-2). These types of measures can provide an understanding of a network's ability to remain resilient and perform tasks efficiently. Network topology provides the planner with an understanding of how the network is organized and structured.

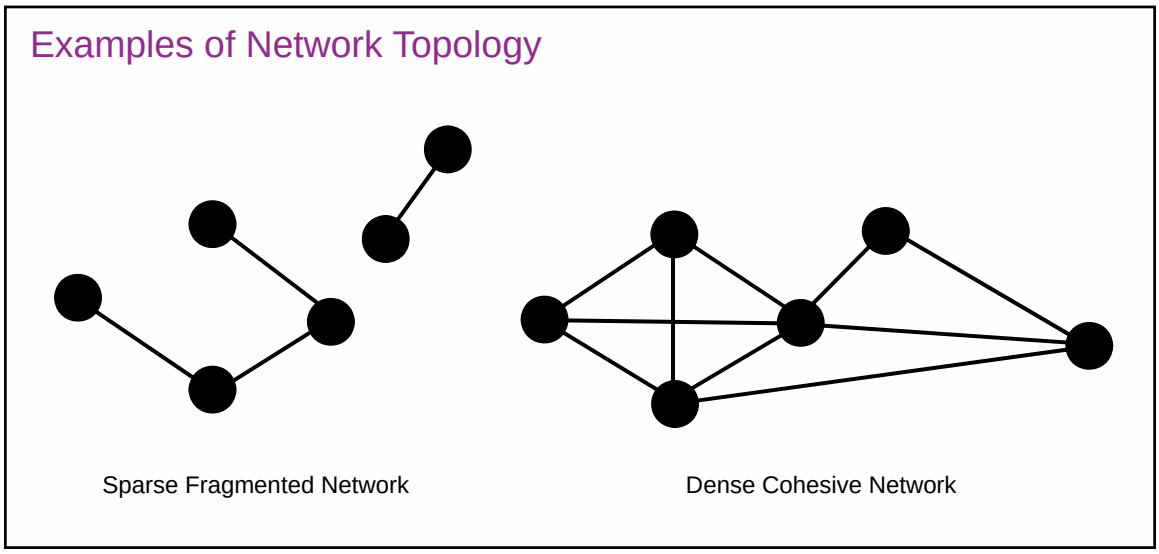


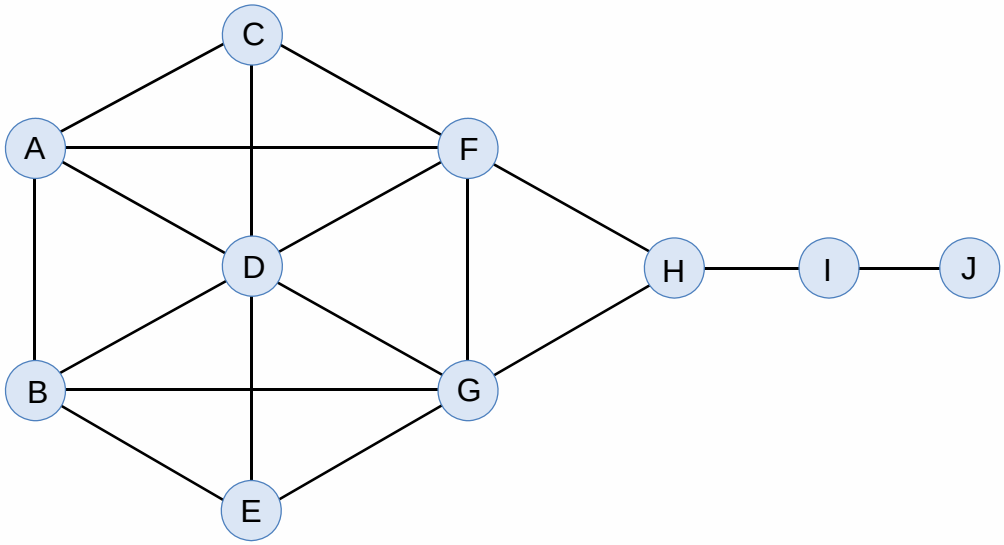
Figure G-2. Examples of Network Topology

(b) **Centrality.** Indicators of centrality identify the key nodes within a network diagram, which may include identifying influential person(s) in a social network. Identification of the centrality helps identify key nodes in the network and illuminate potential leaders and can lead analysts to potential brokers within the network (see Figure G-3). Centrality also measures and ranks people and organizations within a network based on how central they are to that network.

1. **Degree Centrality.** The degree centrality of a node is based purely on the number of nodes it is linked to and the strength of those nodes. It is measured by a simple count of the number of direct links one node has to other nodes within the network. While this number is meaningless on its own, higher levels of degree centrality compared to other nodes may indicate an individual with a higher degree of power or influence within the network. As indicated in Figure G-3, node D has the highest number of direct links to other nodes (high degree of centrality) and is an example of what may be termed a hub. A network centralized around a well-connected hub may be efficient but can fail abruptly if that hub is disabled or removed. In this example, node D would likely be designated a key node. Nodes with a low degree of centrality (few direct links) are sometimes described as peripheral nodes (e.g., nodes I and J in Figure G-3). Although they have relatively low centrality scores, peripheral nodes can nevertheless play significant roles as resource gatherers or sources of fresh information from outside the main network.

2. **Closeness Centrality.** Closeness centrality is the length of a node's shortest path to any other node in the network. It is measured by a simple count of the number of links or steps from a node to the farther node away from it in the network, with the lowest numbers indicating nodes with the highest levels of closeness centrality. Nodes with a high level of closeness centrality have the closest association with every other node in the network. A high level of closeness centrality affords a node the best ability to directly or indirectly access the largest amount of nodes with the shortest path. Closeness is calculated by adding the number of hops between a node and all others in a network (see Figure G-3). A lower score indicates that an individual needs fewer hops to reach others in the network,

Measures of Node Centrality



Measures of Node Centrality

Node D is an example of a "hub" and has the highest measure of "degree centrality" (i.e., number of direct links).

Nodes F and G have fewer direct links than D but occupy positions with shorter direct and indirect paths within and between constituencies A-G and H-J (i.e., high measures of "closeness centrality.")

Node H is an example of a "broker" between two constituencies (Nodes A-G and Nodes I-J), and has the highest measure of "betweenness centrality."

Figure G-3. Measures of Node Centrality

and is therefore closer to others in the network. Nodes with high closeness centrality are in excellent positions to monitor the overall activity flow within the network.

3. **Betweenness Centrality.** Betweenness centrality is present when a node serves as the only connection between small clusters (e.g., cliques, cells) or individual nodes and the larger network. It is not measured by counting like degree and closeness centrality are; it is either present or not present (i.e., yes or no). Having betweenness centrality allows a node to monitor and control the exchanges between the smaller and larger networks that they connect, essentially acting as a broker for information between sections of the network. For example, in Figure G-3, node H would occupy one of the most important locations in the network by serving as the only link between nodes I, J, and the remainder of the network. Node H is an example of a broker node and (assuming nodes I and J were sufficiently important to the network as a whole) it might also be designated as a key node. The elimination of a broker node can fragment a network into several subcomponents. This

demonstrates how a purely decapitation approach against threat network senior leaders may be more difficult and not as effective as targeting other critical nodes.

4. **Eigenvector centrality** measures the degree to which a node is linked to centralized nodes and is often a measure of the influence of a node in a network. It assumes that the greater number or stronger ties to more central or influential nodes increases the importance of a node. It essentially determines the "prestige" of a node based on how many other important nodes it is linked to. A node with a high eigenvector centrality is more closely linked to critical hubs.

(c) **Brokers and Bridges.** Brokerage metrics use a combination of methods to identify either nodes (brokers) that occupy strategic positions within the network or the relationships (bridges) connecting disparate parts of the network (see Figure G-4). Brokers have the potential to function as intermediaries or liaisons in a network and can control the flow of information or resources. Nodes that lie on the periphery of a network (displaying low centrality scores) are often connected to other networks that have not been mapped. This helps the planner identify gaps in their analysis and areas that still need mapping to gain a full understanding of the OE. These outer nodes provide an opportunity to gather fresh information not currently available.

3. Density

Network density examines how well connected a network is by comparing the number of links present to the total number of links possible, which provides an understanding of how sparse or connected the network is. Network density can indicate many things. A dense network may have more influence than a sparse network. A highly interconnected network has fewer individual member constraints, may be less likely to rely on others as information brokers, be in a better position to participate in activities, or be closer to leadership, and therefore able to exert more influence upon them. A network with low interconnectivity may indicate that there are divisions (e.g., along clan or political lines) or that the distribution of power or information is highly uneven and tightly controlled. This may help planners know where to apply resources.

a. **Centralization.** Centralization helps provide insights on whether the network is centralized around a few key personnel/organizations or decentralized among many cells or subgroups. A network centralized around one key person may further allow planners to focus in on these key personnel to influence the entire network.

b. Density and centralization can inform whether an adversary force has a centralized hierarchy or command structure, if they are operating under a core C2 network with multiple, relatively autonomous hubs, or if they are a group of ad hoc decentralized resistance elements with very little interconnectedness or cohesive C2. Centralization metrics can also identify the most central people or organizations with the resistance. This analysis provides the planner with a much deeper understanding of a network besides the often-used leadership hierarchical chart. Although hierarchical charts are helpful, they do not convey the underlying powerbrokers and key players that are influential with a social network and can

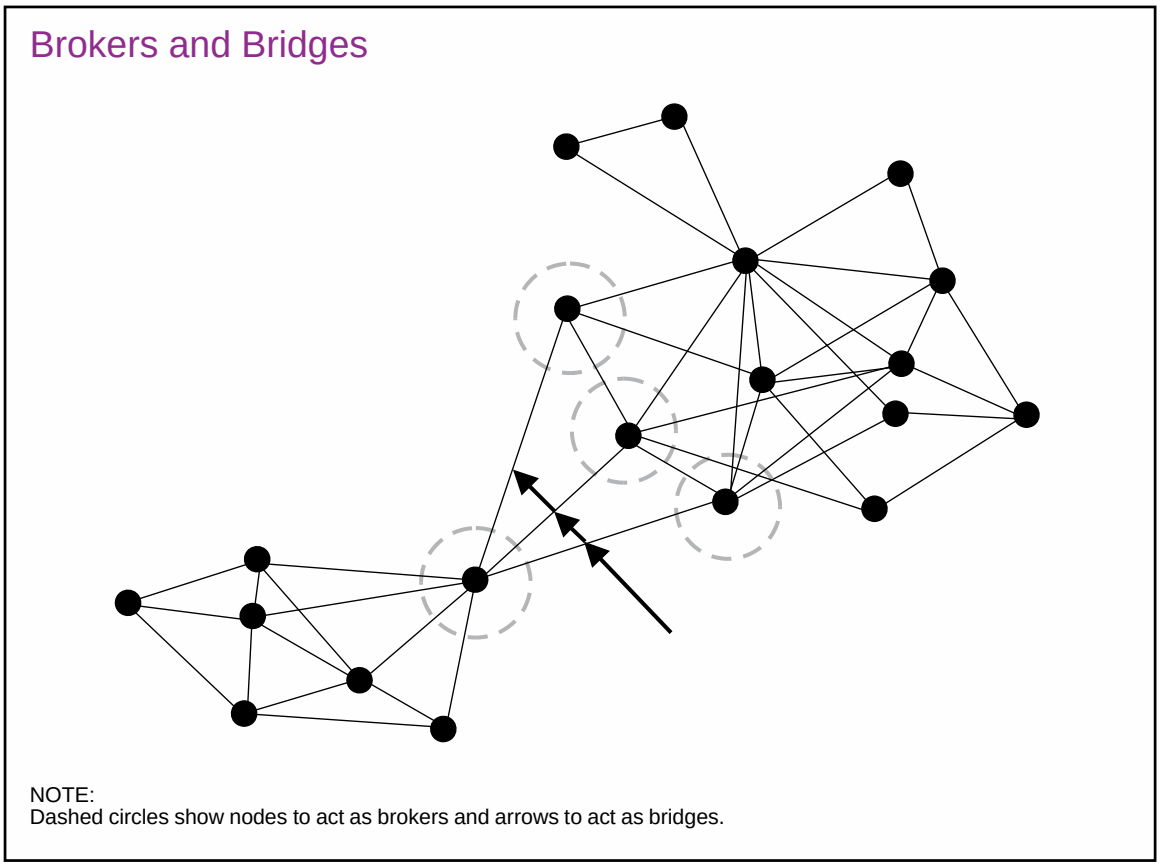


Figure G-4. Brokers and Bridges

often miss identifying the brokers that control the flow of information or resources throughout the network.

4. Interrelationship of Networks

The JFC should identify the key stakeholders, key players, and power brokers in a potential operational area. Using SNA, planners can empirically analyze the population to identify the multitude of networks within the OE and develop a network topography. This understanding usually starts with identifying the density and centralization of the network.

a. People generally identify themselves as members of one or more cohesive networks. Networks may form due to common associations between individuals that may include tribes, sub-tribes, clans, family, religious affiliations, clubs, political organizations, and professional or hobby associations. SNA helps examine the individual networks that exist within the population that are critical to understanding the human dynamics in the OE based upon known relationships. Capturing the attitudes of individuals within identified nodes toward other groups is supported by link analysis (relationships between nodes in the network) and can be used to provide greater clarity of SNA products.

b. Various networks within the OE are interrelated due to an individual's association with multiple networks. SNA provides the staff with understanding of nodes within a single

network, but can be expanded to conduct analysis on interrelated networks. This may provide the joint staff with an indication of the potential association, level of connectivity and potential influence of a single node to one more interrelated network. This aspect is essential for CTN, since a threat network's relationship with other networks must be considered by the joint staff during planning and targeting.

5. Other Considerations

a. **Collection.** Two types of data need to be collected to conduct SNA: relational data (such as family/kinship ties, business ties, trust ties, financial ties, communication ties, grievance ties, political ties, etc.) and attribute data that captures important individual characteristics (tribe affiliations, job title, address, leadership positions, etc.). Collecting, updating, and verifying this information should be coordinated across the whole of USG. USG personnel entering a region should have an understanding of what information gaps on the various social groups currently exist, or need to be updated, and plan to collect that data during the conduct of their mission.

(1) Ties (or links) are the relationship between actors (nodes) (see Figure G-5). By focusing on the preexisting relationships and ties that bind a group together, SNA will help provide an understanding of the structure of the network and help identify the unobserved associations of the actors within that network. To draw an accurate picture of a network, planners need to identify ties among its members. Strong bonds formed over time by connections like family, friendship, or organizational associations characterize these ties.

(2) Capturing the relational data of social ties between people and organizations requires collection, recording, and visualization. The joint force must collect specific types of data in a structured format with standardized data definitions across the force in order to visualize the human factors in systematic sociograms.

b. **Analysis**

Examples of Ties

Examples Types of Ties or Relationships:

- Affiliated/associate with
- Coworker of
- Communicated with
- Friend of
- Imprisoned with
- Linked to
- Possible same as
- Religious leader of
- Classmate of
- Collaborated with
- Enemy of
  - financier of
  - kin of
  - lover of
- Recruiter of
- Superior/subordinate of

Figure G-5. Examples of Ties

(1) Sociograms identify influential people and organizations as well as information gaps in order to prioritize collection efforts. The social structure depicted in a sociogram implies an inherent flow of information and resources through a network. Roles and positions identify prominent or influential individuals, structures of organizations, and how the networks function. Sociograms can model the human dynamics between participants in a network, highlight how to influence the network, identify who exhibits power within the network, and illustrate resource exchanges within the network. Sociograms can also provide a description and picture of the regime networks, or neutral entities, and uncover how the population is segmented.

(2) Sociograms are representations of the actual network and may not provide a complete or true depiction of the network. This could be the result of incomplete information or including or not including appropriate ties or actors. In addition, networks are constantly changing and a sociogram is only as good as the last time it was updated. Since no single SNA metric or tool can capture the dynamics of any network, analysts should draw on a number of metrics and methods to better understand the human factors. Even with limitations, sociograms inform approaches to confirm or deny intuitions, illuminate new insights, and identify information gaps.

c. **Challenges.** Collecting human factors data to support SNA requires a concerted effort over an extended period. Data can derive from traditional intelligence gathering capabilities, historical data, open-source information, exploiting social media, known relationships, and direct observation. This human factor data should be codified into a standardized data coding process defined by a standardized reference. Entering this human factor data is a process of identifying, extracting, and categorizing raw data to facilitate analysis. For analysts to ensure they are analyzing the sociocultural relational data collected in a standardized way, the JFC can produce a reference that provides standardized definitions of relational terms. Standardization will ensure that when analysts or planners exchange analytical products or data their analysis has the same meaning to all parties involved. This is needed to avoid confusion or misrepresentation in the data analysis. Standardized data definitions ensure consistency at all levels; facilitate data and analysis product transfer among differing organizations; and allow multiple organizations to produce interoperable products concurrently.

APPENDIX H
REFERENCES

The development of JP 3-25 is based on the following primary references:

1. General

a. Title 10, *United States Code.*

b. Strategy to Combat Transnational Organized Crime.

c. Executive Order 12333, *United States Intelligence Activities.*

2. Department of Defense Publications

a. Department of Defense Counternarcotics and Global Threats Strategy.

b. Department of Defense Directive (DODD) 2000.19E, *Joint Improvised Explosive Device Defeat Organization.*

c. DODD 3300.03, *DOD Document and Media Exploitation (DOMEX).*

d. DODD 5205.14, *DOD Counter Threat Finance (CTF) Policy.*

e. DODD 5205.15E, *DOD Forensic Enterprise (DFE).*

f. DODD 5240.01, *DOD Intelligence Activities.*

g. DODD 8521.01E, *Department of Defense Biometrics.*

h. Department of Defense Instruction (DODI) O-3300.04, *Defense Biometric Enabled Intelligence (BEI) and Forensic Enabled Intelligence (FEI).*

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

3. Chairman of the Joint Chiefs of Staff Publications

a. JP 2-01.3, *Joint Intelligence Preparation of the Operational Environment.*

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

c. JP 3-07.2, *Antiterrorism.*

d. JP 3-07.3, *Peace Operations.*

e. JP 3-07.4, *Counterdrug Operations.*

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

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

h. JP 3-13.2, *Military Information Support Operations*.

i. JP 3-15.1, *Counter-Improvised Explosive Device Operations*.

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

k. JP 3-20, *Security Cooperation.*

l. JP 3-22, *Foreign Internal Defense*.

m. JP 3-24, *Counterinsurgency*.

n. JP 3-26, *Counterterrorism*.

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

p. JP 3-57, *Civil-Military Operations*.

q. JP 3-60, *Joint Targeting.*

r. JP 5-0, *Joint Planning*.

s. Joint Doctrine Note 1-16, *Identity Activities*.

4. Multi-Service Publication

ATP 5-0.3/MCRP 5-1C/NTTP 5-01.3/AFTTP 3-2.87, *Multi-Service Tactics, Techniques, and Procedures for Operation Assessment.*

5. Other Publications

a. The Haqqani Network: Pursuing Feuds Under the Guise of Jihad? *CTX Journal*, Vol. 3, No. 4, November 2013, Major Lars W. Lilleby, Norwegian Army.

b. Foreign Disaster Response, *Military Review,* November-December 2011.

c. *US Military Response to the 2010 Haiti Earthquake,* RAND Arroyo Center, 2013.

d. *DOD Support to Foreign Disaster Relief,* July 13, 2011.

e. United Nations Stabilization Mission in Haiti website.

f. Kirk Meyer, Former Director of the Afghan Threat Finance Cell—*CTX Journal*, Vol. 4, No. 3, August 2014.

g. *Networks and Netwars: The Future of Terror[ism], Crime, and Militancy*, Edited by John Arquilla, David Ronfeldt.

h. General Martin Dempsey, Chairman of the Joint Chiefs of Staff, Foreign Policy, 25 July 2014, *The Bend of Power*.

i. Alda, E., and Sala, J. L. Links Between Terrorism, Organized Crime and Crime: The Case of the Sahel Region. *Stability: International Journal of Security and Development*, Vol. 3, No. 1, Article 27, pp. 1-9.

j. International Maritime Bureau Piracy (Piracy Reporting Center).

Intentionally Blank

APPENDIX J
ADMINISTRATIVE INSTRUCTIONS

1. User Comments

Users in the field are highly encouraged to submit comments on this publication to: Joint Staff J-7, Deputy Director, Joint Education and Doctrine, ATTN: Joint Doctrine Analysis Division, 116 Lake View Parkway, Suffolk, VA 23435-2697. These comments should address content (accuracy, usefulness, consistency, and organization), writing, and appearance.

2. Authorship

The lead agent for this publication is the US Marine Corps. The Joint Staff doctrine sponsor for this publication is the Director for Operations (J-3).

3. Change Recommendations

a. Recommendations for urgent changes to this publication should be submitted:

TO: Deputy Director, Joint Education and Doctrine (DD JED), Attn: Joint Doctrine Division, 7000 Joint Staff (J-7), Washington, DC 20318-7000 or email: js.pentagon.j7.list.dd-je-d-jdd-all@mail.mil.

b. Routine changes should be submitted electronically to the Deputy Director, Joint Education and Doctrine, ATTN: Joint Doctrine Analysis Division, 116 Lake View Parkway, Suffolk, VA 23435-2697, and info the lead agent and the Director for Joint Force Development, J-7/JED.

c. 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.

4. 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 Website can be found at https://www.jllis.mil or http://www.jllis.smil.mil.

5. Distribution of Publications

Local reproduction is authorized, and access to unclassified publications is unrestricted. However, access to and reproduction authorization for classified JPs must be 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.*

6. 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 http://jdeis.js.smil.mil/jdeis/index.jsp (SIPRNET), and on the JEL at http://www.dtic.mil/doctrine.

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 semi-annually and when received can be locally reproduced for use within the combatant commands, Services, and combat support agencies.

GLOSSARY

PART I—ABBREVIATIONS AND ACRONYMS

AFTTP	Air Force tactics, techniques, and procedures
AOR	area of responsibility
ATP	Army techniques publication
BEWL	biometrics-enabled watch list
C2	command and control
CARVER	criticality, accessibility, recuperability, vulnerability, effect, and recognizability
CBRN	chemical, biological, radiological, and nuclear
CC	critical capability
CCDR	combatant commander
CCIR	commander's critical information requirement
CCMD	combatant command
CD	counterdrug
CDRUSSOCOM	Commander, United States Special Operations Command
CEXC	combined explosives exploitation cell
CFA	critical factors analysis
COA	course of action
COG	center of gravity
COIN	counterinsurgency
CR	critical requirement
CT	counterterrorism
CTF	counter threat finance
CTN	countering threat networks
CV	critical vulnerability
D3A	decide, detect, deliver, and assess
DHS	Department of Homeland Security
DNA	deoxyribonucleic acid
DOD	Department of Defense
DODD	Department of Defense directive
DODI	Department of Defense instruction
DOMEX	document and media exploitation
DOS	Department of State
EEZ	exclusive economic zone
EOD	explosive ordnance disposal
F2T2EA	find, fix, track, target, engage, and assess
F3EAD	find, fix, finish, exploit, analyze, and disseminate
FID	foreign internal defense
FTO	foreign terrorist organization

GCC	geographic combatant commander
HN	host nation
HUMINT	human intelligence
I2	identity intelligence
IED	improvised explosive device
IO	information operations
IRC	information-related capability
ISIL	Islamic State of Iraq and the Levant
J-2	intelligence directorate of a joint staff
J-2E	joint force exploitation staff element
J-3	operations directorate of a joint staff
JFC	joint force commander
JIPOE	joint intelligence preparation of the operational environment
JP	joint publication
JPP	joint planning process
JTF	joint task force
LOE	line of effort
LOO	line of operation
MCRP	Marine Corps reference publication
MISO	military information support operations
MOE	measure of effectiveness
MOP	measure of performance
MOTR	maritime operational threat response
NGO	nongovernmental organization
NMS	national military strategy
NTTP	Navy tactics, techniques, and procedures
OE	operational environment
OPCON	operational control
OSINT	open-source intelligence
PMESII	political, military, economic, social, information, and infrastructure
PN	partner nation
SCA	sociocultural analysis
SFA	security force assistance
SIGINT	signals intelligence
SNA	social network analysis

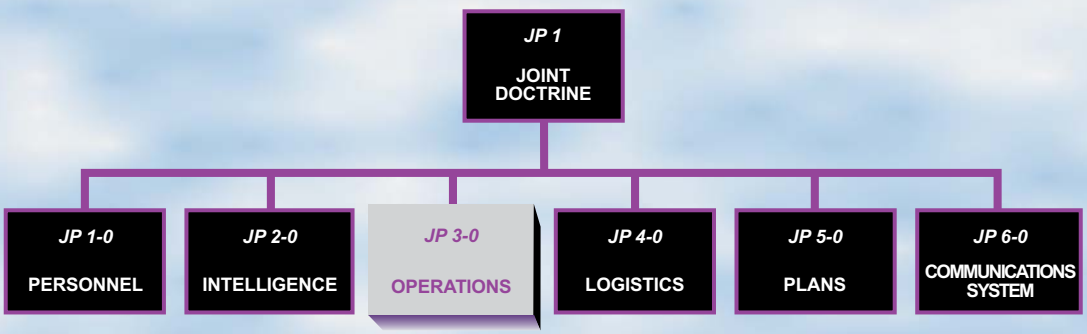
SOF	special operations forces
TTP	tactics, techniques, and procedures
UNCLOS	United Nations Convention on the Law of the Sea
USCG	United States Coast Guard
USG	United States Government
VBSS	visit, board, search, and seizure
WIT	weapons intelligence team
WMD	weapons of mass destruction

PART II—TERMS AND DEFINITIONS

countering threat networks. The aggregation of activities across the Department of Defense and United States Government departments and agencies that identifies and neutralizes, degrades, disrupts, or defeats designated threat networks. Also called **CTN.** (Upon approval of this publication, this term and its definition will be included in the DOD Dictionary.)

network engagement. Interactions with friendly, neutral, and threat networks, conducted continuously and simultaneously at the tactical, operational, and strategic levels, to help achieve the commander's objectives within an operational area. (Upon approval of this publication, this term and its definition will be included in the DOD Dictionary.)

JOINT DOCTRINE PUBLICATIONS HIERARCHY



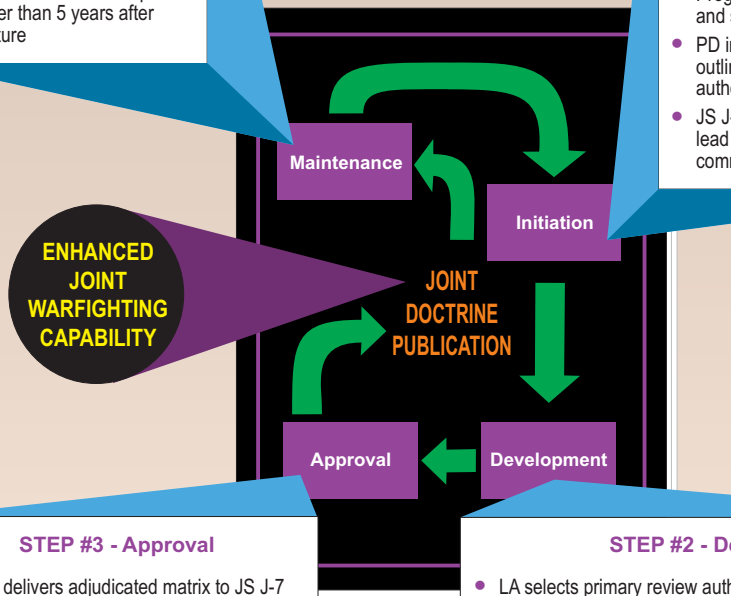
All joint publications are organized into a comprehensive hierarchy as shown in the chart above. **Joint Publication (JP) 3-25** is in the **Operations** series of joint doctrine publications. The diagram below illustrates an overview of the development process:

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