USMC

MCTP 3-02A

MAGTF Network Engagement Activities



US Marine Corps

DISTRIBUTION STATEMENT A: Approved for public release; distribution is unlimited.

PCN 147 000029 00

USMC

DEPARTMENT OF THE NAVY
Headquarters, United States Marine Corps
Washington, D.C. 20350-3000

27 June 2017

FOREWORD

Operational forces must always consider the complexities of their modern, global, and asymmetric operational environments, which consist of a spectrum of interrelated networks that directly and indirectly affect the mission. Using traditional linear adversarial templates against noncontiguous threats is inadequate to address Marine Corps requirements to operate in the complex environments of today and in the future.

Marine Corps Tactical Publication 3-02A, *MAGTF Network Engagement Activities*, presents planning and execution considerations, capabilities and limitations, and targeting and assessment activities for network engagement across the Marine air-ground task force. It will facilitate the commander's ability to synchronize operational activities across a noncontiguous battlespace. Network engagement is supportive of existing processes and complementary of effective command and control.

This publication's target audience includes Marine air-ground task force and major subordinate element commanders and their staffs down to the company level. Additionally, Marine Corps leaders at every level should have an understanding of the concepts and employment considerations of network engagement activities.

Reviewed and approved this date.

BY DIRECTION OF THE COMMANDANT OF THE MARINE CORPS

Robert S. Walsh

ROBERT S. WALSH
Lieutenant General, U.S. Marine Corps
Deputy Commandant for Combat Development and Integration

Publication Control Number: 147 000029 00

DISTRIBUTION STATEMENT A: Approved for public release; distribution is unlimited.

This Page Intentionally Left Blank

MAGTF Network Engagement Activities

Table of Contents

Chapter 1. Nature of the Operational Environment

Complexity 1-2
Interrelated Networks 1-3
Network Engagement Principles 1-3

Chapter 2. Network Engagement Considerations

How Networks Affect Operations 2-1
- Challenges of Understanding Networks 2-2
- Network Considerations in Planning 2-3
- Network Considerations in Intelligence Preparation of the Battlespace 2-3
- Network Considerations in Targeting 2-5
- Assessing Effects on Networks and Operations 2-7

Network Engagement Across the Range of Military Operations 2-8
- Military Engagement, Security Cooperation, and Deterrence 2-8
- Crisis Response and Limited Contingency Operations 2-10
- Major Operations and Campaigns 2-10

Chapter 3. Operational Environment Complexity

Understanding the Operational Environment 3-1
Utilizing Methods to Gain Understanding 3-2
- Information Models 3-3
- Information Models Usage 3-3

Identifying Critical Variables 3-7

Chapter 4. Network Identification and Understanding

Network Terms and Structures 4-1
- Components of a Network 4-1
- Network Formation 4-2

Characteristics of a Network 4-3
Network Categories 4-5
Techniques of Network Analysis 4-6
Network Mapping 4-6
Network Templating 4-7
Social Network Analysis 4-8
Link Analysis 4-10
Nodal Analysis 4-10

Chapter 5. Engagement of Networks

Network Targeting Considerations 5-1
Engaging the Network Through Targeting 5-1
Decide 5-1
Detect 5-5
Deliver 5-5
Assess 5-6

Chapter 6. Network Engagement Assessment

Plan 6-2
Establish a Baseline 6-2
Determine Objectives and Effects 6-3
Develop Measures of Performance 6-3
Develop Measures of Effectiveness 6-3
Identify Indicators 6-4
Monitor 6-5
Considerations When Developing a Collection Plan 6-5
Manage Collected Information 6-7
Evaluate 6-7
Apply Measures of Performance 6-7
Apply Measures of Effectiveness 6-8
Evaluate Metrics/Assessment Plan 6-8
Direct 6-8

Appendices

A Network Engagement Enablers and Resources A-1
B Network Engagement and Identity Operations B-1
C Critical Variables Example and Analysis C-1

Glossary

References

To Our Reader

This Page Intentionally Left Blank

CHAPTER 1
NATURE OF THE OPERATIONAL ENVIRONMENT

Recent operational experience has demanded a shift in Marine Corps warfighting strategy from defeating an overwhelmingly traditional adversary to dominating an adversary that is likely to blend both traditional and irregular methods of conflict within a complex operational environment. The operational environment is a composite of the conditions, circumstances, and influences that influence commanders' decision making about the employment of capabilities. Present within the operational environment are interrelated networks of people, places, and actions that can be categorized as friendly, neutral, or threat networks. The actions taken by any member of a network will impact the operational environment. Therefore, commanders must leverage analytical capabilities in order to successfully operate in these complex operational environments.

To achieve military objectives, the Marine Corps must seek to shatter the enemy's cohesion by engaging friendly, neutral, and threat networks. Our adversaries have learned to hide from superior combat power. By engaging the friendly and neutral networks, Marines seek to isolate and illuminate the enemy in order to render him irrelevant whether by fire and maneuver or by political action at all levels of the environment. Network engagement activities include a number of methods that support or amplify the current command and control processes (i.e., intelligence preparation of the battlespace [IPB], Marine Corps Planning Process [MCPP], targeting, and assessment). Network engagement activities provide commanders and their staffs with an array of lethal and nonlethal tools to shape the battlespace. This allows for a variable response to the complex security environment, ensuring that Marines can thrive in and dominate that environment.

Marines are trained and educated within the maneuver warfare philosophy to enable them to operate and thrive in chaotic environments. Network engagement complements Marine Corps training and education by enabling Marines to cope with various networks and the range of actors that they will encounter. The application of network engagement requires the consideration of all potential domains, operational variables (e.g., economic, political, social, environmental, beliefs), actors (e.g., friendly forces, local population, host nation government, criminal entities, adversaries), and the appropriate application of force, ranging from nonlethal to lethal.

To successfully accomplish mission goals, Marines must equally consider the impact of actions on all potential actors. Intelligence may provide commanders and their staffs 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 of the neutral networks and how they are interrelated with threat networks will provide operating forces with greater opportunities to understand, penetrate, and target those threat networks. Regardless, the consideration of all domains during operational planning and execution marginalizes the adversary. Network engagement activities can decrease

local support of adversaries by eliminating the accommodating environment necessary for the formation and sustainment of threat networks and increasing stability in the area of operations.

In Marine Corps Doctrinal Publication (MCDP) 6, *Command and Control*, the theory and philosophy of command and control for the Marine Corps is stated as "the intent is to describe how we can reach effective military decisions and implement effective military actions faster than an adversary in any conflict setting on any scale." The activities of network engagement are responsive and adaptive, and they enable decentralized execution of lethal and nonlethal actions. They support the commanders' ability to limit threat networks through use of friendly and neutral capabilities and to counter any threat faced across the range of military operations (ROMO).

COMPLEXITY

As presented in MCDP 1, *Warfighting*, war is "a clash between opposed wills." This same doctrinal publication cautions that war is not this simple. It is "a complex phenomenon" in which "each belligerent is not a single, homogeneous will guided by a single intelligence. Instead, each belligerent is a complex system consisting of numerous individual parts."

The challenges facing tactical-level commanders will require forces to operate against threat networks in complex environments. These threats are comprised of various networks that are adaptive to changes within the operational environment and that do not operate within the confines of a single unit's battlespace. As General Anthony Zinni stated, "Our intelligence system is designed to support a Cold War kind of operation. We are 'Order-of-Battle' oriented. . . . It is designed to examine an enemy. . . . The situations you're going to be faced with go far beyond what you're trained for in a very narrow military sense."

Current doctrine is being rewritten to address the complexities within the operational environment and gain a greater understanding of the human dimension. Network engagement is designed to support these efforts and promote the consideration of the interrelated networks that exist within the operational environment as a part of the planning and targeting processes that focus on meeting the conditions of a commander's desired end state.

The analytical challenges posed to forces operating in this complex environment are multifaceted and require the following:

- Gaining a holistic understanding of the operational environment through identification of environmental variables.
- Performing identification of the critical variables that have a direct impact on the mission.
- Developing an understanding of how the critical variables influence the interrelated networks.
- Maintaining the ability to continuously monitor the operational environment to assess the impact of the force's operations and those actions taken by other networks.

INTERRELATED NETWORKS

A network is formed by a direct or indirect tie between two or more nodes sharing a common purpose. Specifically, a human network is an alliance of socially connected individuals who are involved in activities to achieve some form of social, political, monetary, religious, or personal gain. Networks can be large or small, local or global, domestic or transnational, cohesive or diffuse, and centrally directed or highly decentralized.

Individuals are typically associated with numerous networks based on personal characteristics; for example, location of birth, family, religion, social groups, organizations. Commonly, an individual is associated with more than one type of network (friendly, neutral, or threat). Individual identities provide the basis that allows for the interrelatedness between friendly, neutral, and threat networks to exist. (See Joint Publication [JP] 3-25, *Countering Threat Networks*, for a detailed discussion on networks.)

NETWORK ENGAGEMENT PRINCIPLES

Network engagement is designed to identify and understand how these complex networks impact the operational environment. The principles of network engagement are to understand the mission, to leverage network engagement enablers, to understand the operational environment, to understand the networks, to engage the networks, and to assess these activities. This publication is organized to address these principles and their relationship to existing processes. Although many of the principles are supported with analytical techniques and associated with intelligence analysis capabilities, operations and fires sections must continuously maintain visibility and access to these products in support of planning, targeting, and assessing operations. Understanding the outputs from applying network engagement principles is important to provide necessary feedback in the form of requests for information to the intelligence analysts and to maximize the opportunity to leverage the information provided to enhance staff processes. Successful implementation of network engagement principles requires the full collaboration of the staff and is not some specific tasks that can be assigned to one individual or staff section.

This Page Intentionally Left Blank

CHAPTER 2
NETWORK ENGAGEMENT CONSIDERATIONS

The primary purpose of network engagement is to expand commanders' focus from solely on the enemy threat to include comprehensively studying the networks (friendly, neutral, and threat) and their interactions within an area of operations.

Network engagement provides commanders and their staffs with concepts that are proven and designed to strip away the complexity of the contemporary operational environment and organize information for use during—

- The intelligence cycle.
- MCPP.
- IPB.
- Targeting.
- Operations assessments.

Network engagement requires synchronization of the entire staff and the integration of non-organic enablers that provide both analytical and operational support. Network engagement enablers are addressed specifically in appendix A. Commanders task-organize and integrate network engagement enablers based on operational requirements. Figure 2-1, on page 2-2, illustrates how network engagement principles support the intelligence cycle and subsequently support operational processes.

Marine Corps Tactical Publication (MCTP) 2-10A, *MAGTF Intelligence Collection*, provides intelligence analysts with guidance on how to support the force during operations. Network engagement enablers may be leveraged to support the intelligence cycle during planning and direction, collection, processing and exploitation, production, or dissemination stages. Specific intelligence products that focus on analysis of the operational environment and networks are in turn used by the staff for planning, targeting, and assessing. As these processes occur, any additional information requirements are then provided for inclusion in the collection plan.

HOW NETWORKS AFFECT OPERATIONS

Individuals associated with various networks within or outside of the operational environment possess the potential to affect operations with their actions. Commanders do not possess the ability to directly influence the actions of these individuals and must, therefore, conduct contingency planning in order to mitigate additional threats that may be created due to these acts.

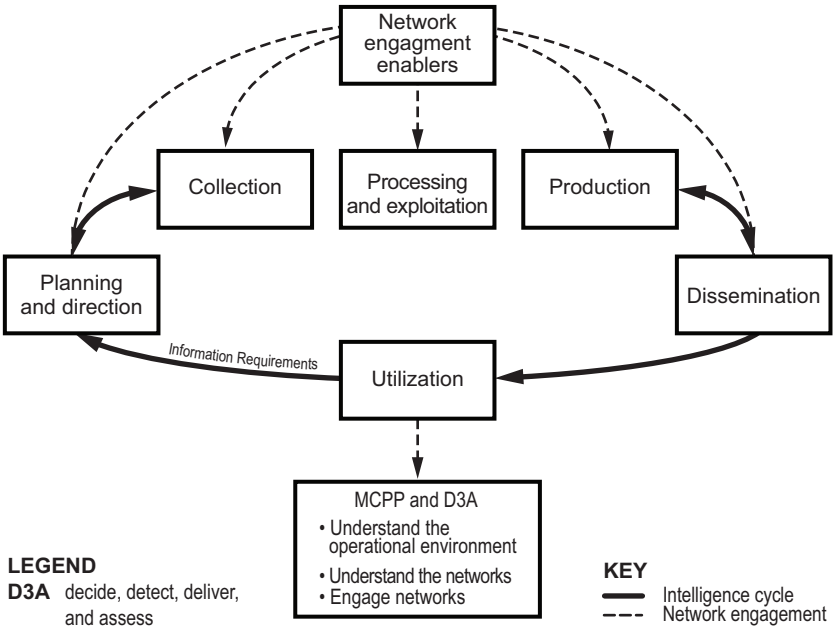


Figure 2-1. Network Engagement Support to the Intelligence Cycle.

Part of the contingency plan may include engaging specific networks, which requires an understanding of how the networks have formed, the relationships that exist between networks, and how the networks sustain themselves. (See JP 3-25 for a detailed discussion on networks.)

With the rising complexity of operational environments and the interrelatedness of networks, it should be understood that any individual (e.g., a known adversary; a military member; any citizen of a friendly, neutral, or hostile nation) can have an impact on both the environment and operations. For example, in 2010, a pastor of the Dove World Outreach Center, a small, nondenominational Christian church located in Gainesville, Florida, gained national and international attention for his plan to burn Qur'ans on the anniversary of the 11 September 2001 attacks in the United States. Although this pastor was not a member of any specific network located in Afghanistan, his intended actions had immediate impacts on the operational environment in Afghanistan. These impacts affected operations and required commanders to increase their force protection posture during this period of time. The dynamics and challenges of understanding and engaging networks are relevant at the strategic, operational, and tactical levels and must be considered during planning and executing operations. (See JP 3-25 for a detailed discussion on networks.)

Challenges of Understanding Networks

Networks are comprised of socially connected humans and possess the ability to adapt to the operational environment in order to grow and survive, which makes understanding and engaging networks particularly challenging. There is no doctrinal template that facilitates understanding of human networks or the certainty of their actions. Any individual can simultaneously belong to multiple and distinct networks. An individual's association with multiple networks will make those networks interrelated. Due to the interrelatedness between networks within the operational environment, one person's actions have the potential to affect many networks within the operational environment, and thus can affect the operational environment as a whole. As the

operational environment changes subsequent to those actions, the networks therein must eventually adapt to remain effective and efficient. Actions against or within networks can change the operational environment.

Network Considerations in Planning

In MCDP 5, *Planning*, planning is described as "the art and science of envisioning a desired future and laying out effective ways of bringing it about." The MCPP is a six-step process designed to help the staff organize and focus efforts during planning. The methods outlined in network engagement provide staffs with an enhanced ability to conduct planning, resulting in a better and more informed decision cycle for commanders. Figure 2-2, on page 2-4, illustrates the network engagement items that should be considered during the various steps of the MCPP. See Marine Corps Warfighting Publication (MCWP) 5-10, *Marine Corps Planning Process*, for specific information on planning.

Network engagement is specifically designed to support problem framing within staff planning. Problem framing is an essential part of the planning process, since no amount of subsequent planning can solve a problem insufficiently understood. Using a holistic approach to gain an understanding of the operational environment, the staff has the ability to consider the entire human dimension and the potential impact of actions by networks that could affect operations. Network engagement methods for understanding the operational environment and the networks therein are addressed in chapters 3 and 4.

Network engagement methods can help commanders identify environmental variables that add to or detract from problem framing. This is accomplished by gaining a greater understanding of the operational environment and its friendly, neutral, and threat networks, which supports each step of the MCPP. Within planning, course of action (COA) development to engage networks is accomplished through targeting, which is addressed in greater detail in chapter 5.

Network Considerations in Intelligence Preparation of the Battlespace

Intelligence analysis is continuous throughout the MCPP, which includes refinement of intelligence products (e.g., IPB, network analysis) to support the planning process. Network engagement activities are intended to examine and consider the entire environment in a comprehensive manner. This is accomplished by considering all of the networks (friendly, neutral, and threat) and their effects on both operations and the operational environment. Figure 2-3, on page 2-5, depicts IPB and network engagement analysis products that should be considered to enhance IPB.

Defining the battlespace environment requires gaining a greater understanding of the operational environment and the interrelated networks contained therein, which will help commanders to determine where they should operate, what they can influence, and what areas are of interest. In describing battlespace effects, the G-2/S-2 and the rest of the staff seek to make a determination of how the environmental factors within the battlespace affect both adversary and friendly operations. To provide commanders with the best situational awareness, network engagement is designed to consider all of the networks (friendly, neutral, and threat) in gaining an understanding of the environment. Without considering all network actions and the reciprocal effects on the operational environment, it is highly probable that adversaries will find and exploit gaps and vulnerabilities that commanders and their staffs may not have anticipated.

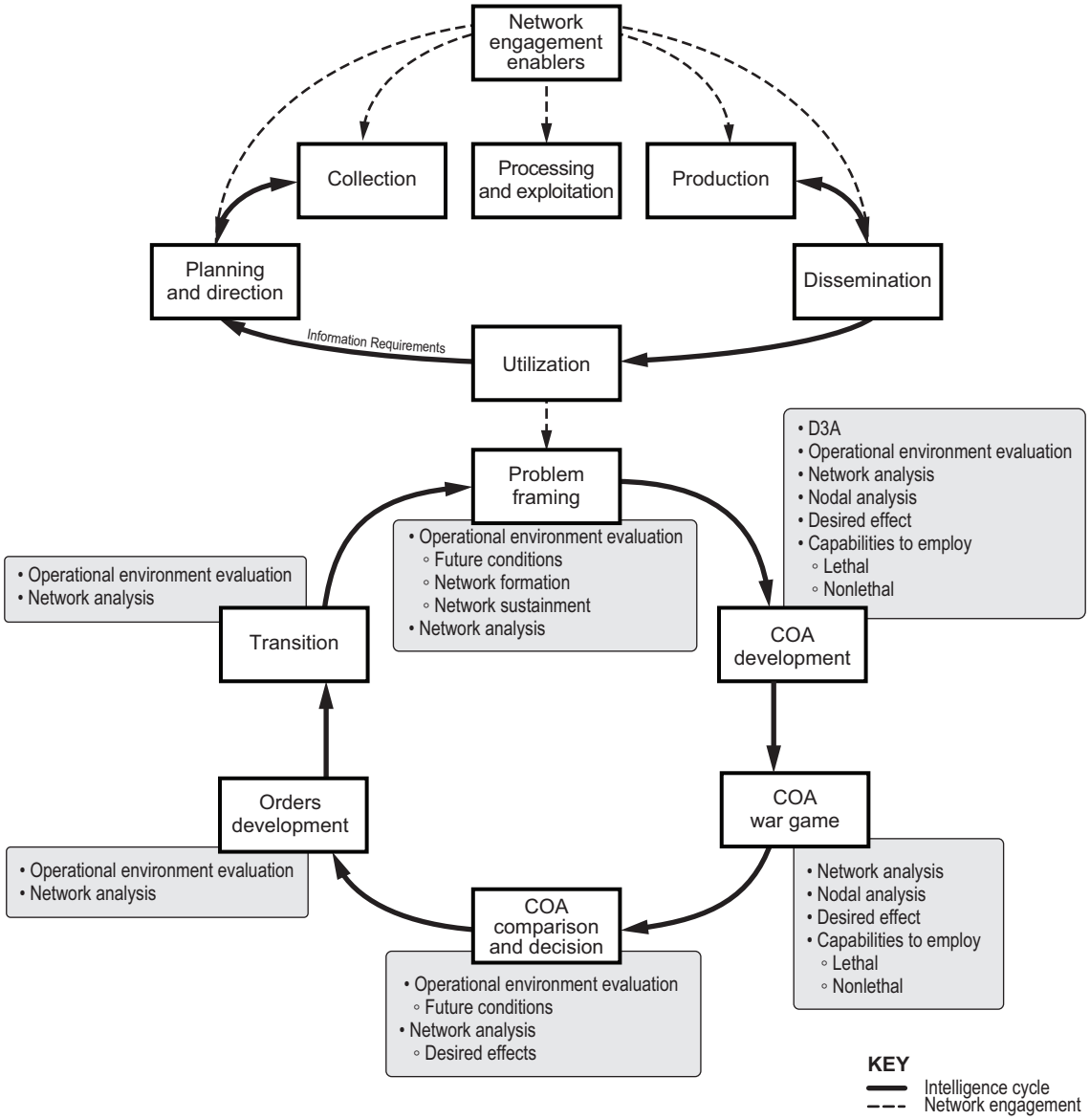


Figure 2-2. Network Engagement Support to the Marine Corps Planning Process.

The commanders and their staffs must recognize a threat to their mission may be manifested from any network within the operational environment. As a method of conducting IPB, analysts must identify and outline all networks within the environment. Analysts must be aware that networks are nonlinear and that the existing adversary templates included in Marine Corps Reference Publication (MCRP) 2-10B.1, *Intelligence Preparation of the Battlefield/Battlespace*, may not be sufficient in gaining an understanding of the structure of a particular network. Network analysis uses various techniques to determine a network's composition, structure, capability, and intentions. Network analysis is further discussed in chapter 4, and the use of identity operations techniques to support confirmation of individual identities is outlined in appendix B.

The final step of the IPB process is to determine the various adversary COAs. A detailed analysis will enable the staff to replicate the set of COAs that the adversary is considering; identify all COAs

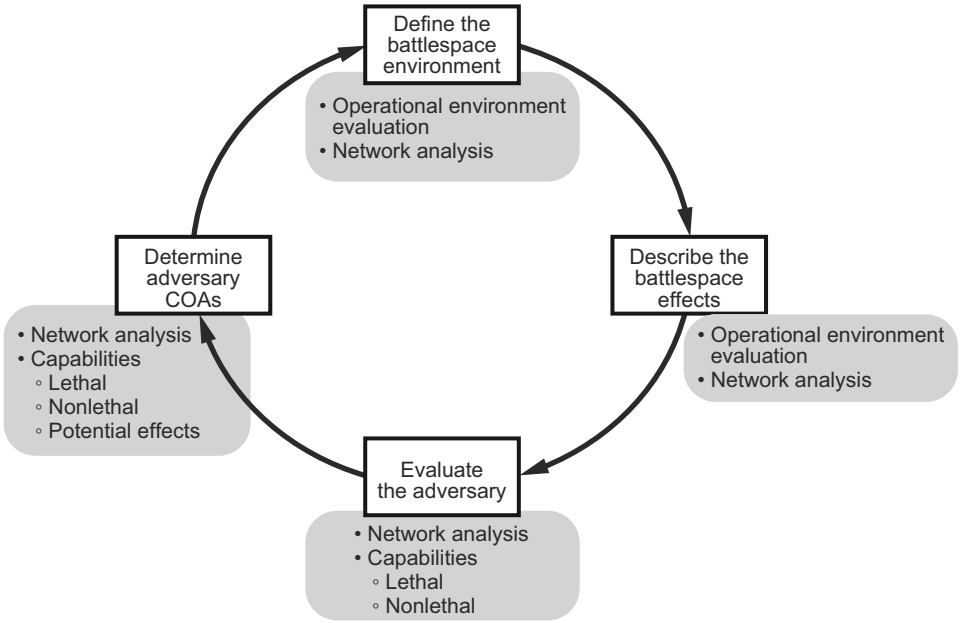


Figure 2-3. Network Engagement Support to Intelligence Preparation of the Battlespace.

that will influence the friendly mission; and identify those areas and activities that, when collected, will indicate which COA the adversary has chosen. Network engagement enablers can provide additional insight on the potential COAs from any network, which will assist the staff in conducting their analysis. Leveraging the network engagement resources and capabilities available, whether integrated or through some type of reachback, will enhance the detail of analysis provided to commanders for planning and targeting.

Network Considerations in Targeting

Targeting is a combination of intelligence functions, planning, battle command, weaponeering, operational execution, and combat assessment. The decide, detect, deliver, and assess (D3A) methodology facilitates an attack on the right target at the right time with the most appropriate asset. Network engagement resources and methods enhance the targeting process by providing options for the staff to analyze the information available and provide commanders with greater situational and target awareness for making decisions on who and how to target the node of a network. Figure 2-4, on page 2-6, illustrates network engagement support of the targeting cycle.

Network engagement enablers support the intelligence cycle, and the products from these efforts are used throughout D3A to support targeting:

- *Decide*. The most resource-exhaustive step of D3A, the decide step requires the use of various intelligence products to decide who is to be targeted, the desired effects of engaging a network, and the type of capability to use in order to generate those effects. It includes analysis of the operational environment, networks, and specific nodes that are provided by network engagement enablers and that support commanders in making targeting decisions.
- *Detect*. Information requirements are submitted back into the intelligence cycle to support the detection of a specific target. The intelligence products used to support the decide step of D3A are again used to assist in the detection of the target.

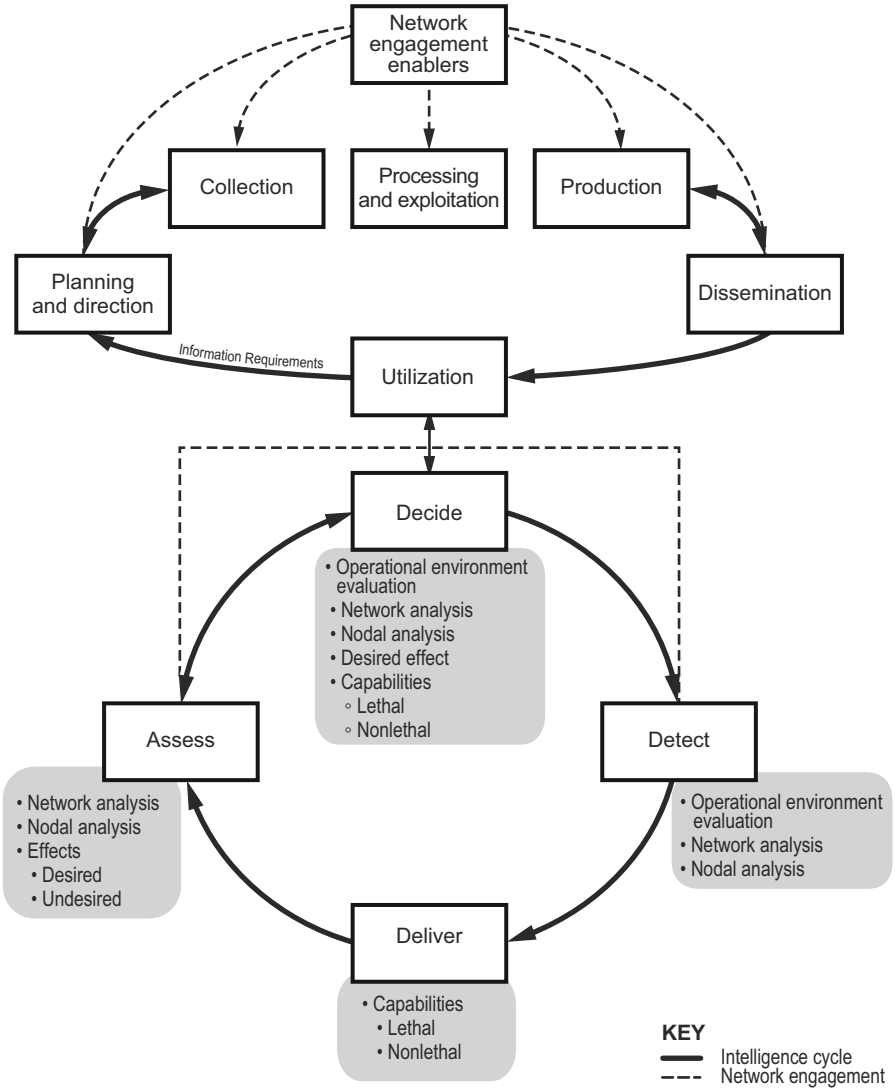


Figure 2-4. Network Engagement Support to Targeting.

- *Deliver*. The deliver step describes the deliberate actions taken to engage a target using lethal and/or nonlethal capabilities.
- *Assess*. Determining if desired effects of engaging a network have occurred requires the assessment of those operations. The measures developed to identify if objectives were achieved are an extension of the operations assessment plan. Assessing in targeting is focused on determining if desired effects on a network have or have not been generated as an outcome of the deliver step. Using the intelligence products that supported the decide step can provide commanders with a baseline or conditions of the operational environment and network prior to engagement. Collection of information requirements as part of the intelligence cycle will provide commanders with conditions of the environment and network post-engagement. Monitoring and evaluating using this information reveals the effects of the targeting efforts.

Engaging networks through targeting is further discussed in chapter 5.

Assessing Effects on Networks and Operations

Assessing the effects of engaging networks must consider both targeting and the subsequent impact on operations. Figure 2-5 depicts the assessment process and identifies where understanding of the operational environment and networks as part of network engagement can support commanders in developing and implementing assessment plans.

Operations Assessments. The purpose of conducting an operations assessment as it relates to network engagement is to gain an understanding of how tasks being conducted are generating the desired effects in the operational environment. These effects are intended to support attaining a commander's objectives by establishing the conditions that meet the desired end state. Conducting an operations assessment requires a commander to—

- Understand the current state and visualize the desired state of the operational environment.
- Monitor the operational environment during and after operations.
- Evaluate the changes within the operational environment to determine if a desired state is being established.

Network engagement methods for analyzing the operational environment outlined in chapter 3 support staffs in gaining a comprehensive understanding of the operational environment and in conducting a refined analysis to identify the critical variables that impact the commanders' objectives.

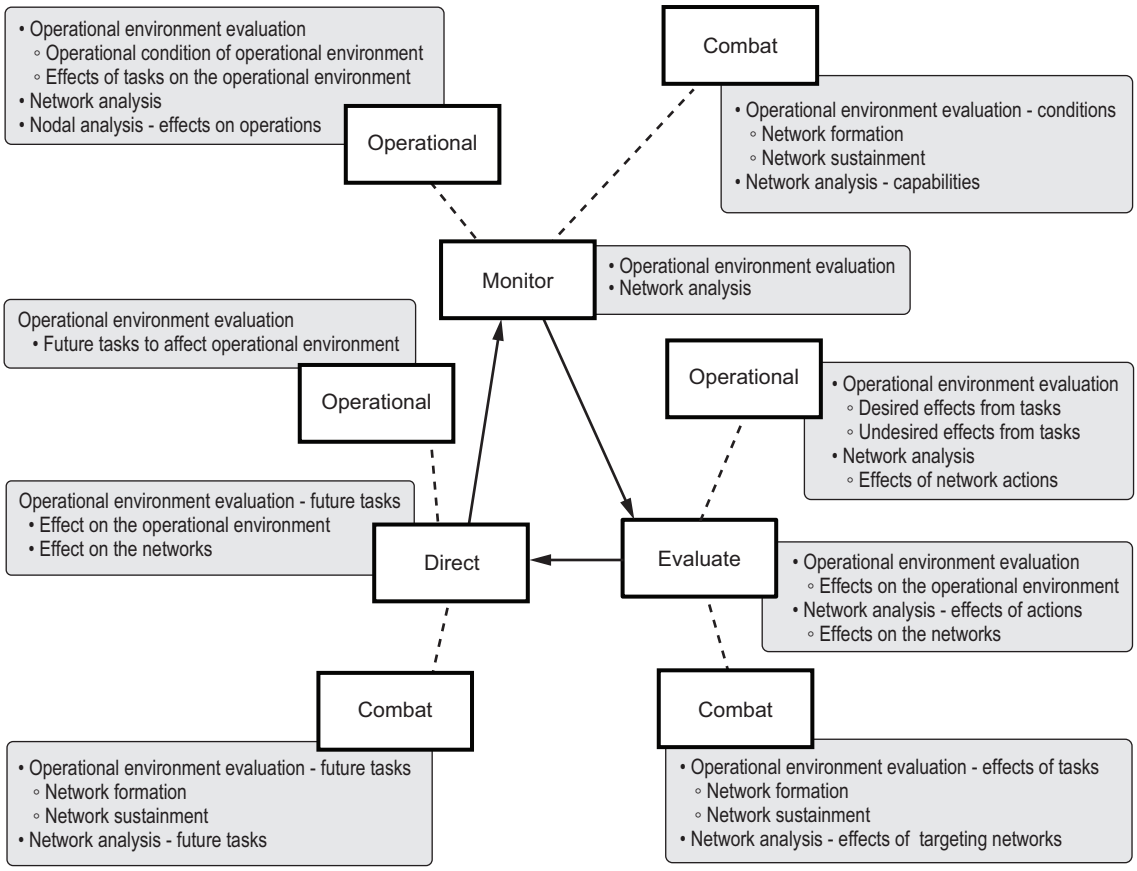


Figure 2-5. Network Engagement and the Assessment Process.

Combat Assessments. The purpose of conducting a combat assessment as it relates to network engagement is to understand if desired effects on networks are being generated from the commander's targeting efforts. This assessment could also be used to identify if undesired effects are being generated, which can then be used by the commander to provide additional guidance for future targeting efforts. Conducting a combat assessment requires the commander to—

- Understand the current state and visualize the desired state of the network.
- Monitor the network being engaged during and after operations.
- Evaluate the changes to the network to determine if desired effects have or have not occurred.

The network engagement methods for analyzing networks outlined in chapter 4 support the staff in gaining an understanding of the structure, associations, and capabilities of the networks and individual nodes.

NETWORK ENGAGEMENT ACROSS THE RANGE OF MILITARY OPERATIONS

Marine expeditionary forces require the capability and flexibility to conduct operations throughout the conflict continuum and across the ROMO. Regardless of the type of operation being conducted, Marines are required to engage networks using lethal and/or nonlethal capabilities. The complexity associated with the battlespace requires that Marines gain a greater understanding of the interrelated networks present within the operational environment. The simple statement that network engagement applies across the ROMO is generally accepted but must be explored as a consideration in planning.

Military Engagement, Security Cooperation, and Deterrence

Examples of how network engagement activities impact operations related to military engagement, security cooperation, and deterrence are provided in the following subparagraphs.

Nation Assistance. Depending on the various nations and international organizations involved in providing assistance, it is essential that Marines are able to identify how these entities impact the operational environment. In many cases, operations of this nature will be conducted as part of a multinational task force, of which the United States may not be the lead. Understanding and engaging the networks present within the operational environment must be planned in a deliberate manner in order to maximize potential opportunities and to mitigate challenges that may negate mission accomplishment.

Humanitarian and Civic Assistance. Humanitarian and civic assistance to the local populace is predominantly provided by US forces in conjunction with military operations and exercises. Planning for these types of operations requires a greater understanding of the local populace, which includes historical considerations, cultural norms, societal norms, and their potential effect on operations. This understanding is also a critical component for the deployed forces routinely engaging networks during operations. As this occurs, the potential exists to gain a greater understanding of the operational environment that should be considered for future operations.

Support to Foreign Internal Defense. This involves the participation by civilian and military agencies of the United States in any of the actions taken by another government or other designated organization to free and protect its society from subversion, lawlessness, and insurgency. The conditions present within the operational environment are the basis for the threat present within the society, which must be identified and considered during planning. Engagement of all networks will be required to support foreign internal defense operations, with the level and type of engagement being determined by the commander.

Maritime Security Operations. Maritime security operations protect sovereignty and resources; ensure free and open commerce; and counter maritime-related terrorism, transnational crime, piracy, environmental destruction, and illegal seaborne immigration. Marines may participate in maritime security operations by conducting visit, board, search, and seizure operations, as in 2010 when elements of the 15th Marine Expeditionary Unit recaptured the MV Magellan Star and rescued its crew from Somali pirates. The complexity of the operational environment and the broad nature of these types of networks make it necessary for units to leverage outside agency assets to assist in gaining a greater understanding of the networks to be engaged. Network engagement enablers and resources available to Marines may provide an understanding of the networks that are responsible for nefarious actions and their relationships to other networks. Targeting the specific nodes of a network may result in the desired effects necessary to achieve a commander's objectives. Depending on the type of operation being conducted and the command relationships that may exist, network engagement may be carried out by outside agencies in support of the operation.

Antiterrorism. Antiterrorism efforts consist of defensive measures used to reduce the vulnerability of individuals and property to terrorist acts. These defensive measures include limited response and containment by local military and civilian forces, such as fleet antiterrorism security teams. Friendly and neutral networks will inherently have a large contribution to these types of operations. An objective of antiterrorism operations may be to influence neutral networks to establish conditions within the operational environment that make it more difficult for threat networks to conduct attacks.

Department of Defense Support to Counterdrug Operations. The Department of Defense (DOD) supports federal, state, local, and foreign law enforcement agencies in their efforts to disrupt the transfer of illegal drugs into the United States. Military forces assist in detecting and monitoring drug trafficking, support interdiction efforts, provide intelligence and logistic support, and integrate communications and intelligence assets dedicated to interdicting the movement of illegal drugs into the United States. The threat networks responsible for drug trafficking must be fully understood in order to facilitate Marine Corps support to these types of operations, especially from the intelligence support aspect of the operations. It may be necessary for Marine Corps forces to partner with United States Government (USG) law enforcement agencies, as their capabilities can be complimentary.

Support to Insurgency. The United States may support an insurgency against an oppressive regime that uses a mixture of political, economic, informational, and combat actions to achieve specific political objectives. This is accomplished by engaging networks using both lethal and nonlethal capabilities in order to set conditions for achieving the identified objectives of the operation.

Crisis Response and Limited Contingency Operations

Crisis response and limited contingency operations encompass a variety of military actions, often in support of other government agencies (friendly networks), to contain or mitigate the effects of natural disasters or calamitous human events. They may occur alongside a variety of nongovernmental organizations (NGOs) (neutral networks) or the forces of other nations (friendly networks) operating—at least initially—without benefit of a commonly stated purpose or formally established divisions of responsibility and authority.

Consequence Management. Consequence management consists of actions taken to maintain or restore essential services and manage and mitigate problems resulting from disasters and catastrophes, including natural, manmade, or terrorist incidents. When conducted within the United States, this will be done as defense support to civil authorities. Engagement of networks will depend upon the nature of the problem that is being mitigated, which must be considered as part of the MCPP's problem framing step. Use of lethal capabilities may be necessary if an objective for the operation is to address a threat network directly. In the event of a natural disaster or catastrophe, use of nonlethal capabilities will be the predominant manner to engage networks in support of achieving objectives.

Noncombatant Evacuation Operations. Noncombatant evacuation operations involve the use of DOD forces under the direction of the Department of State (DOS) or other authorities for the evacuation of individuals, normally US citizens, who are located in a foreign country and faced with the threat of hostile or potentially hostile actions. Such operations may also include the evacuation of US military personnel, citizens of the host country, and third country nationals friendly to the United States as determined by the DOS. Specific lethal engagement with networks may occur as part of the evacuation security plan directed by the rules of engagement (ROE). Unforeseen lethal engagements of networks as part of the operation may result in operational or strategic level impacts for follow-on missions. See MCDP 1-0, *Marine Corps Operations*, for more information.

Peace Operations. Peace operations broadly refer to military, multiagency, and multinational actions to contain conflict, redress the peace, shape the environment to support reconciliation and rebuilding, and facilitate the transition to legitimate governance. Peace operations include peacekeeping, peace enforcement, peacemaking, peace building, and conflict prevention efforts. Depending on the operation and objectives, the ROE will be developed, and could be expanded or diminished, as a result of actions taken by networks and conditions within the operational environment. Friction points that exist between different networks are routinely the source of instability, precipitating the need for peace operations. Assistance to mitigate friction points may be accomplished through engaging select networks in a lethal and/or nonlethal manner. For more information, see MCDP 1-0.

Major Operations and Campaigns

A major operation is a series of tactical actions, such as battles, engagements, or strikes, conducted by combat forces of one or several Services and coordinated in time and place to achieve strategic or operational objectives in an operational area. These actions can occur simultaneously or sequentially in accordance with a common plan. Major operations can become full-scale war with large amounts of conventional forces involved (see MCDP 1-0 for more information). During major combat operations, commanders are routinely focused on engaging and influencing threat

networks. Countering a threat network requires an understanding of a combination of conventional and irregular threat networks. The challenge with these networks is their ability to operate outside of the boundaries established for units, making it difficult to directly generate effects on these networks. As such, the impact of operations on neutral networks should be considered for the planning of later phases of the operation. Depending on the duration of the operation, commanders should ensure that information about the operational environment is passed to follow-on forces for use in their planning efforts.

Counterinsurgency. Counterinsurgency and insurgency reside within a broad category of conflict known as irregular warfare. Network engagement is designed to support commanders conducting counterinsurgency operations and to enhance their ability to gain and maintain situational awareness of the operational environment. Countering a threat network in this type of operation requires a combination of lethal and nonlethal engagements with all networks. The ability to monitor and evaluate the conditions within the operational environment is necessary to assess if a desired end state is being achieved.

Defensive Operations. Although offensive action is generally viewed as the decisive form of combat, it may be necessary, or appropriate, to conduct defensive operations. Conducting defensive operations requires understanding the types of threats that exist and which networks are the nexus for these threats. Focusing specifically on the networks that are directly responsible for the threat may not be adequate in creating the plan for the operations. Threats can be of a lethal or nonlethal manner, which will require commanders to employ various capabilities available to defend or counter the threat. Network engagement provides commanders with an enhanced ability to understand this threat and plan operations.

Offensive Operations. Offensive operations seek to gain, maintain, and exploit the initiative, causing the enemy to react. Offensive operations focus on the enemy. Network engagement methods can provide commanders with information on a specific enemy in support of offensive operations. A challenge to Marines in the future will be to understand and overcome a threat network that applies traditional and irregular approaches in a combined manner. These threat networks are interrelated with multiple networks (friendly, neutral, and/or threat) that must be understood prior to engaging. The ability to assess the effects of the operations will require information attained through the application of network engagement methods and support from network engagement enablers. Regardless of the shape of the battlespace, either linear or nonlinear, network engagement methods can provide greater insight into the enemy and overall situational awareness within the operational environment.

Reconnaissance and Security Operations. Reconnaissance operations use visual observation or other detection methods to obtain information about the activities and resources of an enemy or adversary. Commanders use that information to help them understand the larger environment and the nature of the problem. Security operations, by contrast, are an essential component of all operations. They involve measures taken by a military unit, activity, or installation to protect against all acts designed to impair effectiveness. Maintaining or increasing security conditions requires targeting of specific nodes with lethal and/or nonlethal capabilities. Network engagement enhances the targeting process used to accomplish this. In these types of operations, the information attained through the application of network engagement methods also supports

commanders' operations assessment plans by providing an enhanced understanding of the operational environment and potential effects on the networks due to operations conducted.

Stability Operations. Stability operations encompass various military missions, tasks, and activities conducted outside the United States in coordination with other instruments of national power to maintain or re-establish a safe and secure environment and/or provide essential government services, emergency infrastructure reconstruction, and humanitarian relief. Stability operations occur throughout all phases of conflict and across the ROMO. They require a comprehensive understanding of the operational environment, which includes the various interrelated networks, in order to support planning, targeting, and assessment. Network engagement and the leveraging of network engagement enablers can provide commanders with a greater insight to support these efforts.

Regardless of the type of operation being conducted, it should be understood that the operational environment is complex, and a component of that environment includes various networks that are inherently interrelated. Network engagement is designed to provide commanders and their staffs with options to gain a greater understanding of the entire battlespace. This information and subsequent analysis enhances the existing processes used to conduct any type of operation. Network engagement is employed by commanders completely at their discretion based upon the determination of requirements to attain specific objectives.

CHAPTER 3
OPERATIONAL ENVIRONMENT COMPLEXITY

Complex environments are the totality of networks, actors, influences, and actions coupled with the rapid dispersion of information across the environment. The battlespace, comprised of areas of operation, influence, and interest, is further complicated by the interrelated and overlapping nature of networks and global actors, both internal and external, impacting the operational environment. The blurring of lines between the levels of war, restrictive ROE, multinational operations, and an ever-present media impact operations by adding complexity to commanders' decision making. Networks, like conflicts, are rarely constrained to clearly defined geographic areas or the identified battlespace. They operate across boundaries and within the virtual world. Mission accomplishment in these environments requires commanders to identify the correlation between the operational environment and their objectives.

UNDERSTANDING THE OPERATIONAL ENVIRONMENT

The MCPP requires commanders and their staffs to apply critical thinking to gain an understanding of the operational environment. An in-depth evaluation of the operational environment provides commanders and their staffs with the factors or variables necessary to characterize it. These variables are used to not only focus planning efforts, but also to understand second- and third-order effects produced by targeting networks and assessing operations. Further evaluation of the operational environment from the perspective of the targeted network can help identify the variables that support that network's formation and sustainment. Due to the variety of operations that may be conducted, establishing favorable conditions for mission success requires engaging the multitude of networks within the operational environment to achieve a desired end state.

The necessity for Marines to understand the operational environment extends beyond the physical dimension. Commanders and their staffs must also consider the cognitive and informational dimensions (e.g., social, political, cultural, historical) of the operational environment. This consideration allows an understanding that begets more effective engagement with the various networks and improves their impact on the operational environment. Expeditionary operations taking place in the world's urban and littoral regions involve both a high population density and many organizations with their own agendas and often competing priorities. These organizations, as members of the interrelated networks, add complexity that Marines need to directly or indirectly engage. Continuous monitoring of the operational environment and the networks therein provides commanders the necessary feedback to adjust planning and execution of operations.

UTILIZING METHODS TO GAIN UNDERSTANDING

The information available to characterize the operational environment is extensive, and information models exist to support the evaluation and organization of the information. Each of these models was developed to provide the user with a unique perspective focused on specific aspects of the operational environment. Figure 3-1 graphically depicts some of the information models that are available for use to assist in the evaluation of the operational environment.

Additionally, figure 3-1 depicts the multifaceted and interconnected elements of the operational environment: the base map (formed with US Geospatial Intelligence Foundation data); threats and vulnerabilities; host nations, security forces, and neutral populations; and friendly forces and activities. Although no individual model alone is sufficient to illustrate the complexities of the

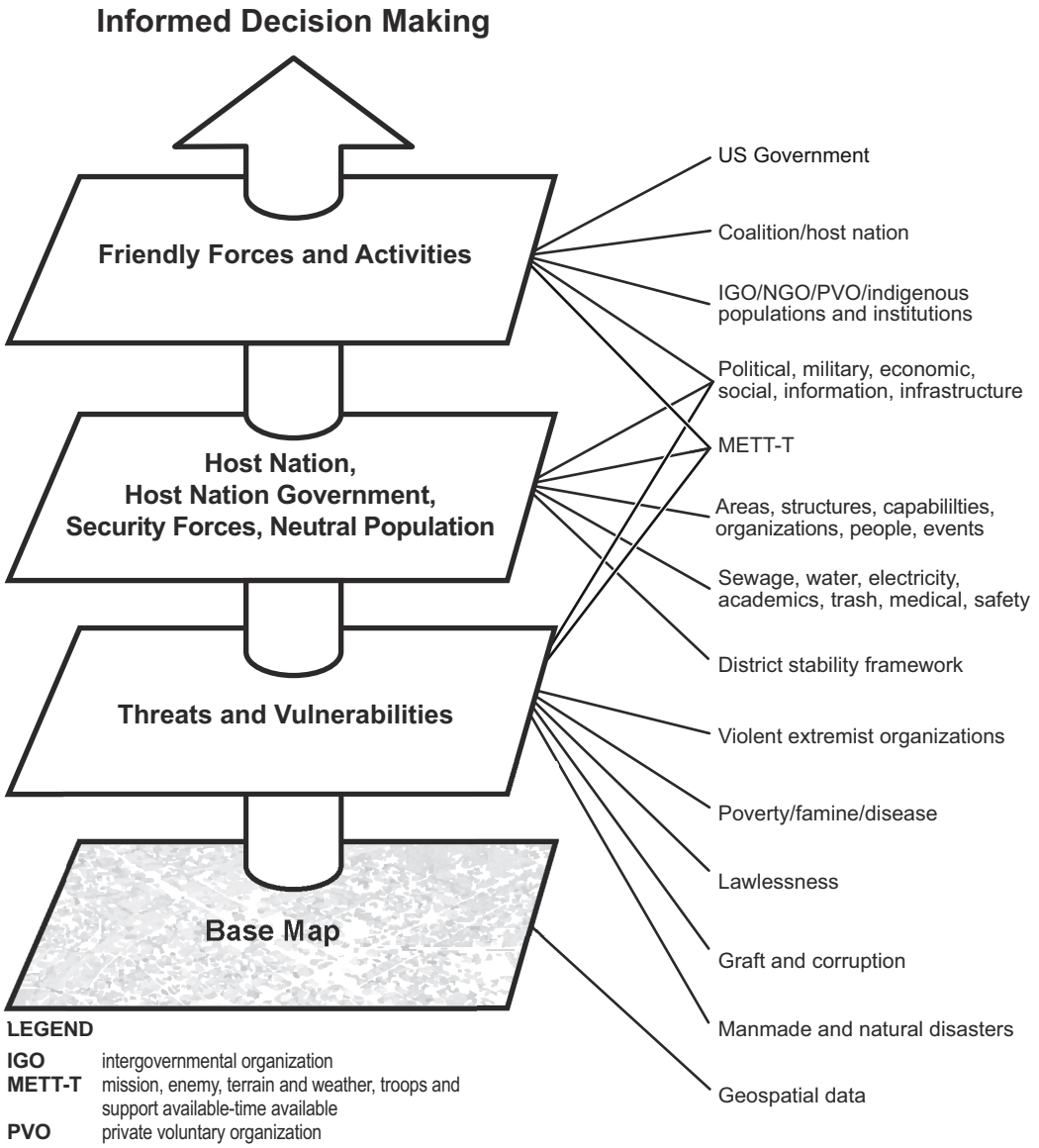


Figure 3-1. Information Models and the Complex Operational Environment.

operational environment, commanders may elect to use various types of models to support evaluation and subsequent management of information.

Information Models

Within network engagement, the political, military, economic, social, information, and infrastructure (PMESII) and areas, structures, capabilities, organizations, people, and events (ASCOPE) models are used to evaluate the operational environment due to their ability to illustrate a correlation between operational and mission variables.

Political, Military, Economic, Social, Information, and Infrastructure. The PMESII is an information model that helps identify operational variables of the operational environment. Applying PMESII allows for an understanding of the various systems present within the operational environment. While the operational variables are traditionally used for planning at the operational level of war, they can be used to help categorize and analyze information to plan at the tactical level.

Areas, Structures, Capabilities, Organizations, People, and Events. The ASCOPE is an information model that was originally designed to provide an understanding of the civil considerations of the operational environment at the tactical level. The ASCOPE model provides commanders with a list of mission variables that helps to describe the operational environment.

Information Models Usage

Table 3-1, on page 3-4, depicts the PMESII/ASCOPE crosswalk, a tool that supports the commanders' abilities to organize, monitor, and evaluate the interdependency of both mission and operational variables. The tool was developed to help gain a greater understanding of how the human environment interacts with and is dependent upon the systems within the operational environment. The use of this tool is intended to help identify the mission variables that not only have a direct impact on the mission, but also impact all of the networks within the operational environment.

The information contained in table 3-1 is not an all-inclusive list of variables, but an example of variables of the operational environment that could be organized into those different areas. Commanders may use the tool as provided in its entirety or modify as necessary. The use of this tool can assist the staff in gaining a better understanding of these variables (see MCWP 5-10 for more information). Further analysis is required to identify how these variables relate to operational efforts and impact conditions for network formation and sustainment. This information can then be used to support assessing both the effects of operations (operations assessment) and the engagement of networks (combat assessment).

Culture. The cultural dimension possesses certain attributes and characteristics that can be used to comprehend unique aspects of networks. Analyzing cultural information is not simply intended to address cultural sensitivity or avoiding social gaffes. It is about identifying culturally significant characteristics of the environment that can impact operational effectiveness and either degrade or enhance mission accomplishment. Understanding the attributes of culture provides a sector for use in an assessment plan intended to evaluate operational effectiveness. Using ASCOPE to understand the social and political systems can help identify specific cultural variables that illustrate how these systems form, operate, communicate, interact, and compete within the

Table 3-1. PMESII/ACOPE Crosswalk.

	P Political	M Military	E Economic	S Social	I Information	I Infrastructure
A Areas	District/provincial boundary	IED/ambush sites Military/insurgent bases	Bazaars Farms Repair shops	Picnic areas Bazaars Meeting areas	Radio Gathering points Graffiti Posters	Irrigation networks Medical services
S Structures	Shura halls Courthouse	Police headquarters Military bases	Bazaars Banks Industrial areas	Mosques Wedding halls	Cell/radio/TV towers Print shops	Roads Bridges Electrical lines Dams
C Capabilities	Dispute resolution Judges Local leadership	Military police Enemy recruiting potential	Access to banks Development Black markets	Traditional structures Means of justice	Literacy rate Phone coverage	Ability to build/ maintain roads, bridges, dams
O Organizations	Government organizations NGOs	Coalition, HN, and enemy forces NGOs	Banks Land holders Economic NGOs	Tribes Clans Families	News organizations Mosques	Governmental ministries Construction companies
P People	Governors Council elders Judges	Coalition, HN, military/police leaders	Bankers Land holders Merchants Criminals	Civic/religious leaders Elders Families	Civic/religious leaders Family heads	Builders Contractors Development councils
E Events	Elections Meetings Speeches Trials	Kinetic events Military police operations	Drought Harvest Businesses opening	Weddings Funerals Births Bazaar days	Festivals Project openings	Road/bridges/ school construction Well digging

Legend
HN host nation
TV television

operational environment. Evaluating the cultural dimension is challenging, and commanders are encouraged to include nonorganic enablers (e.g., civil affairs, military information support operations, DOS) to assist the staff with these efforts.

Language. Language, both spoken and written, is a predominant form of communication in many cultures, so it must be a consideration for network engagement. Specific dialects of a language can help identify social classes, political affiliation, status, or regional alignment. Language as it relates to the operational environment is significant for planning information operations, preparing for key leader engagements, conducting presence patrols, or performing any other type of interaction with the networks in the battlespace. Planning should include providing potential language training, acquiring smart books with key phrases, and identifying interpreter requirements at appropriate levels.

Demographics. Analyzing the people element of ASCOPE within PMESII systems can help commanders gain a greater understanding of the demographics within the operational

environment. Demographic characteristics such as age, gender, political affiliation, length of residency, education level, and country/region/city of birth and origin can often be seen as precursors and indicators of network trends, tendencies, and opportunities. The collection and analysis of data regarding these characteristics assist commanders in gaining an understanding of the conditions of the operational environment, which may provide an accommodating environment and receptive audience for network formation and sustainment. The relevance of these variables to the mission is further understood as problem framing occurs. Commanders are encouraged to leverage nonorganic enablers (e.g., civil affairs, military information support operations, DOS) to assist the staff in this analysis of the operational environment.

Religion. Depending on the culture, religion may play a significant part in the political, economic, social, and information systems of the operational environment. Religion may serve as a catalyst for network formation and sustainment. The staff should consider the impact of religion (e.g., days operations are conducted, engagement practices, treatment of people, ROE limitations) as part of operational planning and engaging networks as they evaluate the operational environment. Depending on the type of operation, religious practices of other member nations of a multinational effort should also be considered during planning in order to reduce potential friction points.

Geography. Terrain is analyzed and described as part of IPB as it relates to maneuver of friendly and enemy forces. Understanding the geography and its impact on the development of the culture is necessary to help commanders gain a better understanding of the operational environment. For example, by examining the geography within the operational environment, it may be identified that previous conflicts between different networks may exist due to competing efforts for limited resources related to the geography (e.g., water, fishing rights, grazing areas, farming areas).

Local Economics. Legitimate and illicit activities must be considered as components of the economic system within the operational environment. The variables identified to describe the economic system may serve as a catalyst for network formation and help foster a receptive audience and accommodating environment. Commanders possess limited resources to affect conditions of the economic systems as part of their operations. Other organizations (e.g., United Nations, DOS, Department of Justice, Department of the Treasury) are assigned the mission and are resourced to engage elements associated with the economic system. Commanders should ensure that their operations are synchronized with these organizations to generate desired effects in support of attaining their objectives.

Key Actors, Tendencies, Relationships, and Potential. These specific factors are better understood through the application of network engagement methods that support network analysis and mapping: social network analysis (SNA), link analysis, and nodal analysis. These techniques are addressed in chapter 4.

Security. Viewing security outside of the traditional force protection lens is necessary to truly understand the interrelated nature of networks and the threats they present to commanders. Security means a variety of things to many different networks and individuals. It can refer to the internal security posture for Marine commanders and their forces, the security climate within a local area, or the external security threats faced by any network. Fundamentally speaking, the greater degrees of security that systems have over a society lead to more restrictive freedoms and fewer actions that are allowed by the populace. It is important to analyze the security climate and condition of the

operational environment and how/whether they influence or contribute to an accommodating environment and receptive audience needed for network formation and sustainment. Commanders should consider the potential undesired or unintended security impacts on other interrelated networks as a result of generating desired effects. The military systems category identified in PMESII is intended to include security considerations for the evaluation of the operational environment, not just formal evaluation of military units or organizations.

Climate. Climate is addressed during IPB and various intelligence estimates. Networks may form and sustain themselves in relation to conditions associated with climate. Patterns of life may be driven with the seasonal changes of the climate and could influence the type and timing of actions taken by networks. Commanders can gain a greater understanding of the networks by considering the aspects of how climate relates to the formation and sustainment of networks and its impact on operations.

Time. Time is perceived differently among various cultures and has an influence on how networks act, relate to the environment, socialize, prioritize activities, and organize themselves. Commanders must realize the unique differences in how time is viewed in different cultures as this will shape how networks are engaged. Without considering the impact of time as it relates to networks, the potential exists to conduct engagements that result in undesired or unintended effects. Time may also be viewed differently by other member nations of a multinational effort and should be considered during planning to reduce potential friction points. For example, US forces on a deployment may hold the perception that long-term objectives are ones that focus on a desired end state that could be 9 to 12 months away. Due to the history and composition of other cultures, 9 to 12 months may be perceived as short-term, and true long-term may be measured in years or even longer. Additionally, US forces plan operations on strict timelines, which in some cases may be difficult to adhere to or understand due to cultural differences. Consideration for how different cultures perceive time is vital in gaining an understanding of the operational environment.

Historical Considerations. Cultures are developed and influenced over time by a long history of events. Understanding the operational environment and the interrelated networks that exist and key historical events that have impacted these components is necessary for Marines as part of the planning process. Additionally, it is important to consider other countries' involvement or impact on the operational environment, especially when operations are part of a multinational effort. For example, if country X, which is part of a multinational effort, had previously occupied country Y, the population of country Y may possess some opinions about the forces from country X. Planning on how to employ these forces must be done with the historical considerations taken into account in order to mitigate undesired effects or to minimize potential friction points. Historic journals and country studies (from civil-military operations or the DOS) are resources that can be used to provide information on historical events for an area. The information gained from the journals and studies could then be identified and organized using the events section of ASCOPE with consideration of the systems represented by PMESII.

IDENTIFYING CRITICAL VARIABLES

Critical variables are resources or conditions that are present within the operational environment, that have a direct impact on the commander's objectives, and that may affect the formation and sustainment of networks. Achieving the commander's desired end state is accomplished by affecting the critical variables of the operational environment. This is realized through the development and implementation of an assessment process, addressed in chapter 6. Additionally, understanding the critical variables as they relate to networks provides key information that can be used to target and assess the effects of engaging specific nodes and/or links that result in broader effects on networks. The process of establishing the context or relationship of each variable within a network is a collaborative effort among the staff and derived from cross-functional entities such as working groups or operational planning teams.

To determine the impact of a critical variable on a particular network, values are assigned to each critical variable in an infographic. One qualitative method is to determine that the critical variable has either negative (-), positive (+), or no impact (0) on a specific network. Full application of this is discussed in appendix C.

A critical variable that is used for planning and assessing operations may result in the development of a commander's critical information requirement (CCIR), but a critical variable alone does not constitute a CCIR in all cases. Through analysis by the staff, recommendations can be made to the commander to identify the critical variables that could be considered as a CCIR to support the commander's decision-making process. See appendix C for an example of how critical variables are identified and analyzed for network engagement.

This Page Intentionally Left Blank

CHAPTER 4
NETWORK IDENTIFICATION AND UNDERSTANDING

A network is formed by a direct or indirect tie between two or more nodes who share a common purpose as defined in chapter 1. While the study, analysis, mapping, and targeting of networks are relatively new concepts within military processes, networks have existed throughout history and have been studied in various academic realms. Recent operations highlight the need to better understand a network's characteristics, components, behaviors, relationships, and effects within the environment. Adaptation of early methods developed in academia is being successfully applied by various law enforcement agencies to better understand networks and their impact on an environment. Network analysis provides commanders with techniques to gain a better understanding of a network's structure and functions.

NETWORK TERMS AND STRUCTURES

Human networks are comprised of socially connected individuals who are involved in activities to achieve some form of social, political, monetary, religious, or personal gain. Networks can be large or small, local or global, domestic or transnational, cohesive or diffused, and centrally directed or highly decentralized. (See JP 3-25 for additional information.)

Components of a Network

Regardless of the type of network (friendly, neutral, or threat) that a unit is attempting to identify and understand, networks share common structural components and features (see fig. 4-1 on page 4-2):

- Nodes—the building blocks of a network. They may be a person (an actor), place, or thing, but a network does not truly exist until nodes connect.
- Links—connections, associations, or some type of involvement that is a conduit for information sharing or interaction between nodes. An example of this is the command or supervisory arrangement that connects a superior to a subordinate. Links are based on relationships, and they may be characterized as familial, proximal, virtual, or specialized.
- Dyads—two nodes connected by a link; the smallest form of a network. Multiple unique dyads may exist to form larger networks, and the analysis of individual dyads may help to further understand these larger networks.
- Cells—organizations that commonly develop within a network, though they are not a required component of all networks.

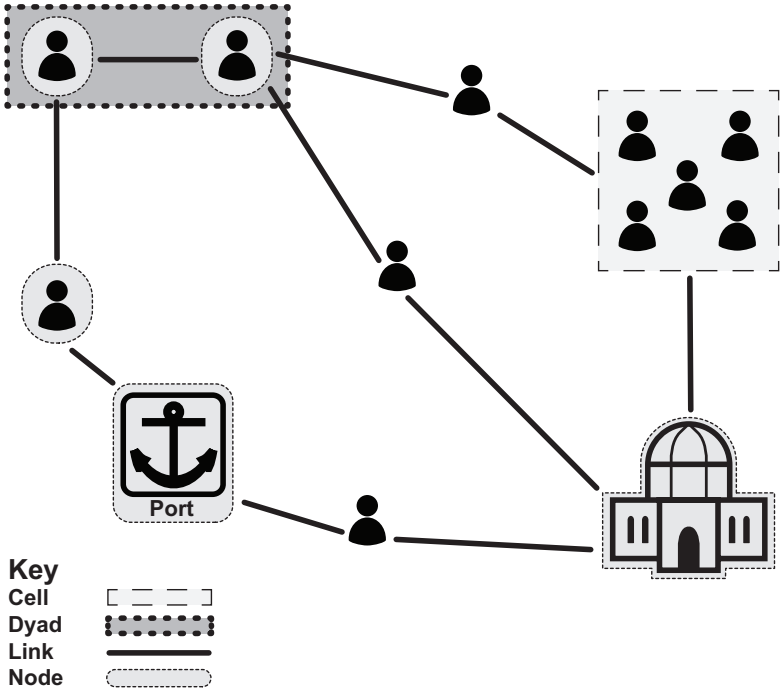


Figure 4-1. Network Components.

Network Formation

Networks are typically formed at the confluence of three conditions: the presence of a catalyst, a receptive audience, and an accommodating environment.

Catalyst. A catalyst is a condition or variable within the operational environment that could motivate or bind a group of individuals together to take some type of action to meet their collective needs. A catalyst may be identified as a critical variable when units conduct their evaluation of the operational environment. A catalyst may be a person, idea, need, event, or some combination thereof. The potential exists for the catalyst to change based on the conditions of the operational environment.

Receptive Audience. A receptive audience is a group of individuals who 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 operational environment.

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

If a commander decides to engage a network, the critical variables that represent the catalyst, receptive audience, and accommodating environment must be identified. Understanding these critical variables helps focus targeting efforts on individual nodes or operations to generate desired effects within the operational environment.

Characteristics of a Network

Networks all possess some common organizational characteristics that include structure, density, and adaptability.

Network Structure. The way a network is structured will determine some of its inherent characteristics. Networks can be hierarchical, nonhierarchical, or a blend of both.

Hierarchical Networks. Hierarchical networks tend to centralize power and authority through a well-defined vertical chain of command and responsibility. Information flows up and down formal organizational channels that correspond to these vertical chains, but may not officially move horizontally through the organization (see fig. 4-2). This type of structure is traditionally associated with established military organizations. Hierarchical organizations feature greater specialization of functions in their subordinate cells (e.g., support, operations, intelligence). These types of networks are comprised of multiple closed systems, meaning that formal connectivity between subordinate cells does not exist. The impact of having multiple closed cells within this type of network may result in positional or nodal targeting that can be effective in destroying network capability.

Nonhierarchical Networks. Nonhierarchical networks are decentralized decision-making structures. Although they do not always have an identifiable organizational structure, nonhierarchical networks have a coherence of objectives or goals (see fig. 4-3 on page 4-4). These networks may contain various open systems, meaning that connectivity between cells can exist. This can increase information sharing across the network. When engaged, these types of networks may become even more decentralized. Group or nodal targeting will likely only cause temporary disruption to this type of network. This is due to this network's ability to regenerate and fill the function of the node that was removed from the network.

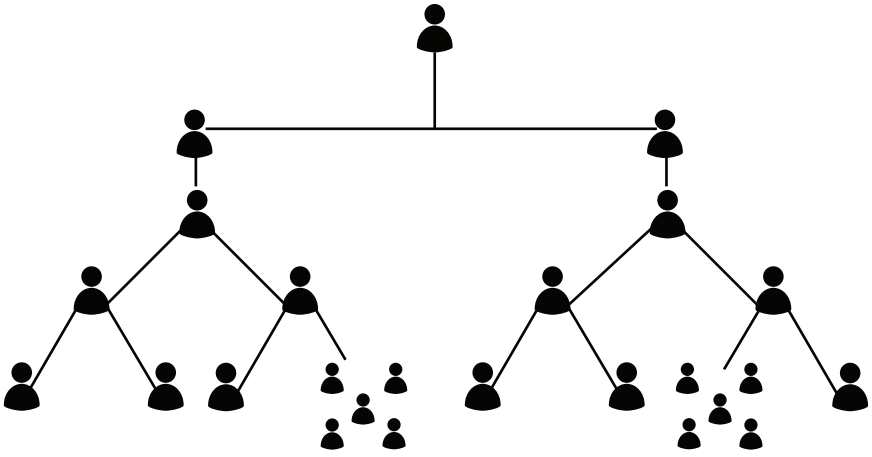


Figure 4-2. Hierarchical Network Diagram.

Blended Networks. Blended networks have a structure that is a combination of hierarchical and nonhierarchical organizations (see fig. 4-4). Impacting the blended network involves all of the challenges associated with the nonhierarchical network. Ultimately, a blended network may resolve to re-organize into a fully nonhierarchical construct in order to survive and function within an environment.

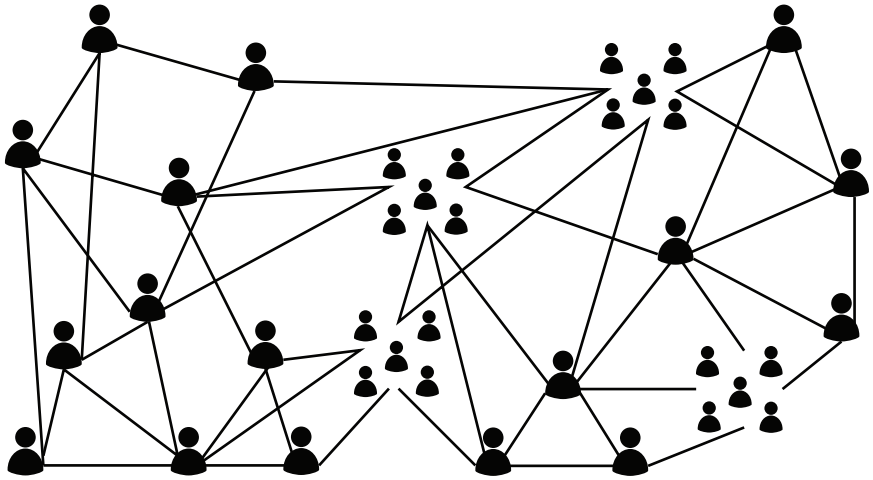


Figure 4-3. Nonhierarchical Network Diagram.

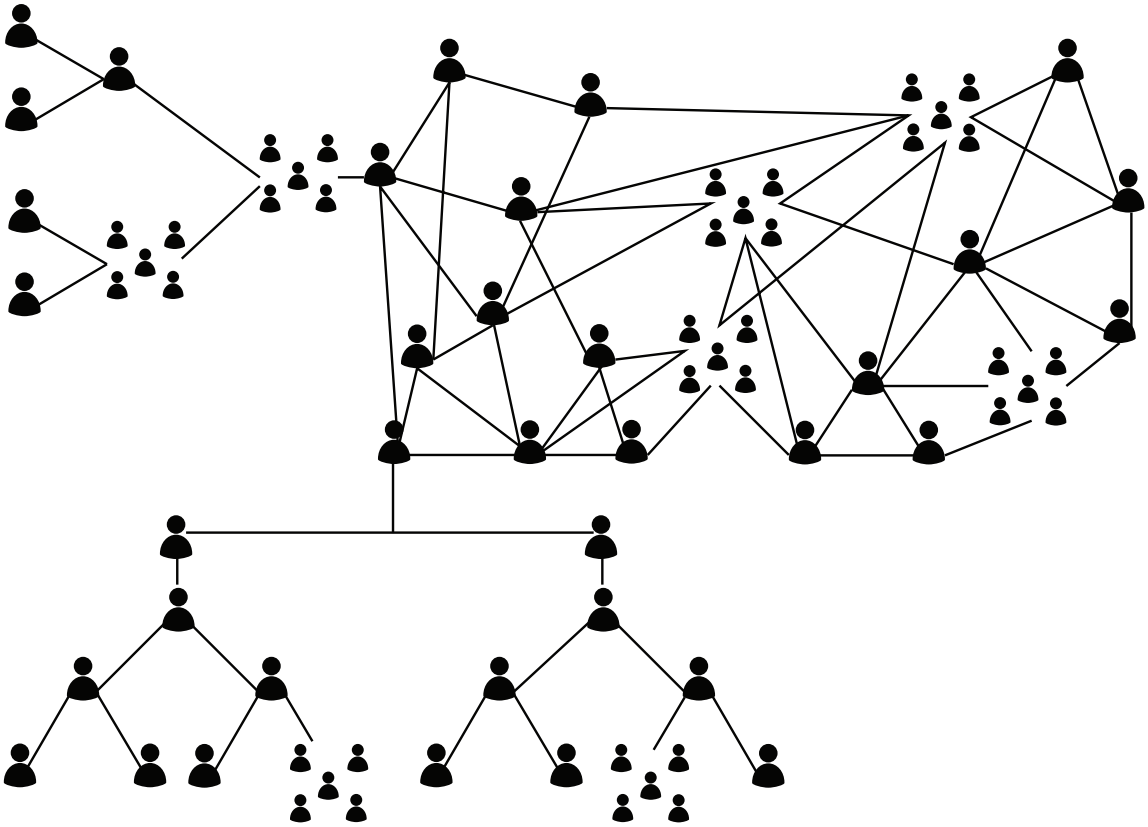


Figure 4-4. Blended Network Diagram.

Network Density. Density is a general indicator of how connected people are in the network as measured by the proportion of ties in a network relative to the total number possible. A network becomes denser as the number of links between nodes, dyads, and cells increases. When a network is highly interconnected or denser, fewer constraints exist for the individuals within it. They may be less likely to rely on others as brokers of information; be in a better position to participate in activities; or be closer to leaders and, therefore, able to exert more influence upon them. A network with low interconnectivity or less density may indicate that there are clear divisions within a network or that the distribution of power or information is highly uneven and tightly controlled. Figure 4-5 depicts two networks for comparison. Both network A and B include seven total nodes. However, network A has a total of 7 links between the nodes, and network B has a total of 12 links between the nodes, illustrating that network B is denser than network A.

Network Adaptability. A network's ability to adapt to the changing conditions within an environment is influenced by its structure and density. Components of adaptability can include command and control structure; individual and shared identity; knowledge, skills, and abilities of group leaders and members; and the ability to compete for resources. The adaptability of a network is a key determinant for the sustainment of the network within the operational environment. Adaptability presents challenges to engaging networks and determining the effects of those efforts. Commanders must consider the adaptability of a network as part of their targeting process for subsequent targeting efforts.

Network Categories

Categorizing a network is an information management technique used to help understand the relationship between a network and the friendly operational efforts. By evaluating the network's affiliation to friendly efforts, analysts may choose to categorize the network as friendly, neutral, or threat. These three broad categories should not be considered a rigid or inflexible construct, but as a starting point for the staff to determine a category that is most appropriate based upon the network's capability and intent.

The Friendly Network. Friendly networks are networks that are sympathetic to or that assist, directly or indirectly, with a commander's mission. Examples of networks that could be

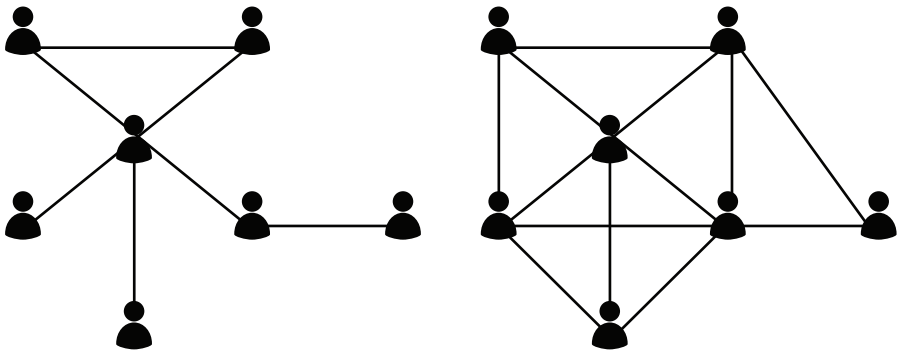


Figure 4-5. Network Density Comparison.

considered friendly include US forces, coalition forces, and USG organizations. Depending on the type of operation being conducted, a host nation government and its forces may be categorized as a friendly network if they are included as part of the coalition or some type of partnership.

The Neutral Network. Neutral networks neither actively support nor oppose US, coalition, and/or host nation interests and are not generally considered a current threat or asset. Successfully engaging neutral actors/nodes is a major challenge for coalition forces because engagements require subtlety, sensitivity, and potentially long durations of time to establish trust and strengthening of relationships. Understanding the catalyst that unites a neutral network assists commanders in determining the network's capability and intent. Friendly networks can comprehensively target and engage neutral networks in order to gain their support or undermine potential support to threat networks. Examples of networks that could be included in this category are elements of the population, NGOs, foreign and domestic private companies, media organizations, and religious groups.

The Threat Network. Threat networks have goals, objectives, or actions that oppose US, coalition, and/or host nation interests and negatively influence or impact the commander's operational goals and actions. A subset of the threat network could include criminal networks whose activities, while not directly hostile, have a negative impact on the commander's objectives. Examples of networks that could be included in this category are conventional armed forces, insurgent groups, criminal organizations, and geopolitical organizations.

TECHNIQUES OF NETWORK ANALYSIS

Network analysis can be described as an evaluation, gathering, and interpretation of data to resolve the presence of associations and relationships among individuals, groups, or other entities. It also includes the context and meaning of the relationships between people to identify the ways in which those associations can be strengthened or weakened. Operational environments will always contain interrelated friendly, neutral, and threat networks that will affect the mission. Analysis of these networks assists the commander in determining which key nodes/actors should be engaged as part of the targeting process. As a part of the targeting process, confirming the identification of a node/actor will be required and is supported by identity operations addressed in appendix B.

With large and complex networks, various software programs can be used to find key nodes and the degrees by which those nodes are connected to other nodes. However, the concept of network analysis and its basic execution can be grasped without special software and even without computers. Network analysis consists of network mapping, network templating, SNA, link analysis, and nodal analysis.

Network Mapping

Network mapping is the graphical representation of the nodes of a network that depicts the link between different nodes within the network. The purpose of this method is to gain an understanding of what links exist between nodes. It is not necessarily focused on the condition of those links, which

is accomplished using link analysis. While network maps can become very large and cumbersome, network mapping is essential for further analysis and ultimately for understanding the network. Figure 4-6 depicts an example of a basic network map. Like many intelligence products that are developed, the network map is continually refined and enhanced over time as information is collected and analyzed.

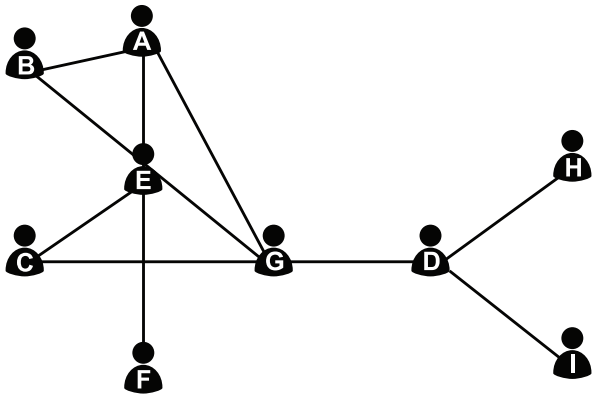


Figure 4-6. Network Map.

Additional analysis of the network map allows for the identification of linked or anomalous nodes to identify patterns within the network. Clusters of nodes can signify the existence of cells, groups, or cliques. Figure 4-7 uses the example of the network map and identifies two different clusters and an anomalous node within the network. These could be indicators of how the network operates or communicates, which focuses an analyst's efforts to gain a better understanding of the overall network.

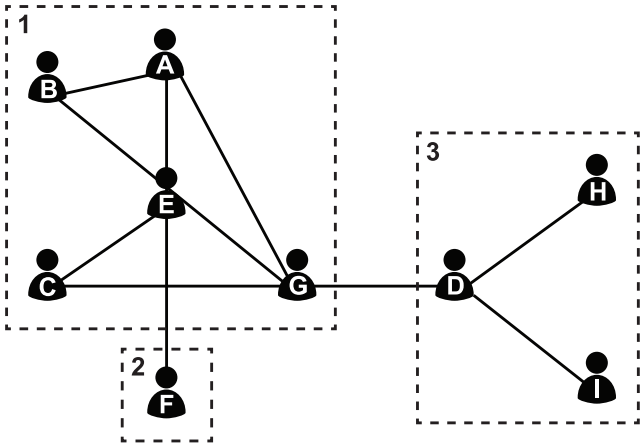


Figure 4-7. Refined Network Map Analysis.

Network Templating

Templates are developed by analysts as a product of the intelligence cycle to provide the commander with the general construct and functions of a network. These templates can be used by the staff to support planning and targeting efforts and may also be used to support the development of a collection plan. Figure 4-8, on page 4-8, depicts an example of a network template.

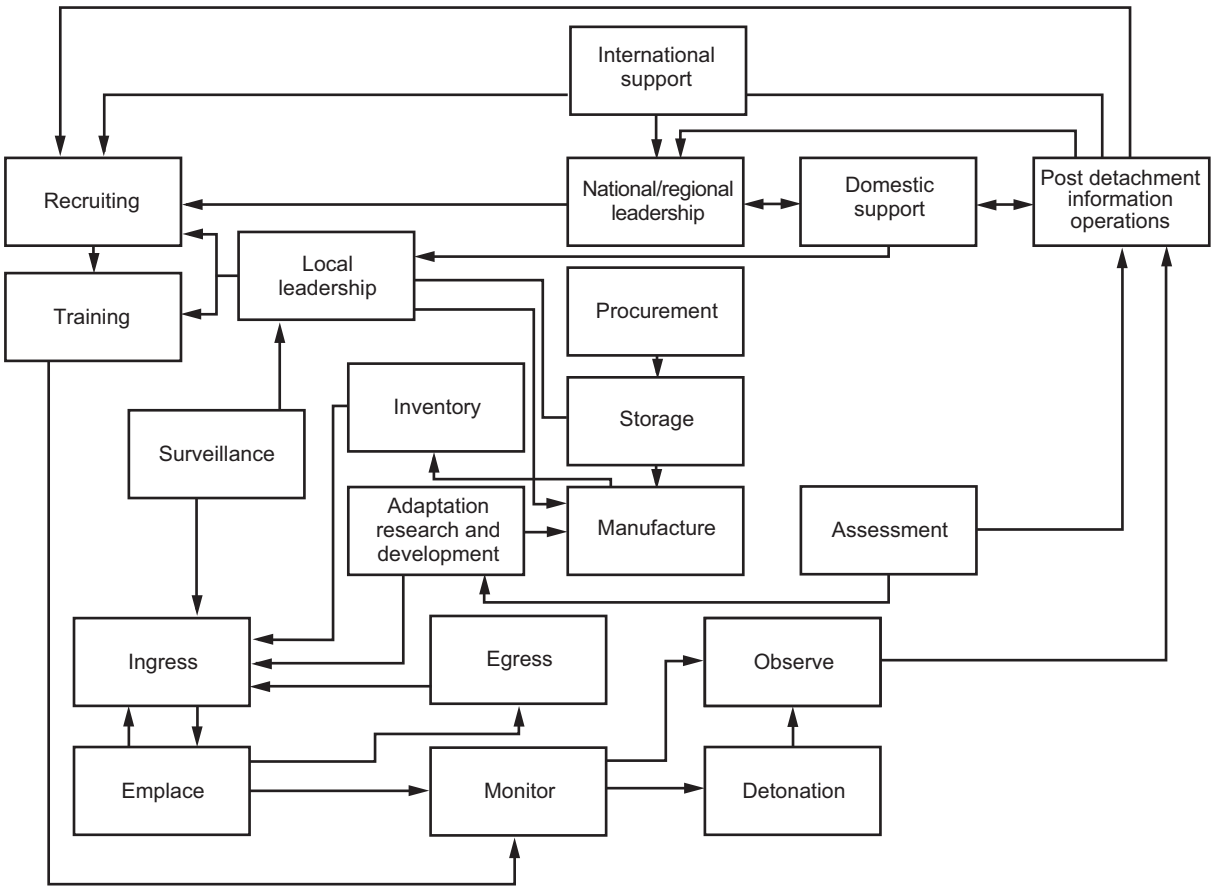


Figure 4-8. Example Network Template.

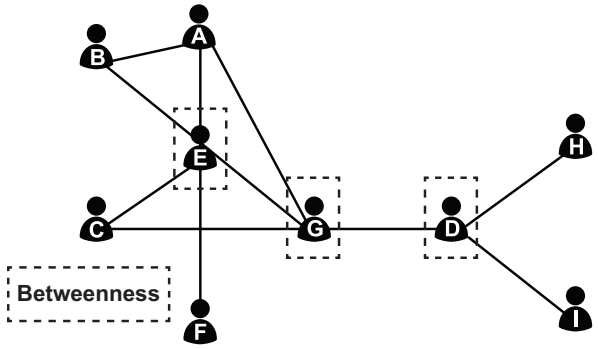
Social Network Analysis

Social network analysis is the identification of key nodes in the network based on consideration of nodes on the periphery of the network map and three types of centrality: degree, betweenness, and closeness. Social network analysis provides quantitative data regarding the frequency and degree of links between nodes. Understanding the level of centrality for a node may support a decision for additional collection and analysis on that node. The quantitative data from SNA may also be considered with other qualitative data for the node to support target prioritization and selection.

Peripheral Nodes. Nodes located on the periphery of a network may serve as useful benchmarks to further map out the initial network to other friendly, neutral, and threat networks. Upon further mapping and analysis of the network, nodes originally considered to be peripheral might later be identified as nodes with betweenness centrality. The network analysis example in figure 4-7 illustrates an examples of a peripheral node in box two that includes node F. Identification of this node may generate additional collection efforts to understand the function and potential relevance of this node to the network.

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. Having degree centrality allows nodes to directly access and to affect the largest amount of people. Figure 4-9 is a mapped network, and each node has been analyzed for its level of degree centrality. Node E is evaluated at five because this node possesses links to five other nodes. Within this network, node E has the highest level of degree centrality. A higher degree of centrality may be an indicator of an individual who would warrant additional analysis or who could potentially be the focus for a collection plan. The level of degree centrality is one data point of many that should be considered by the commander and the staff as part of the overall analysis necessary to support targeting.

Betweenness Centrality. Betweenness centrality is determined when a node serves as the only connection between small clusters or individual nodes (cliques, cells, etc.) and the larger network. Having betweenness centrality allows a node to monitor and control the exchanges between the smaller and larger networks that they connect, essentially to act as a gatekeeper for information for sections of the network. Figure 4-9 illustrates three nodes of a network that have been identified as having betweenness centrality, identified by the boxed nodes E, G, and D. The larger portion of the network (A, B, C, E, and G) is connected to a peripheral node and a cluster of nodes. Node E possesses betweenness centrality in the network due to the link with node F. Elimination of node E in this network would isolate node F since any information being passed from node F to



Node(s)	Centrality	
	Degree	Closeness
E	5	3
G	4	2
A,D	3	3
B	2	4
C	2	3
F, H, I	1	4

Figure 4-9. Centrality Analysis.

other parts of the network must go through node E. Node G possesses betweenness centrality for the cluster D, H, and I. Node D possesses betweenness centrality for nodes H and I.

Nodes that possess betweenness centrality may be a point of interest for the commander to dedicate additional collection efforts on in order to gain a greater understanding of the network. Since these nodes function as gatekeepers for information, the potential exists for leveraging the nodes for messaging efforts or for elimination, which could cause fracturing of the network. Understanding the nodes that possess betweenness centrality is an important data point for consideration during targeting efforts.

Closeness Centrality. Closeness centrality describes the length of the path between one node and all others in the network. Nodes with a high level of closeness centrality are identified as those individuals who do not necessarily have the most links with other nodes, but are those who have the closest association with every other node in the network. Having a high level of closeness centrality affords the node the best ability to directly or indirectly access the largest amount of nodes in a network with the shortest path to other nodes within the network. In figure 4-9, the graphic provides the level of degree and closeness centrality for each node in the network. Node G possesses a level of closeness centrality of two, meaning that the shortest path to any other node within the network is two. Conversely, node E possesses a level of closeness centrality of three, due to the path from node E to nodes H and I. The level of closeness centrality for a node may help an analyst understand the level of influence that a particular node may have within a specific network, which can then be used to support targeting efforts.

Link Analysis

Link analysis identifies and analyzes relationships between nodes in a network. Network mapping provided a visualization of the links that exist between nodes, but it did not provide the qualitative data necessary to fully define the links between the nodes. Analysis of the interrelated networks requires clarity on the type and strength of each link connecting a node to others in order to provide the commander with greater understanding of the network, which supports the target selection process. During link analysis, the analyst examines the conditions of the relationship between nodes (i.e., 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 by the staff during the targeting process.

Nodal Analysis

Individuals are associated with numerous networks due to their individual identities (e.g., location of birth, family, religion, social groups, organizations). Some of the aspects used to help understand and define an individual are directly related to the conditions that support the development of relationships to other nodes. Figure 4-10, on page 4-11, identifies some of the aspects that are considered part of nodal analysis. Understanding this type of information about a specific node will help the commander throughout the targeting process.

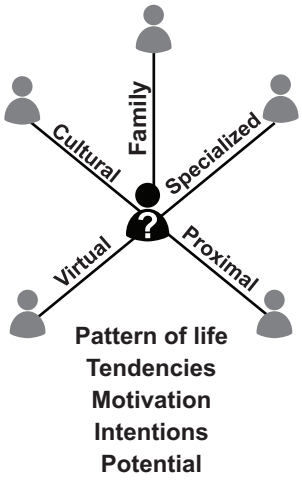


Figure 4-10. Nodal Analysis.

This Page Intentionally Left Blank

CHAPTER 5
ENGAGEMENT OF NETWORKS

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

NETWORK TARGETING CONSIDERATIONS

Initial analysis provides the commander with the basic justification for engaging a particular network. Refined analysis, which happens continuously throughout staff processes, will provide the commander with a comprehensive targeting plan for specific nodes, links, or other network components. It also includes analysis of other networks, providing potential indicators of second- and third-order effects impacting mission accomplishment. Essentially, this refinement moves network analysis from a macro view of network components to a micro view of interrelated networks and network characteristics. If misinterpretation of the networks occurs, it has the potential to diminish the desired effects on a network or the ability to fully exploit potential targeting opportunities.

ENGAGING THE NETWORK THROUGH TARGETING

Engaging networks occurs using the targeting process, a continuous and cyclical effort comprised of the four phases of D3A. Phases occur at the same time when executing current operations and planning future operations. These phases are sequential in the context of any given planning cycle. The commander directs the targeting effort, and this process begins with guidance. The commander's guidance should include expectations for unit tasks, prioritization criteria for potential targets, and the general effects desired by engaging those targets. The staff interprets this guidance to focus network and operational environment analysis in order to identify the key information that is needed to support the commander's decision-making process.

Decide

The decide phase is the first step in the targeting process. This step provides the overall focus and sets priorities for intelligence collection and network engagement planning. Integrated network engagement enablers (see app. A) have the ability to provide the commander with a greater understanding of the interrelated networks within the operational environment. The decide phase

draws heavily upon this detailed operational environment and network analysis, as well as the continuous assessment of the effects of previous targeting efforts.

In the decide phase, the information requirements concerning interrelated networks may be more extensive than what is required for engaging a conventional force using only lethal capabilities. During the decide phase, the following questions are answered:

- *Who to target?* Analysis of networks provides the commander and the staff with the information needed to prioritize potential targets.
- *What are the desired effects on the target?* Understanding the conditions in the operational environment and the future conditions for attaining objectives supports the decision of what type of effects are desired on the target as this relates to supporting overall objectives.
- *How are those desired effects produced?* Both lethal and nonlethal capabilities are available for employment by the commander to directly or indirectly affect a target through engagement. Information available from evaluating the operational environment and analyzing the interrelated networks is used to support this decision.

Support to Target Selection. As the intelligence section and network engagement enablers conduct network analysis, their focus is to provide the commander with relevant information about the network and specific nodes. This analysis can provide the commander with the structure and function of a network (see fig. 5-1), which are targeting considerations. The commander may elect to submit additional requests for information regarding the structure and function of the network being engaged. An example of a request of this nature is the confirmation of the identity of an individual that leverages biometric data and forensic exploitation efforts as a part of identity operations (see app. B).

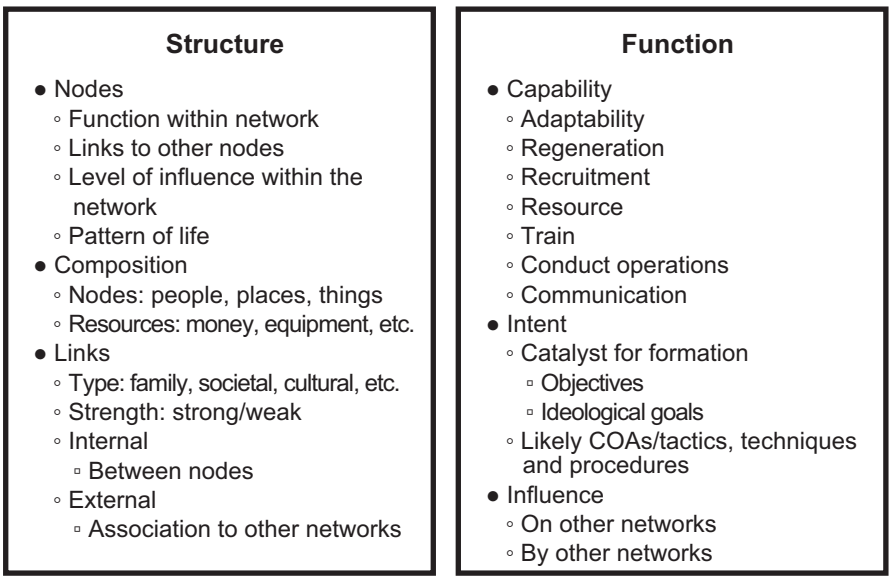


Figure 5-1. Network Structure and Function Considerations.

Desired Effects on Networks.When applying D3A as outlined in existing doctrine, the desired effect is to damage enemy material or cause enemy casualties. Damage effects on material are classified as light, moderate, or severe and are relevant to the application of lethal capabilities. Network engagement takes into consideration the effects of both lethal and nonlethal engagement of networks. Figure 5-2 illustrates the first-, second-, and third-order effects to be considered when deciding to engage a target within a network.

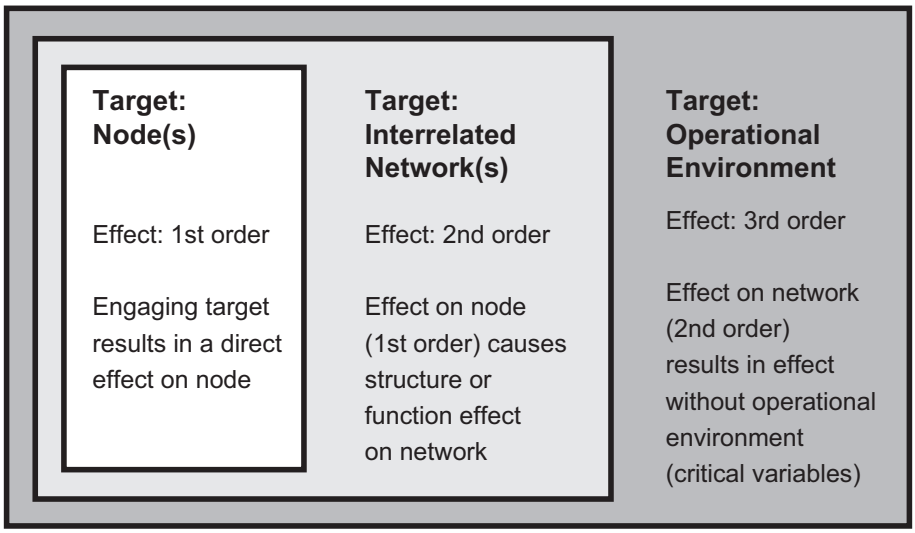


Figure 5-2. Effects of Network Targeting.

When the commander decides to generate an effect on a network through engaging specific nodes or links within that network, the intent may not be to cause damage, but to shape conditions of a mental or moral nature. The result of this shaping is the establishment of conditions within the operational environment to support the attainment of the commander's objectives.

The following are some general categories of effects that the commander may desire to create as a result of network engagement (see table 5-1 on page 5-4):

- Partner—promote, build, partner, resource, train, advise, or assist.
- Engage—co-opt, inform, shape, deter, or leverage.
- Counter—defeat, destroy, kill, capture, mitigate, disrupt, isolate, disorganize, or deceive.

The desired effects selected are the result of a commander's vision of the future conditions within the operational environment that will allow the achievement of military objectives. Although the deliberation on desired effects on a network will occur simultaneously as part of deciding on the target, it is important to understand that any of the effects presented may be applicable in engaging any type of network.

Selection of Capabilities. There are numerous lethal and nonlethal capabilities available to the commander to employ against a selected target. The type of capability to employ is determined

Table 5-1. Potential Effects on Networks.

Effect	Network		
	Friendly	Neutral	Threat
Support			
Promote	X	X	
Build	X	X	
Partner	X	X	
Resource	X	X	
Train	X	X	
Advise	X	X	
Assist	X	X	
Influence			
Co-opt	X	X	X
Inform	X	X	X
Shape	X	X	X
Deter	X	X	X
Leverage	X	X	X
Neutralize			
Defeat			X
Destroy			X
Kill			X
Capture			X
Mitigate			X
Disrupt			X
Isolate			X
Disorganize			X
Deceive			X

relative to the desired effect on the nodes, links, and networks. The following are some questions to consider when deciding the type of capability to employ:

- What resources are available?
- What are the capabilities of those resources?
- What is the timeline for employment and effects?
- What is the effect of employing the capability? How is this assessed?
- What is the scope of the capability or target (node or entire network)?
- What is the collateral damage potential of the capability (undesired first-, second-, and third-order effects)?

Detect

The detect phase of the targeting process determines accurate, identifiable, and timely requirements for collection systems. The targeting section is responsible for ensuring that the collection system asset managers understand these requirements. Information needs for target detection are expressed as priority intelligence requirements and/or information requirements. Their relative priority depends on the importance of the target to the friendly scheme of maneuver, tracking requirements, and the commander's intent. Priority intelligence requirements support the detection of high-value individuals incorporated into the overall collection plan of the unit.

Network engagement enablers, whether organic or nonorganic to the unit, enhance the commander's ability to detect targets through the support of planning, collection, and analysis of information as part of the intelligence cycle. Understanding the operational environment and the interrelated networks provides situational awareness to the staff, which supports the development and implementation of a plan to collect information on indicators that support detecting a potential target.

Deliver

The deliver phase of the targeting process executes the target engagement guidance when enough 'actionable intelligence' has been accumulated, supporting the commander's battle plan. The interrelatedness of networks may allow ripple effects on networks unrelated to the targeting equation, leading to unforeseen effects, which the commander may want to mitigate or exploit. No part of the process is so calcified that prosecution of targets cannot be accelerated or deferred. Tactical patience is the intentional delay of the execution of an operation against a target to allow a fully developed picture of the operational environment or network to emerge. The advantage of a disciplined targeting process is the ability to nest or synchronize operations and intelligence along multiple echelons and event horizons. The D3A process is a mechanism to provide situational awareness and to ensure that high-demand, low-density assets are being utilized.

Plan to Capitalize on Desired Results. Ultimately, successes must achieve a commander's desired end state. To determine how to exploit tactical and operational successes, the commander assesses them in terms of the higher commander's intent. However, success may occur in ways unanticipated during planning. Having a plan for follow-on actions to exploit these unanticipated successes can collapse timelines for achieving overall success.

Plan to Mitigate Undesired Results. Establishing cause and effect when examining changes in human behavior, attitudes, and perception can be difficult, but it is crucial to effective assessment. The commander must guard against drawing erroneous conclusions in these instances. Even when two variables seem to be correlated, the commander must still make assumptions to delineate if the variables are either a cause or an effect. In fact, both may be caused by a third, unnoticed variable. When assumptions are made in support of planning, establishing cause and effect must be recorded explicitly and challenged periodically to ensure the assumptions are still valid. Improvised explosive device (IED) attacks were a common metric used in Iraq and Afghanistan to help determine the level and effectiveness of threat networks. This variable did provide an indication of the threat network's activities in an area, but the correlation between an increase of patrols and an increase in IED attacks was misleading. The misleading aspect was the fact that if

US forces were not operating in an area, the number of IED attacks decreased. An assumption could have been that threat network activities had decreased in a specific area. However, the fact was that if no US forces were present in an area, there was no one for the threat network to attack, nor were US forces able to submit reports on attacks. This variable did provide insight that threat networks were active in attacking US forces and not the neutral networks in the area. Correcting this oversight was accomplished by the staff challenging that variable as part of their battle rhythm. Undesired results are sometimes part of conducting operations, regardless of how carefully a unit plans. Planning to have an identification, notification, and reaction plan in place to overcome or mitigate unforeseen and undesired results can limit the damage on the operational environment. Units are encouraged to establish procedures to address undesired effects of engaging networks in a timely manner as part of their standing operating procedures.

Assess

Assessments of targeting efforts nest and support overall operations assessments conducted by the staff and provide the commander with the necessary feedback to support the decision-making process. Existing doctrine directs the use of combat assessments in support of targeting efforts.

Assessment of network engagement must generate and maintain an understanding of effects on networks through the application of both lethal and nonlethal capabilities. This is accomplished with targeting efforts that are intended to generate desired effects that support the attainment of the commander's objectives. Figure 5-3 illustrates a notional targeting assessment plan in support of network engagement.

Assessing the effects of targeting on a network focuses on understanding the second-order effects that have occurred on the network's structure and function as a result of targeting nodes.

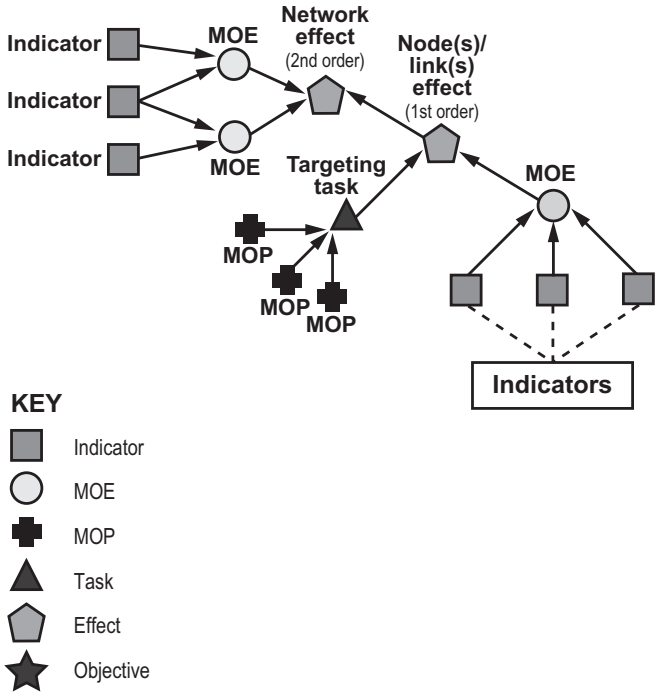


Figure 5-3. Notional Targeting Assessment Plan.

Assessing the first-order effects of the targeting effort is still relevant, since it must be understood if the targeting effort is generating the desired results on a network.

Combat assessments used to support the targeting process have been developed to understand the effects of employing weapons systems on targets. Understanding the effectiveness of engaging networks can only be understood from analyzing the second-order effects on the structure and functions of a network. The staff products developed from the application of network engagement techniques will support the assessment of networks as part of the operations assessment plan. Figure 5-4 depicts considerations for developing targeting assessment criteria in support of network engagement.

Understanding of both the desired end state of the operational environment and of networks of interest directly related to the commander's objectives is a key input for the staff developing an assessment plan. Greater detail on developing and implementing an assessment plan is addressed in chapter 6.

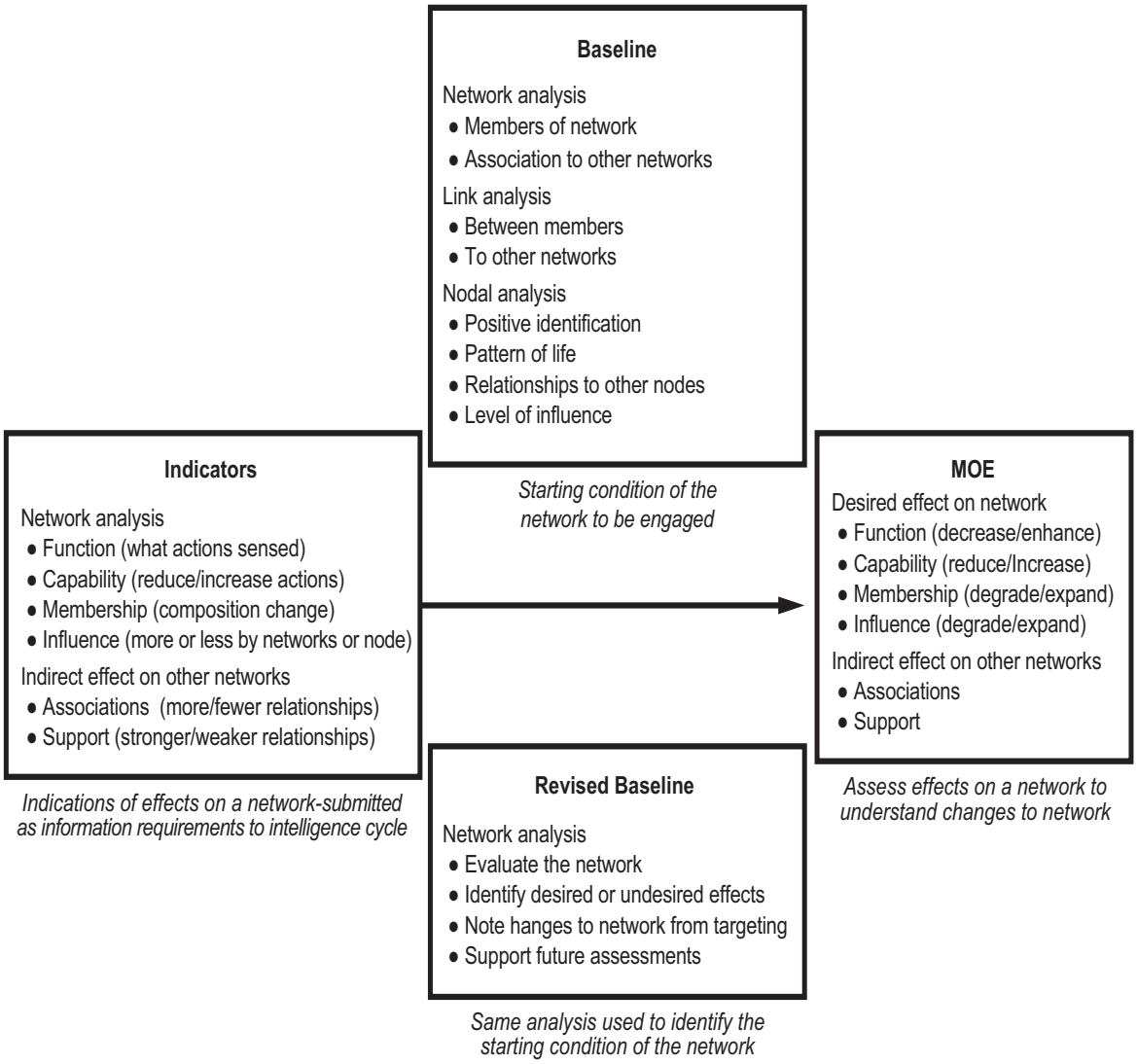


Figure 5-4. Targeting Assessment Criteria Considerations.

This Page Intentionally Left Blank

CHAPTER 6
NETWORK ENGAGEMENT ASSESSMENT

Conducting assessments of operations within a fluid and complex operating environment is both time consuming and challenging for the commander. It is essential that units leverage the analytical capabilities available to assist in this process to understand if operations are generating the desired effects. Assessments of the operational environment must be conducted continuously to avoid missed opportunities or flawed planning for future operations.

The assessment process is a continuous activity that encompasses the three tasks—monitoring, evaluating, and directing—depicted in figure 6-1. This process is intended to be a staff action that allows for evaluation of operations and the subsequent effect of those operations to provide feedback to the commander in the form of recommendations. Network engagement provides the necessary information to support the staff in its implementation of an operations assessment plan.

Effective assessment incorporates both quantitative (observation based) and qualitative (opinion based) indicators. Amassing statistics is easy; however, human judgment is integral to assessment. Using both quantitative and qualitative indicators reduces the likelihood and impact of the skewed perspective that results from an overreliance on either expert opinion or direct observation.

A comprehensive evaluation of the operational environment and identification of the critical variables supports the commander's operations assessment plan. The ability to monitor, evaluate, and recommend actions that will direct conditions in the operational environment is essential for the staff as they work to establish the future conditions required to attain objectives.

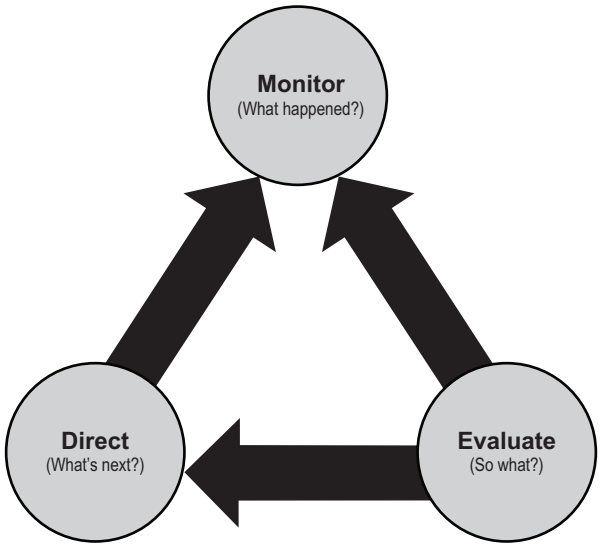


Figure 6-1. Assessment Process.

PLAN

The commander is responsible for ensuring effective assessments by articulating information requirements based on an ability to "see" the fight beyond the range of any visual aids. The commander explicitly describes the end state and its defining conditions for every operation to ensure the cohesion between tactical tasks and the conditions that define the end state. In turn, the staff must have an understanding of the commander's intent and the campaign plan to provide the commander the information needed for decision making focused on achieving the desired end state. The assessment plan is developed to conduct timely evaluations throughout the operation to understand the changes that occur within the operational environment over time. It incorporates several phases or stages, described in the following subparagraphs. Figure 6-2 depicts a notional operations assessment plan.

The assessment plan is developed to understand if desired effects are being generated within the operational environment that meet the commander's intent. Evaluating if these changes are occurring is accomplished with the application of measures of performance (MOPs) and measures of effectiveness (MOEs). Prior to applying these measures, the current conditions of the operational environment must be understood. This initial analysis of the operational environment is done to establish a baseline for the assessment process.

Establish a Baseline

A baseline is a representation of the current conditions as they exist within the operational environment prior to starting operations. Evaluating the operational environment as a part of problem framing provides the necessary information to establish a baseline. Network engagement uses information models to assist the staff in organizing the information about the operational environment and to identify the critical variables that impact the mission. The critical variables are the key conditions within the operational environment that must be shaped to meet the commander's desired end state. As operations continue and assessments are conducted, the baseline for the operational environment is re-established or updated to support future assessments of operations. Establishing the baseline early must be accomplished to have any type of viable assessment plan. Without establishing a baseline, it is impossible for the staff to assess the effects of an operation.

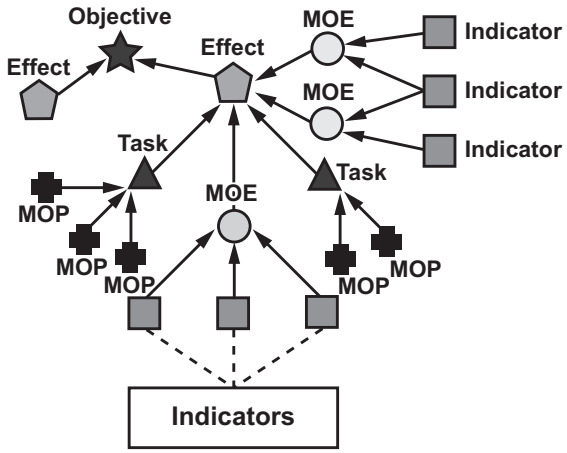


Figure 6-2. Notional Assessment Plan.

Determine Objectives and Effects

Objectives are established by the commander to provide the staff the guidance necessary to meet the desired end state. Attaining these objectives requires establishing conditions within the operational environment and conducting tasks. Assessing if desired effects are occurring requires the assessment of both the tasks being conducted and the effectiveness of these tasks. Regardless of the type of operation being conducted, network engagement supports planning efforts and provides the commander with both situational awareness and the information required to assess unit efforts.

Develop Measures of Performance

Measures of performance are used in all types of combat assessments. They help answer the question: "Are we doing things right?" The MOPs typically require specific, quantitative data or a direct observation of an event to determine accomplishment of tactical tasks, though qualitative attributes can also be applied to task accomplishment. Some examples of MOPs and the type of analysis that would be used to evaluate the measure are provided in table 6-1. Depending on the level of detail needed by the commander, a MOP could be broad in nature or could be focused on specific elements of a task to gauge performance. Quantitative analysis in the form of a true or false value or a numerical value is typically used when applying MOPs, and the baseline for comparison is a standard established by the commander.

Develop Measures of Effectiveness

Measures of effectiveness allow an answer to the question: "Are we doing the right things?" These measures typically are more subjective than MOPs. When developing MOEs as part of the

Table 6-1. Examples of Measures of Performance.

MOP	Type of Analysis/Evaluation
Security patrols are conducted	Quantitative–yes/no
Number of patrols conducted	Quantitative–numerical
Total amount of area patrolled	Quantitative–numerical
Key nodes for engagement identified	Quantitative–qualitative
Individuals biometrically enrolled daily or weekly	Quantitative–numerical
Number of individuals biometrically enrolled daily or weekly	Quantitative–numerical
SSE and TSE conducted on sites of interest	Quantitative–yes/no
Material from SSE and TSE submitted for level two exploitation	Quantitative–yes/no
IEDs located are exploited by EOD teams	Quantitative–yes/no
BOLO handbills distributed during operations	Quantitative–yes/no
Key leader engagements conducted with selected nodes	Quantitative–yes/no

Legend
BOLO be on the lookout
SSE sensitive site exploitation
TSE tactical site exploitation

assessment plan, the staff must ensure that each MOE has the following qualities in order to be effective and efficient:

- Relevant to the task, effect, operation, operational environment, and desired end state.
- Measurable in terms of qualitative or quantitative standards.
- Responsive enough to allow a staff to detect changes quickly and to enable timely decisions by the commander.
- Resourced so that the information necessary is available through some type of collection method.

The steps for developing an MOE are—

1. Identify the purpose.
2. Define the MOE.
3. Identify and examine existing measurement indicators (metrics).
4. Generate new metrics, as required.
5. Rate metrics.
6. Determine collection requirements.
7. Select measurement tools.
8. Establish a baseline.
9. Collect and analyze metric data over time.
10. Finalize metric presentation.
11. Initiate process improvements.

The MOEs are developed for any type of assessment plan. They are used to assess effects on targeting and to assess the effects in the operational environment during operations assessments.

Identify Indicators

Indicators help to answer the question, "What is the current status of this MOE or MOP?" Indicators provide evidence that a certain condition exists or certain results have or have not been attained, and they enable decision makers to assess progress towards the achievement of the objective (JP 2-01.3, *Joint Intelligence Preparation of the Operational Environment*). In the assessment process, an indicator is an item of information, either quantitative or qualitative, that provides insight into MOEs or MOPs. Indicators are used to perform MOE analysis and identify changes to the operational environment or a network's structure and function. A single indicator can inform multiple MOEs and/or MOPs. A good indicator should display the following attributes:

- Be accepted as meaningful to support the mission objectives.
- Identify how well those objectives and goals are being met through operational activities.
- Be simple, understandable, logical, and repeatable.
- Show a trend.
- Be unambiguously defined.
- Feature data that is economical to collect (considering all resources committed to its collection and the impact that the lack of those resources committed to collection will have on other operations).

- Be timely.
- Drive appropriate action for progress towards the desired end state.

Indicators identify those activities that can be directly or indirectly seen (observables) or observed through technical measurement (signatures). Observables are detected through the use of the five human senses (i.e., sight, smell, touch, hearing, taste). Mechanical reproductions of those senses, such as cameras or microphones, are often used to collect observables. Signatures require technical measurement to detect or identify. They can be spatial, spectral, temporal, biometric, or activity-based. Since signatures require technical measurement prior to being analyzed, they usually require specific requests for collection and data processing techniques.

When developing the MOEs and indicators as part of an assessment plan, availability of information and type of analysis should be considered. The staff is encouraged to apply a balance of quantitative (measured data) and qualitative (observed data that is unmeasurable) analysis to provide representative feedback to the commander. Table 6-2, on page 6-6, provides an example of an MOE and some indicators that could be identified to support the application of a measure. In this example, the type of analysis for the indicators and source of information has been provided for consideration.

MONITOR

Monitoring involves the continuous observation of conditions relevant to the operating environment. Within the assessment process, monitoring allows the staff to collect information about the current situation that can be compared with the commander's desired end state (see JP 5-0, *Joint Operation Planning*). Due to the complexity of the operational environment and the adaptive interrelated networks present, the amount of information that is available to support monitoring can become overwhelming. Through the application of network engagement as part of problem framing, the staff possesses the capability to monitor the operational environment with a focus on the critical variables that are directly related to the mission and that support the commander's decision-making process. Collection plans are developed for use in monitoring the operational environment as part of the assessment process.

Considerations When Developing a Collection Plan

The collection plan is designed to support any information requirement for the commander or the staff, which includes efforts in planning, targeting, execution of operations, and the assessment process. The information requirements, which may involve any general or specific subject about which there is a need for the collection of information or the production of intelligence to support the assessment plan, will evolve from the indicators identified to support the implementation of the assessment criteria. The intelligence section must be involved throughout the development of the assessment plan in order to help identify the intelligence collection requirements that are needed to support the implementation of the assessment plan.

Table 6-2. Examples of Measures of Effectiveness and Indicators.

MOE	Indicator	Type of Analysis/ Evaluation	Indicator Description	Source of Information
Threat network's ability to conduct attacks against friendly forces is diminished	Number of weapons caches discovered and exploited	Quantitative/ Qualitative	Quantitative—An increase in number of weapons caches located may indicate fewer resources are available to the threat network.	AARs, SIGACTs
			Qualitative—Types and amounts of material located in caches that is exploited to indicate types of attacks that may be affected.	EOD storyboards, level 2 exploitation reports, WTI reports
	Number of attacks (IED/complex/ indirect fire) against Marine Corps patrols	Quantitative/ Qualitative	Quantitative—Total number of attacks against patrols, specifically categorized by type of attack and frequency indicates potential increase or decrease threat network activities associated with a designated area.	AARs, route clearance patrols, EOD teams, SIGACTs, and ORSA reports
			Qualitative—Quantitative data must be correlated with patrol areas, numbers of patrols, and frequencies, along with any types of significant events in the OE (holidays, weather impacts, seasonal considerations, etc.) to understand what affected threat network activities.	Honesty traces, operations reports, CA reports, HUMINT reports, IPB, and staff OE evaluations
	Effectiveness of attacks against Marine patrols	Qualitative	Qualitative—Attack resulted in casualty and/or level of mobility of a patrol is disrupted. Must consider the duration of the attack and type of weapon systems employed.	AARs, SIGACTs, EOD storyboards
	Amount and type of population reports of threat network activities	Quantitative/ Qualitative	Quantitative—If number of reports on threat network activities have increased, it may indicate an increase in support from the population toward friendly networks. A decrease may indicate less support of the population or increase in influence by the threat network.	AARs, HN, CMOC, CA, HUMINT, NGOs, or any other nonorganic units
			Qualitative—Type and method of reporting of information being reported on threat network activities must be correlated to other engagement activities to understand if other efforts by friendly or threat networks are impacting data collected.	AARs, HN, CMOC, CA, HUMINT, NGOs, or any other nonorganic units
	Members of threat network openly carrying weapons	Quantitative	Qualitative—Reports and observations of an increase in threat networks openly carrying weapons may indicate an increase in freedom of maneuver, while decrease indicates that members may realize the risk of these actions	AARs, SIGACTs and ISR reporting from HN, NGOs, nonorganic units, and population

Legend

AAR	after action report	CA	civil affairs
CMOC	civil-military operations center	HN	host nation
HUMINT	human intelligence	ISR	intelligence, surveillance, and reconnaissance
OE	operational environment	SIGACT	significant activity

The collection manager within the intelligence section is charged with ensuring that information requirements are addressed by leveraging available assets. Network engagement enablers are available to support the intelligence section in the development of the collection plan. In addition to the intelligence, surveillance, and reconnaissance platforms that are available, the staff must also consider reports from subordinate units, nonorganic units within the battlespace, and open-source information as part of the collection plan for necessary information to support evaluation of the indicators.

Manage Collected Information

Implementation of the collection plan as part of the intelligence cycle is followed by processing and exploitation, which result in the production of various intelligence reports that address a multitude of information requirements. For a staff to monitor as part of the assessment process, they must be able to access the required information in a timely manner. The vast amount of information that can be collected must be organized in such a manner that all staff sections can access and share this information. Accomplishing this requires an information management plan to be established that clearly defines the flow and storage of information that is used by the staff for planning, targeting, and assessing. A particular challenge that exists with managing information is that different staff sections may be responsible for different pieces of information. Ensuring that synchronization among all sections occurs as part of routine staff processes will help to overcome this challenge.

The intent of the information management plan is to ensure that information is disseminated efficiently from all staff sections involved with some type of reporting to members of the staff that have a need for that information. A best practice that many units have implemented is the use of an assessment working group. The frequency of this working group is dependent upon the needs of the commander, which may be driven by the operational tempo. In some cases, units may include a discussion on assessments as parts of other working groups, which would not require a need for a separate working group for assessments. Ultimately, the commander makes the determination as to the best manner for the staff to support operations.

EVALUATE

The staff analyzes relevant information collected through monitoring to evaluate the operation's progress, including the effects that have occurred within the operational environment and on the networks as a result of engagements and operations. Evaluation is conducted to provide the commander information that will allow a determination of what is working, what is not working, and how to better accomplish the mission. Depending on the information that is collected to support the application of an indicator, evaluations conducted by the staff can be quantitative, qualitative, or a combination of both.

Apply Measures of Performance

Applying MOPs developed to support the assessment process typically involves the use of quantitative analysis. The information required for assessing the performance of tasks can be observed by the commander and/or the staff or from reporting by subordinate units. The MOPs can provide a starting point for further analysis leading to an adjustment of tactics, techniques,

and procedures to improve the unit's ability to conduct similar tasks in the future when included in after action reports. The staff must be cautioned to not make the assumption that a task successfully executed and confirmed by applying MOPs holds direct causation to an effect. Due to the complexity of operational environments, other conditions may exist that influence a desired effect that may not be the direct result of operations conducted.

Apply Measures of Effectiveness

Applying MOEs allows the staff to evaluate the effects of operations by collecting information that would support the indicators developed for each MOE. Gaining an understanding of effects on the operational environment is particularly challenging, since they result from both the commander's operations and actions taken by other networks. Indicators developed that directly relate to potential effects on networks may be required to support MOEs for the operations assessment.

Evaluate Metrics/Assessment Plan

Assessments in general are very resource and time intensive for commanders and their staffs. The level of effort required to fully develop an assessment plan can become overwhelming and the challenges associated with developing metrics that can accurately assess the effects within a complex operational environment are significant. As a commander uses qualitative analysis of the information provided for the assessment process, that commander should also consider at what intervals to evaluate or validate the effectiveness of the assessment plan. In some cases, units may conduct an entire deployment and never consider evaluating the assessment plan due to operational conditions. However, the risks associated with continued use of metrics that do not provide commanders with the best situational awareness and assessment of operations can be monumental. Much like the best practice of conducting an assessment working group, an evaluation of the assessment plan should be scheduled at the commander's discretion.

DIRECT

Monitoring and evaluating are critical activities; however, an assessment is incomplete without recommendations from the staff to the commander that result in the directing of action. Assessment may diagnose problems, but unless it results in recommended adjustments, its use to the commander is limited. A commander uses the assessment information as feedback for the decision cycle. Recommendations may be accepted, accepted with modifications, or rejected outright. The staff may be directed to conduct further analysis on a recommendation as well. The guidance provided can vary and may include an order to conduct specific operations (initiating the planning process), adjustments to the commander's intent, or a refocus of staff efforts. A point that should be considered (but is sometimes overlooked) is the importance of the commander providing feedback to the staff on the assessment process. If the commander has specific questions that the assessment does not answer, that may indicate that some type of adjustment is necessary in the assessment plan.

APPENDIX A
NETWORK ENGAGEMENT ENABLERS AND RESOURCES

CAPABILITIES TO SUPPORT OPERATIONS

Successfully engaging networks to produce desired effects in support of the commander's mission requires a balanced effort from the entire staff. Although the skills required to support these types of efforts are organic to Marine Corps units to some degree, network engagement enablers provide the commander with a greater analytical capability or specific skillset that extends beyond organic assets. Understanding the resources that are available; the capabilities of those resources; how to leverage those resources through some type of reachback method; or how to integrate assigned, attached, or supporting enablers is essential for the commander to maximize these limited resources.

Identify Staff Requirements

Primary staff members are responsible for various aspects of planning, intelligence support to planning and targeting, fires, and overall feedback and assessment of operations. Commanders must analyze their own units to determine if the depth of skills and capabilities are resident within their table of organization and equipment. Upon identifying gaps, commanders must also identify nonorganic resources and capabilities necessary to accomplish the mission. These resources and capabilities may be available through augmentation or reachback support. The following are steps to consider for determining staff requirements:

- Analyze the skills and capabilities resident within staff to support mission requirements.
- Identify resources and capabilities available through augmentation or reachback support.
- Determine which staff section the resource or capability is assigned to for maximum effectiveness.

Once commanders make the determination of how to organize the resources and capabilities to support their mission, they must monitor and evaluate the performance of their staffs. The intent of monitoring and evaluating is to ensure the resources and capabilities are efficiently supporting mission accomplishment. If the determination is made that a resource or capability may provide a greater operational advantage to a different staff section, commanders must consider the possibility of reorganizing their staffs.

Identify Network Engagement Enablers

An enabler is defined as a Service, joint, interagency, or coalition organization or entity that provides a resource or capability not normally resident within military unit structure to support

staff processes. Recent operations have provided commanders access to external capabilities not commonly found in their battlespace, and connectedness globally is allowing for leverage of both reachback opportunities and forward-deployed enablers. Information requirements are answered faster through enabling capabilities, allowing for a more efficient and clear decision-making process to engage networks, both lethally and nonlethally. Figure A-1 outlines enabler support to the intelligence cycle and, subsequently, the additional processes of planning, targeting, and assessment. While not all-encompassing of what is available or required to operate in any given theater, these enablers provide a general knowledge of the array of capabilities to enhance operations across the conflict continuum.

COUNTERINTELLIGENCE AND HUMAN INTELLIGENCE DETACHMENT

A counterintelligence and human intelligence detachment (CHD) is comprised of personnel with the training and legal authorizations to conduct interrogations, source operations, and related activities. This allows them to collect information about the networks within the operational environment. Additionally, these detachments can collect information and conduct operations to detect and counter enemy terrorism, espionage, sabotage, and subversion. These individuals are typically organized into a team of five collectors with a support staff who are usually in direct support to an infantry battalion.

Capabilities

A CHD collects information to help identify all components of the interrelated friendly, neutral, and threat networks in the operational environment. Counterintelligence estimates can assist unit S-2 with providing networks' motivators and COAs in the counterintelligence estimate, since human intelligence has the unique quality to identify and define the existence, type, and strength of links between nodes in all types of networks. Through preparation of counterintelligence

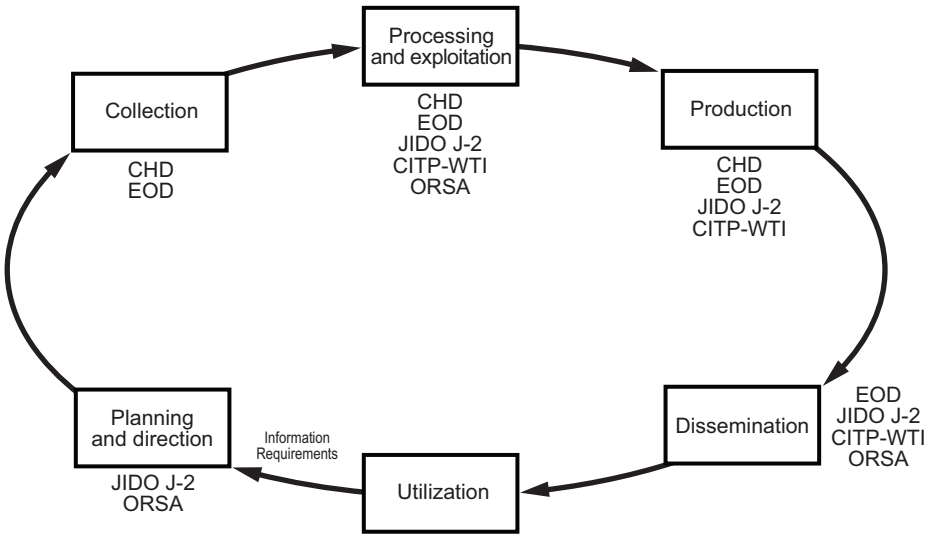


Figure A-1. Intelligence Cycle and Enablers.

estimates, surveys, and plans, it is adept at providing general and detailed information about the patterns of life of various nodes of a network. The addition of this robust and detailed intelligence helps exploit the nodes of a network to identify links to additional nodes and networks. A CHD may map and analyze enemy and neutral networks to assist with planning its own operations. Its knowledge and products can assist the S-2 with mapping all of the interrelated networks in the operational environment. See MCRP 2-10A.2, *Counterintelligence*, for more information about this capability.

Integration Considerations

As a special staff officer to the battalion or unit of assignment, the CHD officer in charge should be involved in all planning processes and should routinely engage with the S-2 and S-3. While the CHD can provide the supported unit with information about the nodes, links, patterns, and characteristics of the network, the S-2 should also consistently provide CHD personnel with the unit's complete and updated mapping of the interrelated networks derived from all-source fusion analysis. With a thorough mapping of the interrelated networks in the operational environment, CHD personnel can maximize their potential to penetrate those networks for further understanding and comprehensive targeting. At all echelons of command, CHD personnel should be involved in the planning, execution, and assessment of unit operations.

EXPLOSIVE ORDNANCE DISPOSAL

The mission of explosive ordnance disposal (EOD) units is to identify, render safe, and dispose of all hazardous explosive ordnance items including conventional, chemical, biological, and nuclear weapons and IEDs. They can be deployed in theater, and they conduct their missions as an EOD team, as part of a regimental landing team, or as a battalion site exploitation team.

Capabilities

Explosive ordnance disposal units provide the following capabilities:

- Evaluate the battlefield geometry at an IED-related attack or site.
- Locate and identify the functionality of IEDs and the associated components.
- Conduct "render safe" procedures of unexploded ordnance and IEDs.
- Conduct post-blast analysis.
- Conduct level one exploitation of IEDs and caches.
- Prepare explosive items for transport and evacuate them for further analysis.
- Prepare reports with technical and tactical analysis, pictures, sketches, and samples as part of level one exploitation.

Integration Considerations

Operationally, EOD teams must be integrated at the lowest possible level. Due to their size, one of the biggest constraints is their inability to secure themselves in order to move and conduct operations. This perpetual challenge results in the integration of EOD teams in support of other

units, and it has provided the flexibility to get that support where it is needed in a timely manner. This enables the supported commander to work with teams to establish priorities of work, thereby allowing synchronization of efforts between EOD assets and combat operations.

JOINT IMPROVISED-THREAT DEFEAT ORGANIZATION

The Joint Improvised-Threat Defeat Organization (JIDO) J-2 leverages existing information and provides strategic capabilities in support of offensive operations against threats. Through the JIDO J-2 fused intelligence products, intelligence formerly classified above SECRET is now available at the SECRET level, making it accessible to warfighters at the tactical level. The JIDO J-2 architecture of partnerships includes more than 30 intelligence agencies and other Federal agencies that support this effort.

Capabilities

The JIDO J-2 offers the following capabilities:

- Provide expertise to persistent surveillance and analysis.
- Provide ground moving target indicator data analysis and research support.
- Provide research and analysis activities worldwide to address intelligence products in support of combat operations.
- Integrate ground moving target indicator data to provide a product depicting a more complete picture of specific analytical issues.
- Disseminate both preliminary and finished ground moving target indicators and geospatial intelligence products.
- Provide access to over 150 different intelligence databases to support requests for information from the field.
- Maintain agreements with interagency partners that are also leveraged to support deployed units and units preparing to deploy.

Integration Considerations

The JIDO J-2 analysts are embedded down to the battalion level and have the ability to reachback to the continental United States for additional support. Forward-deployed analysts possess the ability to fulfill most of the commander's information requirements. Depending on how many JIDO J-2 analysts are assigned, the JIDO J-2 all-source analyst would typically support intelligence efforts of the S-2. The JIDO J-2 operations integrator typically splits time between the S-2 and S-3, depending on the needs of the unit.

COUNTER-IMPROVISED EXPLOSIVE DEVICE TARGETING PROGRAM-WEAPONS TECHNICAL INTELLIGENCE ANALYST

The counter-improvised explosive device targeting program (CITP)-weapons technical intelligence (WTI) analyst serves as an integral component of the CITP. In coordination with the National Ground Intelligence Center, US and coalition intelligence, and other technical and forensic organizations, the CITP-WTI analyst conducts device-specific research, forensic analysis, profiling, and comparative threat analysis to establish attribution between people, devices, and events in support of counter-IED operations against insurgent and related threat networks.

Capabilities

The CITP-WTI analyst offers the following capabilities:

- Match individuals to specific IED incidents by matching and assessing latent prints, fibers, and other data.
- Provide enhanced network analysis capabilities that leverage identity operations to gain a greater understanding of the network being analyzed.
- Integrate within level two exploitation laboratories with a focus on analysis of exploited material.
- Reachback to National Ground Intelligence Center for advanced analytical support as necessary.

Integration Considerations

The CITP-WTI analyst possesses the same capabilities as a CITP analyst, but this position has a unique focus on IEDs and weapons-based intelligence. Due to this unique skillset, CITP-WTI analysts are integrated within the level two exploitation laboratories when deployed, where they have direct access to the information gained from exploited material on a daily basis. Their analysis is focused on identifying individuals associated with this material through biometric matching as a part of identity operations.

OPERATIONS RESEARCH AND SYSTEMS ANALYSIS

The study of military problems undertaken to provide commanders and staff agencies with enhanced decision making to improve military operations is called operations research and systems analysis (ORSA). The scientific techniques used in ORSA are applied to the entire spectrum of military activities and frequently are used to help identify optimal uses of many different scarce resources.

Capabilities

The capabilities provided by ORSA include the following:

- Formulate problems and design research and study methods.
- Conduct and supervise qualitative and quantitative analyses of complex military and related problems.
- Summarize and synthesize complex analyses into simplified terms and present results to decision makers.
- Plan, evaluate, coordinate, and integrate ORSA actions with other staff elements and functions.

Integration Considerations

An analyst is deployed forward at the regimental landing team level and higher. To support network engagement methods, the analyst conducts ORSA in support of the assessment process. For this reason, an analyst with ORSA capabilities is typically integrated into the plans section or intelligence section at the regimental landing team, depending on the requirements of the unit.

APPENDIX B
NETWORK ENGAGEMENT AND IDENTITY OPERATIONS

The concept of identity operations, depicted in figure B-1, has evolved in recognition of the overlapping and mutually supporting capabilities of biometrics, forensics, and identity management (Marine Corps Order 5530.17*, Marine Corps Identity Operations [IdOps]*). The Marine Corps' identity operations capabilities must continue to evolve as the strategies for identity management, identity intelligence, and site exploitation mature. The identity operations strategy provides the framework for synchronizing and integrating all Marine Corps identity operations programs, initiatives, policies, training, and resourcing activities into a single, deliberate effort.

Implementation of identity operations will enable commanders to successfully integrate intelligence, biometrics, forensics, and identity management capabilities into the current and emerging operational capabilities required to fulfill challenging and constantly evolving missions. The capabilities provided with the application of identity operations are fundamental to the commander's ability to confirm the identification of individuals as a part of network analysis and support to targeting efforts.

IDENTITY INTELLIGENCE

Identity intelligence is an extension of all-source intelligence analysis and incorporates biometrics-enabled intelligence (BEI) and forensic-enabled intelligence (FEI) to enable the precise identification of individuals and their association to specific activities, items, or events.

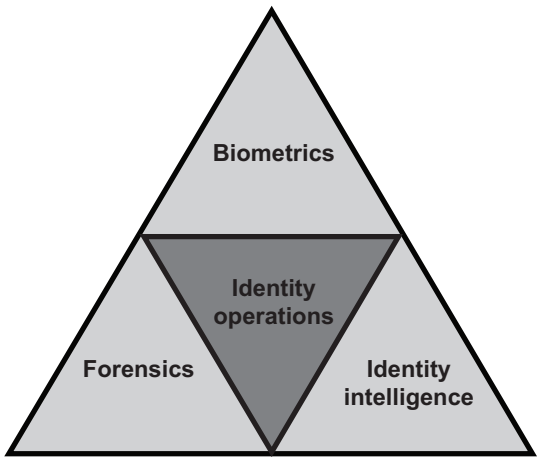


Figure B-1. Identity Operations Activities.

BIOMETRICS

Biometrics can be used to provide commanders a means to confirm the identity of individuals in the area of operations and is used to provide BEI. Biometrics-enabled intelligence is derived from the collection, processing, and exploitation of biometric signatures; the contextual data associated with those signatures; and other available information that answers commanders' or other decision makers' information needs concerning persons, networks, or populations of interest. For more information about BEI, see JP 2-01, *Joint and National Intelligence Support to Military Operations*.

Biometrics is a necessary component of identity operations, but this information is only useful when fused with information from forensic exploitation. During network analysis, network engagement enablers attempt to understand the structure and function of networks in order to support targeting. The ability to confirm or deny the identity of an individual can be accomplished through the use of biometrics. For this to occur, a database of biometric information must be developed, maintained, and made available to commanders for use during operations.

Biometrics in Operations

Various equipment sets are available to facilitate the collection of biometric information from individuals within the battlespace. Regardless of the type of equipment that has been issued to units, collection of biometric information should be a planned part of operations. Commanders may consider the following when planning for biometric collections as part of operations:

- Time required to biometrically enroll an individual.
- Number of individuals that would be available to enroll.
- Type of operation being conducted.
- Requirements for collection from higher headquarters.
- Named areas of interest for collection within the battlespace.
- Time for manifestation of results from collection efforts.

A great deal of effort is required to plan and implement a biometric collection plan. Although many Marines will diligently execute operations to biometrically enroll individuals as part of their operations, the expectation at times is that biometric collection efforts will produce immediate results. Unfortunately, this is not always the case, since the requirement to successfully identify an unknown individual relies on the use of both BEI and FEI. Biometrics-enabled intelligence or FEI individually will not produce the actionable intelligence necessary to support targeting. They both must be used together to produce the desired intelligence. In many cases, confirmation of identify of an individual may not occur until after a unit has departed the theater of operations.

Collection Considerations

Biometric enrollment efforts are the key to success in identification of individuals involved in threat network activities. Without a database of biometric information, network engagement enablers and other intelligence analysts would not have the necessary information available to make positive matches of biometric information exploited by the level two exploitation

laboratory. Depending on the location and type of operation being conducted, limitations may exist that preclude Marines from collecting biometric information from individuals within the battlespace. Consultation with the judge advocate general and guidance from higher headquarters should be sought to provide the best guidance to Marines on the expectations and limitations of their collection efforts. Additionally, commanders should also consider if there are any specific issues that should be considered in regards to societal or cultural norms present within networks or the operational environment. Identifying potential friction points early may allow for planning to overcome these challenges and facilitate collection efforts.

FORENSICS

Forensics is the application of multidisciplinary scientific processes to produce information and/or intelligence connected to an individual, activity, item, or event. Forensic examination leads to actionable information that aid the commander's decision making. (See JP 3-25 for additional information.) Forensics exploitation is conducted using the six forensic functions:

- Recognize—locating and distinguishing materials having potential forensic value. It involves using special methods and advanced training to detect items of value.
- Preserve—protecting materials and data from the moment they are recognized as having potential forensic value. Material is preserved by taking available, reasonable measures (e.g., marking, packaging, tracking) to prevent contamination, loss, or alteration of the material's forensic value.
- Collect—recovering and accounting for material removed from a site. The site is documented and contextual information is recorded within the parameters allowed by the situation, which often includes limited processing of specific items or areas in an effort to detect additional forensically-relevant information. Presumptive testing of materials is also involved.
- Analyze—conducting scientific processes to produce facts. Forensic analysis occurs when materials and contextual information are recognized at the site by a forensic exploitation team, resulting in an in-depth examination at a mobile or traditional (institutional) laboratory. Presumptive testing of materials is often involved. A variety of factors, such as expected use of results, time priorities, and available laboratory resources, dictates the type of analysis performed by a forensic exploitation team.
- Store—maintaining materials and associated information until forensic material disposition is fully adjudicated or resolved. Policies and procedures dictate proper disposition. Balancing information assurance with necessary retrieval capabilities is crucial when storing material and information.
- Share—cataloging and sharing results of forensic analysis in accordance with policies and procedures. Interoperability is essential to developing databases and retrieving information. Sharing information with the relevant organizations, to include the submitting unit, is vital.

The information from applying these functions is used to provide commanders with FEI. Forensic-enabled intelligence is derived from the collection, scientific analysis, and exploitation of materials, weapons, equipment, output signals, and debris that link persons, places, and events

to produce tactical intelligence. Forensic-enabled intelligence includes, but is not limited to, the following scientific areas: deoxyribonucleic acid (DNA); chemical, biological, radiological, nuclear, and explosive analysis; chemistry; metallurgy; firearms and tool marks; fingerprint analysis (record and latent prints); facial and voice recognition; image analysis; video forensics; captured documents; and trace material analysis (JP 2-01).

Expeditionary forensics is provided by the Department of Defense Forensic Science Center of Excellence, combined explosives exploitation cell, and the Terrorist Explosive Device Analytical Center (TEDAC).

Department of Defense Forensic Science Center of Excellence

Under the Army Expeditionary Forensics Division, the Department of Defense Forensic Science Center of Excellence has developed three deployable laboratories and a reachback operations center located at Ft. Gillem, Georgia, to provide full-spectrum forensic operational support to combatant command and joint operations anywhere in the world. The Department of Defense Forensic Science Center of Excellence's expeditionary laboratory provides forensic exploitation only and does not have the ability to perform triage or technical exploitation of explosive components. Without combined explosives exploitation cell augmentation, the Department of Defense Forensic Science Center of Excellence cannot perform forensic exploitation on any item that may contain an explosive hazard. The three laboratories rotate on a deployed, recovering, and ready-to-deploy operational cycle. Each laboratory is staffed with up to 40 Department of the Army civilians of various forensic specialties. The laboratories are modular and scalable, capable of deploying as a single, full-service, continuously open laboratory; as 3 laboratories that operate 12 hours a day, 7 days per week; or as 4 "mini" laboratories with limited functional capabilities. Commanders requesting this capability should consider the logistic requirements necessary to support establishing this type of operation.

Combined Explosives Exploitation Cell

The combined explosives exploitation cell's expeditionary laboratory is a joint Service asset that is managed and maintained by the Naval Explosive Ordnance Disposal Technical Division at Stump Neck Annex, Naval Surface Warfare Center, Indian Head, Maryland. The combined explosives exploitation cell's expeditionary laboratory provides triage for items potentially containing an explosive hazard and provides technical exploitation of devices only. It does not have the capability to perform forensic exploitation.

Triage ensures that any device or component to be forensically or technically exploited is safe to handle. The technicians ensure that all items are properly logged and that items containing forensic evidence are properly labeled, stored, and protected until those items are exploited. Once the items are triaged (with the exception of homemade explosives), an evidence team determines what stations the device or component will go to for exploitation (i.e., DNA, chemical, latent prints, media).

Exploited devices and components contribute to identifying a threat network's tactics, techniques, and procedures; intent; capabilities; area of operations; and logistic support chain, which helps develop a complete picture of the threat network. Network engagement focuses on gaining an understanding of networks and the FEI produced from the exploitation process is necessary to support the identification a network's structure and function. Although FEI can enhance the

network engagement enabler's ability to analyze a network, it is used with other intelligence in a layered effort to gain the best understanding of the network.

Terrorist Explosive Device Analytical Center

The TEDAC's mission is to coordinate and manage the unified effort of law enforcement, intelligence, and military assets to forensically and technically exploit IEDs. The TEDAC focuses on areas of interest to the USG worldwide in an effort to provide actionable intelligence to the offensive missions against terrorism and to the force protection mission. The TEDAC informs its partners, who disrupt those individuals and networks responsible for the design, development, purchase, assembly, and deployment of IEDs by providing scientific and technical exploitation, actionable intelligence, timely response, and forecasts of IED-related threats worldwide.

The Exploitation Process

Much of the focus on exploitation during the past decade has focused on the IED, due to the nature of the threats presented in Iraq and Afghanistan. Any site of interest may be exploited and can provide a plethora of information. The analysis of this information will provide units with key intelligence to support their targeting efforts. As preparations continue for future operations, the exploitation process (see fig. B-2) will be a necessary function for the Marine Corps, regardless of the type of operation being conducted.

Sites of Interest

The exploitation process begins when the unit or the commander identifies a site of interest. Although incidents that are directly related to IEDs have been a focus in the past, due to the lethality of these devices and the wealth of information that can be gained through their exploitation, commanders are encouraged to fully leverage the exploitation process for any site deemed of interest. Sites of interest to consider within operations could include drug laboratories, safe houses, material caches, or detained personnel and their equipment.

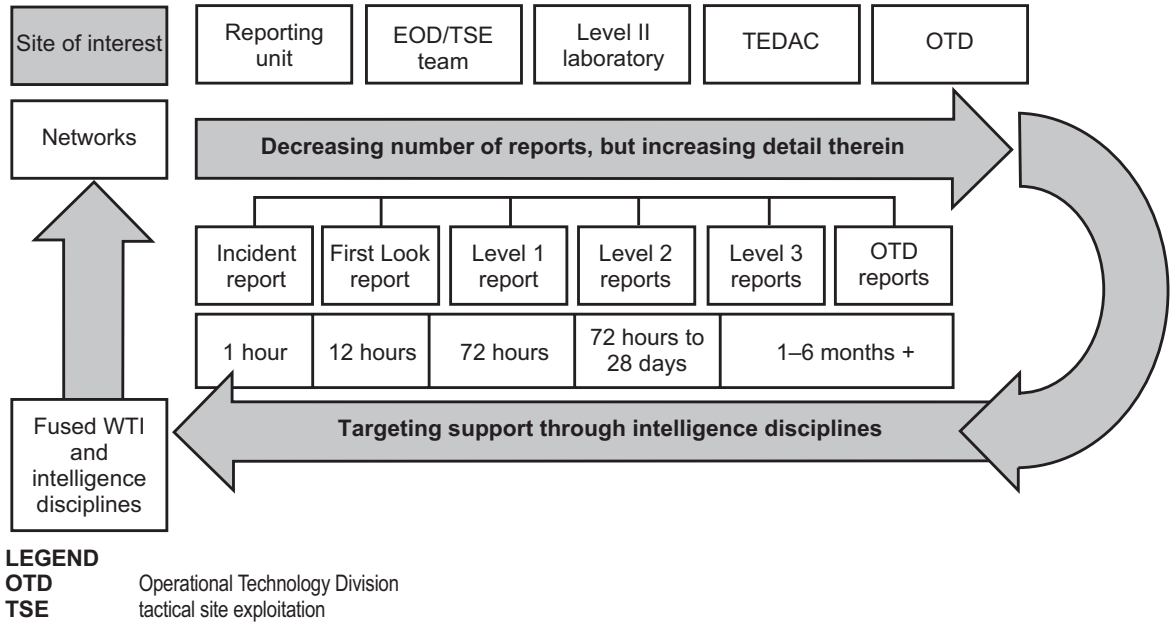


Figure B-2. Exploitation Process.

Level One Exploitation

For any explosive hazard related event, level one exploitation should be conducted by an EOD team. Other sites of interest can have level one exploitation conducted by a tactical site exploitation team that is comprised of personnel within the unit that have received additional training as part of their predeployment training plan.

Level Two Exploitation

Level two exploitation leverages weapons technical intelligence to gain an understanding of specifics associated with any type of weapon recovered, to include IEDs and their components. Weapons technical intelligence evolved from traditional technical intelligence and leverages an enterprise architecture that spans tactical collection through strategic forensic/technical processing and exploitation to focus on IEDs, associated components, improvised weapons, and other weapons systems. Weapons technical intelligence utilizes the processes and capabilities of BEI and FEI to support targeting, force protection, component material sourcing, and legal prosecution of detainees.

Identity intelligence efforts are conducted in conjunction with level two exploitation, since it is at level two where fingerprints and DNA are extracted from evidence collected by units. These efforts may be supported by a number of different network engagement enablers, depending on the maturity of the theater and the level of assets that are deployed. The efforts of units collecting biometric information and evidence from sites of interest are realized through the application of identity intelligence once forensic exploitation of evidence is completed. The intelligence produced from identity intelligence provides identities that can be associated with specific networks, actions, items, or events, which can then be used to support targeting efforts.

Level Three Exploitation

This is accomplished at the TEDAC after the level two exploitation laboratory has evacuated the material from the theater of operation back to the continental United States. This routinely occurred during operations in Iraq and Afghanistan, and it will be available for support in the future.

IDENTITY OPERATIONS SUPPORT TO TARGETING

Identity intelligence is accomplished through the efforts of numerous organizations at various levels and, as an extension of all-source intelligence, identity operations efforts follow and support the intelligence cycle. Figure B-3, on page B-7, depicts the types of identity operations activities and where they nest within the intelligence cycle.

Collection

Collection includes those activities related to the acquisition of data required to satisfy the requirements specified in the collection plan. Collection operations management involves the direction, scheduling, and control of collection assets and resources in order to answer information requests. A collection asset or resource is a collection system, platform, or capability. A collection

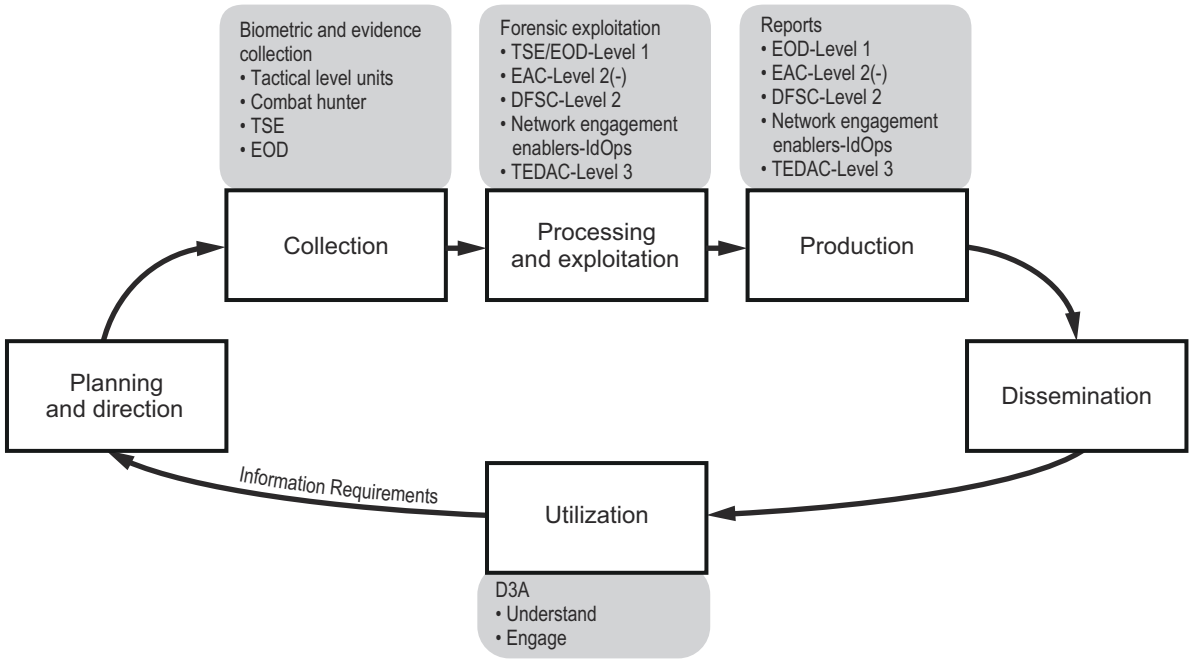


Figure B-3. Intelligence Cycle and Identity Operations.

asset is organic to the Marine air-ground task force, and a collection resource is not. Collection resources must be requested through the appropriate chain of command.

Tactical units conduct collection of biometric information using sets of issued equipment. This may include the BAT [Biometric Automated Toolset], HIIDE [Handheld Interagency Identity Detection Equipment], or SEEKII [Secure Electronic Enrollment Kit II] systems. Training on the implementation of this equipment is available from field service representatives. The field service representative should be available for training prior to deployment and may be available during deployment, depending on the type of operation. Training on these systems should include basic maintenance, troubleshooting, and operation of the system, to include procedures for uploading collected information.

Collection of evidence from sites of interest is conducted by collection teams (e.g., combat hunters, tactical site exploitation teams, EOD teams). Combat hunters and EOD teams are specifically trained to handle and collect evidence from sites to be exploited, with EOD teams being the only ones qualified to handle sites with explosive hazards. Once evidence is collected by the unit, proper handling and documented chain of custody must be established to ensure that evidence can be used for judicial proceedings. Improper collection and handling of evidence may result in contamination, which could hinder the ability for level two exploitation and identity intelligence efforts.

Processing, Exploitation, and Production

During processing and exploitation, raw collected data is converted into forms that can be readily used by commanders, intelligence analysts, and other consumers. This raw data is correlated and organized into a format suitable for the subsequent analysis and production phase.

Level One. Upon successful collection of evidence, the collection teams ensure that the evidence is properly recorded and packaged in preparation for evacuation to the level two laboratory. Reports produced by these teams may include—

- *EOD storyboards (e.g., IED, post-blast, cache)*. These reports include a detailed description of the items encountered on an incident and includes the EOD team leader's assessment of the situation and actions taken.
- *Site exploitation reports*. These reports may be included in the after action report or patrol debrief. Depending on the amount of evidence collected and level of detail necessary, a separate report may be produced as required in accordance with unit standing operating procedures.
- *Chain of custody forms*. DA Form 4137, *Evidence/Property Custody Document*, is the DOD form used to record chain of custody of evidence.

Level Two. Upon arrival of evidence at the laboratory, the evidence proceeds through triage to ensure that there are no hazards that may injure the technicians conducting exploitation. The evidence is then recorded using photographs or video prior to being exploited to latent prints and DNA. Additional exploitation of the evidence is conducted using WTI to identify specifics on devices or weapons, which may include type, function, composition, technical characterization, and electronic engineering. Upon successful completion of exploitation, network engagement enablers can then use the FEI with BEI to produce identity intelligence. The level of exploitation capability available will depend on the type of resources available and the maturity of the theater. Reports that can be expected from level two exploitation may include—

- *Latent print analysis reports*. These include details on number and type of useable fingerprints that were collected from the evidence.
- *Explosive analysis reports*. These provide details on the type of explosives that were used as part of an IED.
- *DNA analysis reports*. These include the details on any DNA collected from evidence.
- *Spectrum analysis reports*. These include analysis of the electronic signatures associated with evidence being exploited.
- *Biometric match reports*. These provide the details on fused BEI and FEI.
- *BOLO [Be on the lookout] reports*. These are produced as a result of the biometric match report and are provided to units to support identifying and locating an individual.
- *Flash reports*. These contain essential technical information related to emerging or evolving enemy tactics, techniques, and procedures. The intent is to notify all units of specific issues to ensure Marines can adjust procedures and mitigate potential risks. Generally, the flash report is generated due to the injury or loss of life of a Service member.

The reports generated at level two directly support identity operations to gain positive identification of an unknown individual and to potentially understand the tendencies of individuals associated with actions, items, or events. This information can significantly assist commanders in both gaining an understanding of a network and ultimately engaging the network through targeting.

Level Three. The TEDAC conducts level three exploitation in the continental United States in support of any theater of operation. The lead time required for level three exploitation may result in reports being produced after the unit collecting the evidence initially has redeployed or deployed to a new theater. Reports at this level are available to commanders through reachback procedures with the TEDAC.

This Page Intentionally Left Blank

APPENDIX C
CRITICAL VARIABLES EXAMPLE AND ANALYSIS

CRITICAL VARIABLES EXAMPLE

The following example shows how critical variables in a complex operational environment could be identified and used to engage networks.

Critical Variables Example

A force has deployed in support of a humanitarian relief operation in a country due to a prolonged drought. Additionally, the government has been challenged by gangs associated with the tribal structure that exists within the country. The gangs in the area have been responsible for numerous attacks on host nation forces and have intimidated the population through violence due to the lack of security being provided in the area. The gangs in the area receive the vast majority of their financing through the drug trade, which is supported through the production of illicit crops by local farmers. Due to the high unemployment rate, many farmers see the growth of these crops as the only means to support their families. However, the drug trade and actions associated with it severely undermine the ability for the host nation to govern effectively. Nongovernmental organizations have been operating in the country prior to the force's arrival providing basic humanitarian relief, but these efforts have been hampered by the conflicts between gangs and the host nation government. Due to the literacy rate of 33 percent amongst the population, the primary means for passing information is through village elders. A private company is also present within the country and is responsible for operating the main port, which is the primary means for the movement of goods within the country. Historically, this company has had a history of violent strikes that have occurred over the working conditions and wages being paid to its workers, but it is still a key source of employment in the port city. Forces being deployed will be responsible for working with the host nation forces to re-establish security in key areas in order to assist the NGOs in resuming their humanitarian relief operations and preparing for a transition to a follow-on force at a later date.

Table C-1, on page C-2, depicts the initial evaluation of the operational environment that has resulted in a list of mission variables. This was accomplished with the application of the PMESII/ASCOPE crosswalk tool to support the evaluation and organize the variables.

Figure C-1, on page C-2, is a commander's mission statement and tasks for the operation. This information is used to support the analysis of the mission variables in order to identify the critical variables.

Table C-1. Mission Variables: Example Evaluation.

	P Political	M Military	E Economic	S Social	I Information	I Infrastructure
A **Areas**	Port city Farming area Port	Port security	Port city Farming area Port			Port city Port
S **Structures**	Port city Port	Port	Port			Port
C **Capabilities**	Drug trade Village elders	HN security	Drug trade	Village elders	Literacy rate 33%	Port city Port
O **Organizations**	US forces NGOs HN forces Private companies Gangs	US forces HN forces Private companies	NGOs Private companies Gangs	Gangs		
P **People**	HN leaders Village elders Gang leaders Company owners	Company owners	Company owners	Village elders Gang leaders		
E **Events**	Drought Violent strikes Attack on HN forces	Violent strikes Attack on HN forces	Drought Violent strikes			

Legend
HN host nation

Mission Statement

Establish security in key areas in order to facilitate the NGOs to resume their humanitarian relief efforts and set conditions for transition of the operations to a follow-on force.

Specified Tasks

- Conduct partnered patrols with host nation forces to increase security.
- Set conditions for transition to follow-on forces.

Implied Tasks

- Ensure logistic capability is maintained to support operations.
- Support host nation efforts to re-establish security and improve ability to govern.
- Support counterdrug operations.

Figure C-1. Example Mission Statement and Tasks.

The networks depicted within the operational environment in the critical variables example include the following:

- Friendly networks
  - –US forces
  - –Host nation government
  - –Host nation forces
- Neutral networks
  - –Population
  - –Private company
  - –NGOs
- Threat networks: gangs

The specific composition of these networks and relationships can be identified with analysis techniques that are included in chapter 6.

Table C-2, on page C-4, illustrates the variables, as indicated by the bold text, identified as critical to the desired end state. With further analysis, critical variables are separated from all previously identified variables present in the operational environment as a means to more efficiently and effectively engage networks. This analysis of the mission variables is qualitative in nature and is dependent upon the staff's interpretation of the mission and tasks.

CRITICAL VARIABLES IDENTIFICATION AND DESCRIPTION

The information identified in different sections of the PMESII/ASCOPE crosswalk may be combined in a manner that is better suited for a particular commander. The seven different critical variables identified have been refined and combined into the following:

- Security.
- Port operations.
- Drug trade.

The following subparagraphs include examples of narratives that describe the critical variables.

Security

The host nation forces are incapable of providing security that would allow for NGOs to conduct their required humanitarian relief operations to the population. The primary group responsible for interrupting these operations has been a gang in the area. The current lack of security is further highlighted by the gang's ability to use violence to intimidate the population and also conduct attacks on host nation forces. This has ultimately provided the gang with freedom of maneuver in the area. The current state of this critical variable (security) is providing an accommodating environment for the gang to take action and is not accommodating for the host nation forces, the

Table C-2. Example Critical Variables.

	P Political	M Military	E Economic	S Social	I Information	I Infrastructure
A Areas	Port city Farming area **Port**	Port security	Port city Farming area **Port**			Port city **Port**
S Structures	Port city **Port**	**Port**	**Port**			**Port**
C Capabilities	**Drug trade** Village elders	**HN security**	Drug trade	Village elders	Literacy rate 33%	Port city **Port**
O Organizations	US forces NGOs **HN forces** Private companies Gangs	US forces **HN forces** Private companies	NGOs Private companies **Gangs**	**Gangs**		
P People	**HN leaders** Village elders Gang leaders Company owners	Company owners	Company owners	Village elders, gang leaders		
E Events	Drought Violent strikes Attack on HN forces	Violent strikes Attack on HN forces	Drought Violent strikes			

Legend
HN host nation

population, and NGOs operating in the area. There have been no reports of the gang's interference with operations at the port or with any other private companies in the area, resulting in a determination that this critical variable does not impact these networks at this time. The current state of security negatively impacts the tasks of providing security, establishing conditions for transition to a follow-on force, and providing support to the host nation force's own security efforts.

Port Operations

The capabilities at the port are adequate to support the requirements for both the humanitarian and military operations executed by the private company operating at the port. There have been no reports of gang activity at the port. Previous historical data available indicates that, although this company is the largest employer in the area, the owners have attempted to pay employees the lowest wage possible and provided work conditions that are very dangerous for the employees. Due to these issues, the historical event of previous labor strikes consisting of violent clashes between the private company and its employees is considered as a potential future event that would affect the port operations. The current state of port operations is positive to the population

from an economic and humanitarian aid perspective, to the NGOs because they receive support in their operations, and to the host nation government because of food distribution to the population. This critical variable has a positive impact on both ensuring security in the area and maintaining the logistics of both the humanitarian relief and the US force's military operations. Interruption of this current capability would result in a degradation of all operations in the area, could negatively impact conditions in the operational environment, and may promote expansion of actions by the gangs, resulting in an increase of their influence in the area.

Drug Trade

The drug trade in the area is being supported by gangs and elements of the local population due to financial gain from these efforts. The local farmers recognize the economic benefits of growing illicit crops. The gangs provide their own level of influence through violence in the area to ensure that anyone supporting the drug trade is allowed to continue. The gang's violent actions tie into the critical variable of security, since they are motivated to continue to make money from the drug trade. This has resulted in undermining the host nation's ability to effectively govern and the host nation security forces' ability to provide adequate security. This critical variable negatively impacts the implied task of supporting counterdrug operations as this directly relates to supporting the host nation government and its efforts to provide a secure area for humanitarian relief efforts. The private companies in the area have not been affected by these actions and will disregard anything that does not directly impact their own profitability in the area.

NETWORK RELATIONSHIP MATRIX AND CRITICAL VARIABLES ANALYSIS

Network interactions within the operational environment can be evaluated to provide commanders with information that is useful in the assessment process. Table C-3 illustrates the interaction of the networks identified with the critical variables. Each critical variable has been evaluated from the perspective of each network identified in the example.

Table C-3. Critical Variables/Network Relationship Matrix.

Critical Variables	Evaluation						
	Friendly			Neutral			Threat
	US Force	Host Nation Government	Host Nation Forces	Population	Private Company	NGOs	Gangs
Security	-	-	-	-	0	-	+
Post operations	+	+	+	+	+	+	0
Drug trade	-	-	-	+	0	0	+

Key
- \- Negative relevance to the network
- 0 Zero relevance to the network
- \+ Positive relevance to the network

Security

The security critical variable is analyzed as follows:

- *US forces*. The current security within the operational environment is perceived as negative to the US forces' mission due to the intimidation of the population by the gangs through violence, attacks on host nation forces, undermining of the host nation government, and the negative impact on the NGOs' abilities to fully conduct humanitarian relief operations. Due to this evaluation, the security critical variable is considered negative for US forces at this time.
- *Host nation government*. The gangs' abilities to undermine the government and exert their will upon the population have resulted in a negative evaluation in security as related to the host nation government. Due to this evaluation, the security critical variable is considered negative for host nation government at this time.
- *Host nation forces*. The gangs' abilities to openly and effectively attack host nation forces, which has been difficult for host nation forces to counter with their current capabilities, have resulted in a negative security environment. Due to this evaluation, the security critical variable is considered negative for host nation forces at this time.
- *Population*. Due to the limited capabilities of host nation forces, gangs have been able to exert their will on the population and create a security environment that inhibits the population's ability to establish a normal pattern of life. Due to this evaluation, the security critical variable is considered negative for the population at this time.
- *Private company*. Security at the port is adequate and has not had a negative impact on operations, resulting in the private company maintaining a neutral position on the current security in the area. Due to this evaluation, the security critical variable does not have an impact on the private company at this time.
- *Nongovernmental organizations*. Lack of security in the area has hampered the NGOs' ability to provide humanitarian relief to the population, but due to their associations with the tribes in the area, some limited relief operations have continued. Due to this evaluation, the security critical variable is considered negative for NGOs at this time.
- *Gangs*. The gangs have freedom of maneuver in the area and routinely attack both forces and the population in support of their efforts. Due to this evaluation, the security critical variable is considered positive for gangs at this time.

Port Operations

Operations at the port at this time are adequate to support operations in the area. Ensuring that port operations continue is critical to the US commander's mission and to other networks within the operational environment. Due to this evaluation, port operations have been determined to be positive at this time for US forces, the host nation government, host nation forces, the population, the private company, and NGOs.

Port operations in the area have no impact on gangs, and gangs have not focused any violent efforts in this area of the country. At this time, gangs have a neutral position toward the port and operations around the port. Due to this evaluation, port operations do not have an impact on gangs at this time.

Drug Trade

The drug trade critical variable is analyzed as follows:

- *US forces*. The drug trade directly supports the gangs in the area that are opposed to the host nation government and host nation forces. Supporting the host nation is part of the US forces' mission, so the drug trade is something to consider, but it does not have a direct impact on the US mission and is viewed as slightly negative in its current state. Due to this evaluation, the drug trade critical variable is considered negative for US forces at this time.
- *Host nation government*. The gangs in the area that directly oppose the host nation government receive the majority of their finances from the drug trade, which is open in the area due to a lack of security. Due to this evaluation, the drug trade critical variable is considered negative for the host nation government at this time.
- *Host nation forces*. Similar to the situation with the host nation government, the gangs' financial supplements from the drug trade has provided capabilities to attack host nation forces, and is therefore viewed as a negative in its current state. Due to this evaluation, the drug trade critical variable is considered negative for host nation forces at this time.
- *Population*. Due to their limited ability to provide income for their families and the social relationships between the gangs and large parts of the population, the drug trade is viewed as slightly positive by the population. Eliminating illicit crops would be detrimental to the population's financial well-being. Due to this evaluation, the drug trade critical variable is considered positive for the population at this time.
- *Private company*. There has been little to no impact on the private company in regard to the drug trade in the area, and they have a neutral position on the variable. Due to this evaluation, the drug trade critical variable has no impact on the private company at this time.
- *Nongovernmental organizations*. Humanitarian relief operations occur in highly populated areas, away from any of the illicit crops being grown in the area. Since the NGOs do not operate in areas associated with the drug trade, there is no impact from the drug trade on them or their operations. Due to this evaluation, the drug trade critical variable has no impact on the NGOs at this time.
- *Gangs*. This is the primary financial source for the gangs to support their antigovernment operations and is currently very positive for them. Due to this evaluation, the drug trade critical variable is considered positive for gangs at this time.

This Page Intentionally Left Blank

GLOSSARY

Section I. Acronyms and Abbreviations

ASCOPE ..... areas, structures, capabilities, organizations, people, and events

BEI ..... biometrics-enabled intelligence

CCIR ..... commander's critical information requirement
CHD ..... counterintelligence and human intelligence detachment
CITP ..... counter-improvised explosive device targeting program
COA ..... course of action

D3A ..... decide, detect, deliver, and assess
DNA ..... deoxyribonucleic acid
DOD ..... Department of Defense
DOS ..... Department of State

EOD ..... explosive ordnance disposal

FEI ..... forensic-enabled intelligence

G-2 ..... intelligence staff section

IED ..... improvised explosive device
IPB ..... intelligence preparation of the battlespace

J-2 ..... intelligence directorate of a joint staff
JIDO ..... Joint Improvised-Threat Defeat Organization (DTRA)
JP ..... joint publication

MCDP ..... Marine Corps doctrinal publication
MCPP ..... Marine Corps Planning Process
MCRP ..... Marine Corps reference publication
MCTP ..... Marine Corps tactical publication
MCWP ..... Marine Corps warfighting publication
MOE ..... measure of effectiveness
MOP ..... measure of performance

NGO ..... nongovernmental organization

ORSA ..... operations research and systems analysis

PMESII .....political, military, economic, social, information, and infrastructure

ROE ..... rules of engagement
ROMO ..... range of military operations

S-2 .....intelligence office
S-3 .....operations office
SNA ..... social network analysis

TEDAC ..... Terrorist Explosive Device Analytical Center (FBI)

US ..... United States
USG ..... United States Government

WTI ..... weapons technical intelligence

Section II. Terms and Definitions

assessment—1. A continuous process that measures the overall effectiveness of employing joint force capabilities during military operations. 2. Determination of the progress toward accomplishing a task, creating a condition, or achieving an objective. 3. Analysis of the security, effectiveness, and potential of an existing or planned intelligence activity. 4. Judgment of the motives, qualifications, and characteristics of present or prospective employees or "agents." (DOD Dictionary)

biometrics—The process of recognizing an individual based on measurable anatomical, physiological, and behavioral characteristics. (DOD Dictionary)

biometrics-enabled intelligence—The intelligence derived from the processing of biologic identity data and other all-source for information concerning persons of interest. Also called **BEI**. (DOD Dictionary)

cell—A subordinate organization formed around a specific process, capability, or activity within a designated larger organization of a joint force commander's headquarters. (DOD Dictionary)

contingency—A situation requiring military operations in response to natural disasters, terrorists, subversives, or as otherwise directed by appropriate authority to protect US interests. (DOD Dictionary)

counter-improvised explosive device operations—The organization, integration, and synchronization of capabilities that enable offensive, defensive, stability, and support operations across all phases of operations or campaigns in order to defeat improvised explosive devices as operational and strategic weapons of influence. Also called **C-IED operations**. (DOD Dictionary)

counterinsurgency—Comprehensive civilian and military efforts designed to simultaneously defeat and contain insurgency and address its root causes. Also called **COIN**. (DOD Dictionary)

crisis—An incident or situation involving a threat to the United States, its citizens, military forces, or vital interests that develops rapidly and creates a condition of such diplomatic, economic, or military importance that commitment of military forces and resources is contemplated to achieve national objectives. (DOD Dictionary)

forensic-enabled intelligence—The intelligence resulting from the integration of scientifically examined materials and other information to establish full characterization, attribution, and the linkage of events, locations, items, signatures, nefarious intent, and persons of interest. Also called **FEI**. (DOD Dictionary)

host nation—A nation which receives the forces and/or supplies of allied nations and/or NATO organizations to be located on, to operate in, or to transit through its territory. Also called **HN**. (DOD Dictionary)

identity intelligence—The intelligence resulting from the processing of identity attributes concerning individuals, groups, networks, or populations of interest. Also called **I2**. (DOD Dictionary)

indicator—1. In intelligence usage, an item of information which reflects the intention or capability of an adversary to adopt or reject a course of action. 2. In operations security usage, data derived from friendly detectable actions and open-source information that an adversary can interpret and piece together to reach conclusions or estimates of friendly intentions, capabilities, or activities. (DOD Dictionary)

insurgency—The organized use of subversion and violence to seize, nullify, or challenge political control of a region. Insurgency can also refer to the group itself. (DOD Dictionary)

link—A behavioral, physical, or functional relationship between nodes. See also **node**. (Part 1 of a 3-part definition.) (DOD Dictionary)

measure of effectiveness—A criterion used to assess changes in system behavior, capability, or operational environment that is tied to measuring the attainment of an end state, achievement of an objective, or creation of an effect. Also call **MOE**. (DOD Dictionary)

measure of performance—A criterion used to assess friendly actions that is tied to measuring task accomplishment. Also call **MOP**. (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 and operational area. (DOD Dictionary)

neutral—In combat and combat support operations, an identity applied to a track whose characteristics, behavior, origin, or nationality indicate that it is neither supporting nor opposing friendly forces. (DOD Dictionary)

neutralize—(See the DOD Dictionary for core definition. Marine Corps amplification follows.) To render the enemy or his resources ineffective or unusable. (MCRP 1-10.2)

node—An element of a system that represents a person, place, or physical thing. (Part 3 of a 3-part definition.) (DOD Dictionary)

weapons technical intelligence—A category of intelligence and processes derived from the technical and forensic collection and exploitation of improvised explosive devices, associated components, improvised weapons, and other weapon systems. Also called **WTI**. (DOD Dictionary)

REFERENCES

Joint Publications (JPs)

2-01	Joint and National Intelligence Support to Military Operations
2-01.3	Joint Intelligence Preparation of the Operational Environment
3-25	Countering Threat Networks
5-0	Joint Operation Planning

Marine Corps Doctrinal Publications (MCDPs)

1	Warfighting
1-0	Marine Corps Operations
5	Planning
6	Command and Control

Marine Corps Warfighting Publication (MCWP)

5-10	Marine Corps Planning Process

Marine Corps Tactical Publication (MCTP)

2-10A	MAGTF Intelligence Collection

Marine Corps Reference Publications (MCRPs)

2-10A.2	Counterintelligence
2-10B.1	Intelligence Preparation of the Battlefield/Battlespace

Marine Corps Order (MCO)

5530.17	Marine Corps Identity Operations (IdOps)

Miscellaneous

Zinni, Anthony. “Non-Traditional Military Missions.” *CAPITAL “W” WAR—A Case for Strategic Principles of War*. Perspectives on Warfighting, no.6, Dr. Joe Strange (Quantico, VA: Marine Corps University, 1998).

To Our Readers

Changes: Readers of this publication are encouraged to submit suggestions and changes to Doctrine Control Branch via e-mail: doctrine@usmc.mil.

Suggestions and changes must include the following information:

- Location of change
  - Publication number and title
  - Current page number
  - Paragraph number (if applicable)
  - Line number
  - Figure or table number (if applicable)
- Nature of change
  - Addition/deletion of text
  - Proposed new text

Additional copies: If this publication is not an electronic only distribution, a printed copy may be obtained from Marine Corps Logistics Base, Albany, GA 31704-5001, by following the instructions in MCBul 5600, *Marine Corps Doctrinal Publications Status*. An electronic copy may be obtained from the United States Marine Corps Doctrine web page:
https://www.doctrine.usmc.mil.

Unless otherwise stated, whenever the masculine gender is used, both men and women are included.