ATP 5-0.6

Network Engagement

JUNE 2017

DISTRIBUTION RESTRICTION: Approved for public release. Distribution is unlimited.

Headquarters, Department of the Army

This publication is available at the Army Publishing Directorate site (http://www.apd.army.mil), and the Central Army Registry site (https://atiam.train.army.mil/catalog/dashboard)

*ATP 5-0.6

Army Techniques Publication
No. 5-0.6

Headquarters
Department of the Army
Washington, DC, 19 June 2017

Network Engagement

Contents

Page

PREFACE ..... **iii**

INTRODUCTION ..... **v**

Chapter 1 OVERVIEW **1-1**
Network Engagement 1-1
Network Engagement Activities 1-2
Supporting Human Networks 1-3
Influencing Human Networks 1-4
Neutralizing Human Networks 1-5
Six Elements of Human Network Analysis for Network Engagement 1-5
Understand the Mission 1-6
Understand the Operational Environment 1-6
Understand The Networks 1-7
Organize for Network Engagement 1-7
Engage the Human Networks 1-9
Assess Effects on Networks 1-10

Chapter 2 HUMAN NETWORKS CATEGORIES, FEATURES, AND STRUCTURES **2-1**
Human Networks 2-1
Unknown Human Networks 2-2
Friendly Human Networks 2-2
Neutral Human Networks 2-3
Threat Human Networks 2-3
Features of a Human Network 2-3
Network Composition 2-4
Network Structure 2-5
Adaptive Nature of Networks 2-5

Chapter 3 ANALYTICAL SUPPORT TO NETWORK ENGAGEMENT **3-1**
Understanding Networks 3-1
Methods Used to Analyze Networks 3-2
Meta-Network Analysis 3-10
Refine Critical Factors Analysis 3-15

Chapter 4 NETWORK ENGAGEMENT WITHIN THE OPERATIONS PROCESS **4-1**
Army Design Methodology 4-1
The Military Decisionmaking Process 4-2
Troop Leading Procedures 4-5

Chapter 5 NETWORK ENGAGEMENT WITHIN THE OPERATIONS PROCESS **5-1**
Network Engagement Collaboration 5-1

DISTRIBUTION RESTRICTION: APPROVED FOR PUBLIC RELEASE. DISTRIBUTION IS UNLIMITED.

Information Collection Supporting Network Engagement 5-4
SOURCE NOTES ..... Source Notes-1
GLOSSARY Glossary-1
REFERENCES..... References-1
INDEX Index-1

Figures

Figure 1-1. Illustrated network engagement concept 1-3
Figure 1-2. Notional structure for coordination 1-8
Figure 3-1. Analytic methods to support network engagement 3-2
Figure 3-2. Example of network functions model 3-5
Figure 3-3. Main components of CFA and steps associated with the CFA process 3-7
Figure 3-4. Example of a link diagram 3-8
Figure 3-5. Network Template 3-10
Figure 3-6. Meta-network analysis workflow..... 3-11
Figure 3-7. Agents connected to event 1 3-12
Figure 3-8. New agent to agent connection created..... 3-12
Figure 3-9. Extracting a social network from a meta-network 3-13
Figure 3-10. Social network analysis application process 3-14
Figure 3-11. Critical factors analysis refinement..... 3-16
Figure 4-1. Network engagement within the operations process 4-2
Figure 4-2. Network engagement within MDMP 4-3
Figure 4-3. Network Engagement within TLP 4-5
Figure 5-1. Assessment Methodology for the Effect of Influence 5-3

Preface

ATP 5-0.6 contains techniques brigade combat team (BCT) and above commanders and staffs can use to synchronize and integrate network considerations into their operational processes. It provides the doctrinal framework to plan for engaging with human networks across the range of military operations. It serves as an authoritative reference (fundamental principles and techniques), for personnel developing materiel, force structure, institutional and unit training, and standing operating procedures for operational and tactical organizations.

The intended audience is Army Corps and below commanders, leaders, and unit staffs (officers, noncommissioned officers, and Soldiers). Commanders and staffs of Army headquarters serving as a joint task force or multinational headquarters should also refer to applicable joint or multinational doctrine.

Commanders, staffs, and subordinates ensure that their decisions and actions comply with applicable United States, international, and in some cases host-nation laws and regulations. Commanders at all levels ensure that their Soldiers operate in accordance with the law of war and the rules of engagement. (See FM 27-10.)

ATP 5-0.6 uses joint terms where applicable. Selected joint and Army terms and definitions appear in both the glossary and the text. Terms for which ATP 5-0.6 is the proponent publication (the authority) are italicized in the text and are marked with an asterisk (*) in the glossary. Terms and definitions for which ATP 5-0.6 is the proponent publication are boldfaced in the text. For other definitions shown in the text, the term is italicized and the number of the proponent publication follows the definition.

ATP 5-0.6 applies to the Active Army, Army National Guard/Army National Guard of the United States and United States Army Reserve unless otherwise stated.

The proponent of ATP 5-0.6 is the United States Army Combined Arms Center. The preparing agency is the Combined Arms Doctrine Directorate, United States Army Combined Arms Center. Send comments and recommendations on DA Form 2028 (*Recommended Changes to Publications and Blank Forms*) to Commander, United States Army Combined Arms Center and Fort Leavenworth, ATTN: ATZL-MCD (ATP 5-0.6), 300 McPherson Avenue, Fort Leavenworth, KS 66027-2337; by e-mail to usarmy.leavenworth.mccoe.mbx.cadd-org-mailbox@mail.mil; or submit an electronic DA Form 2028.

This page intentionally left blank.

Introduction

Humans are complex, social creatures. Attempting to analyze them to determine if we should engage them is a combination of art and science and often depends upon the purpose for that engagement and the paradigms from which we perceive them. The Army engages human networks through the range of military operations in order to achieve U.S. objectives.

Network engagement provides staff orientation for unity of effort. ***Unity of effort*** is coordination, and cooperation toward common objectives, even if the participants are not necessarily part of the same command or organization, which is the product of successful unified action. (JP 1) It is a different way of approaching challenges, but it is not separate from the Army operations process. Network engagement supports the overarching framework provided by mission command to guide the tailored application of current doctrinal processes, such as the Army design methodology, the military decisionmaking process (MDMP) and intelligence preparation of the battlefield/battlespace, targeting, or assessment. Network engagement helps to bind the staff together and introduces them to the networks that exist within their area of operation. As described in this publication, network engagement, can and should be applied in any operational environment (OE) and across the spectrum of conflict.

Operations in the future will be more complex. We will have to work together to plan operations that meet the challenges and opportunities we will face. The last decade of war has shown us that our opponents are often difficult to detect and identify, and seek to blend into civilian populations. We have also learned that long-term solutions for peace and stability in contested regions often come from key allies originating from this same population.

Network engagement is supported by the entire staff. The assistant chief of staff, operations or the battalion or brigade operations staff officer leads the process, collecting, consolidating, and correlating input from all the sections. The intelligence staff section and other staff sections with unique capabilities to analyze the human domain (such as the information operations section, military information support operations staff section, Public Affairs, and Civil Military Operations section) are primary contributors to the process.

The foundational elements of network engagement have been part of the U.S. Army's operations for decades. Once faced with an adversary whose primary weapon was the improvised explosive device, these procedures were refined and codified. The Army, and Joint forces, now recognize that a singular focus on neutralizing threat networks ultimately fails because threat networks adapt, evolve, and may continue to be tolerated or supported by the local populace.

Network engagement is an evolution of attack the network. While attack the network focused on neutralizing the threat network, this focus often led commanders to overlook friendly and neutral networks. Past techniques to grapple with the challenges of some of the different components of network engagement have included forming ad hoc fusion centers, employing the civil military operations center (CMOC), establishing an information operations working group, and enforcing the use of a District Stability Framework (DSF).

Network engagement provides the doctrinal guidance to conduct network engagement activities integrated into the Operations Process. These activities change the commander’s focus from attacking threat networks to identifying, defining, and effectively interacting with friendly and neutral networks, while simultaneously engaging threat networks. There are significant overlaps between network engagement and information operations. Both seek to affect the behavior and will of relevant actors (nodes) and audiences (networks) in the human domain. Network engagement and information operations are tightly connected, mutually supporting, and mutually reinforcing.

All echelons from the BCT up to the Army Service component command level can use the information and techniques within this publication as appropriate. The more widespread these techniques are understood and applied, the more effective network engagement will be executed across echelons. However, network engagement is neither analyzed, planned, nor executed in isolation at any echelon. Effective network

engagement is a shared and collaborative effort across all unified action partners, the entire intelligence enterprise, other communities (for example, civil affairs and information operations), and all echelons down to the BCT. ***Information operations*** is the integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own (JP 3-13). Network engagement requires the detailed integration and synchronization of all warfighting functions and many unique capabilities.

As a part of network engagement, it is important to understand small unit information collection doctrine within ATP 3-55.4.

The analytical requirements to support network engagement are significant. This associated analytical support is both advanced and time-intensive. It requires a certain level of expertise to effectively analyze information from sensitive, technical, and unique sources of information. BCT inclusion of network engagement considerations and execution of specific network engagement tasks is critical. However, BCT analytical capabilities are limited and the BCT is dependent on the other echelons to provide detailed network engagement analytical products. This should be thought of as a top-down push of analytical support and products.

It is important to understand that the intelligence contributions to network engagement are compliant with the rules for all intelligence activities to include intelligence oversight rules involving collection on U.S. persons. Intelligence activities are enabled by and subject to laws, regulations, and policies to ensure proper conduct of intelligence operations. While there are too many to list, legal authorities include the United States Code, executive orders, National Security Council and DOD directives, Army regulations, U.S. SIGINT directives, status-of-forces agreements, rules of engagement, and other relevant international laws. Commanders will request assistance from their servicing judge advocate to interpret or deconflict these legal authorities.

Chapter 1 provides commanders and staffs an overview of the six elements of human network analysis (understand the mission, understand the operational environment, understand the networks, organize for network engagement, engage the networks, assess effects on networks) and the three activities (support, influence, and neutralize) of network engagement.

Chapter 2 introduces the four categories of networks (unknown, friendly, neutral, and threat), human network elements, and network composition and structure.

Chapter 3 introduces the analytical techniques that support network engagement.

Chapter 4 integrates the six elements of network engagement and the three activities into the operations process.

Chapter 5 discusses network engagement activities at theater level and below.

Chapter 1
Overview

NETWORK ENGAGEMENT

1-1. Contingency and operational planning demands that Army units apply network engagement activities throughout the operations process. Additionally, at the tactical level, commanders and staffs have a responsibility to ensure that lower echelon units receive tailored network engagement support through specific analysis, assessments, products, and tasks. Targeting applies to network engagement at all levels and is incorporated into home station training and supported by robust data that supports network analysis and informs the operational plans and tasks that a commander approves. ***Targeting*** is the process of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities (JP 3-0). Targeting at corps and division levels requires the synchronization of unified action partner activities. The focus of targeting is to shape targets to create a range of options for the friendly force, including the lethal effects of deny, destroy, and neutralize, and the non-lethal effects of co-opt, inform, organize, and influence.

1-2. A network is an interconnected or interrelated chain, group, or system. Network engagement uses six elements of human analysis to determine the appropriate actions to support the network engagement activities to support and influence friendly and neutral human networks and to influence and neutralize threat human networks. Human network analysis analyzes groups of humans and depicts them from a networked perspective. A human network is a depiction of the relationships of a broad group that enables understanding of that group. Sub-groups and individuals are nodes in these human networks and can also be depicted as human sub-networks by depicting their relationships. This publication is specific in its use of human network, in instances where the word network is used alone, it should be presumed to refer to a human network.

1-3. Other types of networks such as communications, logistics, financial, commercial, telephone, radio, and computer networks will have specific modifiers in front of them to avoid confusion. Commanders and staffs use the knowledge and perspective gained from human network analysis to engage human networks into three primary activities. These activities support the commander's operational approach and may help determine the appropriate approach to take in order to facilitate achievement of U.S. objectives.

1-4. Commanders and staffs make decisions on which human networks to engage and how to engage them based on a comprehensive understanding of an operational environment (OE), the results of human network analysis, and an understanding of the second and third order potential effects (intended, unintended, primary, secondary, and tertiary) their actions may have upon each human network present within an OE. An ***operational environment*** is a composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander (JP 3-0). Analysis of subgroups and individuals can be done in the same manner using these nodes of the larger human network picture as a departure point for further analysis.

1-5. ***Network engagement*** is the interactions with friendly, neutral, and threat networks, conducted continuously and simultaneously at the tactical, operational, and strategic levels, to help achieve the commander's objectives within an operational area (JP 3-25). Network engagement utilizes the three activities of supporting, influencing, and neutralizing to achieve the commander's desired end state. Commanders and staffs use network engagement activities to support and influence friendly and neutral human networks and to influence and neutralize threat human networks. The three activities may shift in priority depending on the phase of the operation as determined by the commander and the required end state. Typically, these activities align to human networks in the following manners; we seek to support friendly or neutral networks; we seek to influence friendly, neutral, or threat networks; and we seek to neutralize threat networks. Using the six elements of human network analysis for network engagement (see para 1-20) the staff is able to determine how and where to integrate network engagement activities into the operations

process. The ***operations process*** is the major mission command activities performed during operations: planning, preparing, executing, and continuously assessing the operation (ADP 5-0).

NETWORK ENGAGEMENT ACTIVITIES

1-6. The three network engagement activities can be applied concurrently, singly, or in various combinations across different groups and towards different supporting systems within a human network. U.S. Forces or Army forces may be involved only in one or two of the activities and not be required to execute all three. At the tactical level, a company may engage a neutral human network through influence activities, while also conducting neutralizing activities against a node of the threat human network, and conducting influence activities toward a separate threat node. At the operational level an Army Service Component Command will determine which human networks to apply these activities against in support of a theater security cooperation plan.

1-7. Human network analysis provides commanders knowledge that allows them to apply these activities across the range of military operations. Network engagement activities apply to both the stability and defeat mechanisms. See ADRP 3-0 and ADRP 3-07 for more on the stability and defeat mechanisms. No single activity can effectively develop efficiently functioning friendly networks without the support of the local population and the neutralization of threat networks. A singular focus on neutralizing threat networks ultimately fails because threat networks adapt, evolve, and continue to be tolerated or supported by the populace or a subset of the populace. Figure 1-1 on page 1-3 depicts this concept.

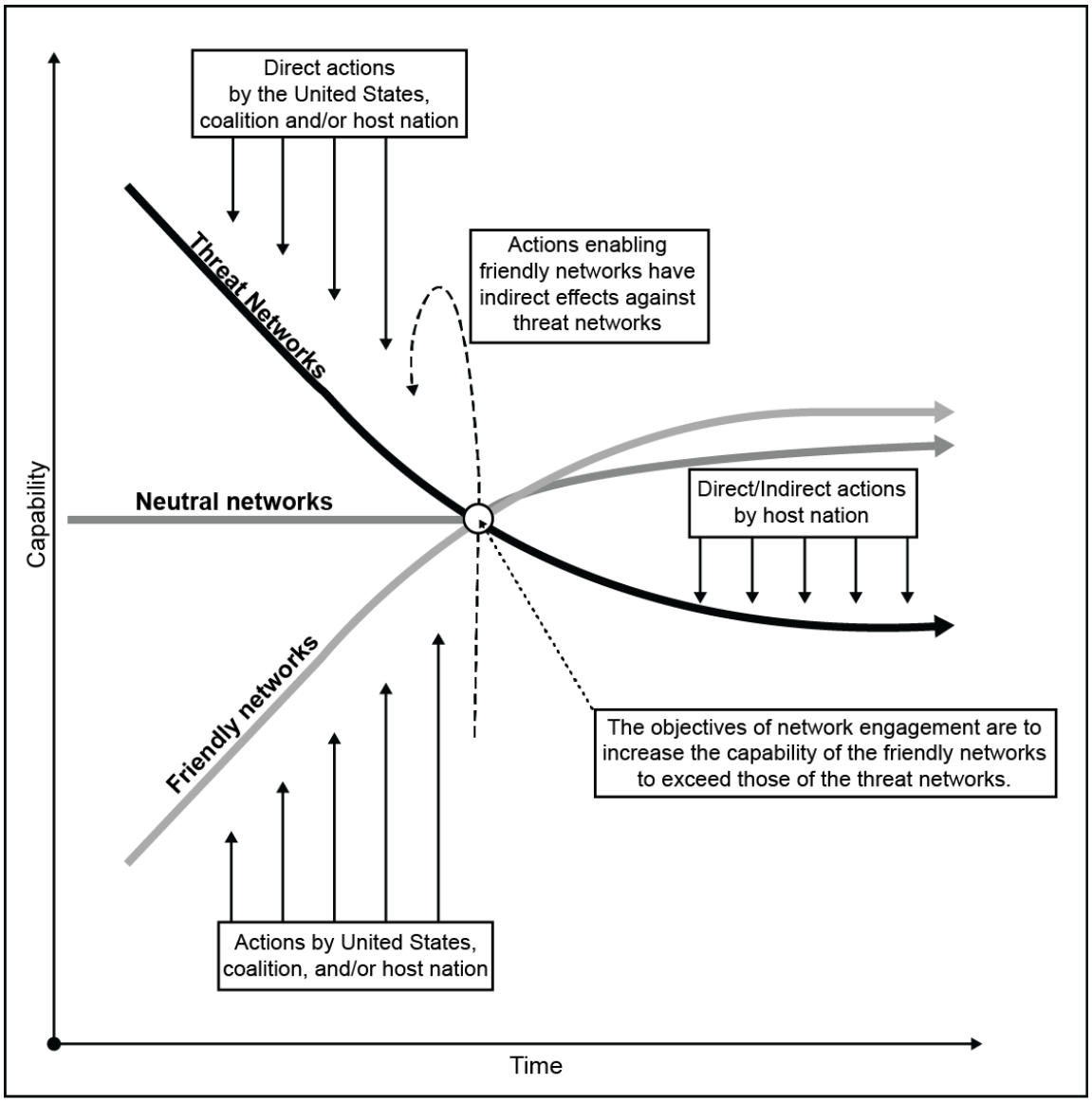


Figure 1-1. Illustrated network engagement concept

SUPPORTING HUMAN NETWORKS

1-8. Supporting activities are conducted towards or for friendly or neutral human networks. In order to support these groups the commander must understand how an OE affects them. At the operational and tactical levels, the Army has a myriad of capabilities that analyze an OE and how it affects various groups. These effects may be named or categorized in a variety of manners including: conditions, vulnerabilities, strengths, ideals, goals, issues, susceptibilities, and influences just to name a few. The human network analysis must incorporate all this input and focus it on the perspective of the group being supported. In other words it does not matter if we think we are supporting them, what matters is the supported network perceives that we are supporting them; whether we are supporting their ideals, causes, issues, security, rights, autonomy or whatever function the support serves. For example establishing information and intelligence sharing protocols with supported groups. From the group's perspective they will see actions taken that support or enable their cause. Self-sufficiency, legitimacy, effective rule of law, and empowerment of friendly human networks is the overriding goal. The following are some activities that are considered supporting:

- Conduct area security operations to provide freedom of maneuver and isolate threat networks from their sources of strength.
- Execute stability tasks that support positive outcomes for friendly and neutral networks.
- Integrate the complimentary effects of combined arms and joint/coalition capabilities.
- Establish information and intelligence sharing protocols with the supported network.
- Establish and maintain unity of effort with unified action partners.
- Comprehensively engage and integrate the full range of actors such as police forces, non-governmental organizations (NGOs), international organizations, host nation organizations and institutions, academia, government officials, media, businesses, as a basis for shared action and reform.
- Negotiate and mediate on behalf of supported human networks.
- Gain visibility on the threat's campaign with HN leadership and actively influence HN leadership to take ownership and invest in solving the problem that created the threat
- Successfully manage security transitions.
- Civilian casualty mitigation.

1-9. Faced with individuals, organizations, and the population that are connected with the operation, commanders identify and interact with those actors that matter to their operational success. Human network analysis gives commanders the requisite knowledge to begin to understand how to interact with these key actors. Army forces can then gain and maintain trust and confidence and obtain further insights into the motivations, issues, grievances, needs, conditions, and vulnerabilities of the groups that these actors are connected with. This information will help shape decisions on how to support, influence, or neutralize groups.

1-10. Conventional and special operations forces coordinate their activities with each other, complementing each other's capabilities, creating interdependence, and unity of effort. Additionally, commanders and staffs coordinate their activities with all unified action partners within an OE. ***Unified action*** is the synchronization, coordination, and integration of the activities of governmental and nongovernmental entities with military operations to achieve unity of effort (JP 1). ***Unified action partners*** are those military forces, governmental and nongovernmental organizations, and elements of the private sector with whom Army forces plan, coordinate, synchronize, and integrate during the conduct of operations (ADRP 3-0). This coordination becomes more important when working in the same area of operations (AO). The effects of coordination enhance isolation of the threat, improve freedom of maneuver, facilitate information-related activities, and improve security.

1-11. Using all available resources (in the AO and through reachback support) facilitates a "whole of government" approach to supporting friendly and neutral networks. Individual communities, government agencies, businesses or religious organizations, and educational institutions have an impact on the population and can alter attitudes and perceptions. Commanders can affect these organizations positively, supporting them in order to influence public attitudes and perceptions. This can also result in increased cooperation, support, movement from neutral to friendly networks, and neutralization or reduced influence of threat networks.

1-12. Infrastructure networks such as cyber, electrical, communications, water, sewer, and others impact all human networks. Infrastructure networks may be leveraged by friendly or threat networks to achieve a desired effect. Knowing which groups interact with and how they are affected by each infrastructure network determines how to leverage each network in a way that has a desired effect for friendly networks.

INFLUENCING HUMAN NETWORKS

1-13. Influencing activities can be applied to friendly, neutral, threat, and even unknown human networks. The purpose of influencing networks is to change or maintain the perceptions, attitudes, and behavior of select network elements so they act in a manner that supports audiences to support the achievement of U.S. objectives. Commanders must exercise particular caution when it comes to influence activities as there are legal restrictions, authorities and permissions that pertain to influencing foreign audiences.

1-14. In order to affect the aforementioned outcomes, commanders and staffs must have a deep understanding of the human networks within the AO and a more general understanding of the other human

networks in an operational environment. Human network analysis provides the foundational information to gain this knowledge. It provides an understanding of the various types or relationships between individuals, organizations, resources, other groups, and sub-groups that can be applied by the commander, staff, and to information related capabilities (IRCs).

1-15. Commanders are challenged to integrate information of human networks with other information provided by the IRCs and then distribute that integrated information back out to the force. They must determine the best method to achieve the desired influence. Commanders rely on the staff and the IRCs to inform decisions on how to influence various elements of the human networks and how and when to integrate these influence activities with other lines of effort. The integrated employment of IRCs can influence political, economic, social, cultural, or religious factors within the information environment to drive change within a single or multiple human networks. An ***information environment*** is the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information (JP 3-13). Information operations is an integrating staff function that focuses on adversaries and potential adversaries and is the staff lead for influence activities directed towards threat human networks. Military information support operations, civil affairs operations, Public Affairs, and civil military operations and the staffs that integrate them can provide staff focus for influence activities directed toward neutral and friendly human networks. See JP 3-13 and FM 3-13 for more information on IRCs and information operations.

1-16. Lasting credibility is critical to positively influence human networks. Unified action partners provide the leverage and support required to respond to a network's needs, gaps, and interests. Establishing and maintaining credibility with a HN can be difficult with deployment rotations. Army forces must create standard operating procedures focused on network engagement and continuously train and rehearse those activities to alleviate the difficulties in building and maintaining relationships. Credibility acquired with one commander must pass as seamlessly as possible to the next so that the influence gained is not lost.

NEUTRALIZING HUMAN NETWORKS

1-17. ***Neutralize*** is a tactical mission task that results in rendering enemy personnel or material incapable of interfering with a particular operation (FM 3-90-1, Change 2). U.S. Forces can expect to face a threat comprised of irregular and hybrid threat networks; potentially assisted by enemy regular forces. Human network analysis provides the necessary network perspective of the relationships of threat elements to other threat elements, neutral, friendly, and unknown elements in a single picture. This information is necessary in order to progress from a myopic threat perspective to one that recognizes that any single entity has an impact on others in an OE.

1-18. Neutralizing threat networks becomes essential when they cannot be influenced to change. Before neutralizing the threat network, commanders must know whether the affect will be positive or negative or have no effect on the friendly and neutral networks that share an OE with them. Positive outcomes may include actions such as creating conditions to allow freedom of maneuver for unified action partners to provide security to the population, freeing populations from the unwanted influence of the threat group and creating secure access to daily needs (commerce, electricity, travel, marketplaces), increase HN capability, and isolate the threat networks from the population. Commanders can then seek to set the conditions for neutralizing activities that cannot be executed yet. For example, effective area security operations provide the time and space to conduct other network engagement-related activities.

1-19. Commanders plan, resource, integrate and execute tactical tasks and mission sets supporting network engagement activities within the context of the larger operational and strategic plans. The targeting process is the primary staff process used to integrate and synchronize activities directed against threat networks. For details on the Army targeting process see ATP 3-60.

SIX ELEMENTS OF HUMAN NETWORK ANALYSIS FOR NETWORK ENGAGEMENT

1-20. Human Network Analysis (a deliberate process that analyzes groups of humans and depicts them from a networked perspective) is based upon six elements. These elements are exercised through the previously

described network engagement activities; although these functions are listed sequentially, these actions occur continuously and simultaneously —

- Understand the mission.
- Understand an OE.
- Understand the networks.
- Organize for network engagement.
- Engage the networks.
- Assess effects on networks.

UNDERSTAND THE MISSION

1-21. Understanding the mission and the commander's intent is key to setting parameters and focus for human network analysis. The human aspects of an OE that human network analysis provides will enable for detailed network engagement planning to achieve tactical, operational and strategic desired end states. In a complex OE, leaders at the lowest level understand the commander's intent for each echelon. It begins with the orders or initial guidance of the higher commander and is part of the military decisionmaking process (MDMP).

1-22. Commanders and staffs at all levels will be required to support strategic level objectives through the effective and efficient use of diplomatic, informational, military, and economic instruments. In addition to understanding their mission, commanders and staffs should understand the mission of other organizations in an OE and how those organizations are connected with various elements. Not every group, organization, or network is bound by a common mission. Understanding the missions, purposes, causes, or binding relationships of the groups being analyzed facilitates understanding of how individuals, groups, sub-groups and the infrastructures they rely on are connected from a networked perspective.

1-23. Network engagement activities will vary in terms of the mix of offense, defense, and stability tasks. ***Stability tasks*** are tasks conducted as part of operations outside the United States in coordination with other instruments of national power to maintain or reestablish a safe and secure environment and provide essential governmental services, emergency infrastructure reconstruction, and humanitarian relief (ADRP 3-07). Stability activities should be occurring frequently within the theater because in order to conclude operations successfully, commanders must integrate and synchronize stability activities with other operations within each major operation or campaign phase. ***Stability activities*** are various military missions, tasks, and activities conducted outside the United States in coordination with other instruments of national power to maintain or reestablish a safe and secure environment, provide essential governmental services, emergency infrastructure reconstruction, and humanitarian relief (JP 3-0).

UNDERSTAND THE OPERATIONAL ENVIRONMENT

1-24. Staffs support the commander in understanding, visualizing, and describing an operational environment to include the characteristics related to network engagement in their planning. As stated in ATP 2-01.3, "the staff should identify all significant civil considerations (this refers to those civil considerations identified as significant characteristics of an operational environment) so that the interrelationship of threat/adversary, friendly forces, and population activities is portrayed."

1-25. For network engagement purposes, OE analysis defines and describes the networks within an OE and provides an understanding of the conditions that allowed the friendly, neutral and threat networks to form.

1-26. As changes within an OE occur, staffs utilize Army design methodology to address these changes quickly. Army design methodology entails framing an OE, framing a problem, and developing an operational approach to solve the problems. Army design methodology results in an improved understanding of an OE, a problem statement, initial commander's intent, and an operational approach that serves as the link between conceptual and detailed planning. It serves as the foundation for more detailed planning, including course of action (COA) development and the production of plans and orders using the MDMP. See FM 6-0, and ATP 5-0.1, for more information on Army design methodology and MDMP.

1-27. Understanding an OE, especially civil considerations, can influence the COA analysis and execution of operations, while helping commanders understand the level of tolerance or support the population has for HN governance and insurgent or threat network activities.

UNDERSTAND THE NETWORKS

1-28. Understanding a group's position in regard to U.S. objectives allows their categorization as friendly, neutral, or threat and to subsequently build out the network picture. When the position is unknown, that group is placed in a fourth category, Unknown Human Networks. (See Chapter 2 for complete descriptions of these categories.) Continuous analysis and the sharing of reports on the common operating picture facilitates the acquisition and maintenance of a comprehensive understanding of the network's relationships within the AO. Understanding the specific human networks requires information and intelligence sharing across unified action partners and facilitates a whole of government approach.

1-29. To comprehensively understand human networks, commanders and staffs need to understand whether the human network they are looking at is a deliberate structure or a network depiction of a portion of an OE. Deliberate human networks require understanding of the basis for development and the conditions that allowed its formation. This is accomplished by understanding:

- **Catalyst.** The condition or variable that brought individuals together to take action.
- **Receptive Audience.** A group of individuals that feel they have more to gain by engaging in the activities of the network than by not participating.
- **Accommodating Environment**. Conditions within an OE that facilitate the organization and actions of a network.

1-30. Network depictions of groups require understanding the relationships between entities, conditions that drive ideology, beliefs, and opinions, conditions that affect daily life, and the infrastructures that are depended upon. This type of network is fluid, perhaps in constant flux. Analysts will rely heavily on the techniques in the following paragraph to obtain some of this understanding.

1-31. Human network analysis relies on several analytical techniques to comprehensively understand the relationships of a group and map them as a network. These techniques not only help determine the orientation of the group, they also help determine the structure, function, survivability, and sustainability of the human network and its sub-networks. Chapter three discusses the analytical techniques to determine the following of friendly, neutral and threat networks:

- Organizational Mapping.
- Network Function Analysis.
- Critical Factors Analysis.
- Link Analysis.
- Network Template Analysis.
- Meta-Network Analysis.

1-32. The staff considers geospatial conditions, political dynamics, social and local dynamics, and other considerations understanding the networks in an OE. See ATP 2-01.3 for additional information the staff considers in understanding an operational environment.

1-33. For more information on IPB see ATP 2-01.3. For information on developing an understanding of the information environment, see FM 3-38. For information about cyberspace electromagnetic activities, see FM 3-13 for information on developing an understanding of the civil or socio-cultural considerations, see ATP 3-57.50.

ORGANIZE FOR NETWORK ENGAGEMENT

1-34. A significant challenge related to network engagement activities is developing situational understanding and unity of effort among a diverse range of organizations and actors found within an OE. Situational understanding and unity of effort facilitate the building of the friendly network. The assistant chief of staff, operations or battalion or brigade operations staff officer leads the process, collecting, consolidating, and correlating input from all the sections. The intelligence staff section and other staff

sections with unique capabilities to analyze the human domain (such as the information operations section, military information support operations staff section, Public Affairs, and Civil Military Operations section), and the Fire Support section are primary contributors to the process. Commanders and staffs organize for network engagement, in part, by establishing unity of effort among diverse members of the unified action partners as depicted in figure 1-2, below.

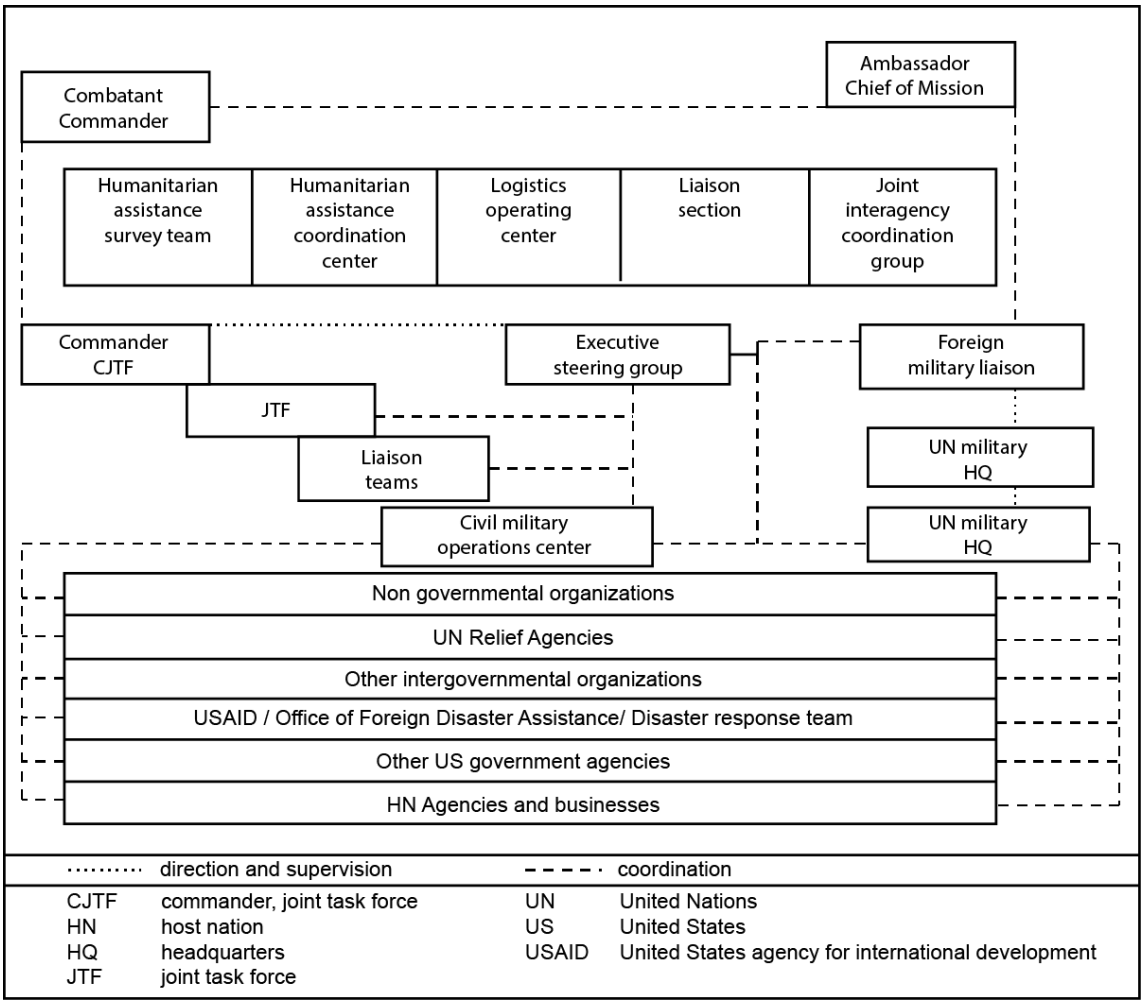


Figure 1-2. Notional structure for coordination

1-35. Network engagement activities should include using the civil-military operations center (CMOC) as a means of coordination and collaboration for the unified action partners that comprise the joint task force. A ***civil-military operations center*** is an organization normally comprised of civil affairs, established to plan and facilitate coordination of activities of the Armed Forces of the United States with indigenous populations and institutions, the private sector, intergovernmental organizations, nongovernmental organizations, multinational forces, and other governmental agencies in support of the joint force commander (JP 3-57). The information gained through this coordination and collaboration will assist the joint task force in understanding an OE and the networks in an OE. The CMOC is a standing capability formed by all civil affairs units from the company to the CACOM with capabilities and functions that increase with each echelon.

1-36. Network engagement requires proper organizational structure and integration of all available organic or external assets when deploying into an area of operations. An ***area of operations*** is an operational area defined by the joint force commander for land and maritime forces that should be large enough to accomplish their missions and protect their forces (JP 3-0). Enablers available to the commander can be organic, deployed

within theater, or available through reachback. Current and future operations require commanders to incorporate unique and specialized unified action partner capabilities into their staff, such as law enforcement professionals, civil affairs, special operation forces and other government agencies. Coordinated reachback support is available, along with HN, coalition, national and international other government agencies (OGAs), and unified action partner capabilities.

1-37. At division and above the commander employs working groups to plan, prepare, execute and assess network engagement activities and make adjustments based on assessments. A working group is an assembly of predetermined staff representatives that provide analysis, coordinate, and provide recommendations for a particular purpose or function. Based on the complementary nature of network engagement and information operations, commanders may leverage the already established information operations working group in coordinating network engagement activities.

ENGAGE THE HUMAN NETWORKS

1-38. Analysis of humans from a network perspective is essential. Engaging human networks includes those actions to support and influence friendly and neutral human networks and their supporting systems and actions to influence and neutralize threat human networks and their supporting systems. Commanders and staffs should plan to engage all networks within their AO.

1-39. Each human network may require a unique engagement strategy. Depending on the phase of the operation, commanders and staffs select, prioritize, and match effective means of supporting and influencing friendly and neutral human networks, and influencing and neutralizing threat human networks. Commanders and staffs determine the desired effects on those networks, predict primary, secondary, and tertiary effects, and utilize lethal and nonlethal means to achieve the commander's desired end state. When engaging a human network, commanders and staffs should be aware of how activity directed toward one network will affect another network. Units gain situational understanding during network engagement by integrating joint and combined capabilities with their actions while conducting information collection, and performing essential stability tasks. ***Information collection*** is an activity that synchronizes and integrates the planning and employment of sensors and assets as well as the processing, exploitation, and dissemination systems in direct support of current and future operations (FM 3-55).

1-40. Commanders and staffs should place significant time and effort on determining indirect approaches to affect networks. They accomplish indirect neutralization of threat networks by directly supporting and influencing friendly and neutral networks. For example, in addition to directly neutralizing a threat network by conducting counter-threat finance operations, the staff can plan economic development programs to support and influence friendly and neutral networks. The resulting support and influence have the effect of strengthening the economy, which indirectly increases the degree to which the threat network is neutralized. This particular approach to network engagement is called integrated financial operations. Staffs have capabilities to apply similar network engagement approaches – combining complementary direct and indirect operations – through missions such as stability activities and information operations. Stability activities and information operations are discussed in detail below. Integrated financial operations are discussed in Chapter 5.

STABILITY ACTIVITIES

1-41. During analysis of an OE as discussed in the second element, commanders and staffs gain understanding of critical requirements of stability activities and which local authorities can best support success, or are likely to impede success. Commanders must also balance achieving progress in assisting economic growth and improved governance with the application of combat power to achieve conditions for that progress.

1-42. Enabling progress in a nation's economy and government is best achieved working with and through local authorities who are members of the neutral, friendly and sometimes threat networks. Army special operations forces provide unique capabilities to shape foreign environments. In particular, Army special operations forces military information support operations and civil affairs units provide unique capabilities that brigade combat team (BCT) and below can leverage, in concert with information operations, when planning network engagement activities. A ***brigade combat team*** is a combined arms organization consisting

of a brigade headquarters, at least two maneuver battalions, and necessary supporting functional capabilities (ADRP 3-90). When planning and conducting stability activities, commanders are well served by understanding root causes of conflict and by applying network analysis and social network analysis to determine the key local authorities to work with, or to oppose. A common obstacle to progress in stability activities is governmental corruption. Gaining an understanding of how corruption works and who is involved in the local area will guide anti-corruption efforts. In many cases, the legitimacy of local governance can be built through improved infrastructure services to the population. Specifically, the sewage, water, electricity, academics, trash, medical, safety, and other considerations that must be improved.

1-43. Developing the infrastructure not only improves the legitimacy of local governance, it also enables economic development. As the unified action partners support the friendly network in improving the services represented by the sewage, water, electricity, academics, trash, medical, safety, and other considerations, the foundation for economic growth becomes stronger. This sets the conditions for successful economic development projects, which are described below in the section on Integrated Financial Operations. Creating economic growth in general and jobs in particular, indirectly neutralizes the threat network because licit economic growth naturally competes with illicit economic growth and having legitimate job opportunities decreases the appeal of job opportunities that the threat network offers.

SYNCHRONIZING INFORMATION RELATED CAPABILITIES

1-44. The fact that information is one of the operational variables and an element of combat power indicates the role it plays in operations. Information operations, through the integration and synchronization of information-related capabilities is a primary means of influencing the networks in an OE. An ***information-related capability*** is a tool, technique, or activity employed within a dimension of the information environment that can be used to create effects and operationally desirable conditions (JP 3-13). Information operations supports all network engagement activities; examples include supporting and influencing friendly and neutral networks by spreading information about economic development projects and how they and related job opportunities are improving quality of life, and informing friendly and neutral networks about the activities and goals of the threat network and how they are decreasing security and quality of life.

ASSESS EFFECTS ON NETWORKS

1-45. Assessment is a continuous process of monitoring and evaluating the situation within an OE and measuring the progress of an operation toward achieving the commander's objectives, see FM 6-0.

1-46. Assessment applies to each activity related to network engagement, measuring the extent to which it achieves desired effects. Assessment also applies to the overall objectives for creating the desired end state. Assessing network engagement activities may have immediate results but may have to be monitored for an extended period of time to determine if the outcome was successful. Commanders and staffs should integrate network engagement considerations into all the tools that support assessment — the operation order, the common operational picture, personal observations, running estimates, and the assessment plan.

1-47. Network engagement activities are conducted to support mission success, and they should be tracked to continually assess the degree to which they are supporting achievement of the commander's desired end state. The commander's desired end state should address or imply how networks should be changed between the current state of an OE and the desired end state. This will guide the staff in recommending the types of network engagement activities that will yield desired effects. The staff needs to understand how those effects will change the behavior, structure, and activity of the human network from the onset of the activity through the desired end state so they can measure overall progress toward that end state with assessments.

1-48. District Stability Framework (DSF), formerly known as the Tactical Conflict Assessment Planning Framework, was designed to help tactical commanders and their staffs identify the root causes of instability, develop activities to diminish or mitigate them, and evaluate the effectiveness of the activities in fostering stability at the tactical level (provincial or local). The DSF should be used to create local stabilization plans and provide data for the Interagency Conflict Assessment Framework, which has a strategic and operational-level (country or regional) focus. See FM 3-07 for more information on DSF.

1-49. At division level and above, commanders and staffs may use the DSF, but they will sometimes be best served by using the Interagency Conflict Assessment Framework, which was designed to guide the collection of information and enable unity of understanding among USG Departments and agencies of dynamics driving and mitigating factors of violent conflict in a country.

1-50. Network engagement planning and DSF or Interagency Conflict Assessment Framework are mutually reinforcing because they share many concepts, such as core grievances, societal patterns, key actor's motivations, and windows of vulnerability and opportunity.

1-51. The assessment process provides several tools and opportunities for theater and below units to track individual network engagement activities, as well as overall progress toward the desired end state of network engagement.

This page intentionally left blank.

Chapter 2
Human Networks Categories, Features, and Structures

HUMAN NETWORKS

2-1. Analysis is a careful study of something to learn about its parts, what they do, and how they are related to each other. Network engagement focuses on human networks and delineates that focus through human network analysis. Once a group's position in regard to U.S. objectives is known, it allows for their categorization as friendly, neutral, or threat and subsequent building of the network picture with that understanding. When the position is unknown, that group is placed in a fourth category, Unknown Human Networks.

2-2. Building the human network picture relies on the analytical techniques—described in Chapter 3 of this publication—regardless of whether the human network is a deliberate structure or a network depiction of a portion of an operational environment (OE). Examples of groups using deliberate structures include criminal organizations, violent extremist organizations, insurgent undergrounds, and groups whom value secrecy or require compartmentalization. While these examples may seem to naturally belong in the threat category, businesses, militaries, and other organizations may have deliberate networked structures. Army Forces let their position in regards to our objective determine their categorization not their structure.

2-3. Human networks that are not deliberately organized may still be depicted as networks. This depiction is the outcome of the human network analysis. It facilitates identification of significant information about a group or groups that might otherwise go unnoticed. For example, analysis can uncover positions of power within a network, show the sub-networks that account for its structure, find individuals or organizations whose removal would greatly alter the network, and facilitate measuring change over time. While the group may be depicted as a network, it should not be confused with the variety of supporting systems the group relies on to function and survive. These systems may be referred to as networks, i.e. communications networks. It is through these supporting systems that activities such as diplomatic and political interaction, military coordination, sustainment, economics, communication, and influence flow. These supporting systems also create sub-systems (sub-networks) that seek to move money, people, and goods for the benefit of the group. These interactions may be sources of stability or instability regardless of the category of the human network using them. There may be a natural bias when analyzing threat human networks to consider that these interactions create instability but this is not necessarily the case and we must recognize that not all supporting networks are a threat to the force and its mission.

2-4. Army intelligence, special operations, military information support operations, civil affairs, information operations, and other related forces identify, define, and leverage human networks within the context of their mission. Army intelligence uses precise methodologies to analyze these same groups. Once their analysis concludes that the linkage or connections between individual humans tie them together to form a unified whole, they describe that unified whole as a network and categorize it as either threat or neutral. military information support operations personnel, for example, begin their analysis of humans by dividing them into large groups based upon demographics, affiliation, motivation and other distinctive, identifiable characteristics. Civil Affairs personnel interact with the indigenous populations and institutions to facilitate military operations. They focus on civil considerations analysis using tools such as areas, structures, capabilities, organizations, people, and events; and political, military, economic, social, information, infrastructure physical environment, and time to determine grievances and identify the root cause of instability within the populace. The assistant chief of staff, operations or battalion or brigade operations staff officer directs all staff members to look at all these different analyses, determine which vulnerabilities are actionable and recommend network engagement activities to support specific courses of action. See ATP 2-33.4, FM 3-57, and ATP 3-57.70 for details on the aforementioned methods.

2-5. Friendly, neutral, unknown, and threat human networks are often interrelated. Some network functions, entities, groups, organizations, and member's activities or relationships span the friendly, neutral, and threat realms, making networks complex and difficult to understand. For example: a financial organization could have affiliations with both friendly and threat groups. Groups and individuals within a network may shift alliances and adapt strategies based upon the conditions present within an OE. Network members may modify their allegiance to groups and individuals based upon personal or group interests (money, security, resources, ideology, etc.). An individual or group can have overlapping affiliations between networks. For example, a government official may be a reservist in the security forces and a member of a tribe that is sponsoring actions against the government. Additionally, there can be sub-networks of different categories within any of the friendly, neutral or threat human networks. Understanding these ties is crucial to determining the true second and third order effects U.S. Forces may have on the larger social, tribal, political, technical, economic, or other networks within an OE.

2-6. In order to correctly identify elements of a network, commanders and staffs rely on all sources of information, recognizing that regardless of the source it may provide information related to any category of human network. Although information collection assets are used to collect information on threat human networks, the members of friendly, unknown, and neutral human networks that are sometimes identified by those assets are often the bridge (or spanners) between these networks. For example, a car mechanic by day may also be a vehicle-borne improvised explosive device (VBIED) maker by night. This fact could become known through weapons technical intelligence exploitation of a VBIED, revealing evidence within the device. This connection could be made through intelligence infrastructures like identity identification databases. The individual's biometric data would need to be recorded in a database, which implies that operational units require the ways and means to enter individuals within an OE into a database. While information collection provides most information about individuals in threat networks, including spanners, liaison, coordination; open source information provides most of what is known about friendly and neutral networks in most environments. In the example above the fact that the individual is a car mechanic and the workplace location could be available through open sources. This understanding assists in categorizing individuals and groups as friendly, neutral or threat.

2-7. Network allegiances are fluid and require constant analysis from the staff to maintain understanding of these complexities. Allegiances may shift based on changes in the conditions within an OE caused by friendly, neutral or threat actions. For example, friendly operations resulting in high civilian casualties may cause individuals or groups within friendly or neutral networks to support the threat network cause.

UNKNOWN HUMAN NETWORKS

2-8. Units may encounter groups whose position in regards to U.S. objectives is unknown. Army forces may be able to analyze the group and depict them as networks. Until their position is determined units categorize them as unknown. One goal of human network analysis is to have no unknown groups. While it may be possible to determine the position of specific elements of a group this may not be representative of the group's position as a whole. In fact there may be a variety of positions within a group. Staffs should exercise caution as there may be pressure to categorize a group as neutral when it is really unknown.

FRIENDLY HUMAN NETWORKS

2-9. A human network whose position tacitly or openly supports objectives that are aligned with U.S. objectives can be categorized as friendly. Friendly human networks can be divided into two groups: U.S. and allied organizations, and those composed of the HN in which operations are being conducted. Examples of friendly human networks may include:

- Military forces.
- Security forces.
- Government officials.
- Supportive business leaders.
- Social leaders and social movement groups.
- Village/Tribal Elders.
- Political leaders and groups.

- Active supporters among the HN population (elements such as ethnic, religious, tribal and regional affiliations must be taken into consideration).
- Nationalist groups.
- Nongovernmental organizations.

NEUTRAL HUMAN NETWORKS

2-10. Neutral networks consist of those groups or elements that neither actively support nor oppose U.S., coalition, and HN interests and activities, and do not negatively impact the commander's operational goals. Commanders should provide focus on neutral networks, and be considerate of their various nuances, in order to effectively support or influence them. Neutral human networks may consist of the following individuals or groups:

- Village / Tribal Elders.
- Business leaders and groups.
- Social leaders and social movement groups.
- Passive elements among the HN population (elements such as ethnic, religious, tribal and regional affiliations must be taken into consideration).
- Criminal organizations.
- Military forces.
- Security forces.
- Political leaders and groups.
- NGOs.

THREAT HUMAN NETWORKS

2-11. Threat networks consist of groups that have goals or objectives that oppose or counter U.S., multinational, and HN interests and negatively impact the commander's operational goals and actions. Any combination of threat networks may align for mutually beneficial effects, but may break their allegiance at any time if they perceive a loss or reduction of benefits. Criminal organizations have the potential to provide much needed funding for operations and facilitate the purchase of equipment for insurgents. The ability to adapt and transition is the most challenging attribute of our adversaries. Threat networks additionally may be comprised of the threats described in ATP 2-01.3, such as irregular forces, criminal organizations, regular forces, and hybrid forces. For more information on how to analyze threat networks see ATP 2-01.3, and ATP 2-33.4.

FEATURES OF A HUMAN NETWORK

2-12. Deliberate human networks, like those described at the beginning of the chapter, have common features including a broad array of elements; foundational components, structures, and features that facilitate adaptability. Ad hoc human networks, those that we create by depicting relationships within a group in a network picture, may or may not have these same features. Staffs must exercise caution when applying these features to an ad hoc human network or when evaluating these human networks against these features. While all human networks are different they share common features which may include the following elements (Chapter three describes the analytical techniques to determine network composition.):

- **Motivation.** A motivation is a need or desire that causes a person to act. A network can only begin when there is a catalyst (person, idea, need, or desire) to initiate action. The individual feels there is something to gain by engaging in activities of the network. Examples include but are not limited to—
  - **Ideology.** A system of ideals or ideas that provides a basis for a normative, guiding view for life.
  - **Money.** A financial gain derived from aligning with a group or cause.
  - **Power.** An increase in influence or control over an area or population.

- **Basic human needs.** The resources necessary to sustain life (water, food, and shelter) or comfort (sewer, electricity, electronic forms of media, and communication).
- **Leaders.** Leaders provide purpose, direction, and motivation to accomplish the mission and improve the organization.
- **Members.** This element assesses how members become part of a network and are socialized into the group norms. Participants in the network might have identifiable roles, functions, or responsibilities.
- **Popular support.** The acceptance of a cause by a portion of the population. Popular support is an important source of power. Popular support can include active participation, open support, clandestine support, or passive acceptance of a network's activity.
- **Operations.** These are the specific activities the network takes to accomplish its objectives.
- **Freedom of movement.** This is the ability of the network to sustain, resupply, recruit, persuade, and influence the local population; communicate, collect information, or attack targets of opportunity for political, economic, or tactical gain.
- **Structure or Organization.** This is the organization of the network as it applies to decision making, and command and control; or mission command as applicable.
- **Disposition.** The geographical location of network elements and how they are deployed, employed, or located.
- **Infrastructure.** The basic physical and organizational structure and facilities needed for the function of the network. Infrastructure can be subcategorized by functional area to include:
- **Logistics.** The design and development, acquisition, storage, movement, distribution, maintenance, evacuation, and disposition of materiel that the network needs to operate. The dependency on logistics fluctuates horizontally and vertically between the various groups and levels of their organizations.
- **Communications.** The methods by which the network passes information internally and externally.
- **Information/Intelligence.** The way the network collects, processes, integrates, evaluates, interprets, and disseminates available data to support network activities.

- **Finance.** The main source of viability to a network, finance pays for services rendered or items purchased. It also takes care of how the network sustains its operations and continues receiving financial support.

NETWORK COMPOSITION

2-13. Network components are the basic elements of a network. These components consist of:

- **Node.** Represent the tangible elements within a system that can be targeted for action, such as people, places, or things (for example, materiel or facilities). (See ATP 2-33.4 for more information.)
- **Critical node.** A critical node is an element, position, or command and control entity whose disruption or destruction immediately degrades the ability of a force to command, control, or effectively conduct operations. A critical node is a point of influence within a network and a potential focal point for targeting of that network. (See ATP 2-33.4 for more information)
- **Link.** Links are the behavioral or functional relationships between nodes. They establish the interconnectivity between nodes that allows them to work together as a system—to behave in a specific way (accomplish a task or perform a function). (See ATP 2-33.4 for more information)
- **Cell.** A cell is a collection of nodes or links that perform a singular purpose or function supporting a larger network.

NETWORK STRUCTURE

2-14. Characteristics of networks include how they are structured, their density, and the degree to which networks are adaptive to their environment. Network structure shows how an organization is connected, how it behaves, and how its connectivity affects its behavior. This can be categorized in three basic forms:

- **Hierarchical.** A tiered decision-making structure, this is a system or organization in which people or groups are ranked one above the other according to status or authority.
- **Nonhierarchical.** Any decentralized decision-making structure.
- **Blended.** A combination of hierarchical and nonhierarchical organization.

2-15. Network density is a general indicator about the number of individual nodes connected in a network relative to the total number of nodes possible. Density does not necessarily indicate the effectiveness of a network, but it does make the network more difficult to disrupt.

ADAPTIVE NATURE OF NETWORKS

2-16. All networks within an OE will adapt as required to meet their objectives, whether friendly, neutral or threat. Many adaptive networks in an OE are actually complex adaptive systems consisting of many diverse and autonomous components that are interrelated, interdependent, and linked through many interconnections. They predominately behave as a unified whole; learning from experience and adjusting to changes in the environment. Al Qaeda is an example of an adaptive network which also acts as an adaptive system.

2-17. Adaptive networks exhibit unique characteristics that must be considered when deciding how to effectively engage them. These characteristics make them highly resilient and require understanding if commanders are to achieve their desired effects. These characteristics may include:

- **Co-adaptive.** The system must continually evolve to survive, and members must adapt to their changing environment and the forces that counter it.
- **Emergent.** Emergence allows collections of dumb or ignorant single components to behave in unpredictable and intelligent ways as a system.
- **Self-organizing.** A system without a central authority or an external element imposing structure upon it through planning is self-organizing. It is a "bottom up" developed organization.
- **Regenerative.** Components are easily replaced within the system. Removal of a single node has minimal impact on the system as a whole.
- **Decentralized (flat).** Adaptive threat networks are generally not organized in a bureaucratic or hierarchal way. In a decentralized system, the capabilities are distributed throughout the system or network. Long-term success against these networks should focus on changing the relationships and links in the networks, and severing the links between networks and its smaller cells.

This page intentionally left blank.

Chapter 3
Analytical Support to Network Engagement

UNDERSTANDING NETWORKS

3-1. Throughout the operations process, commanders develop and improve their understanding of an operational environment and the problem. To achieve understanding of relevant networks, the commander and staff leverage multiple types of information, reporting, analysis, and network related products. The staff continually collects and analyzes information from a variety of sources, including open-source and intelligence reporting, civil information, combat information, and input from tactical unit leaders regarding their personal interactions with the populace during day-to-day operations. This granular level of information is required to more completely understand the networks within an operational environment (OE) and if analyzed thoroughly, will lead to a high-level of understanding of the interrelationships between friendly, threat, and neutral networks. Ultimately the purpose of collection, interpretation, and analysis of information is to illuminate relationships within the networks we are engaging.

3-2. As part of the integrated staff process, each staff element must focus on the relevant aspects of an OE as it pertains to their warfighting function and mission variables. An integrated staff effort can effectively determine how the interactions of friendly forces, enemy forces, and indigenous populations affect each other to continually create outcomes that affect friendly operations. Situational understanding, for example, is a main goal during Intelligence Preparation of the Battlefield (IPB) as part of an integrated staff effort. (See ATP 2-01.3). While this chapter is focused on analytic support to network engagement, this effort involves more than IPB. Integrated staff processes, supported by broad network analysis products and collaboration, are requirements for successfully engaging networks to shape an OE to more closely conform to the commander's desired end-state.

3-3. The Army's primary mission naturally drives training that is threat based and 'dominate phase' oriented. To overcome this training bias, staffs often shift their paradigm to include analysis of friendly and neutral elements. This shift allows analysis to expand to include all aspects of the OE and analyze all networks -- regardless of their category. This is necessary because the activities of network engagement often overlap. As the scope of a staff's analysis expands so do the analytical methods available to them. A staff might choose to use only one or two types of analysis, but in general, the more types it leverages, the greater the likelihood that the staff will gain increased depth of understanding of an OE and the networks within that environment. This depth of understanding better enables the staff to fulfill information requirements and support the decision-making process.

3-4. The commander's intent, specifically the clear framing of desired end state, is a common thread running throughout this process of leveraging multiple analytic techniques to support network engagement. Focusing on the commander's desired end state enables the staff to focus its analysis on network activities that are most directly related to Army forces achieving mission success. The process of conducting these analytic techniques provides the staff with in-depth situational understanding to support planning NE activities.

3-5. The staff develops understanding of an OE as part of mission analysis during the military decisionmaking process (MDMP). This provides general, or foundational, understanding of an OE and the networks within, and supports the broad conceptual analysis phase for planning, as described in Chapter 4 of this publication and in ADRP 5-0. The staff then develops detailed understanding of an OE and the networks within that environment which is supported by the analytic methods of:

- Organizational Mapping.
- Network Function Analysis.
- Critical Factors Analysis.

- Link Analysis.
- Network Template Analysis.
- Meta-Network Analysis.

3-6. These analytical techniques are non-sequential and product development often occurs simultaneously, with outputs from one product feeding incremental development of adjacent products. The analytic methods that support network engagement are shown below in figure 3-1.

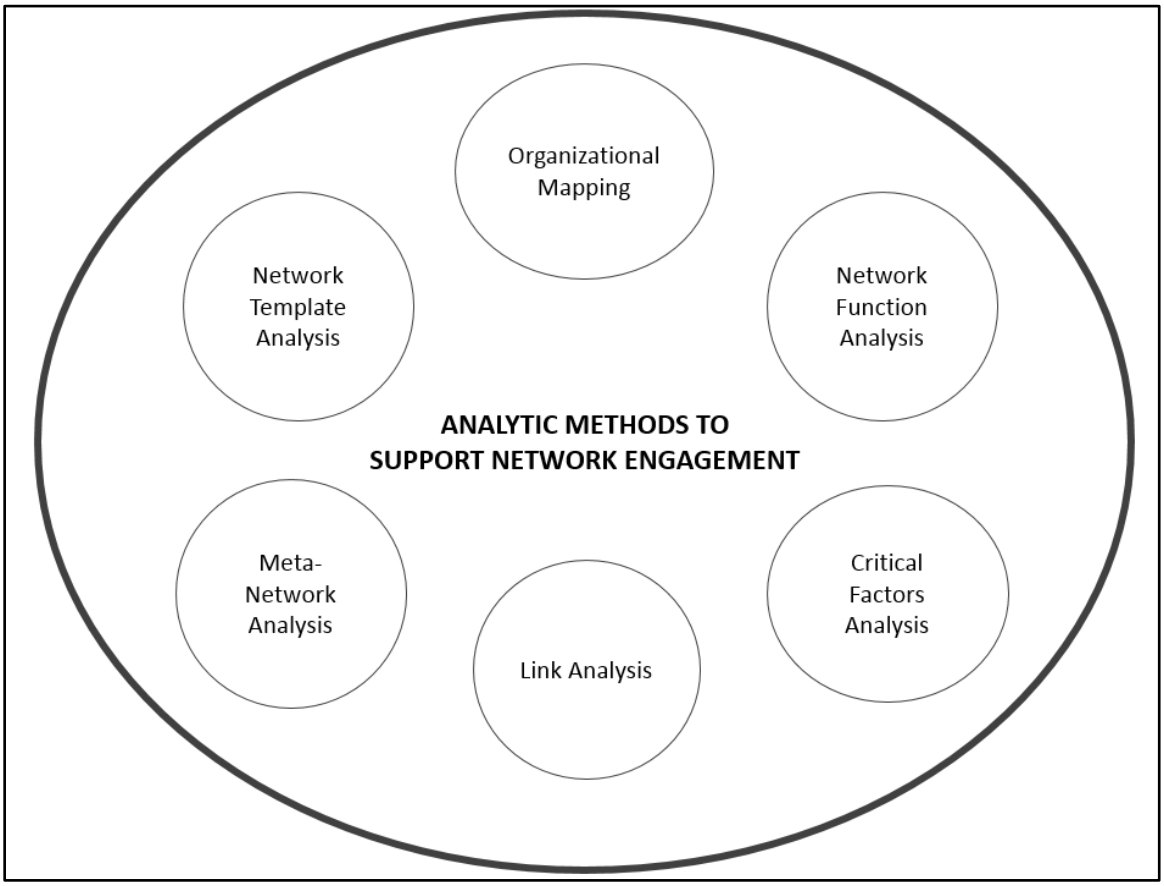


Figure 3-1. Analytic methods to support network engagement

3-7. A staff conducting analysis for network engagement incorporates information from all staff sections. This includes IPB products, staff estimates, and integrating friendly and neutral network analysis to increase understanding of the network elements within an OE. The additional methods discussed below can be utilized by the staff to increase understanding of specific networks and to provide the commander with friendly, neutral, and threat critical vulnerabilities that can be engaged by the unit. Organizational mapping can be leveraged by the commander to better understand the force and its connections and facilitate Mission Command. Organizational mapping enables the unit to better understand itself – its strengths, weaknesses, capabilities and gaps. This understanding guides the commander's decision making related to network engagement.

METHODS USED TO ANALYZE NETWORKS

3-8. ATP 2-33.4, includes a detailed discussion of analytical fundamentals, skills, and techniques used by the intelligence team to assist commanders with understanding complex environments. This chapter relies on these fundamentals and relates specific techniques to network analysis.

3-9. Analysis of friendly and neutral networks, using the same analytical fundamentals outlined in ATP 2-33.4, supports LOEs that include establishing civil security, establishing civil control, restoring essential services, supporting governance and economic development, and synchronizing information related capabilities. Each of these methods directly contributes to the IPB process and can add benefit to and receive benefit from analytical products traditionally completed during IPB. These types of analyses will optimally be fused with other network-related products such as targeting and effects recommendations and information collection plans.

ORGANIZATIONAL MAPPING

3-10. Organizational mapping provides information to enable commanders to better organize their force, while mitigating risk, to more efficiently and effectively engage networks, ultimately enabling success. The unit must know not only the enemy, but also itself, in order to succeed. This applies to network engagement operations, and specifically to the fourth element of human network analysis, organize for network engagement. In order to organize for network engagement, the unit needs to know at a minimum, its strengths, weaknesses, gaps, and resources available. Organizational Mapping reduced to its simplest terms is using network analysis methods to better understand our own organization.

3-11. Organizational Mapping can be applied in various ways. To mitigate risk, units would identify—

- Key strengths, weaknesses, and gaps, including critical vulnerabilities.
- Key personnel for disseminating information, as these often hold a network together.
- Key personnel with specific knowledge, skills, abilities or experiences.

3-12. Regardless of the specific application, the common theme of Organizational Mapping is that the unit can function more effectively when we understand ourselves. While the process should remain somewhat flexible, some basic steps that are often involved in Organizational Mapping are shown below:

- Define data requirements for mission analysis.
- Collect, sort, and aggregate data, considering relationships for future analysis.
- Apply social network analysis (SNA) (SNA techniques are further described in step four (4) of Meta-network Analysis below, and training resources are listed in the training resources section of this publication.)
- Develop products, to include reports and visualizations.
- Assess findings.
- Provide impact of findings.
- Implement and sustain the desired task organization to support mission requirements.
- Monitor progress as part of the unit's assessment plan.

3-13. Achieving unified action is often challenging, in part, because diverse organizations have varying timelines, goals, authorities and priorities. Organizational Mapping can help mitigate these challenges. For example, Organizational Mapping enables the Army division serving as a joint task force during a deployment to form a well-functioning team by mapping organizations and their capabilities to mission requirements. This is a complex requirement because even within the U.S. Interagency, there are a broad array of agencies and capabilities associated with operations. Counter threat finance, for example, would potentially require the involvement of Department of Justice, Department of Treasury, Central Intelligence Agency, Immigration and Customs Enforcement, and others. Commanders and staffs would need to understand the roles of these agencies within counter threat finance in order to understand which agencies needed to be involved in counter threat finance operations for a specific theater during a specific time period.

3-14. Step one (1) involves defining data requirements as part of mission analysis. To illustrate the concept of organizational mapping, a brief vignette is presented on page 3-4:

In one recent case, an organization used these techniques to better support its assigned contingency mission. During the mission analysis phase, the unit defined its data requirements to specifically identify personnel who deployed to this area (step one of Organizational Mapping).

For step two (2), collect and sort data, the organization identified current members who self-reported "on the ground experience" in that location in order to develop an internal network for the command to leverage for future combatant commander and higher headquarters requirements.

For step three (3), the organization applied a social network analysis tool and analyzed the data to determine where the work experience was strong or weak within the specified geographic area. (More information regarding social network analysis and its application to data is included later in this chapter.)

During steps four (4) and five (5), the organization applied the data to a social network analysis software tool to produce visualizations and reports that enabled more in-depth analysis. The organization's visualizations included the use of SNA tools which aided the organization by identifying network clusters and assisted the staff in exploring reasons for this grouping. Applying Organizational Mapping enabled the mission commander to rapidly identify experienced, non-organic personnel from adjacent units that could be called upon to augment the deploying force.

During the final steps of the Organizational Mapping process, the organization assessed its findings and reported and explained results with more specific versions of the following general recommendations:

Mission units should reach out to adjacent units for coordination on combatant commander support augmentation

Additional attribute data should be further collected and analyzed, i.e., language abilities, educational background and overseas peacetime engagement

Units should establish a schedule to gather and maintain information from assigned personnel related to their combatant commander-aligned experience and retain this information in a centralized data warehouse

Units should organize their staff to meet increased requirements for friendly and neutral network analysis. These analysts should receive formal data collection, management and network analysis training.

3-15. Organizational mapping can also be understood in terms of personal, or social interaction between members of the unit and unit member's interactions with those outside their unit. Templates, link diagrams, and social network analysis can all be applied in order to better understand our own organizations. For example, social network analysis can give leaders insight to who in the unit has strong social network measures, revealing informal leaders of the unit. Additionally, while it can be beneficial to analyze a network independently, it is often insightful to analyze these networks as a larger whole in order to better understand how they relate to each other. Understanding who in a unit has links to personnel within a host nation government or security agency may indicate a member who can more easily adapt and succeed in a liaison officer role with that agency. If this disparate data is not collected and analyzed, these insights may not be realized.

3-16. By enabling the unit to better understand itself, organizational mapping enables more effective threat engagements and shaping operations. The basic steps involved in organizational mapping as shown above, is only a guide. These steps can and should be modified and altered for each requirement. Organizations that make the effort will gain insights into their own strengths, weaknesses, gaps, and resources available. They

will also gain a deeper understanding of key personnel who function as reliable information conduits or who tie various networks together, and key personnel with important knowledge, skills, and abilities. This increased awareness and understanding will enable the unit to plan and engage more effectively with friendly, neutral, and threat networks.

NETWORK FUNCTION ANALYSIS

3-17. The network functions model provides a framework that depicts the various functions that constitute the network - people, groups, events, command and control entities, elements, positions, etc. Network function analysis is the examination of dynamic, multi-link relationships characterized by varying degrees of complexity and uncertainty. While hierarchical organizations have a formal leadership structure, day-to-day operations are typically accomplished by an informal network that leverages personal social ties. Terrorist and other irregular threat organizations are often cellular and distributed and may or may not have ties to "official" organizational leadership. Part of the difficulty in countering these types of organizations is to understand how they evolve, change, adapt, and can be destabilized or supported to achieve specific objectives. Network function analysis is informed by analysis of an OE and by input from all staff elements. This analysis results in a model of the network, as depicted in figure 3-2 below.

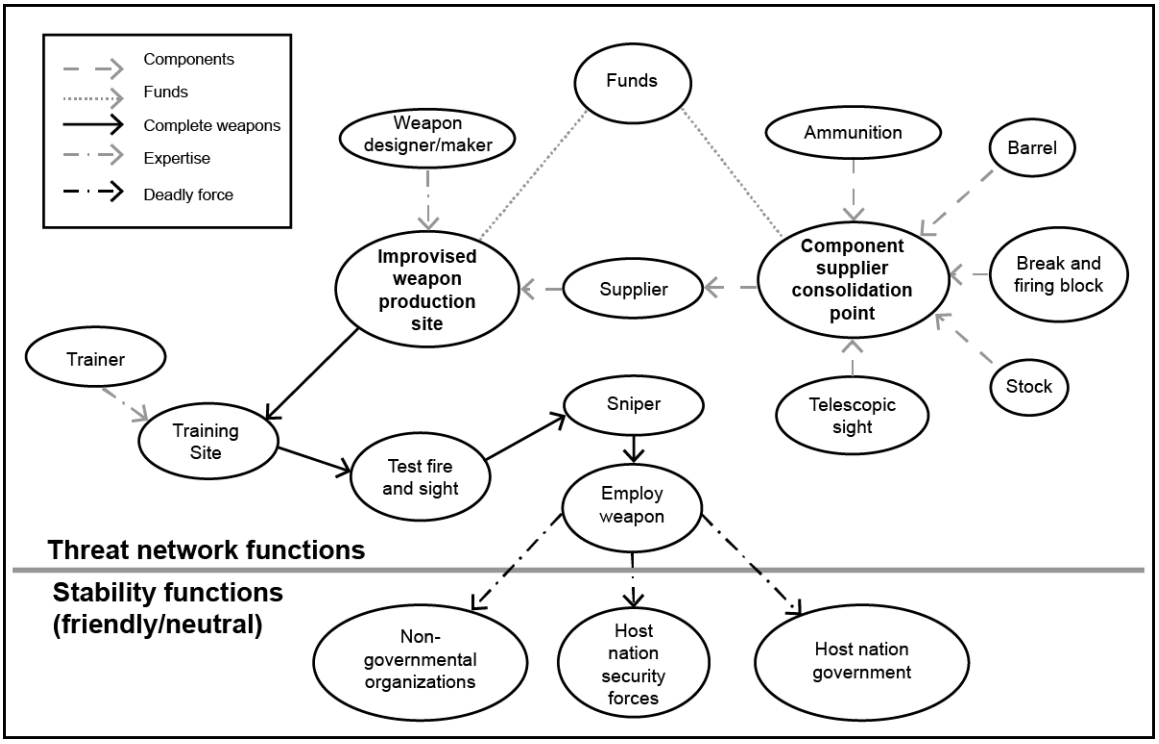


Figure 3-2. Example of network functions model

3-18. The improvised anti-material network functions model in figure 3-2 depicts network functions, activities and specific critical capabilities that the network must perform to continue functioning effectively. Models of this type support functional analysis, which is based on the premise that certain functions must be performed by any network to bring about mission accomplishment. In this example of a network functions model, the weapons cell must perform functions such as establishing a production site and enlisting a knowledgeable weapons designer in order to successfully construct and employ an improvised and technical weapon system. Network models portray the network's basic functions and capabilities and can be produced based on general or foundational information about an OE and the networks. This network functions model analysis is primarily focused on threat network functions (above the line) and its potential negative impact on governmental stability functions (below the line). Function model analysis should also be conducted on friendly and neutral networks.

3-19. The staff develops the network functions model by identifying the structure and flow of major network functions, such as providing components, funds, and SME support, that the network must be able to perform to remain effective. These essential network functions can be labeled critical capabilities and are an important consideration when conducting center of gravity or critical factors analysis.

CRITICAL FACTORS ANALYSIS

3-20. As the staff develops in-depth understanding of network functions and critical capabilities, it applies that knowledge to conduct critical factors analysis (CFA). This method enables the staff to identify critical network vulnerabilities based on analyzing the network's critical capabilities and critical requirements. A ***critical requirement*** is an essential condition, resource, and means for a critical capability to be fully operational (JP 5-0). This section will focus on analytical methods and products used to support CFA. A refined CFA provides the staff with detailed understanding of network critical functions and vulnerabilities. CFA assists the staff in providing the commander with "when, where, why, and how" those critical factors are vulnerable to network engagement activities.

3-21. Step one of the network engagement CFA process, which is also part of the IPB process, is to develop initial understanding of an operational environment and to identify the objective of the network being analyzed. While many units apply this process solely to threat/adversary networks, significant value can be realized by using these analytical methods on friendly and neutral networks.

3-22. Step two identifies the network objective's critical capabilities through functional decomposition of the networks within a given OE, considering friendly, neutral and threat networks. This activity is supported by the previously mentioned network function analysis and the network functions model.

3-23. Step three identifies the network objective's critical requirements. These critical requirements act as a list of more detailed factors needed to accomplish the critical capability. A ***critical capability*** is a means that is considered a crucial enabler for a center of gravity to function as such and is essential to the accomplishment of the specified or assumed objective(s) (JP 5-0).

3-24. Step four identifies the network specific activities (SA) that are needed to accomplish those critical requirements. These specific activities can represent with even more detail, what is needed to accomplish a critical requirement.

3-25. Step five involves analyzing SA's to determine critical vulnerabilities within a given network function being considered. Critical vulnerabilities are going to represent methods for exploiting or removing specific activities so that a critical requirement cannot be accomplished.

3-26. Step six considers friendly element actions that can be recommended to the commander to either mitigate friendly CVs or exploit threat CVs that are identified.

3-27. The CFA process outlined here aids the staff in the course of action (COA) development and COA wargaming phases of the MDMP and may also inform higher level center of gravity (CoG) analysis. Because not all CVs represent the same level of vulnerability to the system, thorough planning and COA analysis must be used to determine the appropriate friendly element actions to take and what resources to apply to it. Identifying and recording CCs, CRs, and CVs essentially maps a series of points that a commander can engage to achieve operational goals. A visual model that represents the relationships between interacting variables is provided in figure 3-3 on page 3-7.

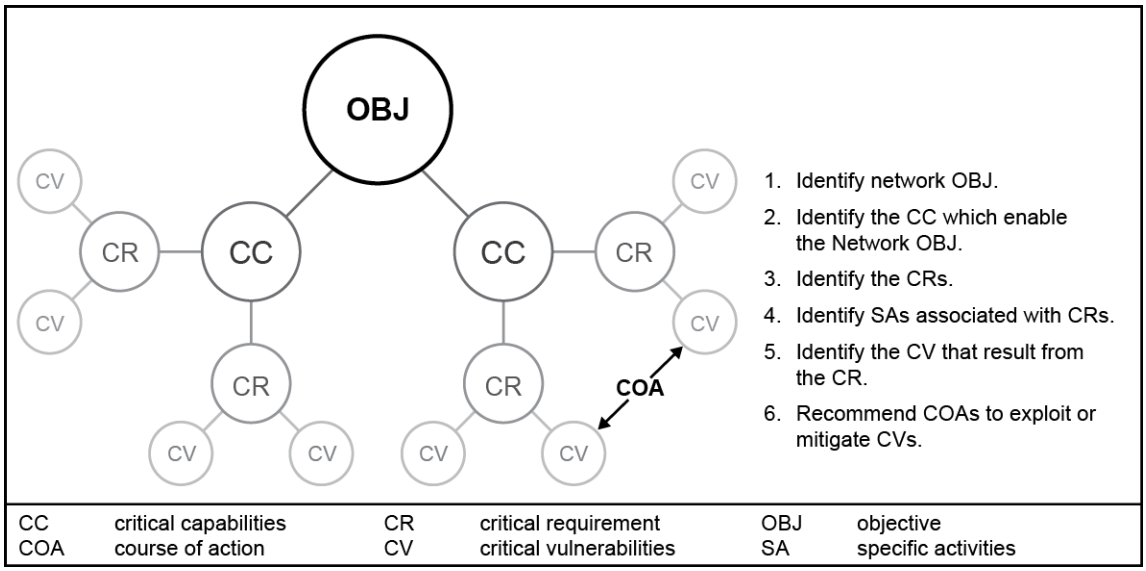


Figure 3-3. Main components of CFA and steps associated with the CFA process

3-28. Analysis of these network activities often provide insights that are beneficial to the intelligence and operations staff in the information collection management effort. Specifically, development of both observable and signature indicators of these activities will often increase relevant and timely information collection, deepen network situational understanding and bring clarity to defining and maintaining a coherent assessment plan. Critical vulnerabilities are those aspects or components of critical requirements that are deficient or vulnerable to engagement in a manner achieving decisive or significant results. In general, the commander must possess sufficient operational reach and combat power or other relevant capabilities to take advantage of a network's critical vulnerabilities while protecting friendly critical capabilities. (For additional general information regarding CFA, see JP 2-01.3, JP 5-0 and JP 3-15.1). This discussion was also informed by the work of the Asymmetric Operations Working Group – more information regarding this version of the CFA process is contained in the reference section of this publication.

LINK ANALYSIS

3-29. In the context of network engagement, link diagrams visually depict who is doing what to (or for) whom, with significant emphasis on identifying individual members or cells of the network and their role or function within that network. Data, information and intelligence to support link diagram development come from a variety of sources. For example, civil affairs and other elements of a staff may find it useful to produce link diagrams for elements of the friendly and neutral networks. The staff can then incorporate these products into a comprehensive network diagram that will then support deeper understanding of the complexity within their OE. The key information from the link diagram are the nodal relationships that are used to enhance previous analyses which often provide a starting point for future analysis, as depicted in figure 3-4 on page 3-8.

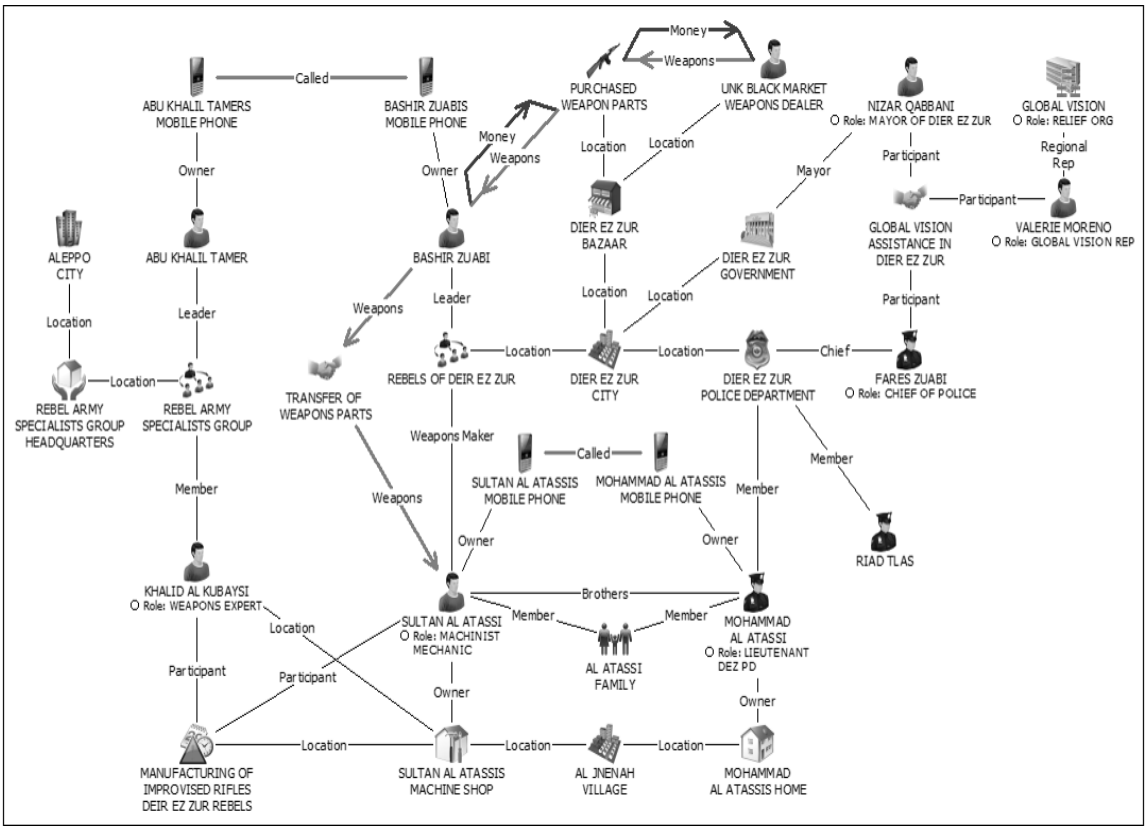


Figure 3-4. Example of a link diagram

3-30. Following the rules listed on page 3-9 when building link diagrams enables the analyst to depict a more robust and realistic representation of an OE by including a variety of node classes and types. Networks that use more than one node class (agents, locations, events, organizations, resources, etc.) are known as multi-mode networks. A group of networks is known as a meta-network. Building a link diagram using these rules supports multi-mode network construction. This directly supports step four, social network analysis (SNA), of meta-network analysis and also supports a staff's requirements to organize data to support distributed operations.

Rules for Producing Link Diagrams to Enhance SNA Outcomes

All reported people, locations, events, organizations, resources, etc.., are depicted as unique nodes.

Avoid directly linking people to people or organizations to organizations. Capture what is linking them together in the form of another node class (event, location, resource, etc.).

Make a link diagram for each report or data set, and save individual link diagrams by report number to merge into master meta-network. Label links to describe the relationships between nodes; color links when possible. Make location nodes as specific as possible, avoid linking individuals to broad locations, and use "unknown location" designation for nodes that are known to exist, but are not yet located.

The link diagram displays known and suspected linkages

A solid figure represents known linkages. Suspected or weak linkages are dashed figures.

Each individual, interest, entity is shown only once in a link diagram

3-31. The inner workings of the network are better understood by analyzing both the critical capabilities in the network functions model (figure 3-2 on page 3-5) and the node relationships in the link diagram (figure 3-4, on page 3-8). For example, the network functions model in figure 3-3 includes "Improvised Weapons Production Site" as one of the network critical capabilities; however, the link diagram, depicted in figure 3-4 adds much more detailed information by identifying Sultan al Atassi as the owner of the machine shop, its general location, activities that occur at the shop, and others who may know more information about the machine shop. This is just one example of how the general elements of foundational OE analysis and the production and analysis of link diagrams support and reinforce each other.

3-32. In addition to providing an understanding of the dynamics behind the current OE conditions, the link diagram also provides insights as to how node relationships could be altered to achieve the conditions envisioned by the commander articulated in their desired end state. For example, studying the node relationships depicted in the link diagram (figure 3-4, above), provides some understanding of why and how nodes interact.

3-33. Understanding how the neutral, friendly and threat networks are connected can be beneficial in identifying possible corrupt officials, insider threats, and can support assessment of how targeting affects those relationships and the network as a whole. These efforts are enhanced by building networks to a common standard across the staff and by incorporating these qualitative diagrams into a quantitative single-mode social network. Assessment of the impacts of targeting can then be measured and incorporated into a staff's assessment plan, thereby offering the commander additional information to support decision-making.

3-34. When mission planning, time, and information support it, conducting network and link analysis at tactical, operational and strategic levels enables staffs at all echelons to develop a common operational picture of the networks within an OE.

Value of Building Network Diagrams to a Common Standard

Building networks to a standard enables a more long-term view of network activities and trends in a given region or area of interest, as these diagrams can be shared with follow-on units or with other unified action partners. When units adopt a standard network-build procedure or standard operating procedure, these networks can then be saved, shared and merged to support more complete situational understanding of the networks in an OE as conditions and missions change.

NETWORK TEMPLATES

3-35. Network templates are derived from CFA and are useful product to support NE COA development and refinement. Network templates provide visualization of the sequence of events for the network critical requirements. The staff applies the sequence of events to the terrain as the locations of the events become known. In this way, developing and refining network templates provides understanding of what the network is doing and in what order, and it supports understanding where the network is doing it. Figure 3-5 provides an example of templating a critical requirement.

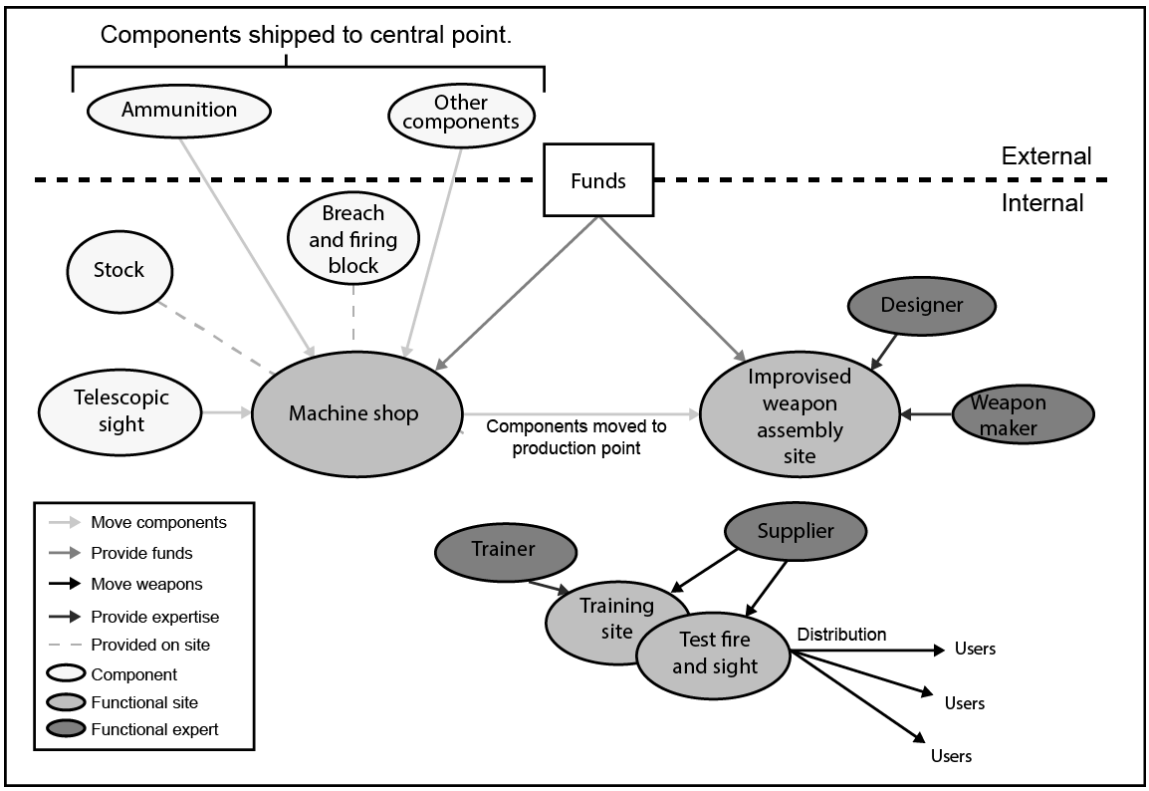


Figure 3-5. Network Template

3-36. A list of specific activities can be developed during critical factors analysis, and further refined concurrently with the development and refinement of the network templates. During the refinement of critical requirements, as shown in figure 3-11, on page 3-16, the analyst visualizes and carefully considers the specific activities required to complete the critical requirement. As the network templates are refined to reflect network functions that occur in time and space, a network's critical vulnerabilities may be revealed for engagement.

META-NETWORK ANALYSIS

3-37. The meta-network is a visually and mathematically accurate representation of known networks in an OE that include aspects of the friendly, neutral, and threat networks and how they interact. Meta-network analysis supports the identification of critical nodes which provides a greater understanding of a networks' critical vulnerabilities.

3-38. Meta-Network Analysis is best described as a four step process that—

- Constructs multi-mode networks.
- Combines multi-mode networks into one meta-network.
- Extracts a social network.

- Applies SNA to identify potential nodes for collection, removal, manipulation, or further analysis. See figure 3-6, below:

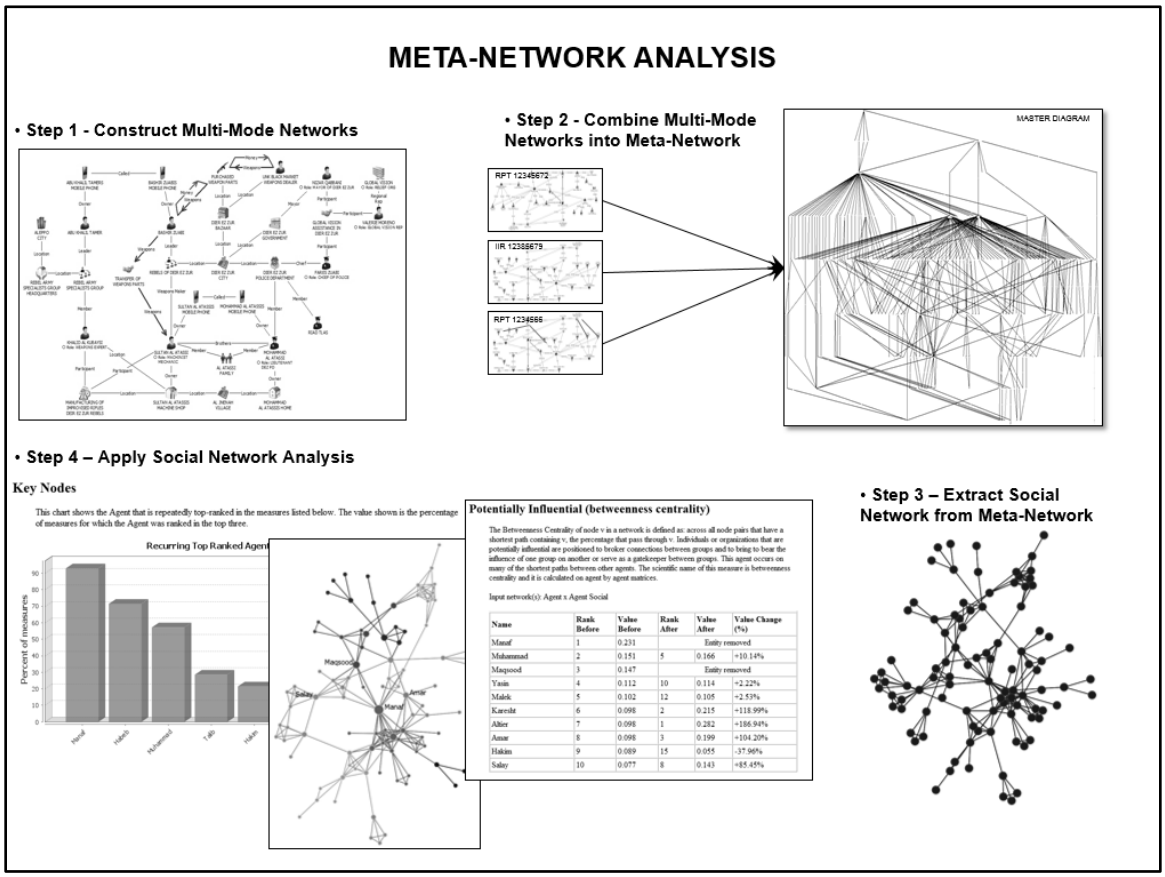


Figure 3-6. Meta-network analysis workflow

STEP ONE – CONSTRUCT MULTI-MODE NETWORKS

3-39. Meta-network Analysis requires analysts to first construct multi-mode (agents, events, locations, resources, organizations, etc.) networks. This step was performed during the link analysis process mentioned above.

3-40. Single Mode Network data consists of only one node type. Examples; a network consisting of only an agent (source) by agent (target) network; cell phone by cell phone network; or financial account by financial account network.

> Multi-Mode Network data consist of more than one node type. Example; a network consisting of agent (source) by agent (target) network, and agent by resource network, and event by location network, and cell phone by cell phone network, and agent by cell phone network.

STEP TWO – COMBINE MULTI-MODE NETWORKS INTO ONE META-NETWORK

3-41. Multi-mode networks are then combined into one meta-network (also known as a master network or master merge network). This step can be conducted manually or through existing software programs such as DCGS-A Link Analysis, Analyst Notebook or other link diagramming software. Developing a network building standard operating procedure will provide cross-functional staff elements the ability to merge

network diagram products. These network analysis activities often occur across the staff, from tactical units to higher level fusion cells.

STEP THREE – EXTRACT SOCIAL NETWORK FROM META-NETWORK

3-42. Existing in the underlying structure of the multi-mode, meta-network is a hidden single-mode agent to agent (person to person) social network. To identify this social network, analysts conducting meta-network analysis use software such as ORA, UCINET, R and others to create new networks based on common nodes shared by agents. This method of network analysis may require additional training for staff members, and is often performed at higher level staff sections. In the absence of software, these new associations can be determined through traditional link analysis methods, however the manual process is much more labor intensive. For example, if Agent 1 and Agent 2 are not connected in the meta-network, but both are linked to Event 1 (figure 3-7), software and the analysis of relationships can be used to create a new network that directly links Agent 1 and Agent 2 based on their sharing of Event 1 (figure 3-8).

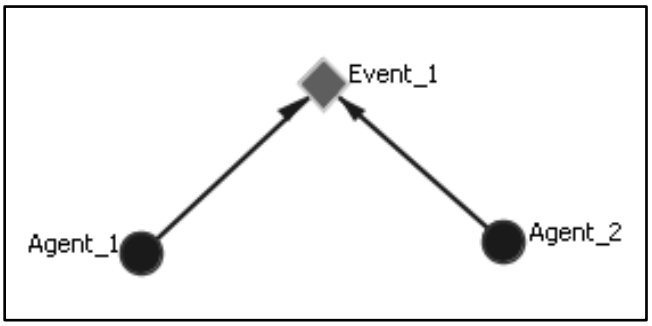


Figure 3-7. Agents connected to event 1

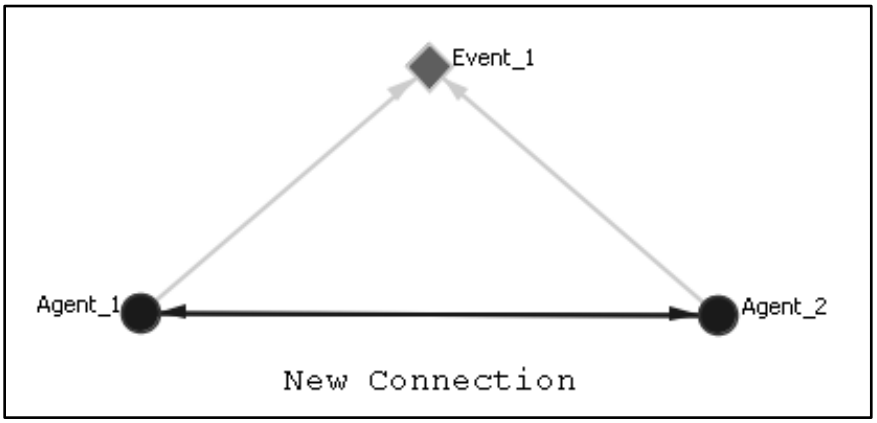


Figure 3-8. New agent to agent connection created

3-43. On a larger scale, extracting a social network from a multi-mode meta-network, as visualized in figure 3-9 on page 3-13, offers a glimpse into the clarity that can be achieved in step three of the meta-network analysis process. Using a software program, as mentioned above, to support this process greatly simplifies this step while retaining the underlying structure of the network which will enable step four of this process, Apply Social Network Analysis Measures. This next step in the network analysis process increases accuracy and timeliness in identifying key or critical nodes that can be engaged to support the commander's objectives.

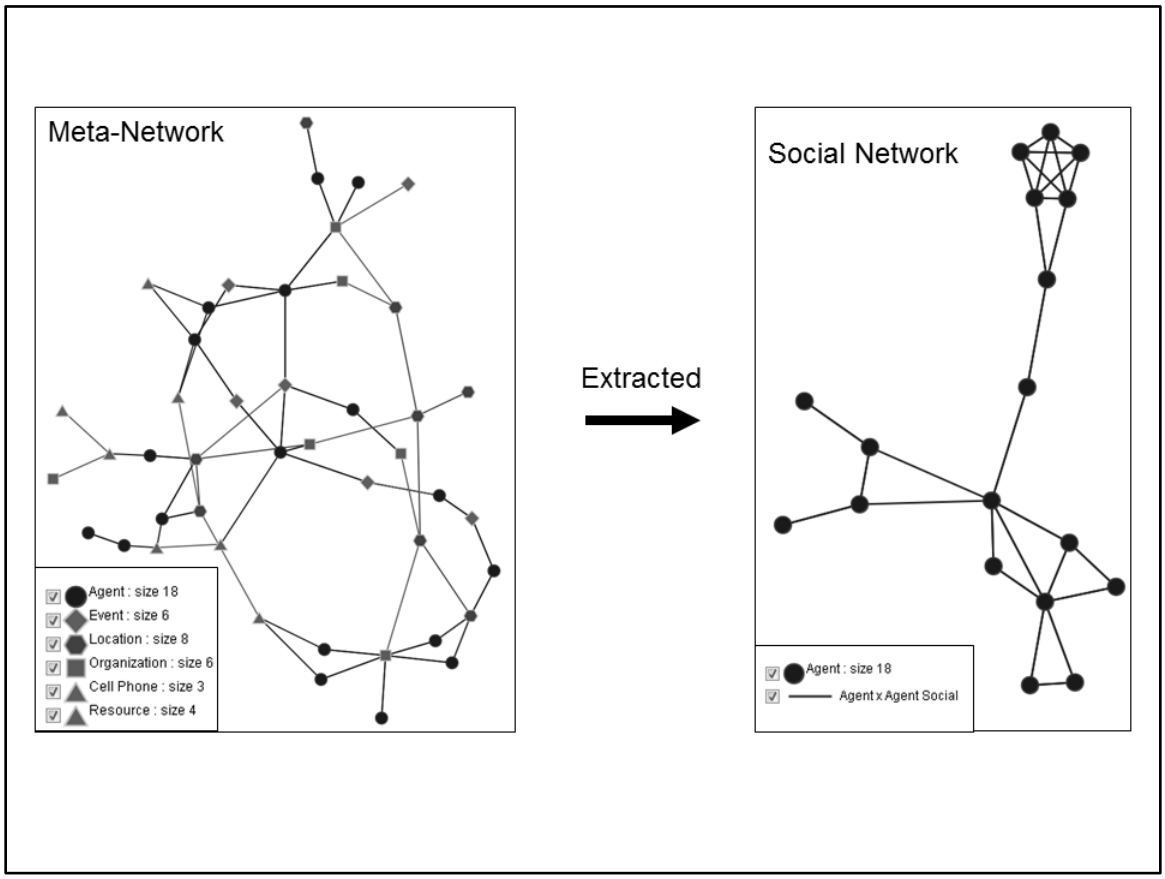


Figure 3-9. Extracting a social network from a meta-network

STEP FOUR – APPLY SOCIAL NETWORK ANALYSIS (SNA)

3-44. SNA is described in FM 3-24 Insurgencies and Countering Insurgencies as a tool for understanding the organizational dynamics of an insurgency and how best to attack or exploit them. Though focused on impacting threat networks, this type of analysis is also relevant to the support of friendly networks and the influencing of neutral networks. A deep understanding of an OE is essential to step three of the MDMP, course of action development. Combining social network analysis with geospatial, temporal and conventional link analysis, a staff trained to conduct SNA can offer depth to cultural and situational understanding by bringing context to a given environments social interactions.

3-45. Social network analysis (SNA) provides understanding of the organizational dynamics of a network and how best to exploit it (if it is a threat network) or how to support or influence it (if it is a friendly or neutral network). It is the mathematical measuring of variables related to the distance between nodes and the types of associations in order to derive meaningful insights from the network link diagram, such as insights about the exposure or influence one node has on another. Additionally, SNA:

- Allows analysts to identify, visualize and understand network structure.
- Shows how a networked organization behaves and how that connectivity affects its behavior.
- Differs from network analysis in that it focuses on the individual and interpersonal relations within the network.
- Supports a commander's requirement to describe, estimate, and predict the dynamic structure of the networks in the area of operations (AO).
- Provides commanders a useful tool to measure or assess operational effectiveness.

3-46. There are five steps in the SNA application process. (See figure 3-10):

- Determine what is to be analyzed, the purpose of analysis, and the significance of the analysis.
- Identify and record data to be analyzed.
- Aggregate and parse data.
- Analyze and interpret through visualization and application of mathematics (software or manually derived).
- Develop and integrate engagement strategies based on analysis results.

3-47. SNA supports staff activities to identify key nodes that enable the engagement of network critical vulnerabilities. Key nodes are those that have special characteristics, such as a high degree of centrality, or have characteristics that make them well suited to achieve desired effects, such as influencing the network, disrupting the network, or exploiting network vulnerabilities. The results of SNA represent a merging of qualitative and quantitative analytical processes. Combining link analysis and SNA provides more balanced analytical results.

3-48. In figure 3-10, the "people" nodes are represented as circles and sized in terms of degree of betweenness centrality. Betweenness centrality measures the extent to which each node lies on the shortest path between all other nodes in a network. Nodes that are high in betweenness centrality are the nodes that connect clusters of nodes within the network. Based on that characteristic, nodes that are high in betweenness centrality are often key nodes to engage in order to maximize fragmentation of a given threat network. Conversely, this measure can be used to determine nodes to target to strengthen or connect disparate sections of a fragmented network to increase communication flow or influence.

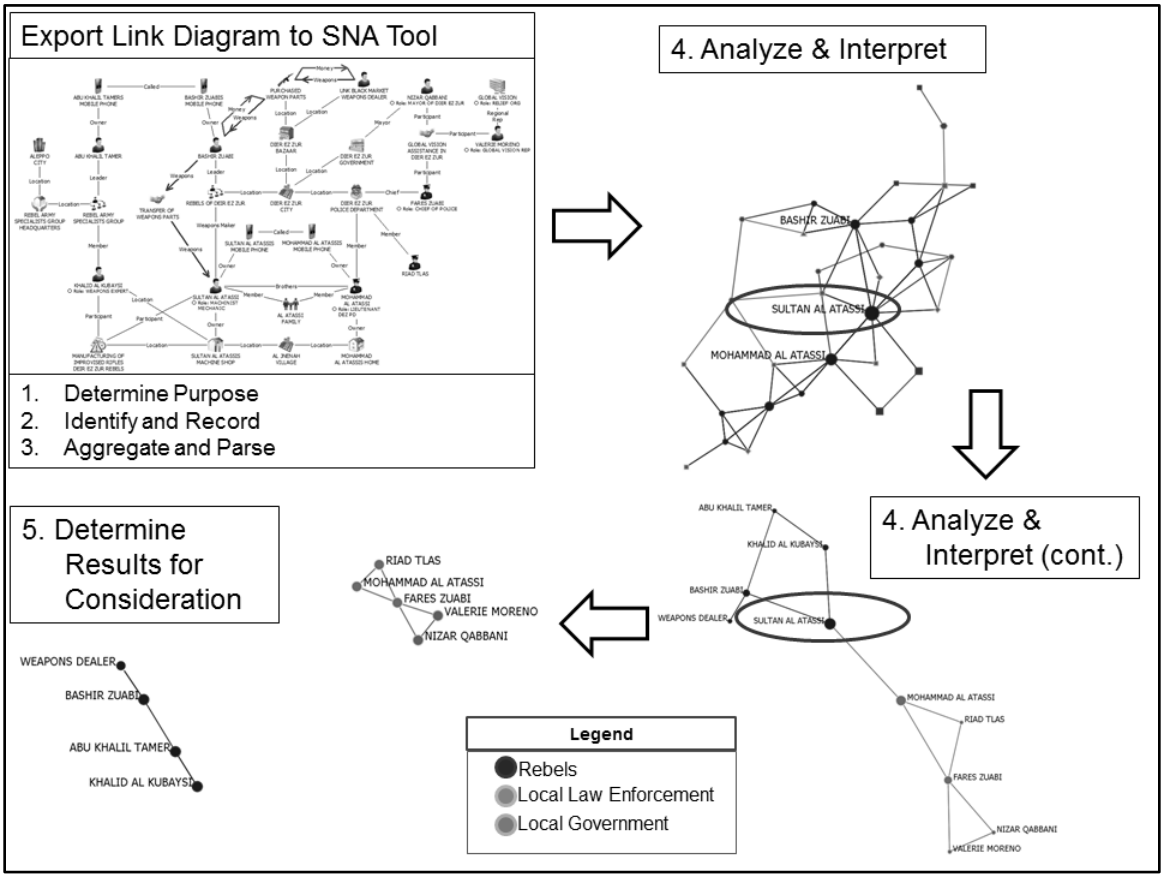


Figure 3-10. Social network analysis application process

Nexus nodes can be defined as those individuals, or other nodes, whose position and linkages provide them the potential to have a significant influence upon at least two of the three basic networks (friendly, neutral and threat).

3-49. In figure 3-10 on page 3-14, Mohammad Al Atassi is a nexus node (highlighted with the oval in step 4) that links the friendly and threat networks. Leveraging the Police Lieutenant, Mohammad, might be the most effective way to create desired effects within the network. Reducing or eliminating the leadership's influence within friendly or neutral networks can often have an even a more significant effect than killing or capturing that leader. Often, reducing or eliminating threat network leadership's influence has a more desirable and durable effect than killing or capturing a given adversarial leader as the population sees the state security and judicial apparatus functioning. This is an example of engaging a friendly node to neutralize a threat network in a manner that supports other network engagement lines of operation.

3-50. In the social network analysis community, nexus nodes are typically known as bridges or spanners. These are the nodes that connect networks, organizations, cells of an organization, or functions of an organization. Spanners score highly in the social network analysis measure betweenness centrality.

3-51. Nexus nodes or spanners are found in all networks. Identifying spanners in the meta-network (group of networks) will help identify how threat, friendly, neutral, and criminal networks are connected. Spanners in a threat, friendly, or neutral network will indicate how organizations and cells are linked, and often reveal different functional aspects of organizations and networks within a given OE. In figure 3-4 on page 3-8, Sultan al Atassi can also be identified as a key spanner in network and functional terms. Not only does he tie the threat network to the friendly network through his brother, he also represents a key function and critical capability within the improvised weapon threat network. Similarly, nexus nodes can and should be identified in friendly and neutral networks, as these nodes often have significant ties to the population, resources, and government functions and are ultimately the true brokers of information within a network. Once these nodes are identified plans can be made to impact or influence these spanners in order to achieve desired network effects. A nexus node's unique status in network function and structure often make it a critical node on which to focus collection and engagement resources.

3-52. Because Sultan al Atassi was identified as a key node and was highest in betweenness centrality within the improvised weapon manufacturing network element during SNA, we know that targeting him will yield significant disruption to the threat's ability to produce improvised weapons. The amount of disruption to this network function is tied to the friendly network (staff's) collection strategy and depth of knowledge regarding 'true' network activities. This type of network analysis will also confirm that Sultan al Atassi is a key network node that enables unified action partners to achieve a desired effect on the network by exploiting a threat critical vulnerability. A ***critical vulnerability*** is an aspect of a critical requirement which is deficient or vulnerable to direct or indirect attack that will create decisive or significant effects (JP 5-0).

REFINE CRITICAL FACTORS ANALYSIS

3-53. In figure 3-11 on page 3-16, CFA is applied to the critical capability. "Equip Units with Improvised Weapons". Step three of CFA is to identify supporting critical requirements, such as "Acquire Gun Barrels". The fourth step is to identify, for each critical requirement, associated specific activities, such as "uploading weapons components onto vehicles at machine shop" and "move components to production site". The staff determines which specific activities can be exploited (for threat networks) or mitigated (for friendly or neutral networks). These are used in steps five and six – that lead to the development courses of action that the commander can select from to achieve a desired end-state.

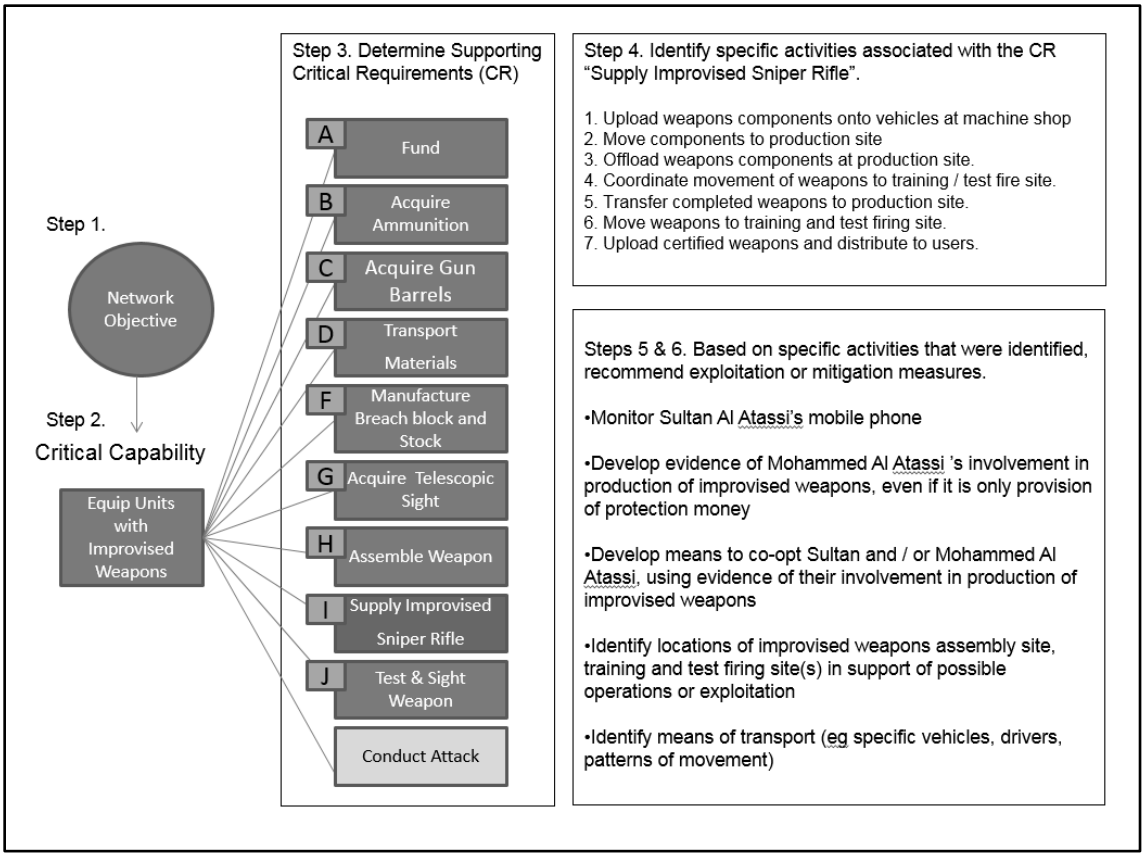


Figure 3-11. Critical factors analysis refinement

3-54. Although there is a sequential flow of logic and information among network analysis products, they should be developed and analyzed as a related group of products so that information can be shared or captured in various products. This enables the staff to gain comprehensive understanding of network individuals, functions, and activities in terms of who, what, where, when, why, and how networks operate. For example, the staff could further refine a link diagram as their understanding of relationships increases.

Analyze Social Ties to Develop Deeper Understanding in an OE

Understanding patterns of behavior within social networks is not limited to social ties between people. These links are nearly always tied to events, tasks, organizations, resources etc. Analysis of an operational environment without a comprehensive analysis of the full complexity of these human factors will be incomplete and will leave gaps in a staff's understanding. Social network analysis reveals patterns in activities and relationships between individuals. It is important to note that SNA measures are based upon known or collected information (data) on a given network. Because an analyst does not see or recognize a connection between two nodes, does not mean that link does not exist. It is also important to remember that network level measures are dynamic and must be considered over time. These network level measures naturally lend themselves to more detailed network engagement assessment planning and impact analysis.

Chapter 4
Network Engagement Within the Operations Process

ARMY DESIGN METHODOLOGY

4-1. As changes within an OE occur, staffs utilize Army design methodology to address these changes quickly. Army Design Methodology enables commanders and staffs to think about the situation in depth. From this understanding, commanders and staffs develop a more informed approach to solve or manage identified problems. (See ATP 5-0.1). ***Army design methodology*** is a methodology for applying critical and creative thinking to understand, visualize, and describe unfamiliar problems and approaches to solving them (ADP 5-0). It results in an improved understanding of an operational environment (OE), a problem statement, initial commander's intent, and an operational approach that serves as the link between conceptual and detailed planning. Using the analysis gathered from the six elements of network engagement facilitates a comprehensive understanding of an OE to include human networks. This understanding serves as a foundation for preparing for more detailed planning, including course of action development and the production of plans and orders using the military decisionmaking process (MDMP) and allows for the integration of the three activities of Network Engagement. The relationship between network engagement and the operations process is visualized in figure 4-1, on page 4-2.

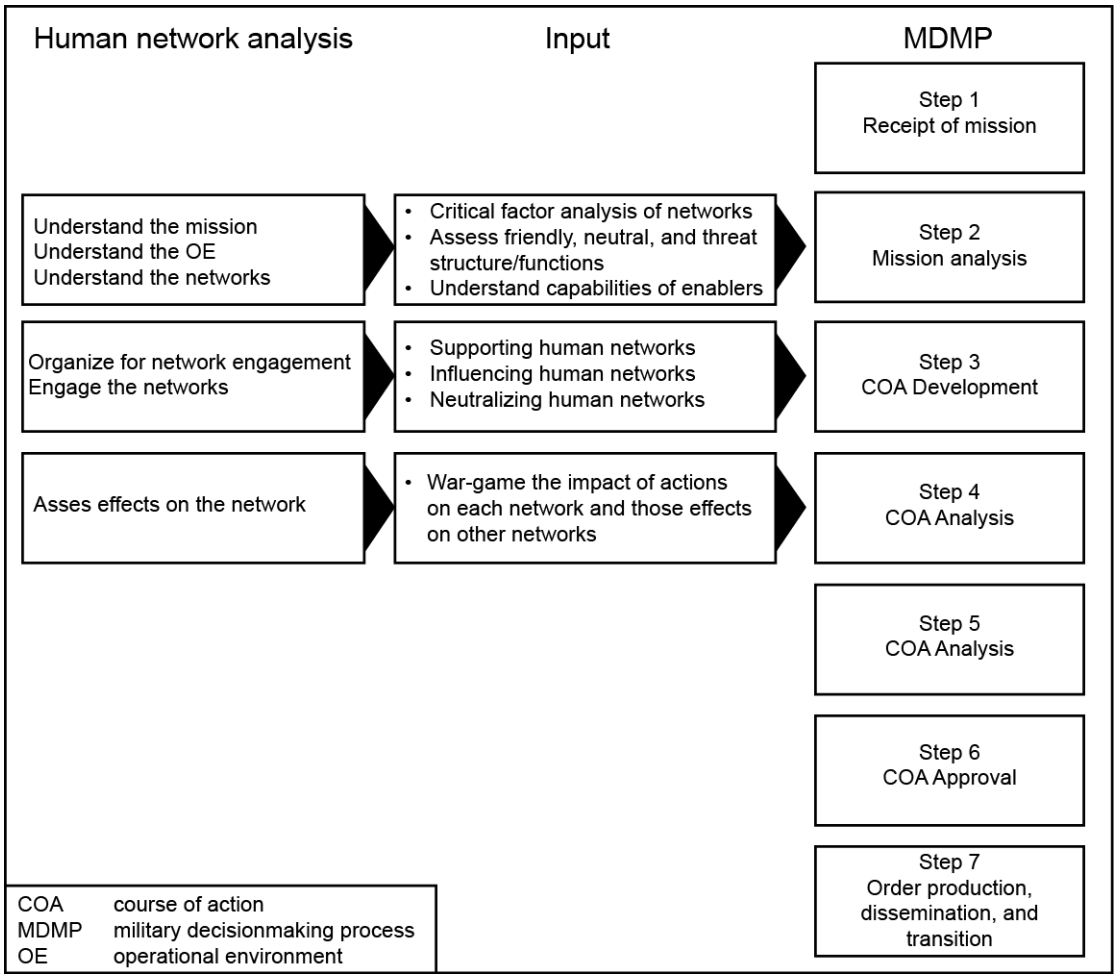


Figure 4-1. Network engagement within the operations process

THE MILITARY DECISIONMAKING PROCESS

4-2. The ***military decisionmaking process*** (MDMP) is an interactive planning methodology to understand the situation and mission, develop a course of action, and produce an operation plan or order (ADP 5-0). Within MDMP, staffs integrate Network engagement activities to fulfill planning and mission execution requirements. These activities are based on the three activities of network engagement: support, influence and neutralize. As depicted in figure 4-2, utilizing the six elements of network engagement, commanders and staff integrate the network engagement operational approach as key inputs during MDMP.

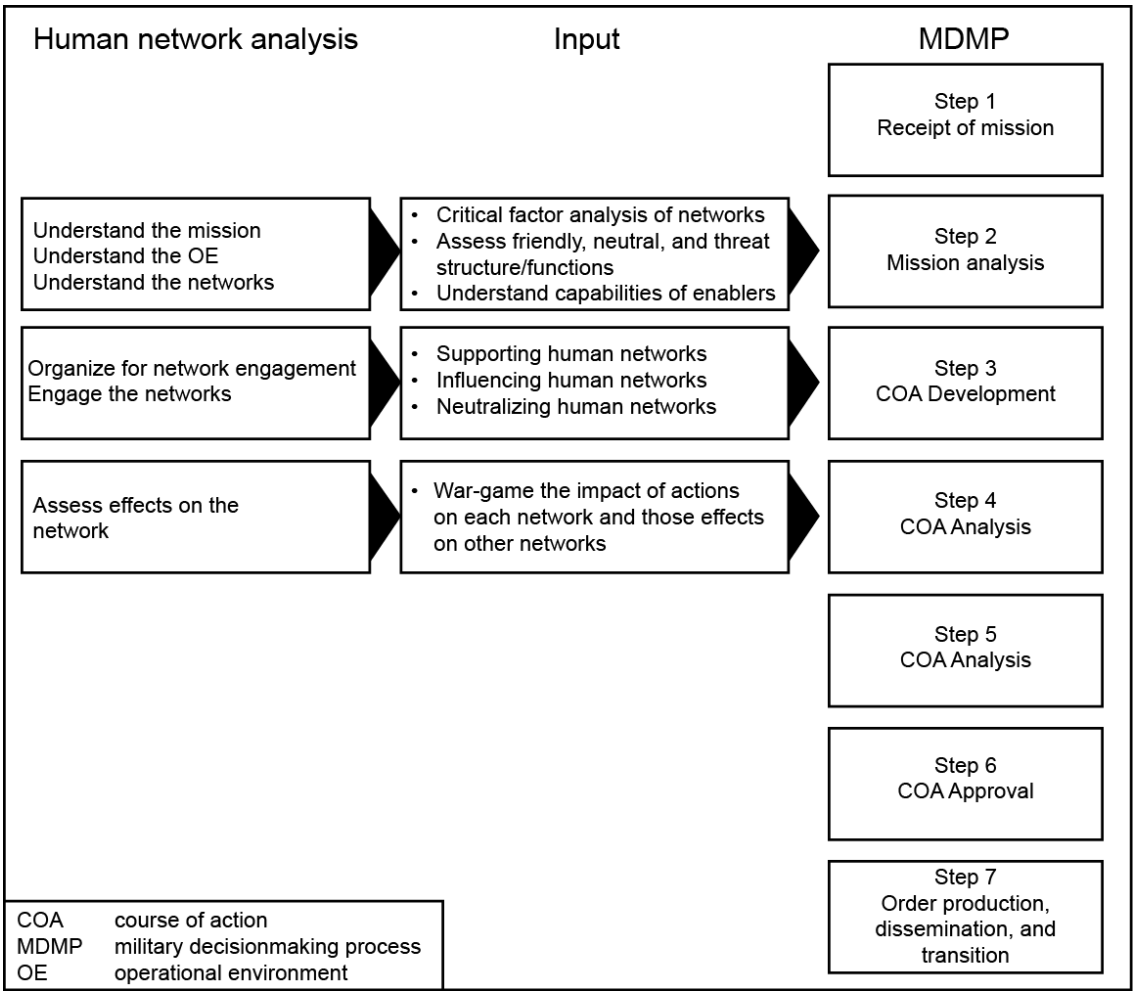


Figure 4-2. Network engagement within MDMP

4-3. During MDMP, commanders and staffs integrate the information from IPB, and other methods to comprehensively understand an operational environment in order to determine the best approach for supporting, influencing, and neutralizing networks within that specific operational environment. The targeting process is used to synchronize actions directed for or against all networks to achieve intermediate objectives in support of the end state developed during the MDMP. Not all sub-steps of MDMP are represented below; the steps identified are most relevant to network engagement.

4-4. **Step 1 — RECEIPT OF MISSION**. During this step, the commander and staff integrate all relevant enablers to participate in mission analysis. The enablers assist the staff with updating running estimates of their capabilities and the capabilities of the networks within an area of operations (AO) to assist the commander with mission planning and execution to achieve the commander's desired end state.

4-5. **Step 2 — MISSION ANALYSIS**. Utilizing the analysis conducted in the first three elements of network engagement, the staff can begin to gather, analyze, and synthesize information and identify capability shortfalls in completing the implied, specified and essential tasks. Commanders and staffs will use the operational variables of political, military, economic, social, information, infrastructure, physical environment, and time to gain situational understanding of an OE and begin to comprehend the complexities of the networks found in the AO. The staff also identifies tasks that support network engagement that will assist the unit to accomplish the mission. Staff processes unique to different sections are synchronized to ensure mutually beneficial support to other sections to achieve integrated staff process products from mission analysis activities.

4-6. Perform Initial Intelligence Preparation of the Battlefield. Identification of what products and supporting actions are required of each staff section is synchronized during staff IPB analysis led by the intelligence staff officer. The staff, utilizing intelligence preparation of the battlefield/battlespace (IPB) products, determine friendly, neutral and threat actors and their supporting networks present in an OE. The staff will also determine those actors and network activities outside of the AO who may have important links to the networks within an OE. When the staff performs IPB, the staff will need to integrate a range of variables, such as operational variables, including: political, military, economic, social, information, infrastructure, physical environment; and time and mission variables in terms of significant aspects of the environment which in turn guide planning for network engagement.

4-7. Determine Specified, Implied, and Essential Tasks. The staff identifies the specified, implied, and essential tasks required to engage networks within an OE.

4-8. Review Available Assets. Identify unified action partners with unique capabilities that contribute to network engagement. The staff considers the specified, implied, and essential tasks required to engage the networks in an OE and the available assets. Information from that analysis is used to identify additional resources required to accomplish the unit's mission.

4-9. Determine Constraints. The commander and staff identify any constraints to engaging networks. These constraints may be political, legal, and cultural for example.

4-10. Identify Critical Facts and Develop Assumptions. The commander and staff identify critical facts and assumptions pertinent to engaging these networks. The commander and staff need to be aware that these facts and assumptions are fluid and can change quickly based on actions within the OE. For example, the commander and staff should be aware when a potential threat is engaged through non-lethal actions and becomes part of the friendly network.

4-11. **STEP 3 — COURSE OF ACTION DEVELOPMENT**. During this step, planners incorporate the network engagement operational approach into the development of courses of action (COAs). Engaging networks, as part of COA development, is implemented through the targeting process.

4-12. **STEP 4 — COURSE OF ACTION ANALYSIS AND WAR-GAMING**. When conducting war-gaming, commanders and staffs need to consider intended and unintended impacts on friendly, neutral, and threat networks. For example, an action to support a friendly network potentially can cause a reaction from the threat network, and requiring a counter action by the friendly network.

TROOP LEADING PROCEDURES

4-13. Troop leading procedures (TLP) extend the MDMP to the small-unit level and provide small-unit leaders a framework for planning and preparing for operations. Leaders begin TLP when they receive the initial warning order or receive a new mission (See FM 6-0) When tasked from higher headquarters, tactical units perform one or more of the three activities of network engagement. Therefore, leaders at the small unit level need to know how to integrate network engagement tasks into TLP. Some of those tasks and the networks that they may affect are depicted in figure 4-3.

		Effect		
		Support	Influence	Neutralize
		Partner	Inform	Isolate
		Resource	Mediate	Security Operations
		Train	Negotiate	Counter Reconnaissance
		Advise	Deter	Disrupt
		Assist		Interdict
Network	Friendly	X	X	
	Neutral	X	X	
	Threat		X	X

Figure 4-3. Network Engagement within TLP

This page intentionally left blank.

Chapter 5
Network Engagement Within the Operations Process

NETWORK ENGAGEMENT COLLABORATION

5-1. Network engagement activities require a shared and collaborative effort across the entire intelligence enterprise, other communities, and specific combatant command down to the BCT (brigade combat team) level. As mentioned in Chapter 3 of this publication, a standardized network link diagramming process will facilitate the transmission of network data and fusion at higher levels. Higher echelons have more time, resources, and expertise to push network engagement analytical products and assessments down to lower level tactical units. This allows tactical units to realistically include network engagement into their operations process.

5-2. Units at lower echelons benefit from understanding network activities at higher levels to gain a broader context of network activities beyond their AO. Therefore, commanders and staffs must think globally when attempting to gain understanding of an OE. For example, a U.S. unit operating in Africa could perform its mission more efficiently by understanding the global nature of the activities that follow. The Lebanese Canadian Bank (LCB) was engaged in money laundering and activities where used cars were purchased and shipped from the U.S. to be sold in Africa. The profits from drugs sold in Europe were mixed with the legitimate profits from car sales in Africa, and those funds were transferred through exchange houses in Lebanon to the LCB. These funds were in fact being diverted to Hezbollah. This money laundering system extended even to Asia where money from the LCB was sent through U.S. accounts to pay Asian suppliers for consumer goods. The activities of networks that units encounter will often be international in scope. (For more information on the Lebanese Canadian Bank example, see the references section of this publication.)

5-3. Theater army level planning for network engagement must involve a range of actors from interagency and non-governmental organizations to multinational partners because theater army enables combatant commands while also enabling the Army to accomplish its strategic roles – prevent, shape, and win. A theater army enables the geographic or functional combatant commands to accomplish its strategic goals by aligning its support to theater security cooperation. Security cooperation is all Department of Defense interactions with foreign defense establishments to build defense relationships that promote specific U.S. security interests, develop allied and friendly military capabilities for self-defense and multinational operations, and provide U.S. forces with peacetime and contingency access to a host nation. (For more on security cooperation, see FM 3-22).

5-4. The theater army conducts security cooperation through sustained military engagement; deterring aggression and violence; and when necessary, by compelling enemy behavioral change or compliance. All theater armies continually conduct security cooperation activities. These interactions are diverse and intended to create a broad array of effects related to networks. For example, security force assistance activities are intended to support friendly networks; humanitarian disaster and civic aid efforts are intended to influence neutral networks, and combating terrorism programs are intended to neutralize threat networks.

5-5. ***Regionally aligned forces*** (RAF) provide a combatant commander with up to joint task force capable headquarters with scalable, tailorable capabilities to enable the combatant commander to shape the environment. They are those Army units assigned to combatant commands, those Army units allocated to a combatant command, and those Army capabilities distributed and prepared by the Army for combatant command regional missions (FM 3-22). RAF include Army total force organizations and capabilities that are forward stationed; operating in a combatant command area of responsibility; supporting from outside the area of responsibility, including providing reach-back assistance. Combatant command requirements determine regional missions. RAF regional mission and training focus include understanding of the assigned OE and the languages, cultures, geography, and militaries of the countries where they are most likely to be employed. The RAF must also be able to support, influence, and neutralize those networks as required by

their assigned mission. Units support joint combined arms operations by developing their individual and unit proficiency in security operations at the tactical level. RAF assist partners in developing security sector programs that professionalize and strengthen their ability to synchronize and sustain security cooperation operations.

5-6. Theater army level organizations must help the global combatant commander in preventing conflict and shaping the security environment. The RAF aids in the establishment of a global landpower network to shape security environments and prevent conflict. Network engagement provides a comprehensive methodology for commanders and staffs to support these requirements.

CORPS AND DIVISION LEVEL

5-7. Contingency and operational planning demands the Army corps and division level units apply network engagement activities through the operations process –plan, prepare, execute, and assess. Additionally, at the tactical level, corps and division commanders and staffs have a responsibility to ensure that lower echelon units receive tailored network engagement support through specific analysis, assessments, products, and tasks. Included within the operations process are the supporting processes of the Army Design Methodology, IPB, information collection, lethal and non-lethal targeting, and assessment.

5-8. Targeting applies to network engagement at all levels. From strategic to tactical, targeting is incorporated into home station training and supported by robust data that supports network analysis and informs the operational plans and tasks that a commander approves. Targeting at corps and division levels requires the synchronization of unified action partner activities. The focus of targeting at the corps level is to shape targets at the operational or tactical level to create a range of options for the friendly force, including the lethal effects of deny, destroy, and neutralize, and the non-lethal effects of co-opt, inform, organize, and influence.

5-9. Figure 5-1 on page 5-3, is an example of engaging a neutral network to achieve the effect of influence. The success of targeting at all levels is assessed by measures of effectiveness and the assessment of the staff of the degree to which intended effects have been achieved. In this example, the unit might use election results as data supporting the metric that measures the extent to which the populace was influenced to support a democratically elected government and an independent country. This is an example of influencing neutral and friendly networks.

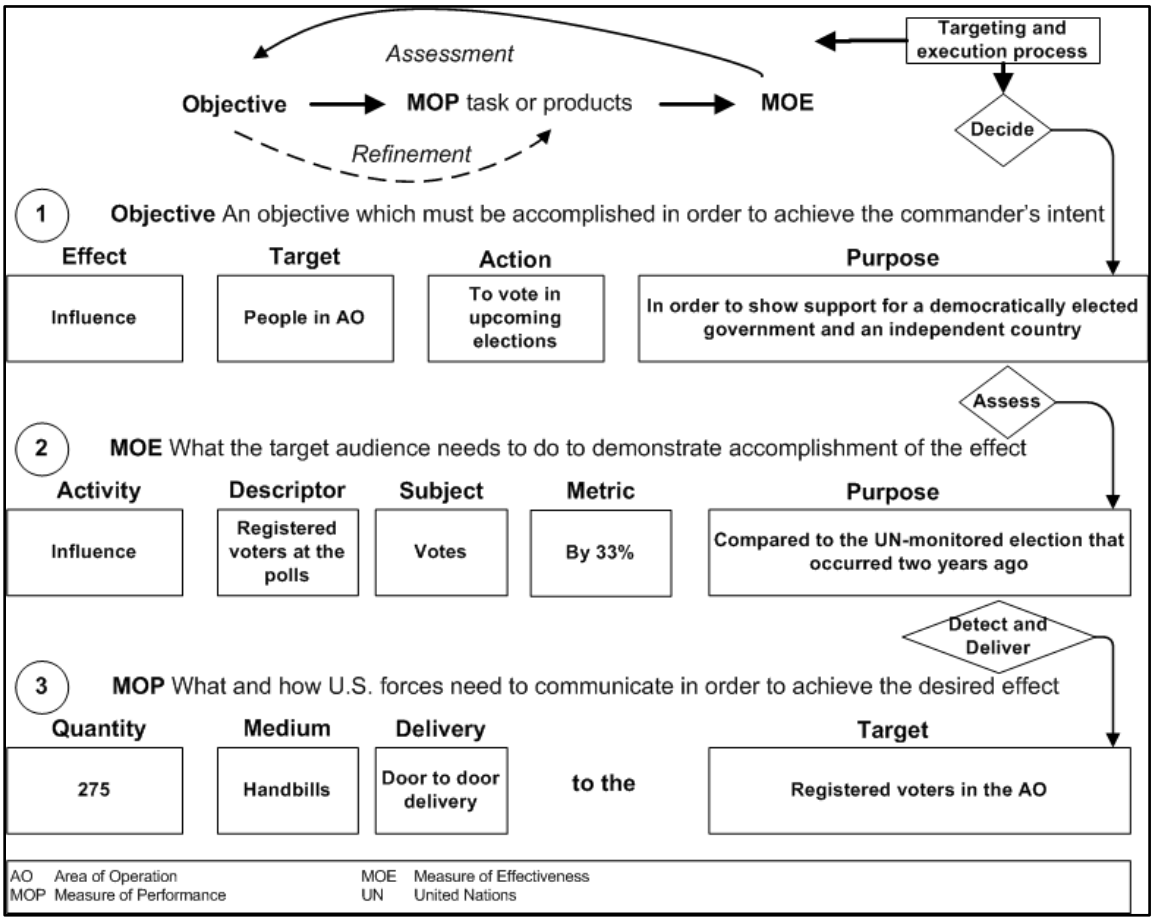


Figure 5-1. Assessment Methodology for the Effect of Influence

BRIGADE COMBAT TEAM AND BATTALION TASK FORCE LEVELS

5-10. The BCT and battalion task force levels have far less analytical capability but must account for network engagement considerations and execute operations in support of network engagement activities. BCT and below units conduct operations that support lethal and non-lethal effects to neutralize threat networks, while supporting and influencing neutral and friendly networks with non-lethal effects based on planning at the division and corps level. At BCT and below levels networks are engaged at their most basic level (node).The targeting working group includes staff who focus on lethal and non-lethal effects, such as representatives from the information operations, civil affairs, public affairs, military information support operations and Staff Judge Advocate cells, to achieve this full range of effects. Targeting working groups develop clear tasks for units to perform, fully considering and articulating the potential operational and strategic effects (intended and unintended) of tactical operations.

RELEVANT INFORMATION

5-11. Planning and executing network engagement requires information from numerous sources. The quantity of organic information collection assets available will vary significantly based on the many factors, however, access across the intelligence enterprise supports all operations. A great deal of relevant information to support the staff's efforts to build situational understanding of networks within an OE comes from information collection, civil affairs, information sharing, and publicly available information.

INFORMATION COLLECTION SUPPORTING NETWORK ENGAGEMENT

5-12. The intent of most Army missions dictates that most, if not all, of the information collection is focused on the threat. A unit that focuses solely on collecting information related to a threat, however, will likely find itself with limited understanding of how the threat exists within the context of its operational environment.

5-13. As previously mentioned, friendly, neutral and threat networks are often interrelated. Some network members' activities or relationships span the friendly, neutral, and threat realms, making networks complex and difficult to understand. Although information collection assets are used to collect information on threat networks, the members of friendly and neutral networks that are sometimes identified by those assets are often the bridge (or spanners) between these networks. For example, a car mechanic by day may also be a vehicle-borne improvised explosive device (VBIED) maker by night. This fact could become known through weapons technical intelligence exploitation of a VBIED, revealing evidence within the device. For this connection to be made, the individual's biometric data would need to be recorded in a database, which implies that operational units require the ability to enter individual's biometric enrollments into a database. While information collection provides most information about individuals in threat networks, including spanners, civil affairs, information sharing, and publicly available information provides most of what is known about friendly and neutral networks in most environments.

5-14. The complex nature of an OE and the networks within it is further complicated by the dynamic nature of networks. As network members are influenced by events and other people, some friendly and neutral members may become threats, while some threat members may become neutral or friendly. Information sources, therefore, should support understanding the combined network of networks, which includes friendly, neutral, and threat networks.

5-15. People and processes, especially those within threat networks, can be difficult to locate when they intentionally hide among the populace. But in many cases, their activities can be detected. For example, the processes, materials, and places associated with drug activity often leave physical and chemical traces that can be found even when no people are present. By understanding and collecting against all of these network elements, more of these network elements are vulnerable to detection and exploitation. As a part of network engagement, it is important to understand small unit information collection doctrine within ATP 3-55.4. Comprehensive information collection supports comprehensive understanding of the networks within an OE.

CIVIL AFFAIRS, INFORMATION SHARING, AND PUBLICALLY AVAILABLE INFORMATION

5-16. A wealth of information on friendly and neutral networks comes from sources, such the civil affairs community, non-governmental organizations (NGOs), historical military documents, social media sites, press reporting, government literature, and the Multinational community. This information can be entered into the operations process through a fusion cell in, or through a U.S. or coalition operations center. One example of what that might look like is provided by the civil military operations center (CMOC). The CMOC is a primary means for coordination between the joint force commander and other stakeholders. The primary purpose of the CMOC is coordination. Because the organizations represented in the CMOC tend to have frequent, direct contact with neutral and friendly networks, they can potentially provide a great amount of information to increase understanding of those networks. In gathering such information, units must be careful to avoid even the appearance of actively collecting intelligence through the CMOC. Information that is freely shared, however, can significantly increase understanding of friendly and neutral networks. (For more on the CMOC, see JP 3-57, FM 3-57, and ATP 3-57.70.)

SUMMARY

5-17. U.S. efforts must take active steps and integrated planning for network engagement in order to properly consider the elements of an OE at all levels, consider the human, cultural, and political elements of an OE and recognize that conflict is not easily divided into discrete levels. These efforts include developing situational awareness and understanding, which are guided by the techniques captured in this publication, to analyze the friendly, neutral and threat human networks within their given operational environment, and fill gaps in their understanding

Source Notes

This division lists sources by page number. Where material appears in a paragraph, it lists both the page number followed by the paragraph number.

5-1, 5-2 The Lebanese Canadian Bank…": U.S. Department of the Treasury, *Treasury Identifies Lebanese Canadian Bank SAL as a Primary Money Laundering Concern, 10 February 2011*. (https://www.treasury.gov/press-center/press-releases/Pages/tg1057.aspx), online.

This page intentionally left blank.

Glossary

SECTION I – ACRONYMS AND ABBREVIATIONS

ADP	Army doctrine publication
ADRP	Army doctrine reference publication
AO	area of operations
ATP	Army techniques publication
BCT	brigade combat team
COA	course of action
CFA	critical factors analysis
CMOC	civil-military operations center
DSF	District Stability Framework
MDMP	military decisionmaking process
OE	operational environment
RAF	regionally aligned forces
SNA	Social network analysis
TLP	troop leading procedures
VBIED	vehicle borne improvised explosive device

SECTION II – TERMS

Army design methodology

A methodology for applying critical and creative thinking to understand, visualize, and describe unfamiliar problems in approaches to solving them. (ADP 5-0)

area of operations

An operational area defined by the joint force commander for land and maritime forces that should be large enough to accomplish their missions and protect their forces. Also called AO. (JP 3-0)

brigade combat team

A combined arms organization consisting of a brigade headquarters, at least two maneuver battalions, and necessary supporting functional capabilities. Also called BCT. (ADRP 3-90)

critical capability

A means that is considered a crucial enabler for a center of gravity to function as such and is essential to the accomplishment of the specified or assumed objective(s). (JP 5-0)

civil-military operations center

An organization normally comprised of civil affairs, established to plan and facilitate coordination of activities of the Armed Forces of the United States with indigenous populations and institutions, the private sector, intergovernmental organizations, nongovernmental organizations, multinational forces, and other governmental agencies in support of the joint force commander. Also called CMOC. (JP 3-57))

critical requirement

An essential condition, resource, and means for a critical capability to be fully operational. (JP 5-0)

critical vulnerability

An aspect of a critical requirement which is deficient or vulnerable to direct or indirect attack that will create decisive or significant effects. (JP 5-0)

information collection

An activity that synchronizes and integrates the planning and employment of sensors and assets as well as the processing, exploitation, and dissemination systems in direct support of current and future operations. (FM 3-55)

information environment

The aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. (JP 3-13)

information operations

(DOD) The integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own. (JP 3-13)

information-related capability

A tool, technique, or activity employed within a dimension of the information environment that can be used to create effects and operationally desirable conditions. (JP 3-13)

operational environment

A composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander. (JP 3-0)

operations process

The major mission command activities performed during operations: planning, preparing, executing and continuously assessing the operation. (ADP 5-0)

regionally aligned forces

Those forces that provide a combatant commander with up to joint task force capable headquarters with scalable, tailorable capabilities to enable the combatant commander to shape the environment. They are those Army units assigned to combatant commands, those Army units allocated to a combatant command, and those Army capabilities distributed and prepared by the Army for combatant command regional missions. (FM 3-22)

stability activities

Various military missions, tasks, and activities conducted outside the United States in coordination with other instruments of national power to maintain or reestablish a safe and secure environment, provide essential governmental services, emergency infrastructure reconstruction, and humanitarian relief. (JP 3-0)

stability tasks

Tasks conducted as part of operations outside the United States in coordination with other instruments of national power to maintain or reestablish a safe and secure environment and provide essential governmental services, emergency infrastructure reconstruction, and humanitarian relief. (ADP 3-07)

targeting

The process of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities. (JP 3-0)

unified action

The synchronization, coordination, and/or integration of the activities of governmental and nongovernmental entities with military operations to achieve unity of effort. (JP 1)

unified action partners

Those military forces, governmental and nongovernmental organizations, and elements of the private sector with whom Army forces plan, coordinate, synchronize, and integrate during the conduct of operations. (ADRP 3-0)

unity of effort

Coordination, and cooperation toward common objectives, even if the participants are not necessarily part of the same command or organization—the product of successful unified action. (JP 1)

This page intentionally left blank.

References

All urls accessed 25 May 2017.

REQUIRED PUBLICATIONS

These documents must be available to intended users of this publication and are available at http://www.apd.army.mil/.

ADRP 1-02. *Terms and Military Symbols*. 16 November 2016.
DOD Dictionary of Military and Associated Terms. May 2017.

RELATED PUBLICATIONS

These documents contain relevant supplemental information.

JOINT PUBLICATIONS

These documents are available at https://jdeis.js.mil/jdeis/index.jsp. Most joint publications are available online: http://www.dtic.mil/doctrine/new_pubs/jointpub.htm

JP 1. *Doctrine for the Armed Forces of the United States* 25 March 2013.

JP 2-01.3. *Joint Intelligence Preparation of the Operational Environment*. 21 May 2014.

JP 3-0. *Joint Operations*. 17 January 2017.

JP 3-13. *Information Operations,* 27 November 2012.

JP 3-15.1. *Counter-Improvised Explosive Device Operations*. 9 January 2012.

JP 3-25. *Countering Threat Networks*. 21 December 2016.

JP 3-57. *Civil-Military Operations*. 11 September 2013.

JP 5-0. *Joint Operation Planning. 11 August* 2011.

ARMY PUBLICATIONS

Most Army doctrinal publications are available online: www.apd.army.mil.

ADP 3-07. *Stability*. 31 August 2012

ADP 5-0. *The Operations Process*. 17 May 2012.

ADRP 3-0. *Operations*. 11 November 2016.

ADRP 3-07. *Stability*. 31 August 2012.

ADRP 3-90. *Offense and Defense*. 31 August 2012.

ADRP 5-0. *The Operations Process.* 17 May 2012.

ATP 2-01.3/MCRP 2-3A. *Intelligence Preparation of the Battlefield/Battlespace.* 10 November 2014.

ATP 2-33.4. *Intelligence Analysis.* 18 August 2014.

ATP 3-55.4. *Techniques for Information Collection During Operations Among Populations.* 5 April 2016.

ATP 3-57.50. *Civil Affairs Civil Information Management*. 6 September 2013.

ATP 3-57.70 *Civil-Military Operations Center.* 5 May 2014.

ATP 3-60. *Targeting*. 7 May 2015.

ATP 5-0.1. *Army Design Methodology.* 1 July 2015.

FM 3-07. *Stability*. 02 June 2014.

FM 3-13. *Information Operations.* 6 December 2016.

FM 3-22. *Army Support to Security Cooperation*. 22 January 2013

FM 3-24. *Insurgencies and Countering Insurgencies*. 13 May 2014.

FM 3-38. *Cyber Electromagnetic Activities.* 12 February 2014.

FM 3-55. *Information Collection.* 3 May 2013.

FM 3-57. *Civil Affairs Operations*. 31 October 2011.

FM 3-90-1. *Offense and Defense Volume 1*. 22 March 2013.

FM 6-0. *Commander and Staff Organization and Operations.* 5 May 2014.

FM 27-10. *The Law of Land Warfare.* 18 July 1956.

RECOMMENDED READINGS

MCoE AtN: https://atn.army.mil/media/FOUOdocs/StaffATNTSPTrifoldV19TDodd99.pdf.

WEBSITES

Asymmetric Warfare Group (AWG): https://www.milsuite.mil/wiki/Department_of_Defense_Social_Network_Analysis_Community_of_Practice.

Asymmetric Operations Working Group (AOWG): https://dnnpro.outer.jhuapl.edu/aowg/Home.aspx (Critical Factors Analysis (CFA).

Carnegie Mellon University Computational Analysis of Social and Organizational Systems (CASOS): http://www.casos.cs.cmu.edu/.

Headquarters Department of the Army (HQDA): http://www.hqda.army.mil/hqda/main/home.asp.

Joint Special Operations University: http://jsou.socom.mil/Pages/Courses.aspx.

Marine Corps Tactical Operations Group: http://www.29palms.marines.mil/Units/MC-Tactics-and-Ops-Group/.

Naval Post Graduate School Defense Analysis Department, Common Operational Research Environment (CORE) Laboratory: https://my.nps.edu/web/core/certficate-program.

United States Military Academy West Point Network Science Center: http://www.westpoint.edu/nsc/SitePages/Home.aspx.

US Army TRADOC G-2 Foreign Military Studies Office: http://fmso.leavenworth.army.mil/.

US Army TRADOC G-2 University of Foreign Military and Cultural Studies/Red Teaming: http://usacac.army.mil/organizations/ufmcs-red-teaming.

MCoE AtN: https://atn.army.mil/media/FOUOdocs/StaffATNTSPTrifoldV19TDodd99.pdf.

PRESCRIBED FORMS

This section contains no entries.

REFERENCED FORMS

Unless otherwise indicated, DA Forms are available on the Army Publishing Directorate (APD) web site: www.apd.army.mil.

DA Form 2028. *Recommended Changes to Publications and Blank Forms.*

Index

Entries are by paragraph number.

A

area of operations, 1-10, 1-36, 3-45, 4-4

army design methodology, 1-26, 4-1, 5-7

B

betweenness, 3-48, 3-50, 3-52

brigade combat team, 1-42, 5-1, 5-10

C

civil-military operations center, 1-35

combatant commander, 5-5—5-6

commanders, 1-1, 1-3—1-5, 1-7, 1-9—1-11, 1-13—1-15, 1-18—1-19, 1-22—1-23, 1-27, 1-29, 1-34, 1-36—1-42, 1-46, 1-48—1-49, 2-6, 2-9, 2-14, 3-1, 3-8, 3-10, 3-13, 3-45, 4-1—4-3, 4-5, 4-12, 5-2, 5-6—5-7

course of action development, 3-44, 4-1, 4-11

critical capability, 3-20, 3-23, 3-51, 3-53

critical requirements, 1-41, 3-20, 3-23—3-24, 3-28, 3-35—3-36, 3-53

D

District Stability Framework, 1-48

E

effects, 1-1, 1-4, 1-8, 1-10, 1-20, 1-39, 1-46—1-47, 2-5, 2-11, 2-17, 3-9, 3-47, 3-49, 3-51—3-52, 5-4, 5-8—5-10
- lethal, 1-1, 5-8, 5-10
- non-lethal, 1-1, 5-8, 5-10

H

human network, analysis, 1-2—1-5, 1-7—1-9, 1-14, 1-17, 1-20—1-21, 1-31, 2-1, 2-3, 2-8, 3-10

human networks, 1-2—1-6, 1-8, 1-12—1-16
- neutralizing, 1-17
- neutral, 1-2, 1-5, 1-8, 1-38—1-39, 2-6, 2-9
- unknown, 1-13, 1-28, 2-1, 2-8
- supporting, 1-8

I

information collection, 1-39, 2-6, 3-9, 3-28, 5-7, 5-11—5-13, 5-15, 5-17

information operations, 1-15, 1-34, 1-37, 1-40, 1-42, 1-44, 2-4, 5-10

information sharing, 5-11, 5-13, 5-16

information-related capabilities, 1-44

infrastructure, 1-12, 1-22—1-23, 1-30, 1-42—1-43, 2-4, 2-6, 2-12, 4-5—4-6

M

meta-network analysis, 1-31, 3-5, 3-12, 3-30, 3-37—3-39, 3-42—3-43

military decisionmaking process, 3-5, 4-1

mission analysis, 3-5, 3-12, 3-14, 4-4—4-5

N

network engagement activities, 1-1—1-2, 1-5—1-7, 1-19—1-20, 1-23, 1-34—1-35, 1-37, 1-42, 1-44, 1-46—1-47, 1-51, 2-4, 3-20, 4-2, 5-1, 5-7, 5-10

network function analysis, 1-31, 3-5, 3-17, 3-22

network functions, 3-17—3-20, 3-22, 3-31, 3-36

nodes, 1-2, 1-4, 2-10, 2-12, 3-32, 3-37—3-38, 3-42—3-43, 3-45, 3-47—3-48, 3-50—3-51

O

operational environment, 1-4, 1-14, 1-24, 1-32, 2-2, 3-1, 3-21, 3-54, 4-1, 4-3, 5-12, 5-17

operational planning, corps and division level, 1-1, 5-7

operations process, 1-1, 1-5, 3-1, 4-1, 5-1, 5-7, 5-16

organizational dynamics, of a network, 3-44—3-45

organizational mapping, 1-31, 3-5, 3-7, 3-10—3-16

R

receipt of mission, 4-4

S

security cooperation, 5-3 —5-4

security cooperation plan, 1-6, 5-3—5-5

situational understanding, 1-34, 1-39, 3-2, 3-4, 3-28, 3-44, 4-5, 5-11

social network, 3-33, 3-38, 3-42—3-43
- analysis, 1-42, 3-12, 3-14—3-15, 3-30, 3-43—3-45, 3-50, 3-54
- stability activities, 1-23, 1-40—1-42

stability tasks, 1-23, 1-39

T

targeting, 1-1, 1-19, 2-10, 3-9, 3-33, 3-52, 4-3, 5-7—5-10

threat human networks, 1-2, 1-5, 1-15, 1-38—1-39, 2-3, 2-5—2-6, 2-10, 5-17

troop leading procedures, 4-13

U

unified action, 1-1, 1-8, 1-10, 1-16, 1-18, 1-28, 1-34—1-36, 1-43, 3-13, 3-34, 3-52, 4-8, 5-8

unified action, synchronization of, 1-1

unified action , partner activities, 1-1, 5-8

unified action, partners, 1-8, 1-10, 1-16, 1-18, 1-28, 1-34—1-35, 1-43, 3-34, 3-52, 4-8

unity of effort, , 1-8, 1-10, 1-34

This page intentionally left blank.

ATP 5-0.6
19 June 2017

By Order of the Secretary of the Army:

MARK A. MILLEY
General, United States Army
Chief of Staff

Official:



GERALD B. O'KEEFE
Administrative Assistant to the
Secretary of the Army
1715905

DISTRIBUTION:
Active Army, Army National Guard, and United States Army Reserve: Distributed in electronic media only (EMO).

PIN: 201963-000