May 2011

Attack the Network Lexicon

DISTRIBUTION STATEMENT D. Distribution authorized to the Department of Defense and U.S. DoD contractors only (Deputy Secretary of Defense Memorandum dated April 2006, Policy on Discussion of IEDs and IED-Defeat Efforts in Open Sources) (20110524), FOIA Exemption 2 applies. Disclosure and release of this document is authorized to ISAF and GCTF coalitions and NATO members. Refer all other requests to the Joint IED Defeat Organization, J5 Division. Provision of this information does not imply a commitment on the part of the United States government to furnish, transfer, or export information or equipment referred to herein.

Attack the Network Lexicon

INTRODUCTION

Attack the Network (AtN) Lexicon

INTRODUCTION

This first edition of the Attack the Network (AtN) Lexicon was produced by the Joint Improvised Explosive Device Defeat Organization (JIEDDO). The lexicon contents were developed after extensive interviews with military units who successfully employed AtN principles and practices to reduce the number and effectiveness of Improvised Explosive Devices (IEDs) in the Counter-Insurgency (COIN) environment where they encountered multiple and sometimes interconnected adversary networks. The lexicon contents were further developed and refined by subject matter experts from over fifty organizations across the Departments of Defense, Justice, and Homeland Security.

PURPOSE

This lexicon is intended to provide a common operational vocabulary across the many organizations and technical/military disciplines who must coordinate their efforts to successfully attack the many different varieties of adversary networks. Adoption and widespread use of the terms in this lexicon will improve information exchange among AtN practitioners at the tactical, operational, and strategic levels. This lexicon will:

- Standardize reporting and improve database content management

- Enable AtN-related education and training

- Serve as an information resource for staffs preparing to enter an AtN operational environment

- Support the harmonization and development of AtN policy and doctrine

SCOPE

While the original requirements and applications that led to the creation of this AtN Lexicon involved IED networks in the COIN environment, the terminology herein is not limited to that particular AtN application. The AtN Lexicon provides terminology commonly used to attack networks in a more generic sense so that this document can be used for AtN in any application domain (IED, drug, criminal, insurgent, etc.)

APPROACH

This lexicon is intended to be a living document that is updated to reflect changes in the state of the art for AtN principles and practices.

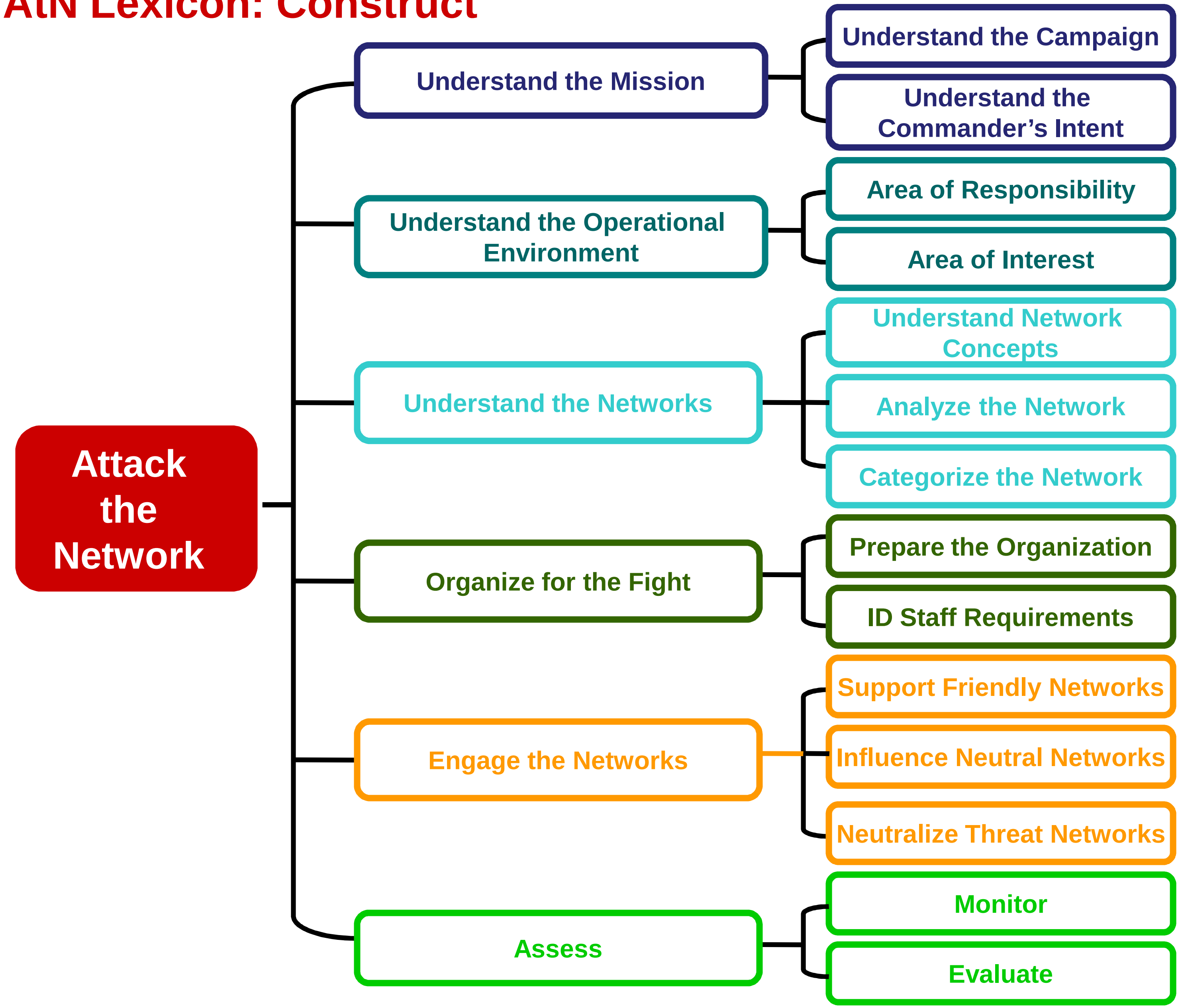
Comments/change proposals or requests for copies (printed or electronic) of the most current version of the Attack the Network Lexicon can be submitted to:

atn_lexicon@jieddo.dod.mil

The field guide will be posted and available to download and print from https://jknife.jieddo.dod.mil, under the C-IED References tab. It will also be available on BICES at http://knife.act.nato.int/portal under C-IED Information and on the Afghan Mission Network on the CENTRIXS-ISAF site http://www.jknife.usa.isaf.cmil.mil under C-IED Resources/CIED References.

CONTENTS

AtN Lexicon: Construct



- Attack the Network
  - Understand the Mission
    - Understand the Campaign
    - Understand the Commander's Intent
  - Understand the Operational Environment
    - Area of Responsibility
    - Area of Interest
  - Understand the Networks
    - Understand Network Concepts
    - Analyze the Network
    - Categorize the Network
  - Organize for the Fight
    - Prepare the Organization
    - ID Staff Requirements
  - Engage the Networks
    - Support Friendly Networks
    - Influence Neutral Networks
    - Neutralize Threat Networks
  - Assess
    - Monitor
    - Evaluate

GENERAL TERMS

Attack the Network (AtN)

This line of operation (LOO) consists of lethal and nonlethal actions and operations against networks conducted continuously and simultaneously at multiple levels (tactical, operational, and strategic) that capitalize on, or create, key vulnerabilities and disrupt activities to eliminate the enemy's ability to function in order to enable success of the operation or campaign.

Understand the Mission

To place AtN operations in the broader operational context in which they are conducted. It has two components: Understanding the Campaign (i.e. the broader objectives that are trying to be achieved) and Understanding the Commander's Intent (i.e. the immediate objectives of current and planned operations) AtN operations must be devised to reinforce and support both components of the mission.

Understand the Operational Environment (OE)

Understanding the operational environment is to comprehend the composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander.

Understand the Networks

Understanding the network or local cells means having an appreciation for the nature of adaptive networked threats, their structure, characteristics, dynamics, and purpose.

Organize for the Fight

Organize for the fight is to identify, organize and direct the resources (personnel, tools and equipment) that are needed to facilitate attack the network operations.

Engage the Networks

To engage the networks is to use lethal and nonlethal means to support, influence, or neutralize network members or cells or an entire network.

Assess

To measure continuously the overall effectiveness of employing joint force capabilities during military operations.

GENERAL TERMS

Arms Control and Disarmament

The identification, verification, inspection, limitation, control, reduction, or elimination of armed forces and armaments of all kinds under international agreement including the necessary steps taken under such an agreement to establish an effective system of international control, or to create and strengthen international organizations for the maintenance of peace.

Nation Assistance (Host-National Support)

National assistance is civil and/or military assistance rendered to a nation by foreign forces within that nation's territory during peacetime, crises or emergencies, or war based on agreements mutually concluded between nations. Nation assistance programs include, but are not limited to, security assistance, foreign internal defense, other US Code Title 10 (DOD) programs, and activities performed on a reimbursable basis by Federal agencies or international organizations.

Foreign Humanitarian Assistance

Foreign humanitarian assistance is programs conducted to relieve or reduce the results of natural or manmade disasters or other endemic conditions such as human pain, disease, hunger, or privation that might present a serious threat to life or that can result in great damage to or loss of property. Humanitarian assistance provided by US forces is limited in scope and duration. The assistance provided is designed to supplement or complement the efforts of the host nation civil authorities or agencies that may have the primary responsibility to render such aid.

Consequence Management

Consequence management are actions taken to maintain or restore essential services and to manage and mitigate problems resulting from disasters and catastrophes. These catastrophes include natural, man-made, or terrorist incidents.

Effective IED Attack

Any IED Event that causes at least one Coalition Force, Afghan National Security Force, and/or Afghan Civilian Casualty.

Ineffective IED Attack

Includes Early Detection (Found and Cleared), Detonation without Casualty, and turn-ins.

IED Efficacy

The number of effective IED attacks divided by the number of IED incidents.

IED Events/Incidents

All IED Events/Incidents regardless of damage or casualty. Includes detonations without casualties, detonations with casualties, found and cleared, turn-ins, interdiction.

GENERAL TERMS

Recovery Operations

Recovery operations are actions taken to search for, locate, identify, recover, and return isolated personnel, human remains, sensitive equipment, or items critical to national security.

Homeland Defense

Homeland defense is the protection of United States sovereignty, territory, domestic population, and critical defense infrastructure against external threats and aggression or other threats as directed by the President.

Civil Support

Civil support is support by the Department of Defense to US civil authorities for domestic emergencies, and for designated law enforcement and other activities. Also known as Defense Support to Civil Authorities (DSCA).

Strikes

Strikes are attacks to damage or destroy an objective or a capability.

Raids

Raids are operations to temporarily seize an area in order to secure information, confuse an adversary, capture personnel or equipment, or to destroy a capability. It ends with a planned withdrawal upon completion of the assigned mission.

Show of Force

A show of forces is an operation designed to demonstrate US resolve that involves increased visibility of US deployed forces in an attempt to defuse a specific situation that, if allowed to continue, may be detrimental to US interests or national objectives.

Enforcement of Sanctions (Peace Enforcement)

Enforcement of sanctions is the application of military force, or the threat of its use, normally pursuant to international authorization, to compel compliance with resolutions or sanctions designed to maintain or restore peace and order.

Protection of Shipping Operations

Protection of shipping is the use of proportionate force by US warships, military aircraft, and other forces, when necessary for the protection of US flag vessels and aircraft, US citizens (whether embarked in US or foreign vessels), and their property against unlawful violence. This protection may be extended (consistent with international law) to foreign flag vessels, aircraft, and persons.

GENERAL TERMS

Freedom of Navigation Operations

Freedom of navigation operations are planned actions to demonstrate US or international rights to navigate air or sea routes.

Peace Operations

Peace operations are organized actions that encompass multiagency and multinational crisis response and limited contingency operations involving all instruments of national power to contain conflict, redress the peace, and shape the environment in order to support reconciliation and rebuilding and facilitate the transition to legitimate governance. Peace operations include peacekeeping, peace enforcement, peacemaking, peace building, and conflict prevention efforts.

Non-combatant Evacuation Operations (NEOS)

Non-combatant evacuation operations are planned actions by the Department of State or other appropriate authority, in conjunction with the Department of Defense, whereby noncombatants are evacuated from foreign countries when their lives are endangered by war, civil unrest, or natural disaster to safe havens as designated by the Department of State.

Line of Operation

Lines of operations are logical lines that connect actions on nodes and/or decisive points related in time and purpose with an objective(s).

Line of Effort

A line of effort is a line that links multiple tasks and missions using the logic of purpose—cause and effect—to focus efforts toward establishing operational and strategic conditions.

Decisive Points

A decisive point is a geographic place, specific key event, critical factor, or function that, when acted upon, allows a commander to gain a marked advantage over an adversary or contributes materially to achieving success.

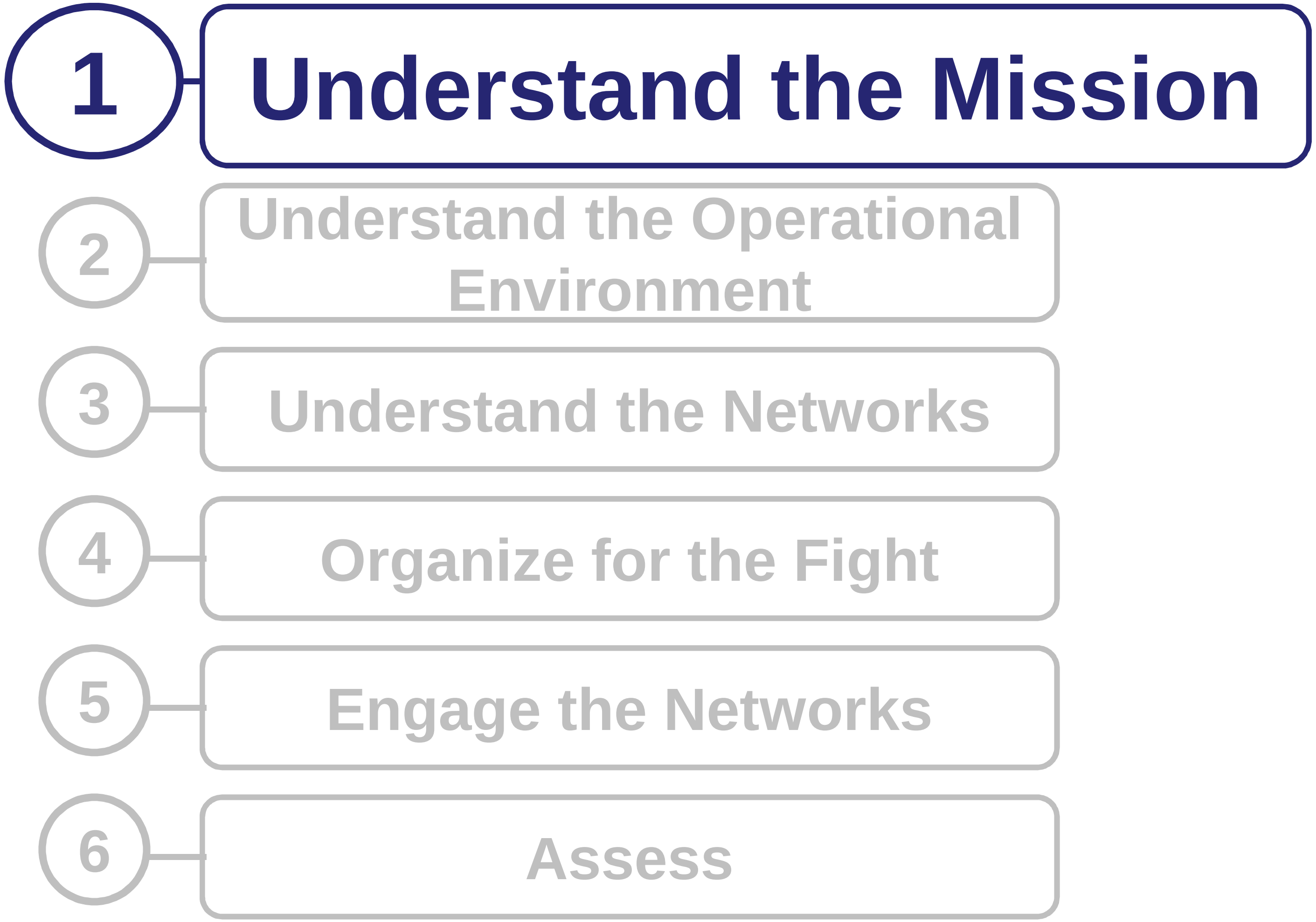
Shaping Operation

A shaping operation is an operation at any echelon that creates and preserves conditions for the success of the decisive operation.

Sustaining Operation

A sustaining operation is an operation at any echelon that enables the decisive operation or shaping operations by generating and maintaining combat power.

Six pillars of Attack the Network:



1 Understand the Mission

2 Understand the Operational Environment

3 Understand the Networks

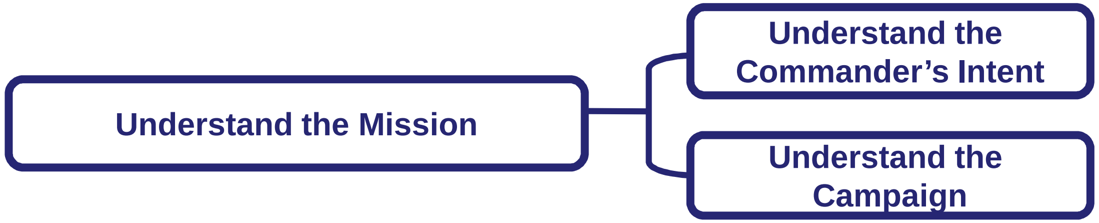
4 Organize for the Fight

5 Engage the Networks

6 Assess

1 UNDERSTAND THE MISSION

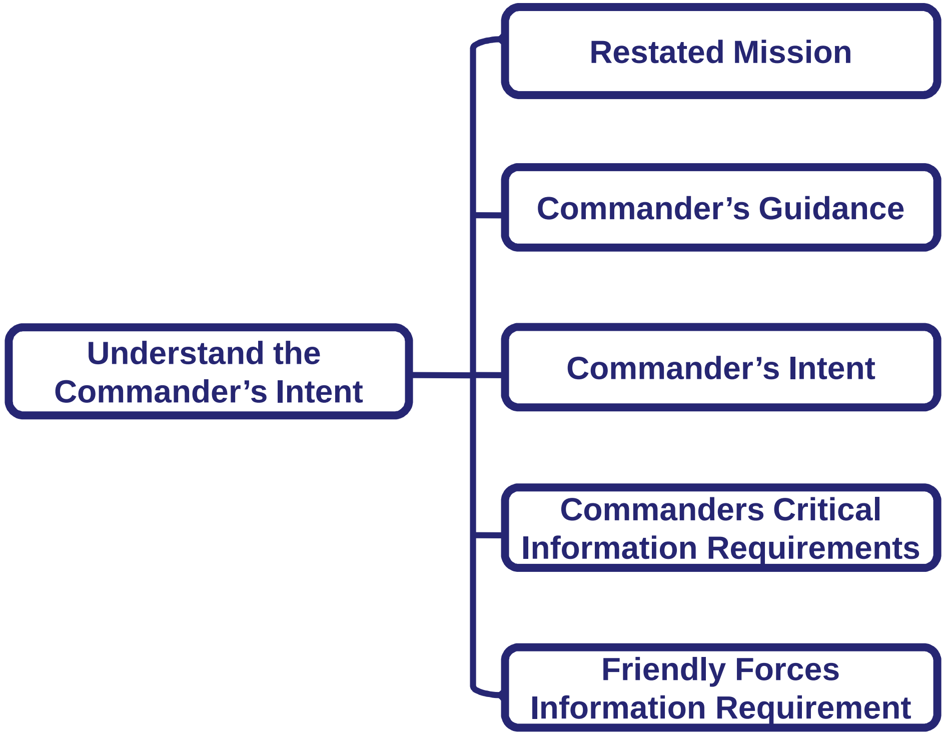
To place AtN operations in the broader operational context in which they are conducted. It has two components: Understanding the Campaign (i.e. the broader objectives that are trying to be achieved) and Understanding the Commander's Intent (i.e. the immediate objectives of current and planned operations) AtN operations must be devised to reinforce and support both components of the mission.



Understand the Mission

Understand the Commander's Intent

Understand the Campaign



Understand the Commander's Intent

Restated Mission

Commander's Guidance

Commander's Intent

Commanders Critical Information Requirements

Friendly Forces Information Requirement

Understand the Commander’s Intent

Understand the Commander’s Intent

Understanding the commander's intent is to comprehend the purpose of the operation and the desired end state. It may also include an assessment of where and how much risk is acceptable during the operation.

Restated Mission

The mission statement after operational planning that is a short sentence or paragraph that describes the organization’s essential task (or tasks) and purpose — a clear statement of the action to be taken and the reason for doing so. The mission statement contains the elements of who, what, when, where, and why, but seldom specifies how. It forms the basis for planning and is included in the planning guidance, the planning directive, staff estimates, the commander’s estimate, the CONOPS, and the completed plan.

Commander’s Guidance

Guidance developed by the commander and staff intended to ensure focused and effective planning, the commander and staff develop and communicate planning guidance that will accompany tentative courses of actions to subordinate and supporting commanders for their estimates of feasibility and supportability. As a minimum, the planning guidance should include the mission statement; assumptions; operational limitations; a discussion of the national strategic end state; termination criteria; military objectives; and the JFC’s initial thoughts on desired and undesired effects. The planning guidance should also address the role of agencies and multinational partners in the pending operation and any related special considerations as required.

Commander’s Intent

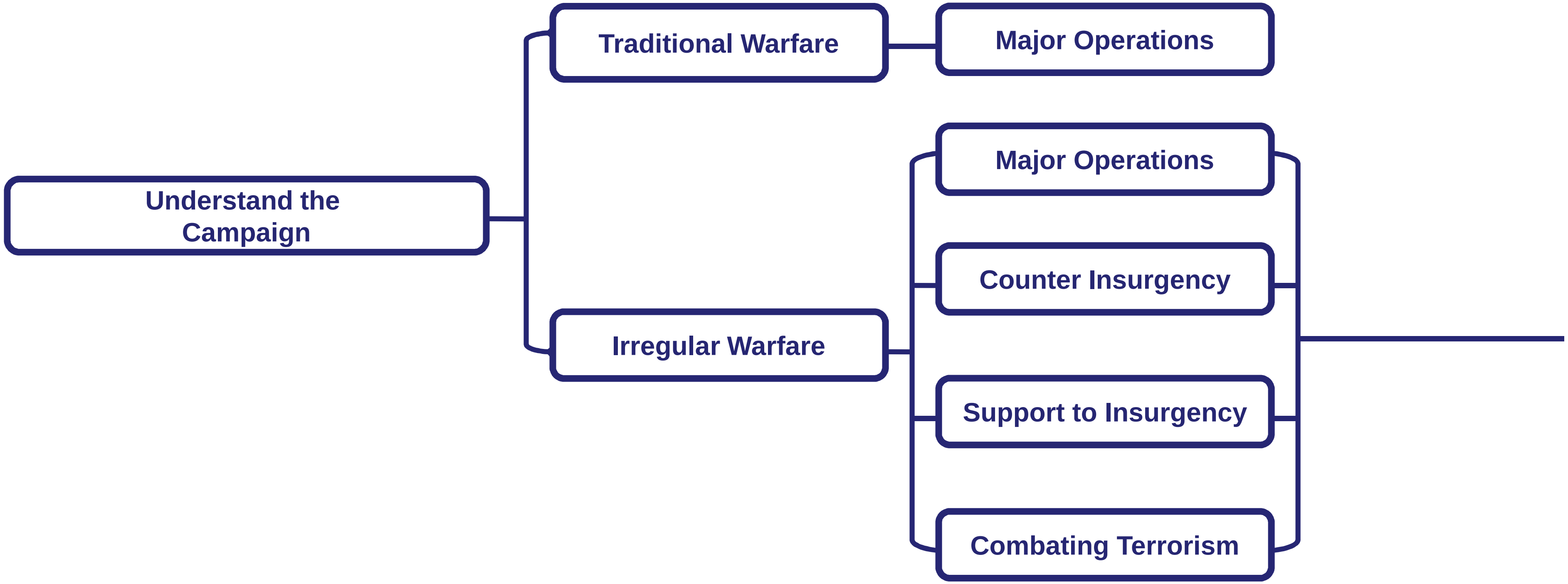
The commander’s intent is a clear and concise expression of the purpose of the operation and the military end state. It provides focus to the staff and helps subordinate and supporting commanders take actions to achieve the end state without further orders, even when operations do not unfold as planned.

Commander's Critical Information Requirement (CCIR)

Commander's Critical Information Requirement (CCIRs) are information requirements identified by the commander as critical for facilitating timely decision-making. The two key elements are friendly force information requirements and priority intelligence requirements.

Friendly Force Information requirement (FFIR)

Friendly Force Information Requirements (FFIRs) are information requirements identified by the commander that are important for understanding the status of friendly force and supporting capabilities.



Understand the Campaign

Traditional Warfare

Major Operations

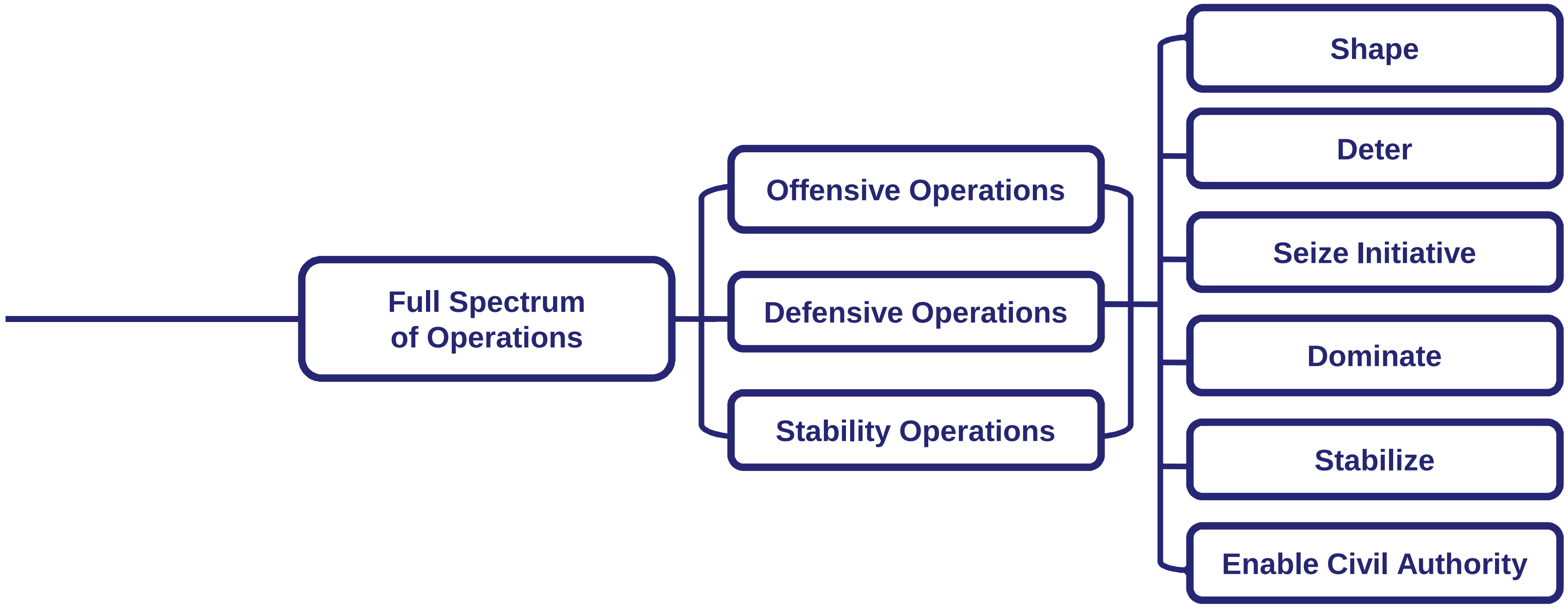
Irregular Warfare

Major Operations

Counter Insurgency

Support to Insurgency

Combating Terrorism


Full Spectrum of Operations
Offensive Operations
Defensive Operations
Stability Operations
Shape
Deter
Seize Initiative
Dominate
Stabilize
Enable Civil Authority

Understand the Campaign

Understand the Campaign

To comprehend a joint operational plan for a series of related major operations aimed at achieving strategic or operational objectives within a given time and space . In an AtN context, understanding the campaign allows planners to design AtN operations that reinforce and support the larger campaign.

Traditional Warfare

Traditional warfare is characterized as a confrontation between nation-states or coalitions/alliances of nation-states.

Major Operations

Major operations are a series of tactical actions (battles, engagements, strikes) conducted by combat forces of a single or several services, coordinated in time and place, to achieve strategic or operational objectives in an operational area. These actions are conducted simultaneously or sequentially in accordance with a common plan and are controlled by a single commander.

Irregular Warfare

Irregular warfare is a violent struggle among state and non-state actors for legitimacy and influence over the relevant population(s). Irregular warfare favors indirect and asymmetric approaches, though it may employ the full range of military and other capacities, in order to erode an adversary's power, influence, and will.

Counterinsurgency

Comprehensive civilian and military efforts taken to defeat an insurgency and to address any core grievances.

Support to Insurgency

To provide aid or comfort to an insurgency, which is an organized, protracted politico-military struggle designed to weaken the control and legitimacy of an established government, occupying power, or other political authority while increasing insurgent control.

Combating Terrorism

Combating terrorism are those actions, including antiterrorism and counterterrorism, taken to oppose terrorism throughout the entire threat spectrum.

Full Spectrum Operations

Offensive, defensive, and stability or civil support operations conducted simultaneously as part of an interdependent joint force to seize, retain, and exploit the initiative, accepting prudent risk to create opportunities to achieve decisive results. They employ synchronized action—lethal and nonlethal—proportional to the mission and informed by a thorough understanding of all variables of the operational environment.

Offensive Operations

Offensive operations are combat operations conducted to defeat and destroy enemy forces and seize terrain, resources, and population centers.

Understand the Campaign

Defensive Operations

Defensive operations are combat operations conducted to defeat an enemy attack, gain time, economize forces, and develop conditions favorable for offensive or stability operations.

Stability Operations

Stability operations encompass various military missions, tasks, and activities conducted outside the United States in coordination with other instruments of national power to maintain or reestablish a safe and secure environment, provide essential governmental services, emergency infrastructure reconstruction, and humanitarian relief.

Shape

To shape is to conduct kinetic and/or nonkinetic actions to manipulate enemy activities.

Deter

To deter is to prevent undesirable action by the adversary by demonstrating the capabilities and resolve of the joint force.

Seize Initiative

To seize the initiative is to execute offensive operations at the earliest possible time, forcing the adversary to offensive culmination and setting the conditions for decisive operations.

Dominate

To dominate is to break the enemy’s will for organized resistance or, in noncombat situations, to control the operational environment. Success in this phase depends upon overmatching joint force capability at the critical time and place.

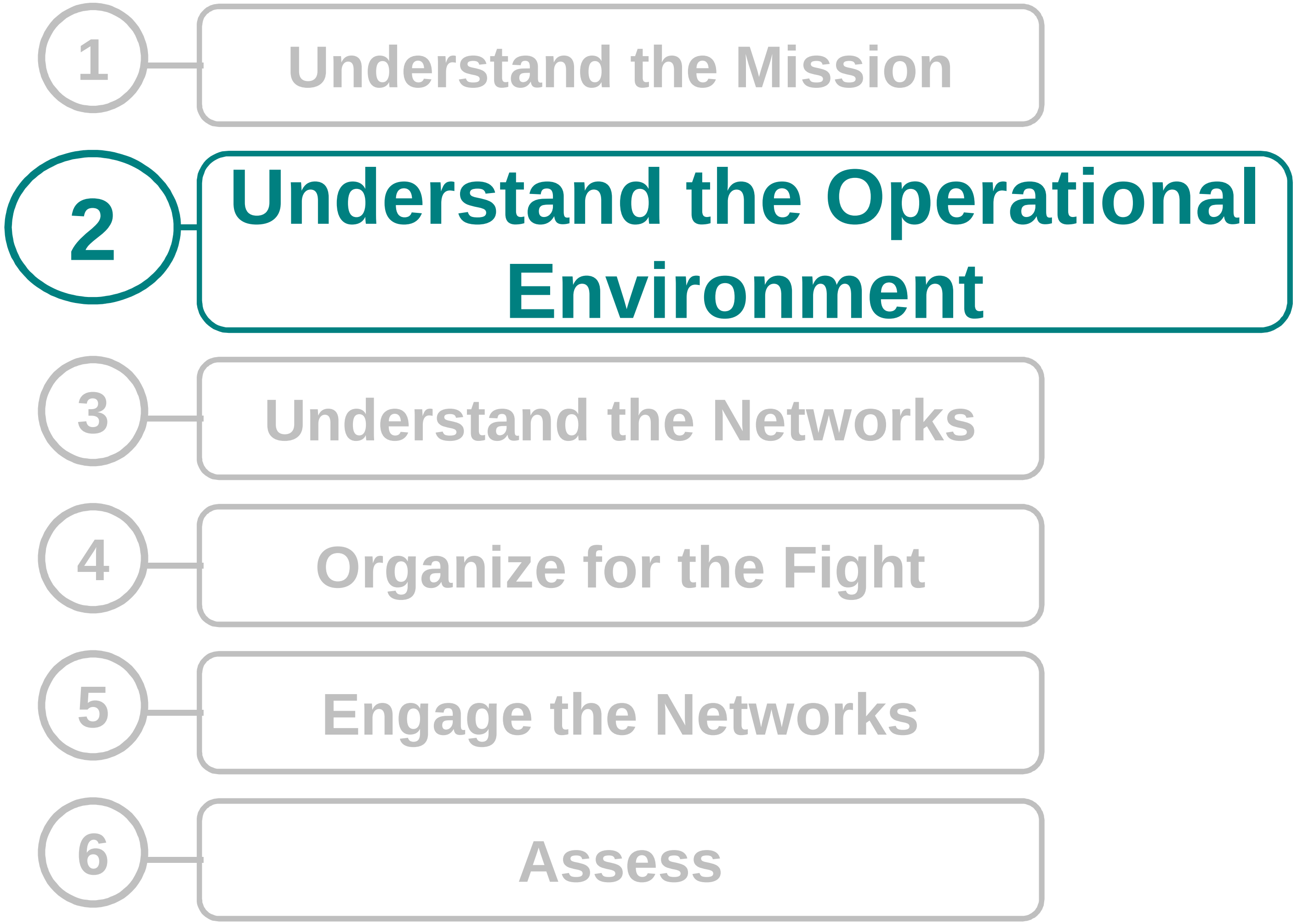
Stabilize

To stabilize is to employ processes by which underlying tensions that might lead to resurgence in violence and a breakdown in law and order are managed and reduced, while efforts are made to support preconditions for successful long-term development.

Enable Civil Authority

To enable civil authority in an operation or campaign is to take those actions that support legitimate civil governance in theater.

Six pillars of Attack the Network:



1 Understand the Mission

2 Understand the Operational Environment

3 Understand the Networks

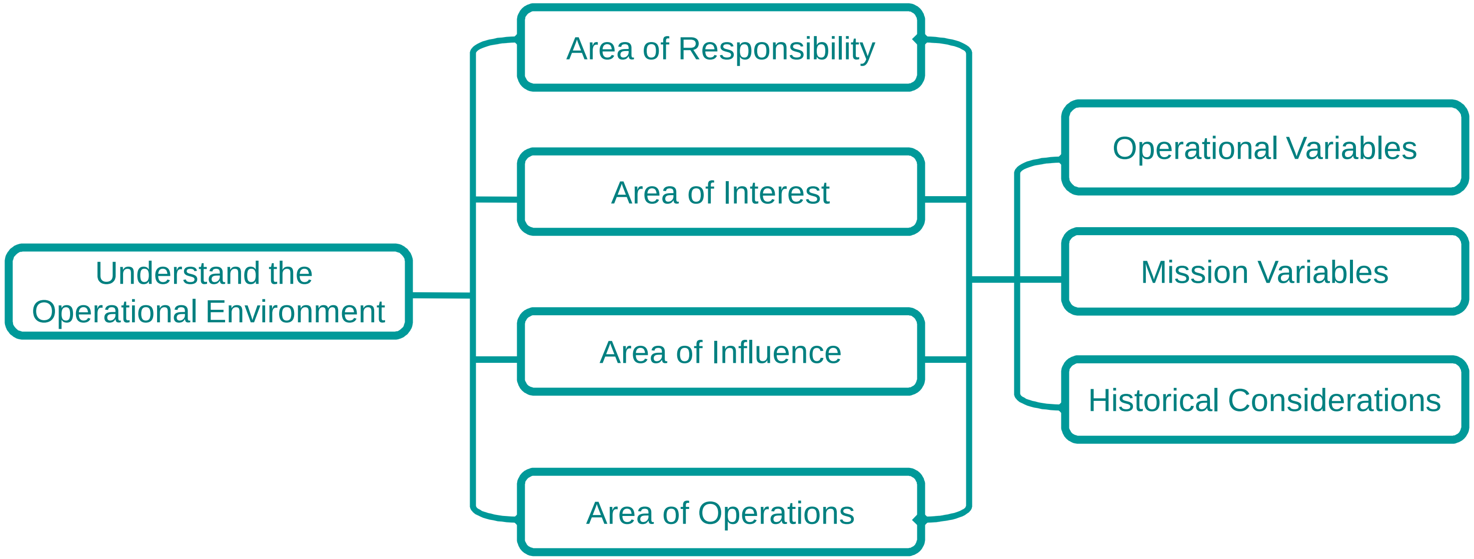
4 Organize for the Fight

5 Engage the Networks

6 Assess

2 UNDERSTAND THE OPERATIONAL ENVIRONMENT

Understanding the operational environment (OE) is to comprehend the "composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander.



Understand the Operational Environment

Area of Responsibility

Area of Interest

Area of Influence

Area of Operations

Operational Variables

Mission Variables

Historical Considerations

Understand the Operational Environment

Area of Responsibility

An area of responsibility is the geographical area associated with a command within which a commander has authority to plan and conduct operations.

Area of Interest

An Area of Interest (AOI) is an area beyond the area of influence that contains forces and/or other factors that could jeopardize friendly mission accomplishment. In combat operations, the AOI normally extends into enemy territory to the objectives of current or planned friendly operations if those objectives are not currently located within the assigned operational area.

Area of Influence

An area of influence is a geographic area in which a commander can directly influence operations by maneuver or fires capabilities normally under the commander's command or control. The area of influence normally surrounds and includes the assigned operational area.

Area of Operations

An area of operations is geographical space on the earth that is defined by the joint force commander for land and maritime forces. Areas of operation do not typically encompass the entire operational area of the joint force commander, but should be large enough for component commanders to accomplish their missions and protect their forces.

Operational Variables

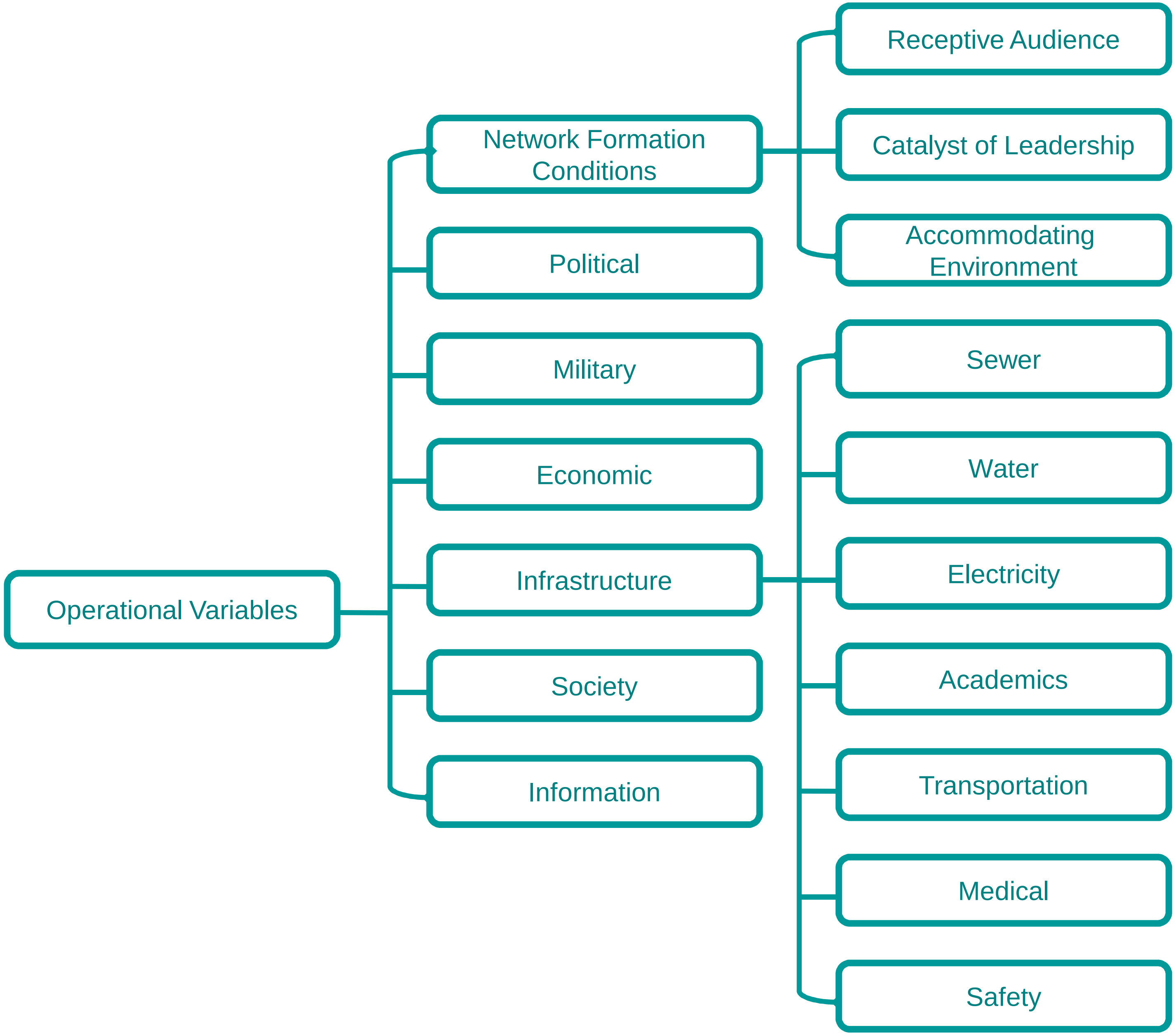
Operational variables are those general factors within an operational environment or situation around which a unit, system, or individual is expected to operate and which may affect performance.

Mission Variables

Mission variables are those aspects of the operational environment that directly affect a mission. They consist of mission, enemy, terrain and weather, troops and support available, time available, and civil considerations.

Historical Considerations

Historical considerations includes the cultural norms, religious beliefs, and past military and political events of a region as they impact the adversary's capabilities and should be considered in operational planning.


Operational Variables
Network Formation Conditions
Political
Military
Economic
Infrastructure
Society
Information
Receptive Audience
Catalyst of Leadership
Accommodating Environment
Sewer
Water
Electricity
Academics
Transportation
Medical
Safety

Operational Variables

Network Formation Conditions

Network formation conditions are those existing state of affairs in the operational environment that allow a series of direct and indirect ties from one actor to a collection of others (a network) to develop.

Receptive Audience

A receptive audience is a body of persons each of whom feels that he has something to gain by engaging in the activities of the network.

Catalyst of Leadership

In the context of network formation a catalyst leader is a motivating person that serves as an initiator for formation of the network. This can but does not necessarily take the form of personal leadership by an individual(s).

Accommodating Environment

The tangible elements (such as infrastructure and terrain) and intangible attributes (such as culture and governance) environment that are required for any network to form or operate.

Political (operational variable)

Political variables are those operational variables that describe the distribution of responsibility and power at all levels of governance.

Military (operational variable)

Military variables are those operational variables that include the military capabilities of all armed forces in a given operational environment.

Economic (operational variable)

Economic variables are those operational variables that encompass individual and group behaviors related to producing, distributing, and consuming resources.

Infrastructure

Infrastructure variables are those operational variables that comprise the basic facilities, services, and installations needed for a society’s functioning.

Sewer

Sewer infrastructure is an artificial usually subterranean conduit to carry off sewage and sometimes surface water (as from rainfall).

Water

Water infrastructure refers to a source, means, or process of supplying water (as for a community) usually including reservoirs, tunnels, and pipelines.

Electricity

Electricity infrastructure consists of the power stations and conduits necessary for delivering electric power to a society.

Academia

Academia is the life, community, or world of teachers, schools, and education.

Operational Variables

Transportation

The range of infrastructure (rail, road, air, etc,) that moves people, property, and commerce within a society. The nature and extent of this infrastructure and the implications to AtN planning must be understood when conducting operations.

Medical

The range of professional services that provide medical care to a society. The nature and extent of this infrastructure and the implications to AtN planning must be understood when conducting operations.

Safety

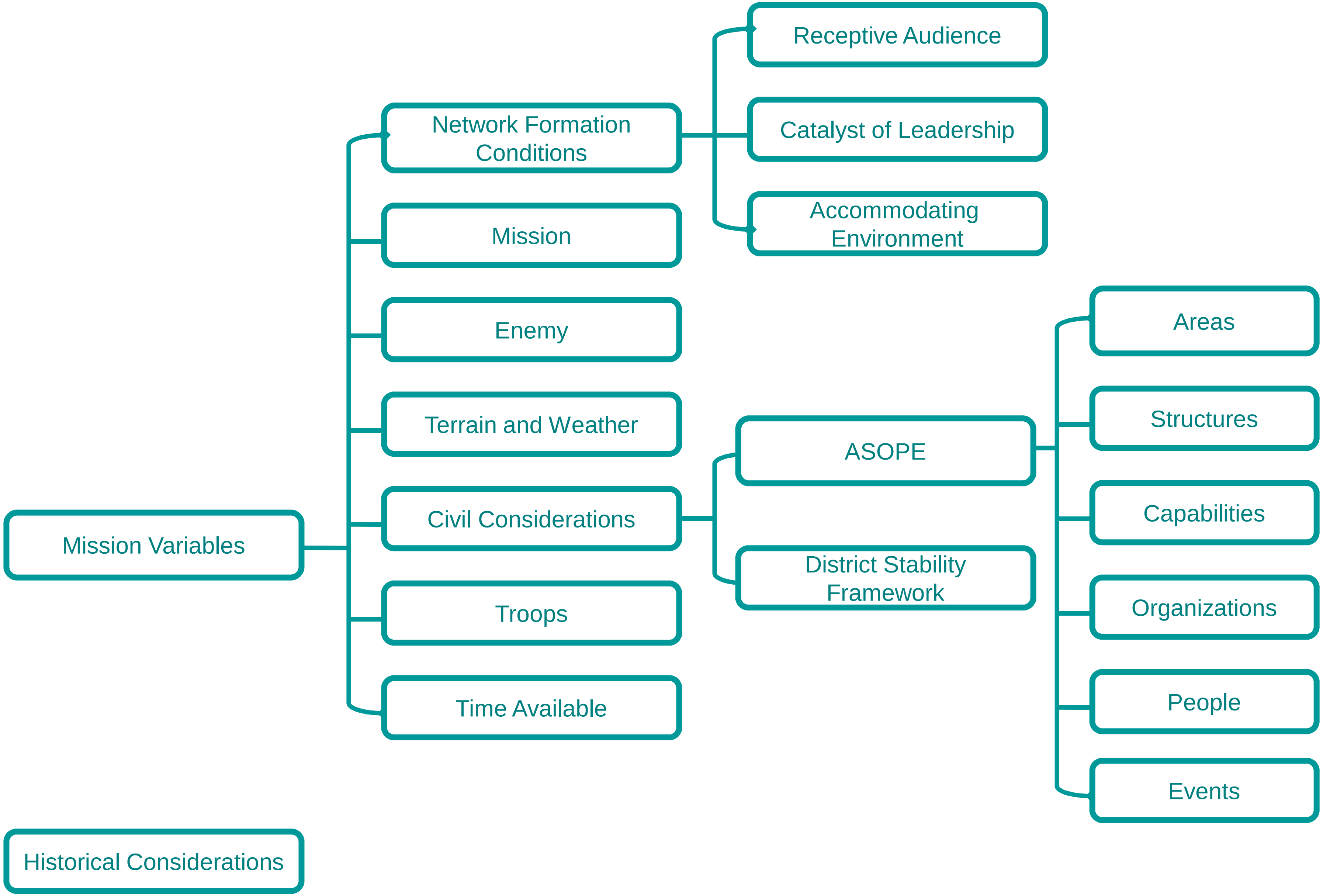
The range of services that protect the people in a society from fire and crime or that respond to disasters. The nature and extent of this infrastructure and the implications to AtN planning must be understood when conducting operations.

Societal

Societal variables are those operational variables that describes societies within an operational environment. A society is a population whose members are subject to the same political authority, occupy a common territory, have a common culture, and share a sense of identity.

Information Variables

Informational variables are those operational variables that whereby individuals, organizations, and systems collect, process, disseminate, or act on information.



Receptive Audience

Network Formation Conditions

Catalyst of Leadership

Accommodating Environment

Mission

Enemy

Areas

Terrain and Weather

Structures

ASOPE

Capabilities

Mission Variables

Civil Considerations

District Stability Framework

Organizations

Troops

People

Time Available

Events

Historical Considerations

Mission Variables

Mission

Identifying the mission before a military action is to determine the task, together with the purpose, that clearly indicates the action to be taken and the reason therefore.

Enemy

An enemy is a party identified as hostile against which the use of force is authorized.

Terrain and Weather

Identifying the terrain and weather before a military action is to determine the natural features (such as rivers and mountains) and man-made features (such as cities, airfields, and bridges) that will affect the mission as well as the effect of the weather on the mission.

Civil Considerations

Civil considerations entails reflecting before the mission how the manmade infrastructure, civilian institutions, and attitudes and activities of the civilian leaders, populations, and organizations within an area of operations will influence the conduct of the mission. *The Marine Corps does not recognize civil considerations as a mission variable.

Mission Variables

ASCOPE

ASCOPE is a memory aid when making civil considerations during mission analysis: areas, structures, capabilities, organizations, people, events .

Areas

Areas in the context of the memory aid ASCOPE are localities or physical terrains that have direct impact on the population and its activities. Examples include tribal regions, police districts, political boundaries, religious boundaries, territorial boundaries, military boundaries, polling stations, and government centers.

Structures

Structures in the context of the memory aid ASCOPE are existing important infrastructure. Examples include hospitals, bridges, communications towers, and power plants.

Capabilities

Capabilities are key functions and services. They include, but are not limited to, administration, safety, emergency services, food distribution, agricultural systems, public works and utilities, health, public transportation, electricity, economics, and commerce. Sewage, water, electricity, trash, medical, and security (SWEAT-MS) are the essential services local authorities must provide.

Organizations

Organizations in the context of the memory aid ASCOPE are groups of individuals that have associated themselves around some purpose or interest. They can be religious, fraternal, criminal, media, patriotic or service, and community watch groups. They include media, IGOs, NGOs, merchants, squatters, and other groups.

People

People in the context of the memory aid ASCOPE are all nonmilitary personnel in the area of interest.

Events

Events in the context of the memory aid ASCOPE are routine, cyclical, planned, or spontaneous activities that significantly affect the operating environment.

District Stability Framework

The District Stability Framework (formerly TCAPF) was a practical framework designed to assist commanders and their staffs identify the causes of instability in an area of operation, develop activities to diminish or mitigate them, and evaluate the effectiveness of the activities in fostering stability.

Mission Variables

District Stability Framework

A practical framework designed to assist commanders and their staffs identify the causes of instability in an area of operation, develop activities to diminish or mitigate them, and evaluate the effectiveness of the activities in fostering stability.

Troops

Identifying the troops before a military action is to determine the number, type, capabilities, and condition of available friendly forces and support that are required for the given mission. These forces include resources from joint, interagency, multinational, host-nation, commercial (via contracting), and private organizations. It also includes support provided by civilians.

Time Available

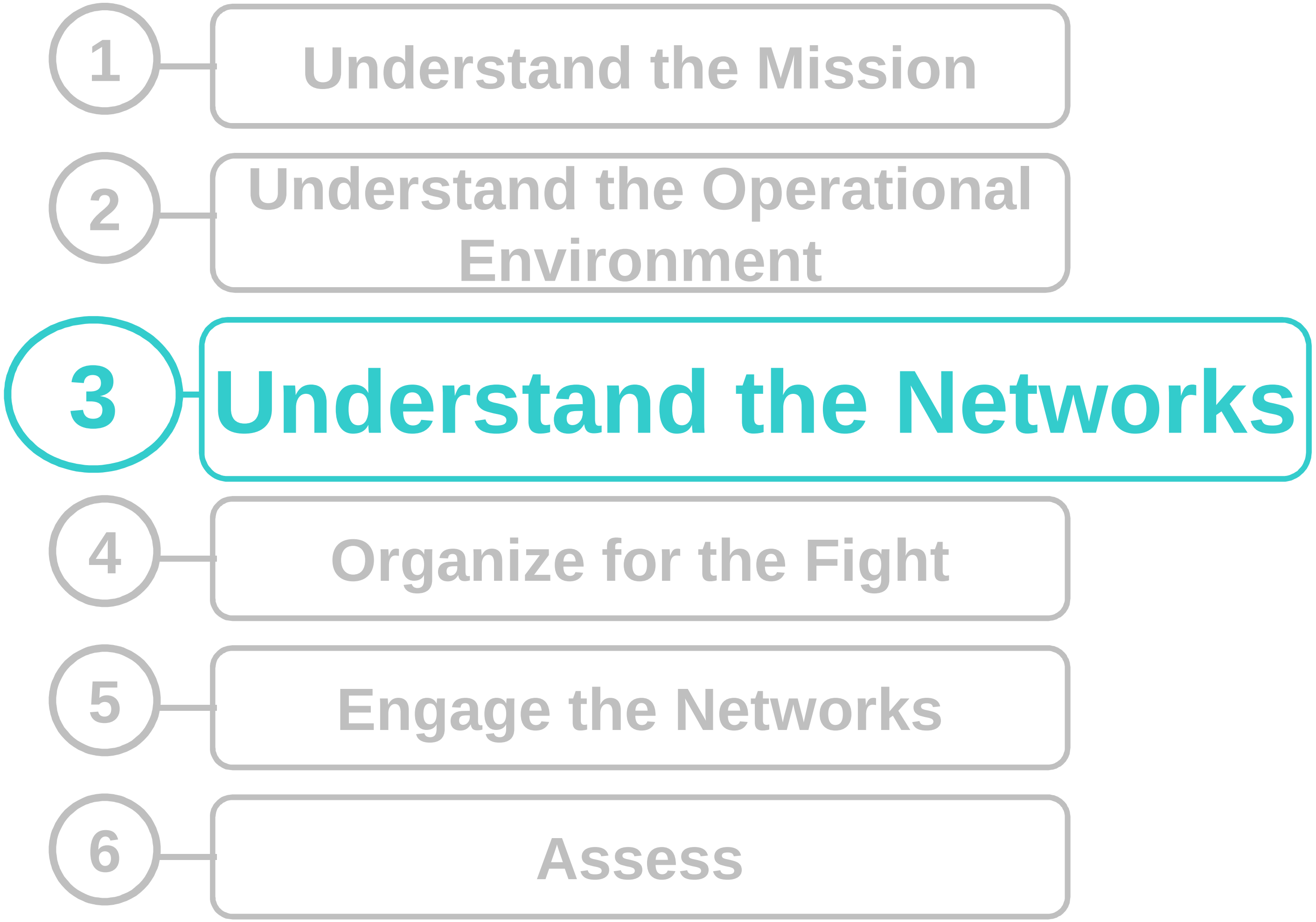
Identifying the time available before a military action is to assess the time available for planning, preparing, and executing the mission. This includes the time required to assemble, deploy, and maneuver units to where they can best mass the effects of combat power. Includes time to plan and prepare operations.

Historical Considerations

Historical Considerations

Historical considerations include the cultural norms, religious beliefs, and past military and political events of a region as they impact the adversary's capabilities and should be considered in operational planning.

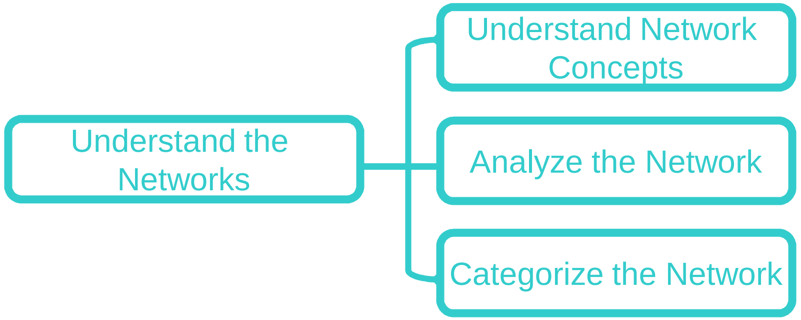
Six pillars of Attack the Network:



1. Understand the Mission
2. Understand the Operational Environment
3. Understand the Networks
4. Organize for the Fight
5. Engage the Networks
6. Assess

3 Understand the Networks

Understanding the network or local cells means having an appreciation for the nature of adaptive networked threats, their structure, characteristics, dynamics, and purpose.



Understand the Networks

Understand Network Concepts

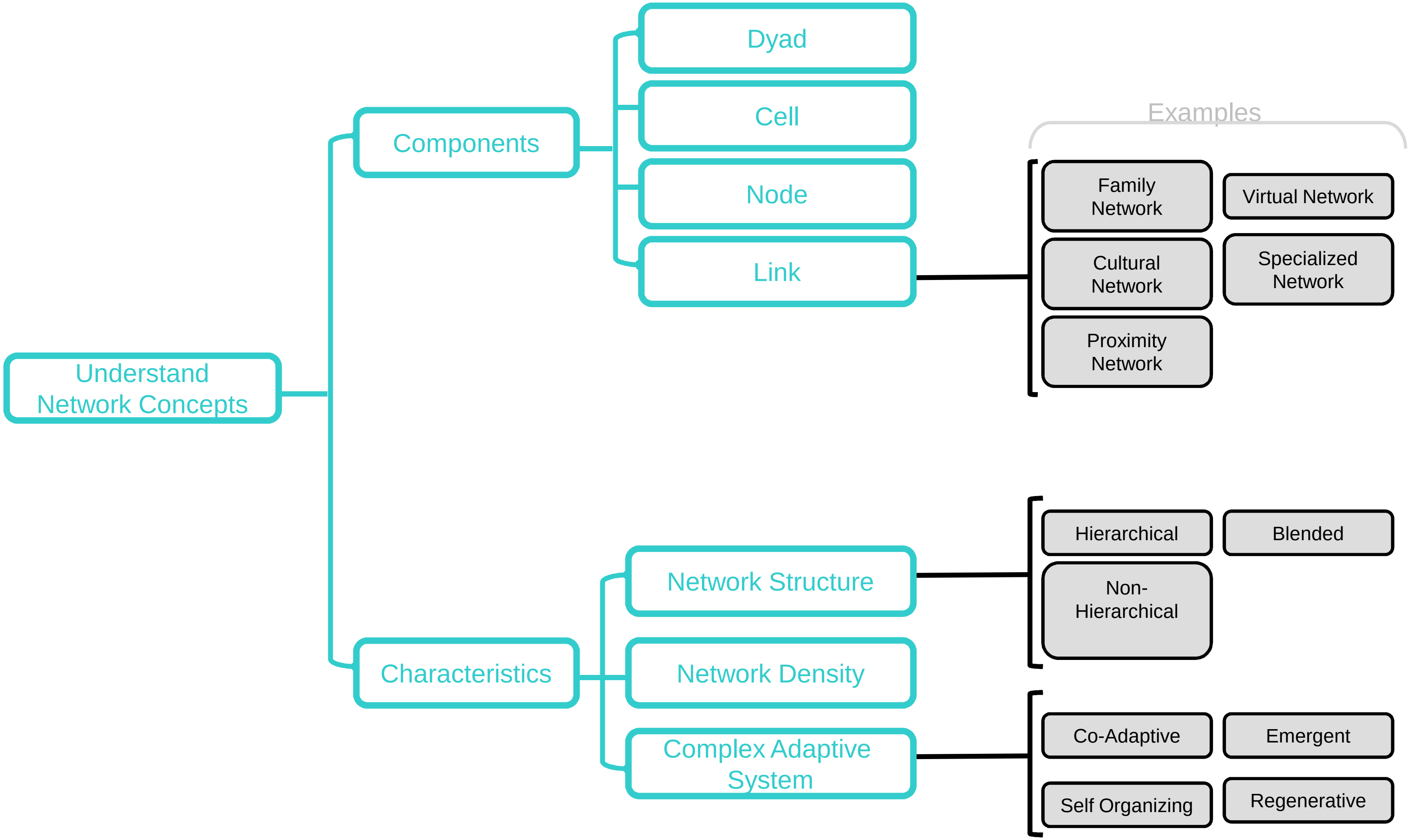
Understanding network concepts is the comprehension of the general characteristics of networks to include network components, network structures, network dynamics, and related concepts and terms.

Analyze the Network

Analyze the Network is the application of analytical techniques to produce intelligence that describes the friendly, neutral, and threat network goals, characteristics, and TTP's, and to understand the operational environment in which they operate.

Categorize the Network

Categorize the Network is the recognition that any network (particularly in a Counterinsurgency environment where the people are the center of gravity) can be considered to be friendly, neutral, or a threat .


Understand Network Concepts
Components
Dyad
Cell
Node
Link
Examples
Family Network
Virtual Network
Cultural Network
Specialized Network
Proximity Network
Characteristics
Network Structure
Network Density
Complex Adaptive System
Hierarchical
Blended
Non-Hierarchical
Co-Adaptive
Emergent
Self Organizing
Regenerative

Understand Networks Concepts

Components

Network components are the elemental parts of a network when graphically mapping a social network.

Dyad

A dyad in a social network analysis consists of two nodes and a single link. Individuals in a network are called actors or nodes. (Actor and node are often used interchangeably.) The contacts between nodes are called links. The basic element of a social network graph is the dyad.

Cell

A cell in social network analysis consists of a small group of individuals who work together for some common purpose.

Node

A node in social network analysis is an element of a system that represents a person, place, or physical thing. Individuals in a network are called actors or nodes.

Link

A link in social network analysis represents the contacts between nodes or actors.

Family Network

A family network is a series of direct and indirect ties among various actors that belong to the same family. These can be cross-generational.

Cultural Network

A cultural network is a series of direct and indirect associations among various actors that belong to the same culture; that is, a shared language, religion, ideology, country of origin and/or sense of identity. Some of these networks may evolve over time from being culturally to proximity based.

Proximity Network

A proximity network is a series of direct and indirect associations among various actors due to the geographical ties of its members (ex. past bonding in correctional or other institutions, or living within specific regions or neighborhoods). Members may also form a network with proximity to an area strategic to their criminal interests (ex. a neighborhood or key border entry point). There may be a dominant ethnicity within the group, but they are primarily together for geographical reasons.

Understand Networks Concepts

Virtual Network

A virtual network is a series of direct and indirect associations among various actors that may never physically meet, but work together through the Internet or other means of communication (ex. networks involved in online fraud, theft or money laundering).

Specialized Network

In a specialized network, individuals come together to undertake activities primarily based on the skills, expertise or particular capabilities they offer.

Characteristics

Characteristics of a human network are the discernible physical, operational, and technical features of a human network.

Network Structure

The network structure shows how an organization is connected, how it behaves, and how its connectivity affects its behavior. Network structure may be a variation of several basic nodal concepts, a node being an individual, a cell, another networked organization, or even a hierarchical organization.

Hierarchical

Hierarchical networks have a well-defined vertical chain of command and responsibility. Information flows up and down organizational channels that correspond to these vertical chains, but may not move horizontally through the organization. This is more traditional, and is common of groups that are well established with a command and support structure. Hierarchical organizations feature greater specialization of functions in their subordinate cells (support, operations, intelligence).

Non-Hierarchical

Non-hierarchical networks are any decentralized decision-making structure.

Blended

A blended network has a structure that is a combination of hierarchical and non-Hierarchical organizations.

Network Density

A property of a network pertaining to the number of nodes connected within the network.

Understand Networks Concepts

Complex Adaptive System

Complex adaptive systems consist of many diverse and autonomous components or parts which are interrelated, interdependent, and behave as a unified whole in learning from experience and in adjusting to changes in the environment.

Co-Adaptive

Symbiotic systems adapt to something that is adapting to it. These systems must continually evolve to survive, and members must adapt to their changing environment and the forces that counter it.

Self Organizing

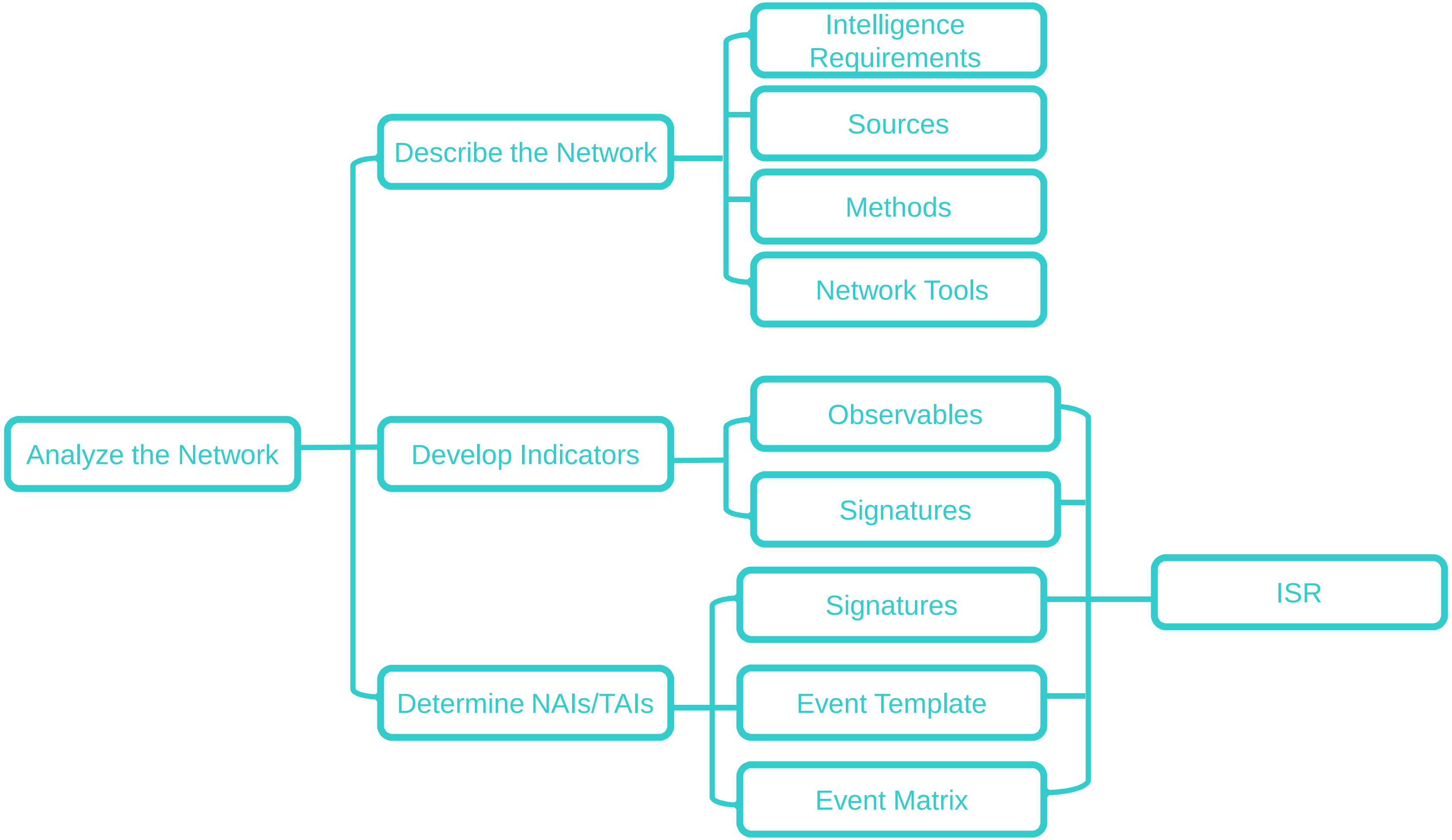
Self-organizing systems operate without a central authority or external element imposing structure upon it. This is basically a ‘bottom up’ developed organization.

Emergent

Emergent systems display characteristics that are ambiguous, that cannot be anticipated from the properties of its components or parts.

Regenerative

A regenerative systems is a complex, adaptive system that can rebuild itself after attack. Removal of a single node has minimal impact on the system as a whole.



Analyze the Network

Describe the Network

Intelligence Requirements

Sources

Methods

Network Tools

Develop Indicators

Observables

Signatures

Determine NAIs/TAIs

Signatures

Event Template

Event Matrix

ISR

Analyze the Network

Describe the Network

An act of characterizing and representing a network to others in words and pictures as accurately to reality as possible in order to make estimates of the network and to take actions against it. This is done through various tools and repeatable approaches.

Intelligence Requirements

Intelligence requirements (IRs) are documented needs for information that when satisfied will fill a gap in the command's knowledge or understanding of the operational environment or threat forces.

Sources

A source of intelligence is a person, thing, activity or agency from which information is obtained.

Methods

Methods for describing the network are the systematic procedures, analytical techniques, or modes of inquiry used to characterize or represent a network.

Network Tools

Network tools are the various collection and analytical systems that enable a network analyst to represent, analyze, and make estimates on networks.

Develop Indicators

In intelligence usage, to develop indicators is to collect information that reflects the intention or capability of an adversary to adopt or reject a course of action.

Observables

Observables are indicators that can be directly or indirectly observed through collection.

Signatures

Signatures are indicators that can be inferred through measurements.

Determine NAIs/TAIs

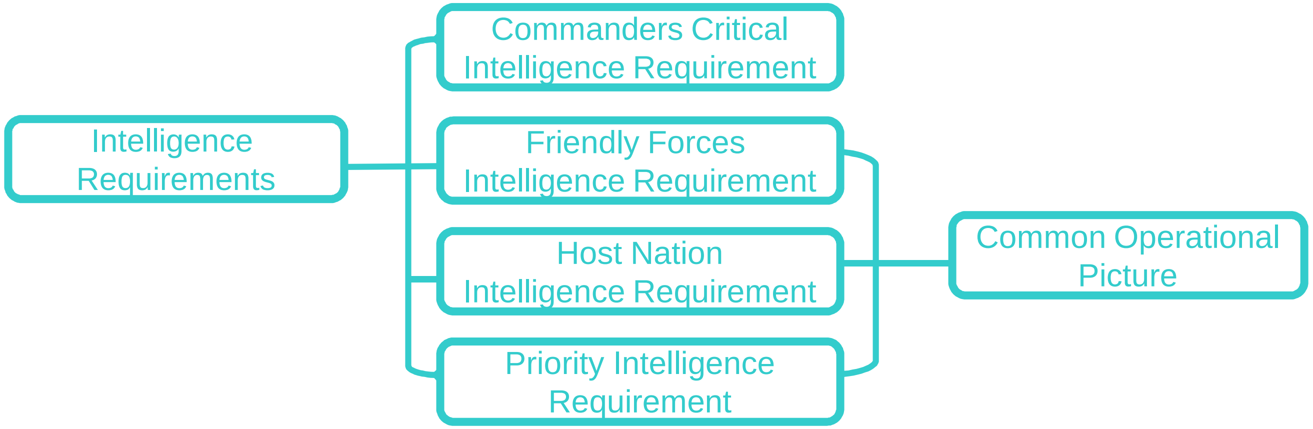
A Named Area of Interest (NAI) is the geospatial area or systems node or link against which information that will satisfy a specific information requirement can be collected. A Target Area of Interest (TAI) is the geographical area where high-value targets can be acquired and engaged by friendly forces.

Event Template

An event template is a guide for collection planning. The event template depicts the named areas of interest where activity, or its lack of activity, will indicate which course of action the adversary has adopted.

Event Matrix

A description of the indicators and activity expected to occur in each named area of interest. It normally cross-references each named area of interest and indicator with the times they are expected to occur and the courses of action they will confirm or deny. There is no prescribed format.



Intelligence Requirements

Commanders Critical Intelligence Requirement

Friendly Forces Intelligence Requirement

Host Nation Intelligence Requirement

Priority Intelligence Requirement

Common Operational Picture

Intelligence Requirements

Host Nation Intelligence Requirement (HNIR)

A Host Nation Intelligence Requirement (HNIR) is an intelligence requirement, stated as a priority for intelligence support, that the commander and staff need answered to understand the host nation's government, defense, or intelligence agencies or their respective activities.

Priority Intelligence Requirements (PIR)

Priority Intelligence Requirements (PIRs) are intelligence requirements that are stated as a priority for intelligence support and that the commander and staff need to understand the adversary or the operational environment. They are subordinate to or lower in priority than Essential Elements of Information (EEIs).

Common Operational Picture

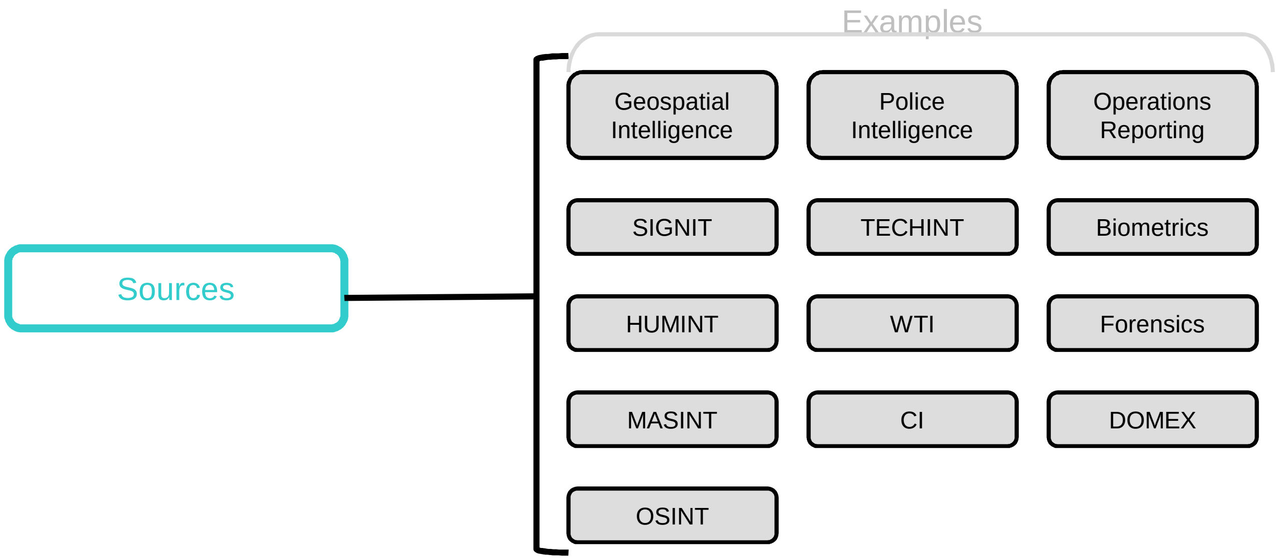
A common operational picture (COP) is a single identical display of relevant information shared by more than one command. A common operational picture facilitates collaborative planning and assists all echelons to achieve situational awareness.

Commander's Critical Information Requirement (CCIR)

See page 13.

Friendly Force Information requirement (FFIR)

See page 13.



Sources
Examples
Geospatial Intelligence
Police Intelligence
Operations Reporting
SIGNIT
TECHINT
Biometrics
HUMINT
WTI
Forensics
MASINT
CI
DOMEX
OSINT

Sources

Geospatial Intelligence

Geospatial Intelligence (GEOINT) is knowledge gained from the exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on the Earth. Geospatial intelligence consists of imagery, imagery intelligence, and geospatial information. Also called GEOINT.

Signals Intelligence (SIGINT)

Signals Intelligence (SIGINT) is a category of intelligence comprising either individually or in combination all communications intelligence, electronic intelligence, and foreign instrumentation signals intelligence, however transmitted.

Human Intelligence (HUMINT)

Human Intelligence (HUMINT) is a category of intelligence derived from information collected and provided by human sources.

Measurement and Signatures Intelligence (MASINT)

Measurement and Signatures Intelligence (MASINT) is a category of intelligence that is obtained by quantitative and qualitative analysis of data (metric, angle, spatial, wavelength, time dependence, modulation, plasma, and hydromagnetic) derived from specific technical sensors for the purpose of identifying any distinctive features associated with the emitter or sender, and to facilitate subsequent identification and/or measurement of the same. The detected feature may be either reflected or emitted.

Police Intelligence

Police intelligence results from the application of systems, technologies, and processes that analyze applicable data and information necessary for situational understanding and focusing policing activities to achieve social order.

Open Source Intelligence (OSINT)

Open Source Intelligence (OSINT) is a category of intelligence that is draw from information that is available to the general public.

Technical Intelligence (TECHINT)

Technical Intelligence is a information derived from the collection, processing, analysis, and exploitation of data and information pertaining to foreign equipment and materiel for the purposes of preventing technological surprise, assessing foreign scientific and technical capabilities, and developing countermeasures designed to neutralize an adversary's technological advantages.

Weapons Technical Intelligence (WTI)

Weapons Technical Intelligence (WTI) is a category of intelligence derived from the forensic and technical collection and exploitation of improvised explosive devices (IEDs), associated components, improvised weapons, and other weapon systems.

Sources

Counterintelligence (CI)

Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities.

Operations Reporting

Operations reporting is a source of information generated in the prosecution of operations.

Biometrics

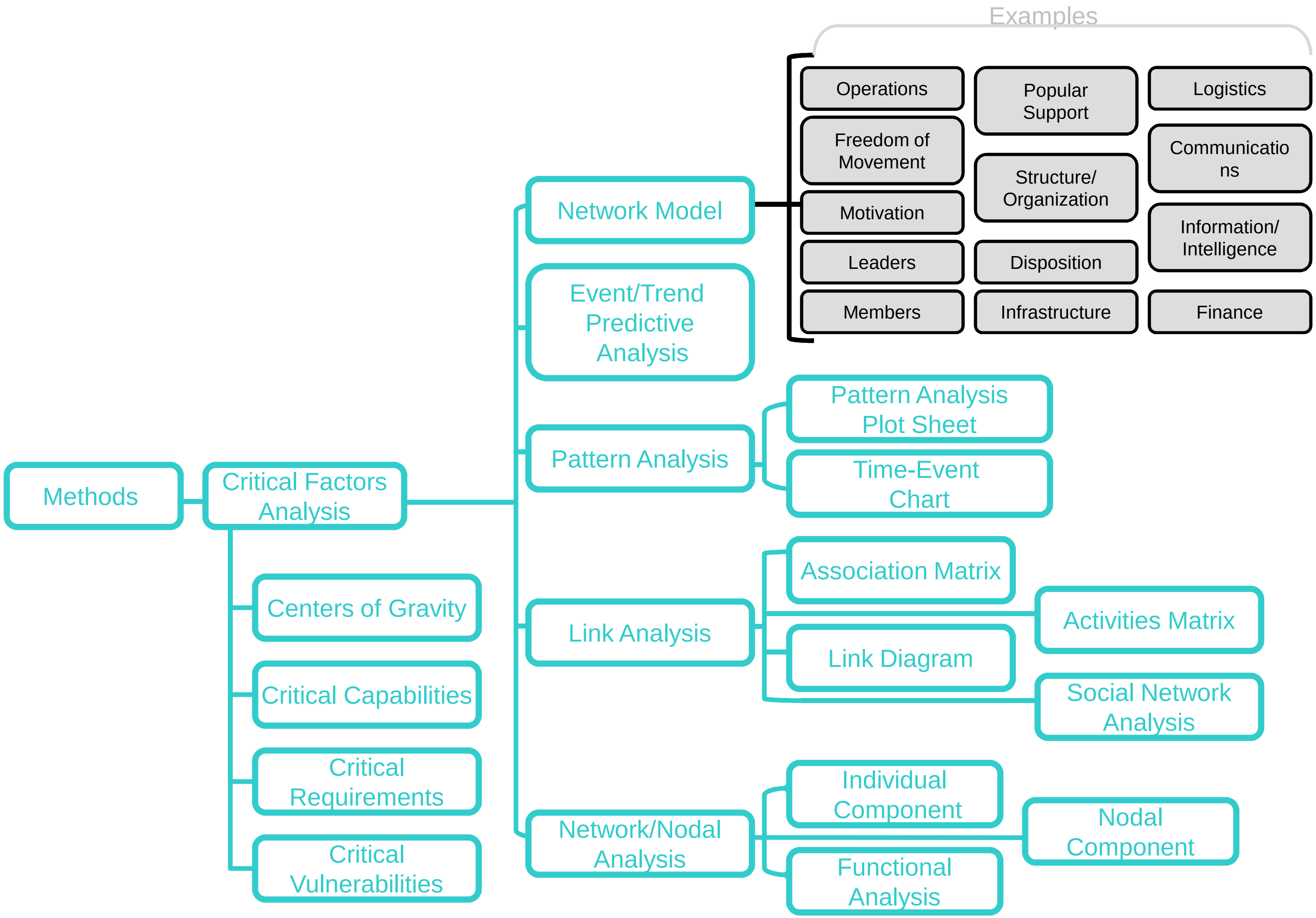
Biometrics is the process of recognizing an individual based on measurable anatomical, physiological, and behavioral characteristics.

Forensics

Forensics is the application of multi-disciplinary science capabilities to establish facts.

Document and Media Exploitation (DOMEX)

The Document and Media Exploitation (DOMEX) center is responsible for the rapid and accurate extraction, exploitation, and analysis of captured enemy documents, media, and material collected during operations.


Examples
Operations
Popular Support
Logistics
Freedom of Movement
Communicatio ns
Structure/ Organization
Motivation
Information/ Intelligence
Leaders
Disposition
Members
Infrastructure
Finance
Network Model
Event/Trend Predictive Analysis
Pattern Analysis Plot Sheet
Pattern Analysis
Time-Event Chart
Methods
Critical Factors Analysis
Association Matrix
Centers of Gravity
Activities Matrix
Link Analysis
Link Diagram
Critical Capabilities
Social Network Analysis
Critical Requirements
Individual Component
Nodal Component
Network/Nodal Analysis
Critical Vulnerabilities
Functional Analysis

Methods

Critical Factors Analysis

Critical Factors Analysis is the methodical examination of the critical capabilities, critical requirements, specific activities, observable and measureable indicators, and critical vulnerabilities of an adversary.

Centers of Gravity

Centers of gravity are the sources of power for an adversary that provide moral or physical strength, freedom of action, or will to act.

Critical Capabilities

Critical capabilities are inherent abilities that enable a CG to function as such. Critical Capabilities “provide the primary capacity for achieving specific objectives.

Critical Requirements

Critical requirements are the essential conditions, resources, and means for a critical capability to be fully operational.

Critical Vulnerabilities

Critical vulnerabilities are aspects of a critical requirement that are deficient in an adversary or vulnerable to direct or indirect attack in him, which when attacked will create decisive or significant effects.

Network Model

Factors representative of a network that can be used as a framework to develop a model of the network.

Operations

The series of actions carried out by the members of a network that are directed toward the objectives of the network.

Freedom of Movement

The conditions for or resources available to a network that allows its actors to move when and where it wants to.

Motivation

Motivation in the network is the source and the degree to which leaders and members of the network are inspired to continue in the operations of the network.

Leaders

Leaders in a network refer to individuals who exhibit the characteristics and the specific personalities of those with authority in the network.

Members

Members in a network refer to individuals who exhibit the characteristics and the specific personalities of those serving in the network.

Popular Support

The degree to which the network has the explicit or implicit backing of the public .

Structure/Organization

The composition of the networks (hierarchical, cellular, etc.).

Disposition

The geographic location of network elements .

Infrastructure

Refers to the physical facilities that a network utilizes to conduct operations.

Methods

Logistics

Logistics is the science of planning, preparing, executing, and assessing the movement and maintenance of forces.

Communications

Communications refers to the kind and quantity of assets that a network uses to exchange information; it also includes the means by which it exchanges information.

Information/Intelligence

Refers to the intelligence system that a network exercises to include the sources it has, the means of collection and analysis, and the persons engaged in the intelligence enterprise.

Finance

Finance refers to the provision of venture or financial capital to another individual, company, or organization, with the expectation that the initial invested principal will be returned with interest, or a specified percentage rate of return; or the provision of funding to another individual, company, or organization; or the provision of loans, trade credit, or similar financial instruments to individuals, companies, or organizations; or the provision of any financial service that promotes, facilitates, or enhances fund-raising, financing, payment, or investment plans, actions, and activities by individuals, companies, or organizations.

Event/Trend Predictive Analysis

Event/trend, and predictive analysis are various analytical methods that attempt to anticipate enemy behavior based on past behavior.

Pattern Analysis

The use of prior actions and activities to identify trends in activities or behaviors. Once identified, these patterns can be used to predict future enemy actions and to plan ISR activities.

Pattern Analysis Plot Sheet

A pattern analysis plot sheets helps distinguish patterns in activities associated with particular days, dates, or times when they are depicted graphically. Analysts may choose to modify this product to track longer or shorter period as appropriate.

Time-Event Chart

The time event chart is a chronological record of an individual's or a group's activities. It is designed to store and display large amounts of information in as little space as possible.

Link Analysis

Link analysis is an analytical method for determining the relationships between critical personalities and members within their network.

Methods

Association Matrix

The association matrix displays a relationship between individuals. It reflects associations within a group or similar activity, and is based on the assumption that people involved in a collective activity know one another. The format of an association matrix is a right angle; each name requires a row and column. The association matrix shows known and suspected associations. Analysts determine a known association by "direct contact" between individuals. Direct contact is defined as face-to-face meetings or confirmed telephonic conversation between known parties and all members of a particular organization. This is depicted as a filled circle and placed in the square where the two names meet within the matrix. An unfilled circle indicates suspected or weak associations. When an individual dies, a diamond is added at the end of his or her name.

Activities Matrix

The activities matrix determines connectivity between individuals and anything other than persons (interest/entity). The activities matrix reveals an organization's membership, organizational structure, cell structure and size, communications network, support structure, linkages with other organizations and entities, group activities and operations, and, national or international ties.

Link Diagram

A link diagram depicts the linkages in a network between actors, their interests, entities, events, organizations, or other factors.

Social Network Analysis

Social network analysis (SNA) is a tool for understanding the organizational dynamics of an insurgency and how best to attack or exploit it. It allows analysts to identify and portray the details of a network structure.

Network/Nodal Analysis

Nodal analysis is a qualitative examination of the interrelationships and interactions among multiple target systems to determine the degree and points of interdependence and linkages of their activities. Nodal analysis results in the identification of the specific functional nodes that empower that network.

Individual Component

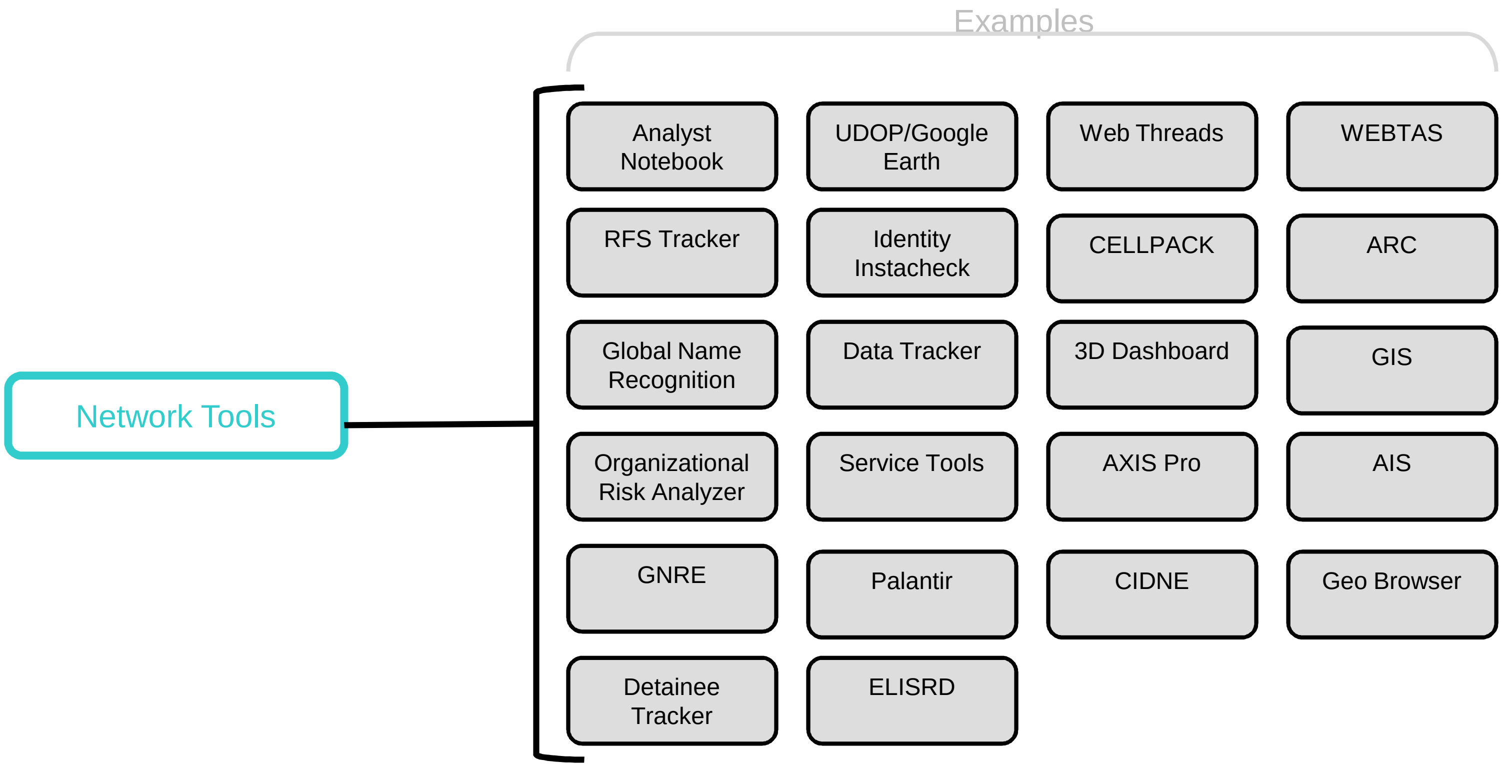
When conducting nodal analysis, a component is a constituent part of the network.

Nodal Component Analysis

Nodal component analysis is the analysis of how nodes of a designated system function in relation to one another.

Functional Analysis

In network nodal analysis, functional analysis is the examination of the purposes of the network and its components.



Network Tools

Examples

- Analyst Notebook
- RFS Tracker
- Global Name Recognition
- Organizational Risk Analyzer
- GNRE
- Detainee Tracker
- UDOP/Google Earth
- Identity Instacheck
- Data Tracker
- Service Tools
- Palantir
- ELISRD
- Web Threads
- CELLPACK
- 3D Dashboard
- AXIS Pro
- CIDNE
- WEBTAS
- ARC
- GIS
- AIS
- Geo Browser

Network Tools

Analyst Notebook

Analyst Notebook is a commercial link analysis and visualization tool that quickly turns large sets of disparate information into high-quality and actionable intelligence to prevent crime and terrorism.

RFS Tracker

RFS Tracker is a database created in-house at the JIEDDO COIC to document and track requests for support from the warfighter.

Global Name Recognition

The Global Name Recognition System is a commercial product used by the COIC that constraints the best of breed technologies designed to address specific needs and demands of managing, searching, analyzing, and comparing multicultural name and data fields.

Organizational Risk Analyzer

Organizational Risk Analyzer (ORA) is a dynamic meta-network assessment and analysis tool developed by CASOS at Carnegie Mellon. It contains hundreds of social network, dynamic network metrics, trail metrics, procedures for grouping nodes, identifying local patterns, comparing and contrasting networks, groups, and individuals from a dynamic meta-network perspective. ORA has been used to examine how networks change through space and time.

Global Name Reference Encyclopedia (GNRE)

The Global Name Reference Encyclopedia (GNRE) is a JIEDDO COIC tool that includes much of the detailed information that one needs in order to perform name analysis work on networks.

Detainee Tracker

The Detainee Tracker is a JIEDDO COIC tool that searches for intelligence on released detainees in order to discover those actor who have reengaged on the battlefield.

UDOP/Google Earth

A JIEDDO/COIC data-mining tool that supports the situational awareness through the delivery of products formatted for geospatial visualization.

Identity Instacheck

Identify Instacheck is a COIC tool that provides identity resolution support and analysis by massing and fusing sources of contextual data and results of biometric matches.

Data Tracker

The COIC tool is a web-deployable client application that converts tracking data in MS Excel format to Google Earth.

Service Tools

Service tools are the various collection and analytical systems procured by a service (Air Force, Navy, Army, or Marine Corps) that enable a network analyst to represent, analyze, and make estimates on networks.

Network Tools

Palantir

Palantir is a commercial tool used by the JIEDDO COIC that integrates, visualizes, and analyzes various data, to include structured, unstructured, relational, temporal, and geospatial data.

ELISRD

ELISRD is an ISR analysis tool used by the JIEDDO COIC that automatically correlates ISR coverage with user driven points of interest or key events in theater to highlight "exploitation opportunities."

Web Threads

Web Threads is a JIEDDO COIC tool to assist Counter Threat and Force Protection analysts corroborate human intelligence reporting of Terrorist/Force protection threats through the fusion of space systems-generated data.

CELLPACK

CELLPACK is a program used by the JIEDDO COIC to analyze and data mine a list of phone numbers in order to return multiple results as an HTML page.

3D Dashboard

The 3D Dashboard is a tool used by the JIEDDO COIC to view, navigate, and mark 3D map models.

AXIS Pro

Axis Pro is a JIEDDO COIC tool that links entities to original data sources and enables advanced queries of data contained with separate link nodal projects.

Combined Information Data Exchange Network (CIDNE)

Combined Information Data Exchange Network (CIDNE) is the CENTCOM-directed reporting tool within Iraq and Afghanistan. CIDNE serves as the primary bridge between disparate communities who might not otherwise share data by providing a standardized reporting framework across intelligence and operations disciplines. This common framework allows structured operational and intelligence information to be shared vertically and horizontally as part of flexible, user-defined workflow processes that collect, correlate, aggregate and expose information.

WebTAS

WebTAS is a Government Off-The-Shelf (GOTS) software toolkit providing visualization, integration and analysis of disparate data in a Service Oriented Architecture (SOA) compliant platform. Built using non-proprietary software, WebTAS provides both Java thick client and web browser-based access, visualization and analysis capabilities.

ARC/GIS

ARC/GIS is a system for people who rely on accurate geographic information to make decisions. It facilitates collaboration and lets you easily author data, maps, globes, and models on the desktop and serve them out for use on a desktop, in a browser, or in the field, depending on the needs of your organization.

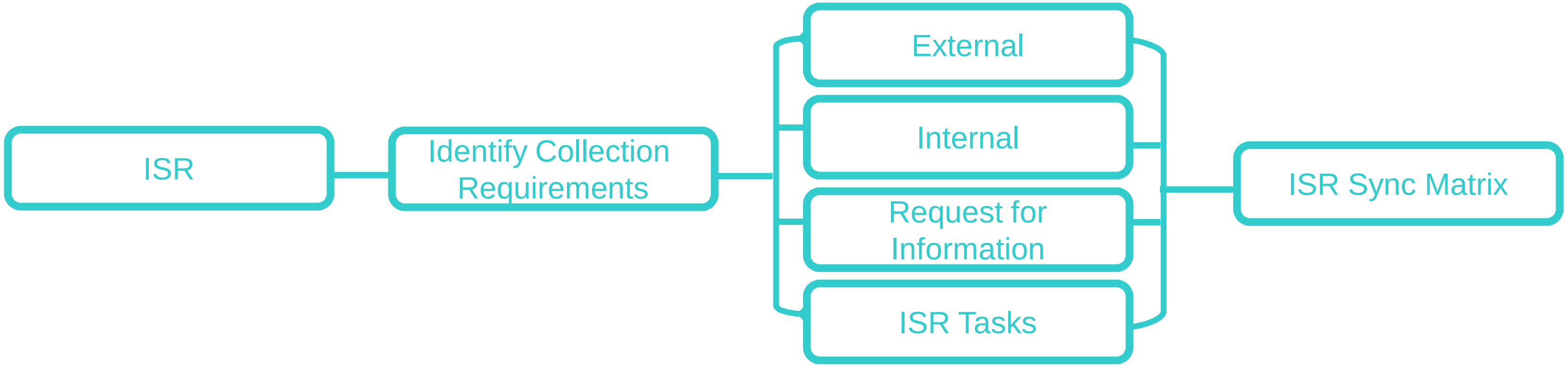
Network Tools

Automated Information System (AIS)

Automated Information System is an assembly of computer hardware, software, and/or firmware configured to collect, create, communicate, compute, disseminate, process, store and/or control data or information.

Geo Browser

GEO Browser is a tool used by the JIEDDO COIC for situational awareness and data mining. The tool displays and correlates the COIC Multi-INT Core both spatially and temporally.



ISR

Identify Collection Requirements

External

Internal

Request for Information

ISR Tasks

ISR Sync Matrix

ISR

Provide ISR collection recommendations

To provide ISR collection recommendation is to make informed suggestions to an authority on the proper sequence and combination of ISR collection assets based upon the mission at hand.

External ISR collection capabilities

External ISR collection capabilities are those intelligence, surveillance an reconnaissance collection assets that are non-organic to a unit and must be requested.

Internal ISR collection capabilities

Internal ISR collection capabilities are those intelligence, surveillance and reconnaissance collection assets that are organic or natural to a unit and therefore do not have to be requested for their utilization.

Request for Information (RFI)

A Request for Information (RFI) is any specific, time-sensitive, ad hoc requirement for intelligence information or products to support an ongoing crisis or operation not necessarily related to standing requirements or scheduled intelligence production. An RFI can be initiated to respond to operational requirements and will be validated in accordance with the combatant command's procedures.

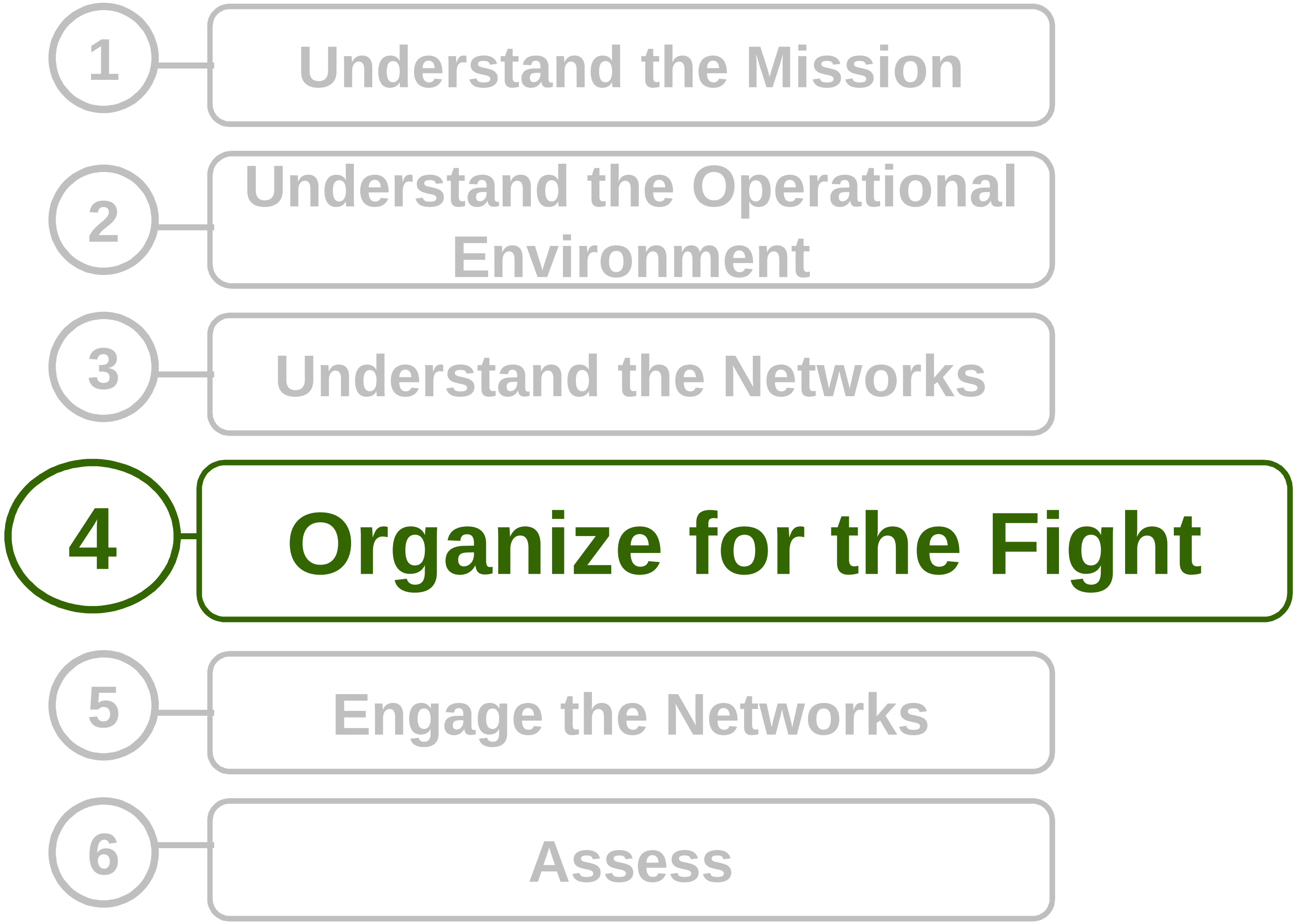
ISR Tasks

ISR tasks are the actions of the intelligence collection effort. These actions synchronize or integrate the planning and operation of sensors, assets, and processing, exploitation, and dissemination systems in direct support of current and future operations.

ISR Sync Matrix

The ISR sync matrix is a tool to plan and direct the collection effort. It may consist of a list of available collection means, plus brief notes or reminders on current intelligence requirements and specific information to collect. The S-2 section initially prepares the ISR synchronization matrix, which the ISR working group completes, and the S-3 authorizes as part of the ISR plan.

Six pillars of Attack the Network:



1 Understand the Mission

2 Understand the Operational Environment

3 Understand the Networks

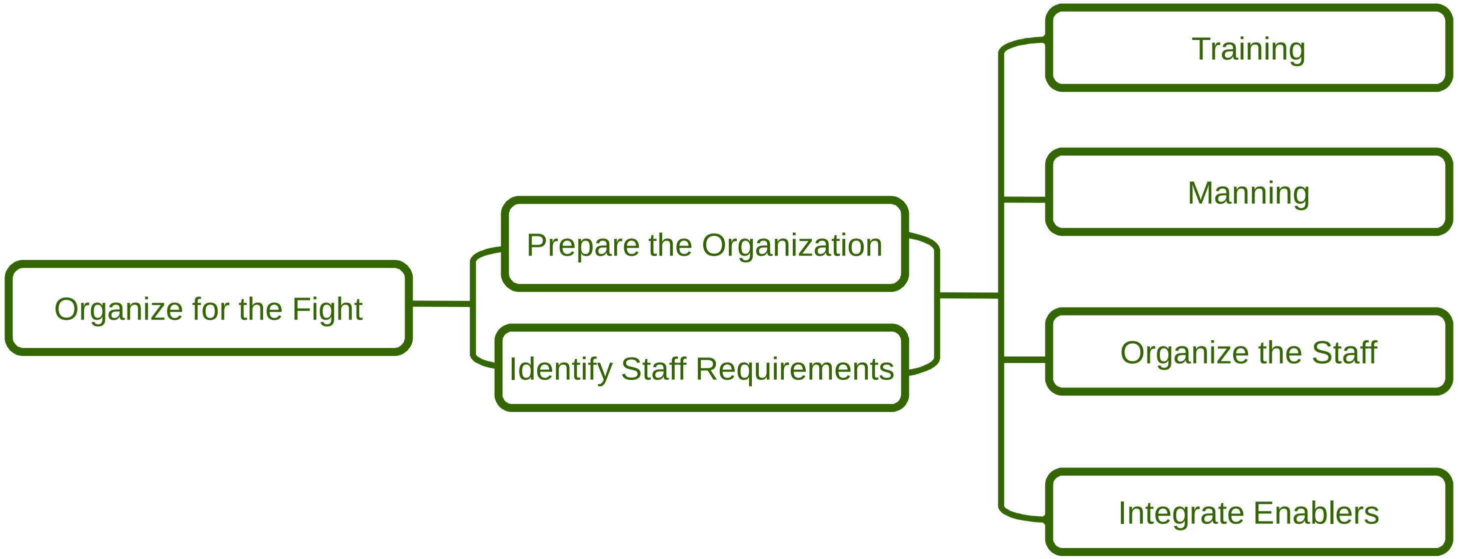
4 Organize for the Fight

5 Engage the Networks

6 Assess

4 ORGANIZE FOR THE FIGHT

Organize for the fight is to identify, organize and direct the resources (personnel, tools and equipment) that are needed to facilitate attack the network operations.



Organize for the Fight

Prepare the Organization (for attacking the network)

Preparing the organization is the planning, training, organization and outfitting of an organization with the personnel and capabilities necessary for conducting attack the network operations.

Identify Staff Requirements

To identify staff requirements is to characterize systematically and to quantify the skills and the training in those skills that are necessary for the staff to conduct attack the network operations.

AtN Training

AtN Training is the instruction of personnel to enhance their capacity to perform specific AtN functions and tasks. It is also the exercise of one or more military units conducted to enhance their combat readiness.

Manning

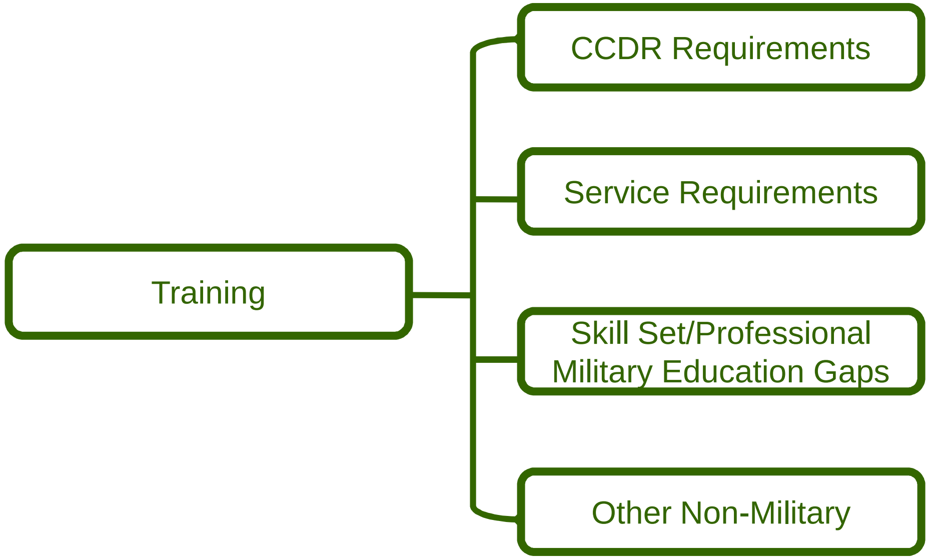
Manning is the analysis of the skills and their quantities in persons that are needed for conducting a specific AtN operation or it is the process of identifying and providing such manpower for an operation.

Organize the Staff

To organize the staff is to define the structure, roles, and responsibilities of a unit and its leadership in order to conduct attack the network operations. Organizing the staff is different at the theater, division, and tactical levels because their missions, their composition, and the enablers available to them are different.

Integrate Enablers

To integrate enablers is to blend efficiently and effectively the necessary organic and inorganic experts, tools, and material for attack the network operations.



Training

CCDR Requirements

Service Requirements

Skill Set/Professional Military Education Gaps

Other Non-Military

Training

CCDR Requirements (for training)

CCDR requirements are those skills or materials mandated by the Combatant Command in anticipation of attack the network operations in theater.

Service Requirements (for training)

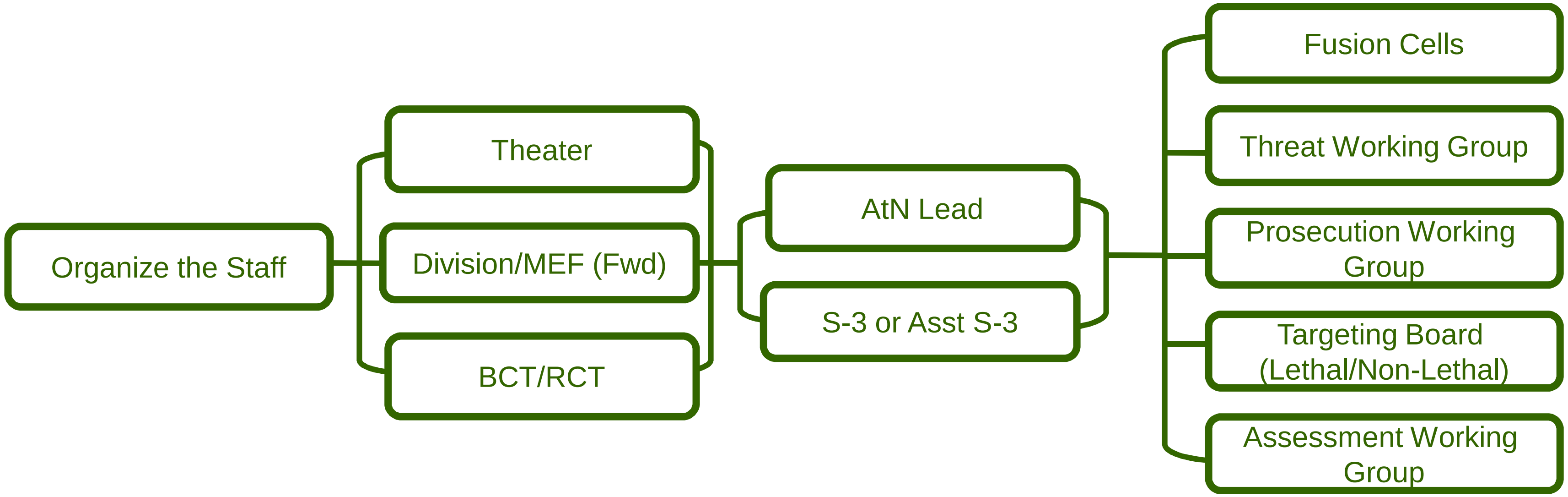
Service requirements are those skills or materials mandated by the service (Air Force, Marine Corps, Army, or Navy) in anticipation of attack the network operations in theater.

Skill Set/Professional Military Education Gaps

Identifying PME gaps is the deliberate identification of those skills necessary for conducting attack the network operations and the inventory of the unit's current skills against those necessary skills.

Other Non-Military (training)

Other non-military training are those skills or materials that are not standard or typical for the military, but should be acquired in anticipation of attack the network operations in theater (e.g. criminal forensic analysis).



Organize the Staff

Theater

Division/MEF (Fwd)

BCT/RCT

AtN Lead

S-3 or Asst S-3

Fusion Cells

Threat Working Group

Prosecution Working Group

Targeting Board (Lethal/Non-Lethal)

Assessment Working Group

Organize the Staff

Organize the Theater Staff

Organize the theater staff is to define the structure, roles, and responsibilities for the theater-level staff in order to conduct attack the network operations.

Organize Division Staff

Organizing the staff at the division-level is to define the structure, roles, and responsibilities for the division-level staff in order to conduct attack the network operations."

Organize the BCT/RCT Staff

Organizing the staff at the regimental or brigade-level is to define the structure, roles, and responsibilities for the tactical-level staff in order to conduct attack the network operations.

AtN Lead

The Attack the Network Lead is that individual whose function is to organize and supervise the attack the network activities within the staff, to include the various fusion cells and working groups.

S-3 or Assistant S-3

The S-3 or Assistant S-3 is the operations officer of a battalion or regiment that typically would direct AtN operations for the unit.

Fusion Cells

Theater level fusion centers called the Joint Intelligence Operations Center (JIOC), are a DoD and Combatant Command (CCDR) level organization. The JIOC mission is to seamlessly integrate all DoD intelligence functions and disciplines, ensuring all sources of information are available across the DoD, and improving the integration of intelligence with traditional operations and plans functions to increase the speed, power and combat effectiveness of DoD operations.

Threat Working Group

The threat working group is cross-functional by design and includes membership from across the staff, liaison personnel, and other partners outside the headquarters. The threat working group identifies, prioritizes, and recommends targets to the operational arm of the staff.

Organize the Staff

.

Prosecution Working Group

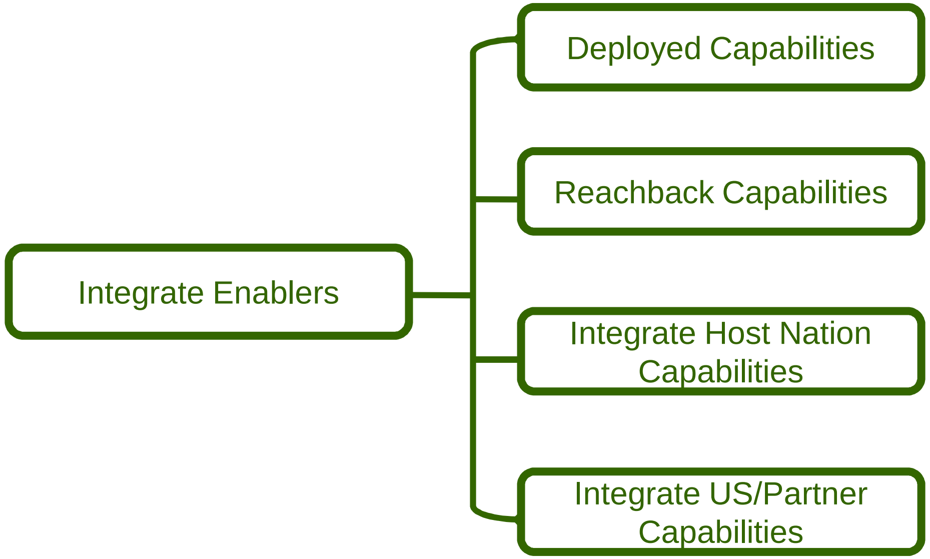
The prosecution group is cross-functional by design and includes membership from across the staff, liaison personnel, and other partners outside the headquarters. This working group identifies, prioritizes, and coordinates actions regarding targets for non-lethal targeting by removing him from the battlefield by using intelligence collection and analysis to build a case that will effectively prosecute him in a host nation's criminal system.

Targeting Board (Lethal/Non-lethal)

A targeting board is a temporary grouping of designated staff representatives with decision authority to coordinate and synchronize the targeting process.

Assessment Working Group

The assessment working group is cross-functional by design and includes membership from across the staff, liaison personnel, and other partners outside the headquarters. The assessment working group fuses assessment information to provide a comprehensive assessment of the operation. They consolidate and discuss emerging trends, issues, and impacts relating to events over the various planning horizons.



Integrate Enablers

Deployed Capabilities

Reachback Capabilities

Integrate Host Nation Capabilities

Integrate US/Partner Capabilities

Integrate Enablers

Deployed Capabilities

Deployed capabilities are the personnel, tools, services, and material that are resident in theater versus the personnel, tools, services, and material that are available by reach back to the continental US for support.

Reach Back Capabilities

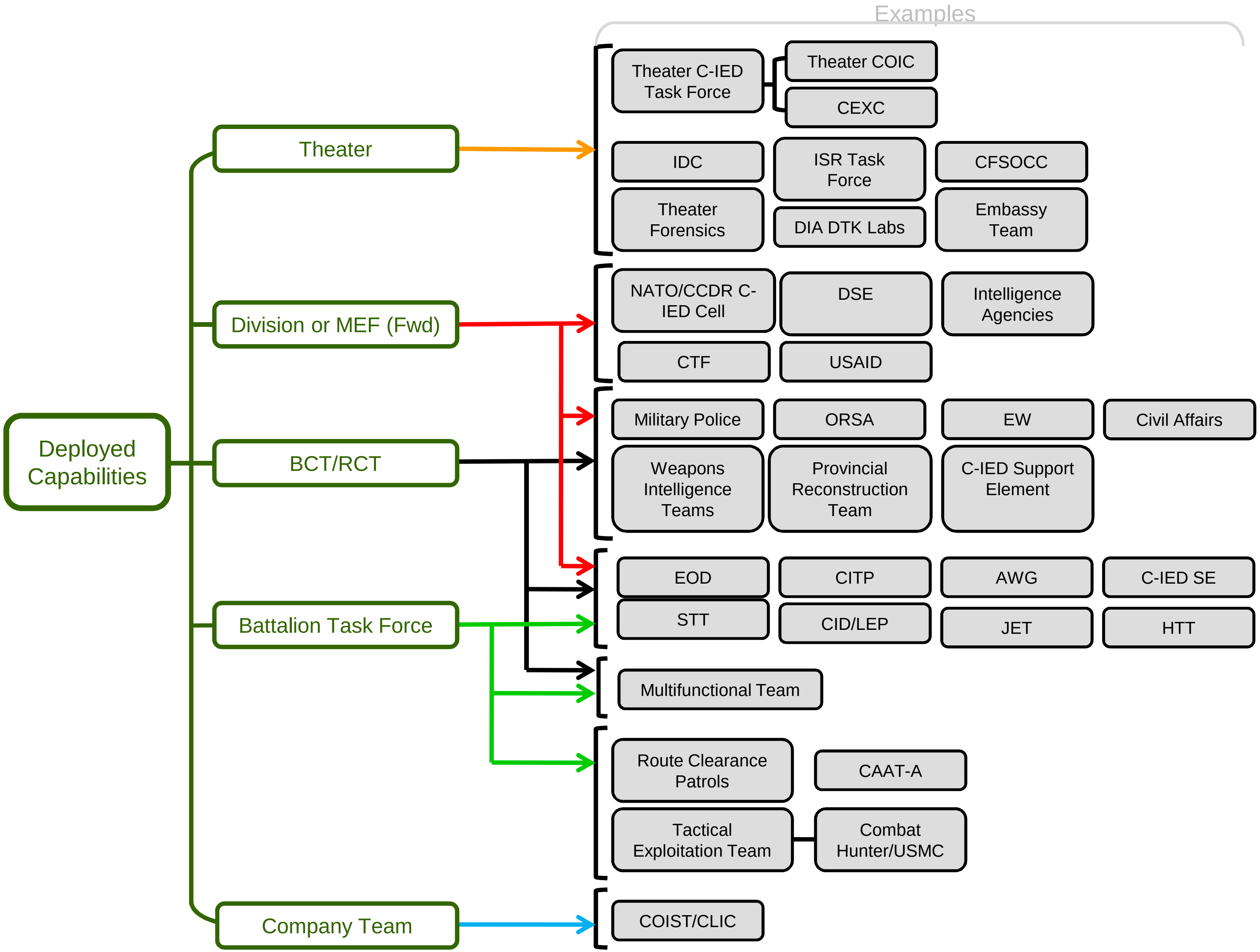
Reach back capabilities are those experts, tools, equipment, services, or material that are provided by organizations that are not forward deployed.

Integrate Host Nation Capabilities

To integrate Host Nation capabilities is to blend efficiently into attack the network operations the relevant national assets and services of the host nation where the US and its coalition are operating. These assets and services span the diplomatic, intelligence, legal, law enforcement, informational, military, and economic functions of commercial, government, and non-government organizations.

Integrate US/Partner Capabilities

The integration of US/Partner capabilities is achieved by blending efficiently into attack the network operations the relevant national assets and services of the US and its coalition partners. These assets and services span the diplomatic, intelligence, legal, law enforcement, informational, military, and economic functions of commercial, government, and non-government organizations.



Examples
Deployed Capabilities
Theater
Division or MEF (Fwd)
BCT/RCT
Battalion Task Force
Company Team
Theater C-IED Task Force
Theater COIC
CEXC
IDC
ISR Task Force
CFSOCC
Theater Forensics
DIA DTK Labs
Embassy Team
NATO/CCDR C-IED Cell
DSE
Intelligence Agencies
CTF
USAID
Military Police
ORSA
EW
Civil Affairs
Weapons Intelligence Teams
Provincial Reconstruction Team
C-IED Support Element
EOD
CITP
AWG
C-IED SE
STT
CID/LEP
JET
HTT
Multifunctional Team
Route Clearance Patrols
CAAT-A
Tactical Exploitation Team
Combat Hunter/USMC
COIST/CLIC

Deployed Capabilities

Theater C-IED Task Force

A Task Force designed and deployed to specifically address or counter the IED threat in a given theater of operation.

Theater COIC

The theater COIC has the same mission - albeit with fewer personnel and tools - as the national COIC. It provides all source analytical products on IEDs in order to conduct counter-IED operations.

Combined Explosives Exploitation Cell (CEXC)

The Combined Explosives Exploitation Cell (CEXC) is a U.S. Navy led task organized unit created to meet the technical and forensic intelligence requirements for the combatant commander. The CEXC provides expert level technical and forensic exploitation and analysis of WTI- related material in order to determine enemy tactics, identify IED trends and bomb makers, and assist in the development of defensive and offensive C-IED measures. The CEXC conducts investigations of significant events; exploits IED devices, recovering frequencies from RC IED devices to update EW equipment; tests explosive residue; recovers and evaluates forensic and biometric material; identifies IED trends and bomb maker signatures; creates profiles to better enable offensive operations; and conducts limited component tracking.

Information Dominance Center (IDC)

The Information Dominance Center (IDC) supports Army commands and units worldwide through G-2 channels for intelligence-reach operations. The IDC can provide tailored intelligence products to the field to meet their operational requirements on a quick response basis. The IDC monitors potential trouble spots, preparing to support contingency operations with intelligence related products. The IDC continues to explore new analytical technologies and emerging concepts to support Army warfighters.

Theater Forensics

Theater forensics labs include Expeditionary Forensics Labs (EFLs) and the Combined Explosives Exploitation Cell (CEXC).

ISR Task Force

The ISR Task Force is established to maximize and optimize currently deployed ISR capabilities, especially those in Iraq and Afghanistan.

Deployed Capabilities

DIA DTK Labs

The DIA DTK Lab is a strategic-level forensics lab for IEDs and CBRNE.

CFSOCC

Combined Forces Special Operations Component Command (CFSOCC) is the forward headquarters for SOCCENT and has operational control (OPCON) over SOF units in the CENTCOM AOR.

Embassy Team

The embassy team is the group of political, economic and cultural experts at the United States Mission in country and operates under the oversight of the Department of States.

NATO/CCDR C-IED Cell

The Counter-IED team provided by NATO or the CCRD that provides C-IED analysis, C-IED services, and liaison to other C-IED capabilities.

DSE

The Division C-IED Support Element (DSE) coordinates and integrates C-IED operations within the division operational area, and integrates C-IED enablers, analysis, and products into the division targeting process in order to support the division in maintaining freedom of action and defeating insurgent networks. The Division C-IED Support element is comprised of a mix of specialized C-IED personnel such as CEXC, CITP, intelligence analysis, operations research/systems analyst, LEP) along with intelligence and operations staff.

CTF

Counter threat finance is the prevention, inhibition, or interdiction of the generation, movement, storage, management, control, investment, accounting, distribution, disbursement, and expenditure of funds, assets, and/or valuable commodities that can be used to fund, finance, pay for, or facilitate lethal and non-lethal actions and activities by illicit adversaries and networks.

USAID

US Agency for International Development (USAID) is an independent federal government agency that receives overall foreign policy guidance from the Secretary of State. Our Work supports long-term and equitable economic growth and advances U.S. foreign policy objectives by supporting economic growth, agriculture and trade; global health; and, democracy, conflict prevention and humanitarian assistance.

Intelligence Agencies

Sixteen national-level agencies specialize in the collection and analysis of intelligence are relevant to attack the network operations. Most provide some sort of deployed or reach back capability to warfighters in theater. Those agencies include CIA, DIA, NGA, NSA and others.

Deployed Capabilities

Military Police

Military police are those law enforcement experts that are organic to the military with skills relevant to AtN, to include weapons handling, small-unit tactics, special weapons employment, convoy escort, riot control, traffic control, prisoner and detainee handling and processing, police intelligence, criminal intelligence, criminal handling, stations management.

Weapons Intelligence Teams (WIT)

The Weapons Intelligence Team or C-IED teams are assigned to the C-IED TF. Normally an EOD company, with a direct support WIT, will be placed in direct support of each brigade combat team. They will be placed OPCON to the TF's C-IED commander.

ORSA

Operational Research/ Statistical Analysis is the analytical study of military problems undertaken to provide responsible commanders and staff agencies with a scientific basis for decision on action to improve military operations.

C-IED Support Element

The C-IED Support Elements are teams designed to assist the maneuver unit in the planning, coordination and integration of their immediate C-IED operations, and they act as a liaison to the C-IED TF. The C-IED support elements also coordinate the unit's IED infrastructure targeting efforts.

Electronic Warfare

Electronic Warfare are those military actions involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. Electronic warfare consists of three functions: electronic attack, electronic protection, and electronic warfare support. Some EW actions are successful in disrupting IED devices.

Provincial Reconstruction Team

A Provincial Reconstruction Team (PRT) helps stabilize the operational environment in a province or locality through its combined diplomatic, informational, military, and economic capabilities. It combines representatives from interagency and international partners into a cohesive unit capable of independently conducting operations to stabilize the environment by enhancing the legitimacy and the effectiveness of the Host Nation government.

Deployed Capabilities

Civil Affairs

Civil Affairs teams are designated Active and Reserve Component forces and units organized, trained, and equipped specifically to conduct Civil Military Operations. These are activities that establish, maintain, influence, or facilitate relations between military forces, governmental and nongovernmental civilian organizations and authorities, and the civilian populace in a friendly, neutral, or hostile operational area in order to facilitate military operations, to consolidate and achieve operational US objectives. Civil-military operations may include performance by military forces of activities and functions normally the responsibility of the local, regional, or national government. These activities may occur prior to, during, or subsequent to other military actions. They may also occur, if directed, in the absence of other military operations. Civil-military operations may be performed by designated civil affairs, by other military forces, or by a combination of civil affairs and other forces.

Explosive Ordnance Disposal

Explosive Ordnance Disposal units are comprised of personnel with special training and equipment who render explosive ordnance safe (such as bombs, mines, projectiles, and booby traps), make intelligence reports on such ordnance, and supervise the safe removal thereof.

STT

The Stability and Transition Team facilitates the transition from Major Combat Operations (MCO) to Stability Security, Transition and Reconstruction (SSTR) operations.

Counter Insurgency Targeting Program (CITP)

The Counterinsurgency Targeting Program (CITP) is located at the NGIC in Charlottesville, Virginia and conducts WTI-related identity analysis, biometric analysis, and device or component analysis to support the targeting of key individuals in adversary IED networks. It works with the NGIC’s biometrics effort to rapidly match individuals to specific IED incidents by matching and assessing latent prints, fibers, and other data.

CID/LEP

The Criminal Investigative Division (CID) and Law Enforcement Programs (LEP) bring together experienced law enforcement professionals from the Drug Enforcement Agency, Federal Bureau of Investigation, police departments, and other agencies in order to lend their expertise to teach and support military personnel to investigate bomb-making networks, investigate incidents, question witnesses and suspects, and collect evidence for pending C-IED operations and prosecutions.

Human Terrain Team

A Human Terrain Team is a group of civilian anthropologists attached to brigades and battalions. This team helps the unit understand local cultures. These social scientists aid leaders in better understanding relevant cultural history, engaging locals in a positive way, and incorporating knowledge of tribal traditions to help resolve conflicts.

Deployed Capabilities

Joint Expeditionary Team

A Joint Expeditionary Team (JET) supports all echelons of the joint force, interagency, and multinational partners. Its purpose is to train, advise, observe, analyze, and to collect and disseminate tactics, techniques, and procedures (TTPs), lessons learned, and best practices to mitigate the IED threat. It will normally operate in two to three man teams and be placed OPCON to the TF's C-IED commander.

AWG

The Asymmetric Warfare Group (AWG) is a Sensitive Activity under the HQDA G-3/5/7 that provides operational advisory assistance in support of Army and joint force commanders. The AWG was created by the Army to enhance the combat effectiveness of the operating force and enable the defeat of asymmetric threats to include IEDs. The AWG deploys its forces worldwide to observe, assess and analyze information regarding the evolving operating environment and the threat. It also assists in the development, dissemination and integration of material and non material solutions including countermeasures. The AWG serves as an agent of change providing key observations and perspectives for leaders when considering policy and resource decisions.

C-IED/SE

The C-CIED Site Exploitation teams recognize, collect, process, preserve, or analyze information, personnel, and materiel found during the conduct of C-IED operations for follow-on use by the intelligence or warfighting functions of the staff.

Multi-functional Team

Multi-functional teams are created out of personnel that are organic to the Division. The teams combine SIGINT, HUMINT, and IMINT to perform time-sensitive targeting.

Counterinsurgency Advisory and Assistance Team – Afghanistan (CAAT-A)

The CAAT-A's mission is to assist commanders in integrating all aspects of COIN operations. Its purpose is to assist Commanders, identify trends, and disseminate lessons learned to facilitate ISAF organizational and cultural change.

Deployed Capabilities

Tactical Exploitation Team

Tactical Exploitation Teams deploy from the C-IED task forces on short-notice to provide site exploitation. Site exploitation are those activities that recognize, collect, process, preserve, or analyze information, personnel, and materiel found during the conduct of C-IED operations.

Route Clearance Patrols

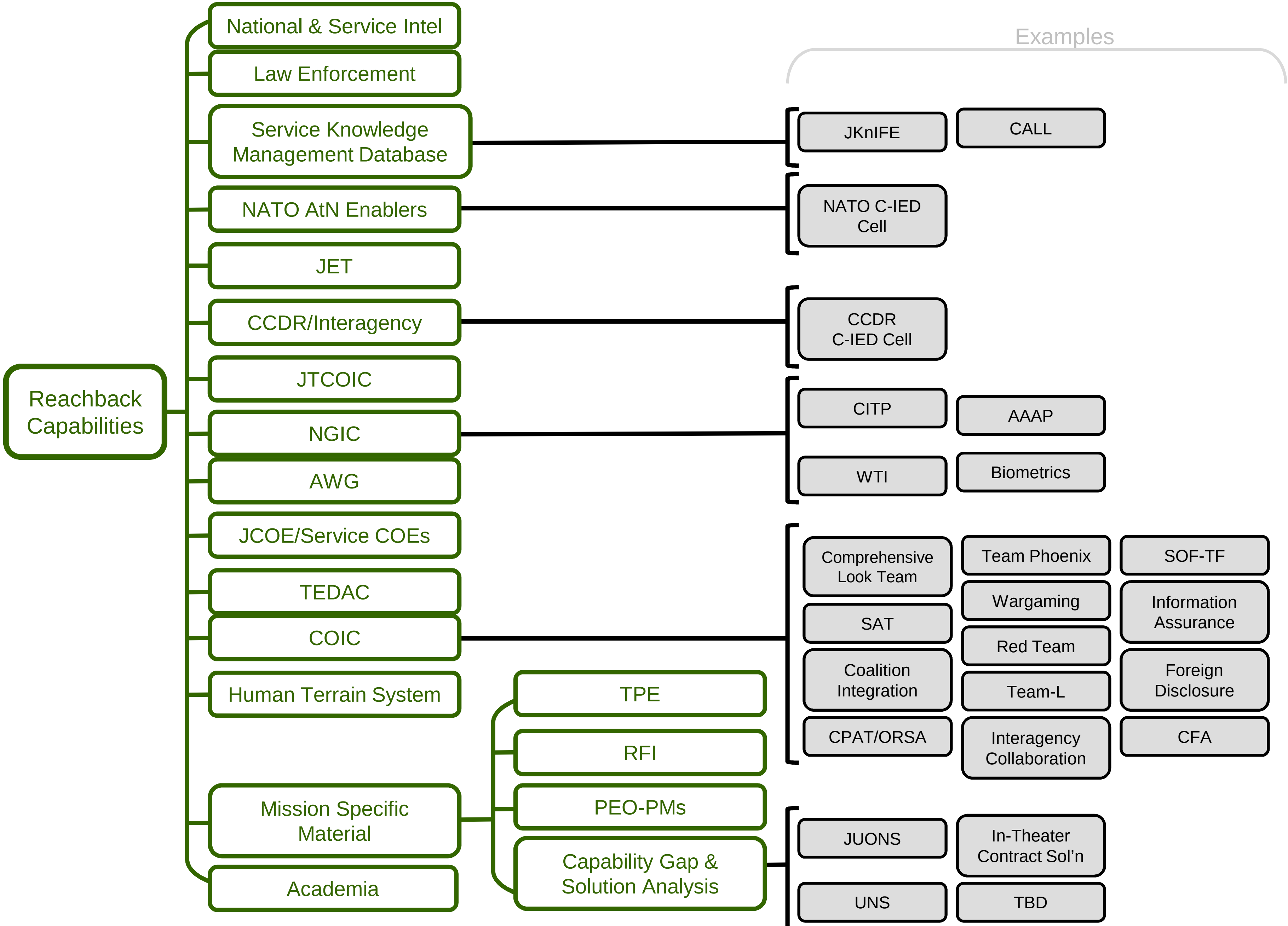
Route clearance patrols detect, investigate, mark, report, and neutralize explosive hazards (EH) and other obstacles along a defined route to enable assured mobility for the maneuver commander. It is a combined arms operation that relies on a reconnaissance of the route to be cleared. The goal of route clearance is to detect and neutralize EH and improve and know the route to be able to conduct future change detection operations.

Combat Hunter (USMC)

Combat Hunter is a ten-day course provided by the Marine Corps to create a hunting mindset by integrating enhanced observation, combat profiling, and combat tracking skills in order to produce a more ethically minded, tactically cunning, and lethal infantryman that is better prepared to succeed across the range of military operations.

COIST/CLIC

Company Intelligence Support Teams (COISTs) or Company-level Intelligence Cells (CLICs) are a recently developed capability to provide analytical products (that have typically been resident at the battalion level and higher) down to the company-level.



Reachback Capabilities

- National & Service Intel
- Law Enforcement
- Service Knowledge Management Database
- NATO AtN Enablers
- JET
- CCDR/Interagency
- JTCOIC
- NGIC
- AWG
- JCOE/Service COEs
- TEDAC
- COIC
- Human Terrain System
- Mission Specific Material
  - TPE
  - RFI
  - PEO-PMs
  - Capability Gap & Solution Analysis
- Academia

Examples

- JKnIFE
- CALL
- NATO C-IED Cell
- CCDR C-IED Cell
- CITP
- AAAP
- WTI
- Biometrics
- Comprehensive Look Team
- Team Phoenix
- SOF-TF
- Wargaming
- Information Assurance
- SAT
- Red Team
- Coalition Integration
- Foreign Disclosure
- Team-L
- CPAT/ORSA
- Interagency Collaboration
- CFA
- JUONS
- In-Theater Contract Sol'n
- UNS
- TBD

Reachback Capabilities

National & Service Intelligence

The sixteen national-level agencies specialize in the collection and analysis of intelligence and are relevant to attack the network operations. Most provide some sort of deployed or reach back capability to warfighters in theater. Those agencies include CIA, DIA, NGA, NSA and others.

Law Enforcement Capabilities

Law enforcement capabilities are those police functions that are not organic to the unit and must be requested from the continental United States.

Service Knowledge Management Databases

Service knowledge management encompasses the various electronic repositories of organized information that are relevant to AtN operations and are maintained by the various services to include the Army Center for Lessons learned and the Marine Corps Lessons Learned Center.

JKnIFE

Joint Knowledge and Information Fusion Exchange acts as the DOD central repository for IED related information. Its primary purpose is to exchange information, consolidate best practices and respond to requests for information related to the asymmetric application of IED related TTPs by both enemy and friendly forces.

Center for Army Lessons Learned (CALL)

The Center for Army Lessons Learned one of the Army's central knowledge management organization that rapidly collects, analyzes, disseminates, and archives observations, insights, lessons (OIL), TTP and operational records in order to facilitate rapid adaptation initiatives and conduct focused knowledge sharing and transfer that informs the Army and enables operationally based decision making, integration, and innovation throughout the Army and within the Joint Interagency Intergovernmental Multi-national (JIIM) environment.

NATO AtN Enablers

NATO AtN enablers are personnel, services, tools, and material from NATO partners that are used to supplement, enhance, and complement US and coalition forces capabilities for conducting attack the network operations.

NATO C-IED Cell

The NATO C-IED cell is the counter-IED team provided by NATO that provides C-IED analysis, C-IED services, and liaison to other C-IED capabilities.

JET

A Joint Expeditionary Team (JET) supports all echelons of the joint force, interagency, and multinational partners. Its purpose is to train, advise, observe, analyze, and to collect and disseminate tactics, techniques, and procedures (TTPs), lessons learned, and best practices to mitigate the IED threat. They will normally operate in two to three man teams and be placed OPCON to the TF’s C-IED commander.

Reachback Capabilities

CCDR/Interagency Capabilities

The various skills and services that are inorganic to deployed forces but are provided by the Combatant Commander or partner agencies of the USG.

CCDR C-IED Cell

The CCDR C-IED cell is the counter-IED team formed and staffed by CCDR that provides C-IED analysis, C-IED services, and liaison to other C-IED capabilities.

JTCOIC

The Joint Training Counter-IED Operations Integration Center (JTCOIC) was officially opened in April 2009 to ensure Army and joint organizations are aware of and able to employ rapidly fielded counter-IED capabilities. Established as a partnership between JIEDDO and TRADOC, the state-of-the-art center combines the operational focus of the Department of Defense's lead counter-IED organization with the training resources and expertise of the Army's premier training command.

NGIC

The National Ground Intelligence Center, located in Charlottesville, Virginia, is assigned to INSCOM and is under the operational control (OPCON) of the Army G-2. NGIC is the Service National production center for ground forces intelligence and has DODIPP primary production responsibility for most ground force intelligence functional codes.

CITP

The Counterinsurgency Targeting Program (CITP) is located at the NGIC in Charlottesville, Virginia and conducts WTI-related identity analysis, biometric analysis, and device or component analysis to support the targeting of key individuals in adversary IED networks. They work closely with the NGIC’s biometrics effort to rapidly match individuals to specific IED incidents by matching and assessing latent prints, fibers, and other data.

WTI

Weapons Technical Intelligence is a category of intelligence derived from the technical and forensic collection and exploitation of IEDs, associated components, improvised weapons, and other weapon systems.

AAAP

The Anti-Armor Analysis Program (AAAP) is an analytic program run by the National Ground Intelligence Center that analyzes and discerns trends in adversary development, manufacture, procurement and use of anti-armor weapons.

Biometrics

Biometrics is the process of recognizing an individual based on measurable anatomical, physiological, and behavioral characteristics.

Reachback Capabilities

Asymmetric Warfare Group (AWG)

The Asymmetric Warfare Group (AWG) is a Sensitive Activity under the HQDA G-3/5/7 that provides operational advisory assistance in support of Army and joint force commanders. The AWG was created by the Army to enhance the combat effectiveness of the operating force and enable the defeat of asymmetric threats to include IEDs. The AWG deploys its forces worldwide to observe, assess and analyze information regarding the evolving operating environment and the threat. They also assist in the development, dissemination and integration of material and non material solutions including countermeasures. The AWG serves as an agent of change providing key observations and perspectives for leaders when considering policy and resource decisions.

Joint Center of Excellence/Service Centers of Excellence (JCOE/COE)

The Joint Center of Excellence (JCOE) is the execution arm of JIEDDO's C-IED training program. JCOE is located at Fort Irwin, Ca. and has been operational since April 2006. Together with the four service-specific centers of excellence (COEs), JCOE provides deploying forces with training on rapidly fielded C-IED equipment and capabilities. JCOE and the service COEs facilitate individual, collective, and unit C-IED training; develop and publish IED defeat tactics, techniques and procedures; and make available to deploying units C-IED lessons learned from those returning from theater.

Terrorist Explosives Device Analytical Center (TEDAC)

The FBI created the Terrorist Explosives Device Analytical Center (TEDAC) in December 2003. TEDAC provides a single federal program responsible for the worldwide collection, complete forensic, technical analysis, and timely dissemination of intelligence related to terrorist bombing incidents.

Counter-IED Operations Intelligence Integration Center

The COIC leverages existing information and provides strategic capabilities in support of offensive operations against IED networks. Through COIC's fused intelligence products, formerly highly classified intelligence is now available at the secret level, making it accessible to warfighters at the tactical level. The COIC's architecture of partnerships include more than 20 intelligence agencies and other federal agencies supporting this effort.

Comprehensive Look Team

The Comprehensive Look Team at JIEDDO's COIC provides comprehensive, multi-disciplinary intelligence analysis in support of the C-IED mission and other attack the network operations as required.

Signatures Analysis team (SAT)

The Signatures Analysis Team (SAT) provides predictive analysis of both terrain and force oriented problems via signatures analysis.

Reachback Capabilities

Coalition Integration

The COIC facilitates coalition integration by integrating coalition multi-discipline databases into its network analysis process.

COIC Pattern Analysis Team (CPAT)

The COIC Pattern Analysis Team (CPAT) identifies, analyzes, and resolves tactical patterns in support of JIEDDO/COIC and its partners in the Defense, Intelligence, and National Security communities, and applies tactical pattern analysis methods to other problems in response to requests for support from authorized users worldwide.

Team Phoenix

A military organization that integrates intelligence, operations, and technology with training to enable pre-emptive analysis to attack networks.

Wargaming

Wargaming from the JIEDDO COIC provides standing, on-demand wargaming capability to enhance C-IED strategy development using threat scenarios and modeling and simulation resources to assess future operations in the context of friendly and enemy courses of action (COA), concepts of operations (CONOPS), tactics, techniques, and procedures (TTP), and emerging technologies.

Red Team

The mission of the Red Team at JIEDDO's COIC is to provide its parent organization with a continuous process of analysis and counter-analysis that assesses: the likely enemy operational and tactical TTP innovations; countermeasures; wargaming the effectiveness of those countermeasures. The Red Team also identifies gaps, challenges assumptions and predicts 2nd and 3rd order effects. The Red Team does that through adversarial emulation, independent analysis, and critical review in support of current operations, plans, and capabilities for committed units and JIEDDO in order to enhance the Counter-IED fight.

Team-L

Team L is a Comprehensive Look Team at the JIEDDO COIC that supports offensive operations focused on attacking networks as part of the overall Joint Improvised Explosive Devise Defeat Organization (JIEDDO), Counter-IED Operations Integration Center (COIC) C-IED support structure.

Interagency Collaboration

The JIEDDO COIC hosts and collaborates with multiple agency liaisons to facilitate integration of intelligence community capabilities in support of warfighter operations.

Special Operations Forces Task Force (SOF-TF)

SOF-TF Provides multi-discipline intelligence analysis, fusion and integration to support SOCOM Operations.

Reachback Capabilities

Information Assurance

COIC Information assurance supports integration of innovative advanced technologies and methodologies required to better identify threat networks through gaining interim authority to operate on government communications systems (Source: COIC Support Capabilities Document).

Foreign Disclosure

Foreign disclosure supports the transfer of classified information through approved channels to an authorized representative of a foreign government or international organization.

Critical Factors Analysis (CFA)

Critical Factors Analysis: The Critical Factors Analysis (CFA) Comprehensive Look Team (CLT) analyzes Blue, Red, Green, and White critical capabilities (CC), critical requirements (CR) and deduces critical vulnerabilities (CV) for exploitation to facilitate US force interests against threat networks at strategic, operational and tactical levels.

Human Terrain System (HTS)

The Human Terrain System (HTS) is a proof of concept program, run by the U.S. Army Training and Doctrine Command (TRADOC), and serves the joint community. The near term focus of the HTS program is to improve the military's ability to understand the highly complex local socio-cultural environment in areas where they are deployed.

Mission Specific Material

Items that are necessary for a mission, but since they are situational-dependent, they cannot be accurately identified in advance.

Theater Provided Equipment (TPE)

Theater Provided Equipment (TPE) is equipment that is not organic to the unit nor does the unit have to procure it for itself; the Combatant Commander or the JTF commander provides the equipment to the deployed unit.

Request for Information (RFI)

A Request for Information (RFI) is any specific, time-sensitive, ad hoc requirement for intelligence information or products to support an ongoing crisis or operation not necessarily related to standing requirements or scheduled intelligence production. An RFI can be initiated to respond to operational requirements and will be validated in accordance with the combatant command's procedures.

Reachback Capabilities

Peace Enforcement Operations/Peace-Making (PEO-PM)

Peace Enforcement Operations (PEOs) are generally coercive in nature and rely on the threat of or use of force; however, PEOs also rely on the development of working relationships with the local population. The impartiality with which the peace operating force treats all parties and the nature of its objectives separate PEO from COIN and major combat operations. Peace-making (PM) is a diplomatic process that may include mediation, negotiation, or conciliation. PM efforts may take advantage of seams in insurgent organizations by establishing separate agreements with individual organizations or groups that make up an insurgency movement. Commanders should constantly seek opportunities for PM throughout COIN.

Capability Gap & Solution Analysis

Capability gap & solution analysis is a part of the systematic procurement process established by the DOD to identify a missing or incomplete capabilities and the solutions to provide the capability. The Functional Solutions Analysis follows the Functional Need Analysis that identifies the capability requirement in detail.

Joint Urgent Operational Need Statement (JUONS)

A Joint Urgent Operational Need Statement (JUONS) is an urgent operational need identified by a combatant commander involved in an ongoing named operation. A JUONS main purpose is to identify and subsequently gain Joint Staff validation and resourcing of a solution, usually within days or weeks, to meet a specific high-priority combatant commander need.

Universal Needs Statement (UNS)

An universal needs statement (UNS) is an official request submitted to a service's requirements process by which a unit makes a request for current and future wartime capabilities.

In-theater Contract Solution

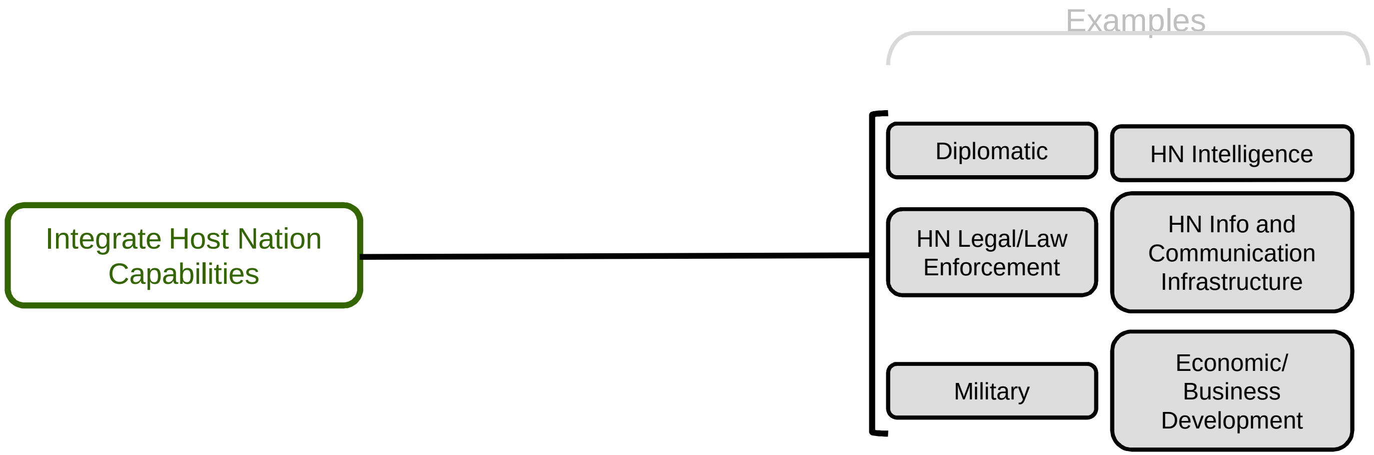
The provision of basic goods, support services, minor construction, and other services that occur through contracting officers and from vendors located in the theater of operations.

To Be Determined Capabilities

Capabilities that will be needed in the future, but at the current time are indeterminable.

Academia

Academia is the life, community, or world of teachers, schools, and education.



Integrate Host Nation Capabilities

Examples

Diplomatic

HN Intelligence

HN Legal/Law Enforcement

HN Info and Communication Infrastructure

Military

Economic/ Business Development

Integrate Host Nation Capabilities

Diplomatic

Actions taken by State Department or senior US/coalition military leaders to align, coordinate, and harmonize the diplomatic efforts with those of the host nation to maintain common purpose and achieve common goals and objectives.

Host Nation Intelligence

Host Nation Intelligence is the national government's traditional information resources and the integrating of central and local government intelligence capabilities.

Host Nation Legal/Law Enforcement

Host Nation Law Enforcement capabilities are those host nation faculties that provide for the public safety.

Host Nation Information and Communication Infrastructure

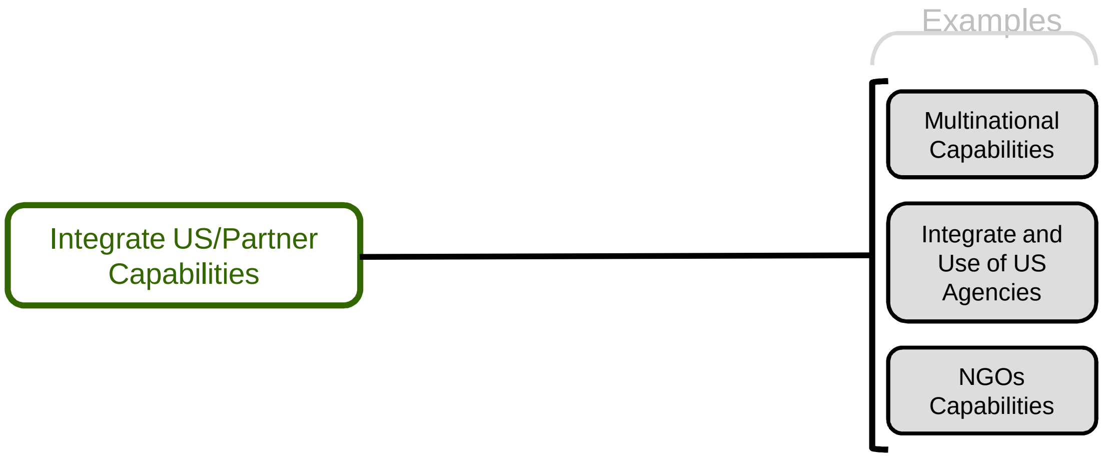
Host Nation information and communications infrastructure which may be written, visual, audio, word-of-mouth, etc. and avoiding noticeably foreign messaging to legitimize local government. Be conscious of tribal, ethnic, religious, professional, school, messaging venues/distribution channels (etc. mosques, schools, tribal, local medium).

Host Nation Military Capabilities

Actions taken by US and coalition military leaders to align, coordinate, and synchronize military planning, operations and capabilities with those of the host nation to achieve agreed upon military goals and objectives.

Economic/Business Development

Actions taken by US and coalition government agents (like USAID) in partnership with commercial interests to provide for host nation economic development. The efforts must be sensitive to provide for short term goods and services as well as ensuring longer term host nation growth and self reliance.



Integrate US/Partner Capabilities

Examples

Multinational Capabilities

Integrate and Use of US Agencies

NGOs Capabilities

Integrate US/Partner Capabilities

Integrate US/Partner Capabilities

The integration of US/Partner capabilities is achieved by blending efficiently into attack the network operations the relevant national assets and services of the US and its coalition partners. These assets and services span the diplomatic, intelligence, legal, law enforcement, informational, military, and economic functions of commercial, government, and non-government organizations.

Multinational Capabilities

Determine and leverage multi-national capabilities and limitations within the theater of operations (e.g. law enforcement, health professionals, engineers, etc.).

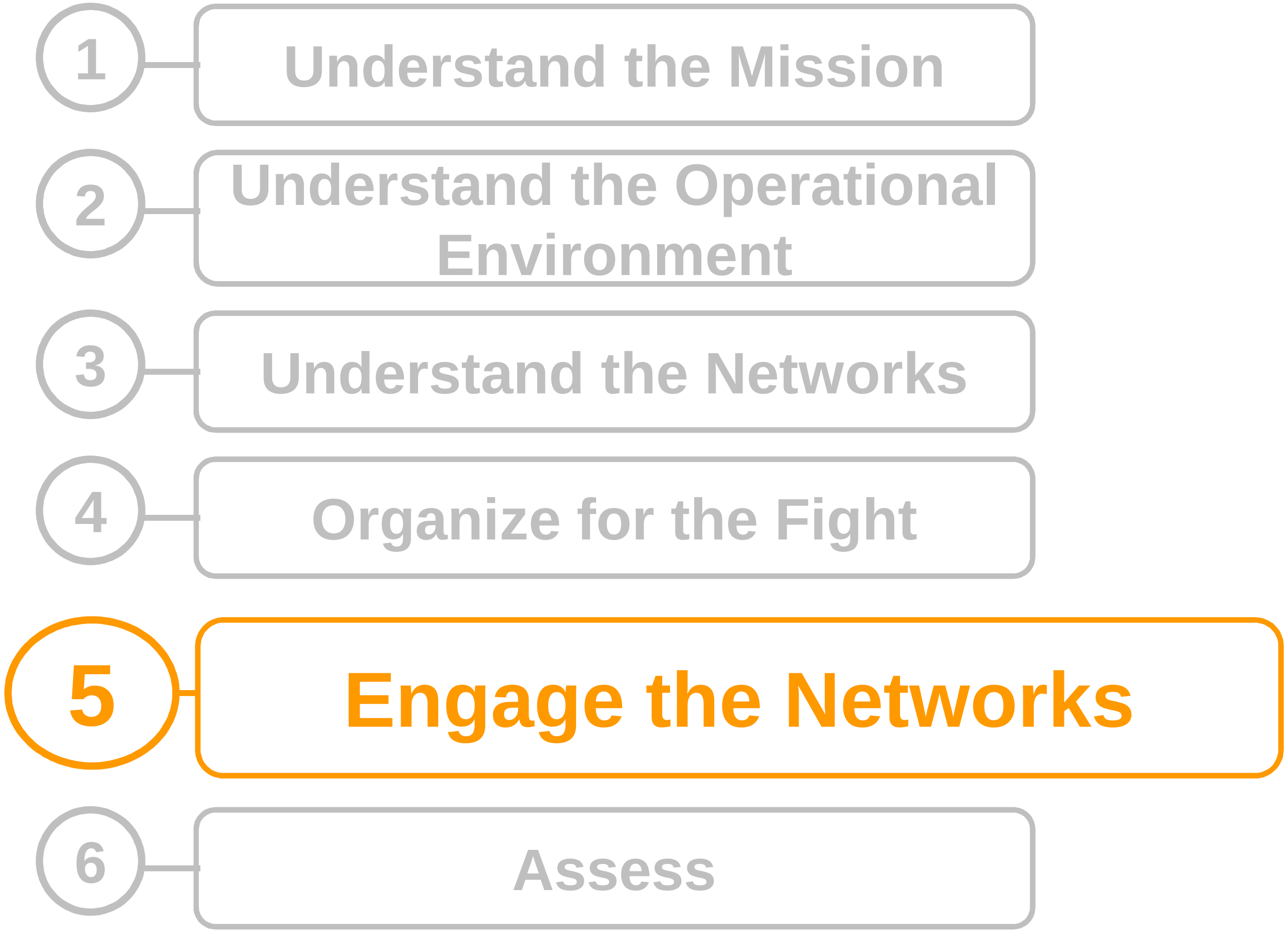
Integrate and Use of US Agencies

Identify and leverage US agencies that have a knowledge and interest in the commander's AOR.

Non Governmental Organization Capabilities

Where NGOs' are willing to cooperate with friendly forces and to the extent they are willing to cooperate, commanders should plan to include NGO capabilities in developing their plans.

Six pillars of Attack the Network:



1 Understand the Mission

2 Understand the Operational Environment

3 Understand the Networks

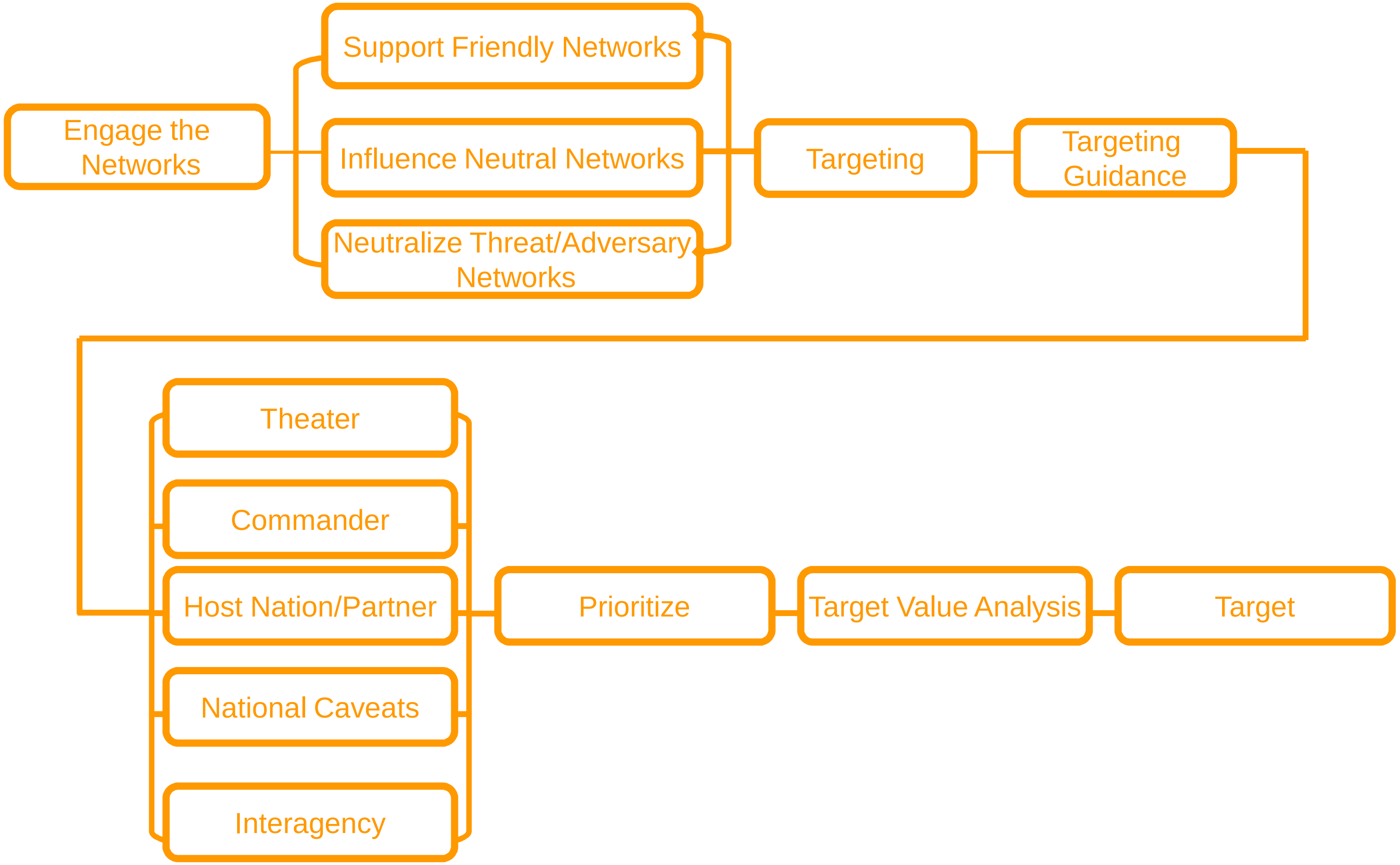
4 Organize for the Fight

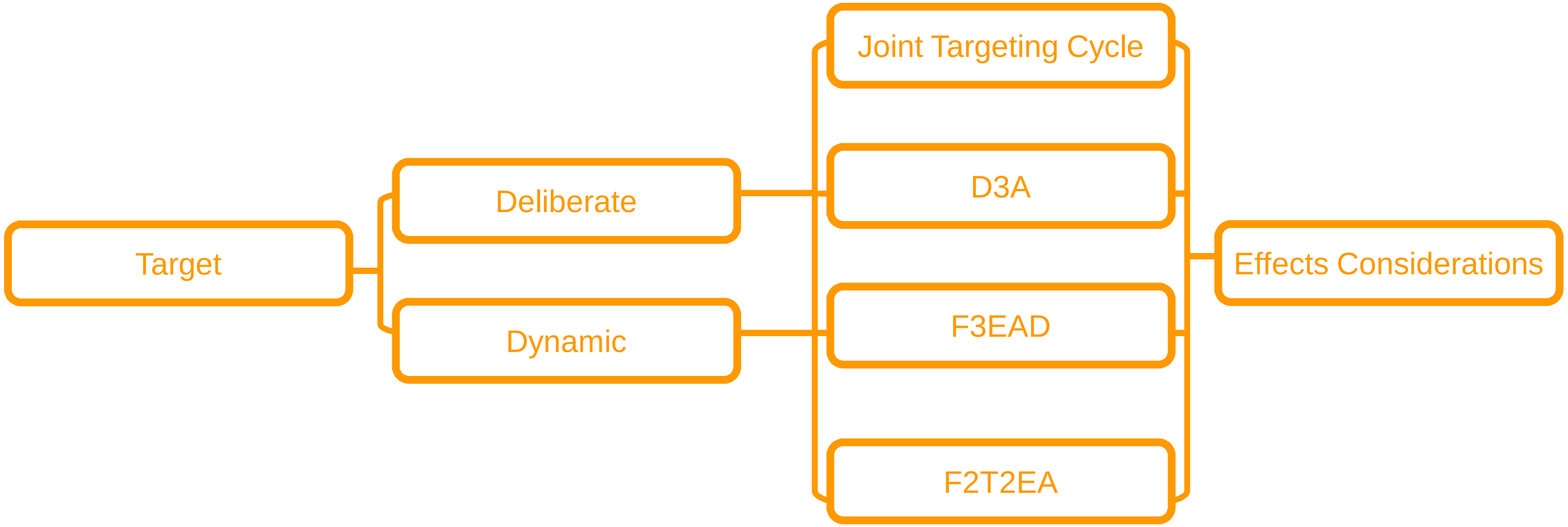
5 Engage the Networks

6 Assess

5 ENGAGE THE NETWORKS

To engage the networks is to use lethal and nonlethal means to support, influence, or neutralize network members or cells or an entire network.





Target

Deliberate

Dynamic

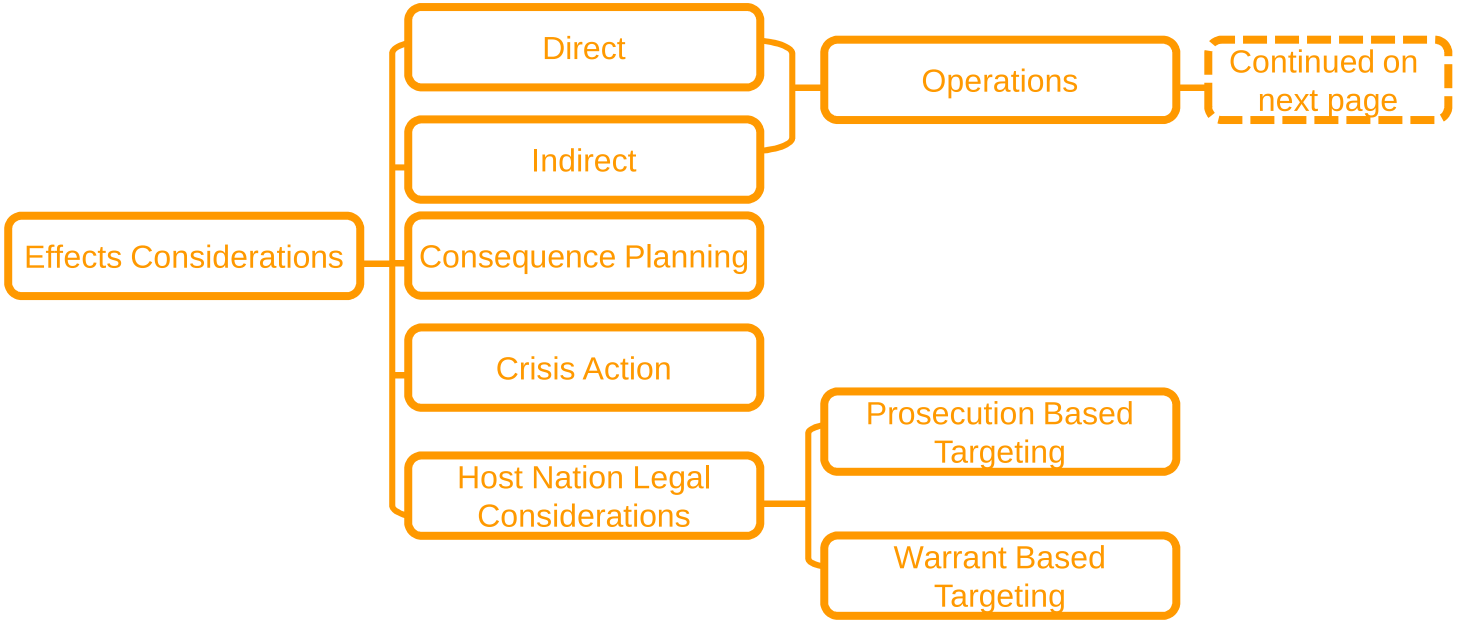
Joint Targeting Cycle

D3A

F3EAD

F2T2EA

Effects Considerations



Effects Considerations

Direct

Indirect

Operations

Continued on next page

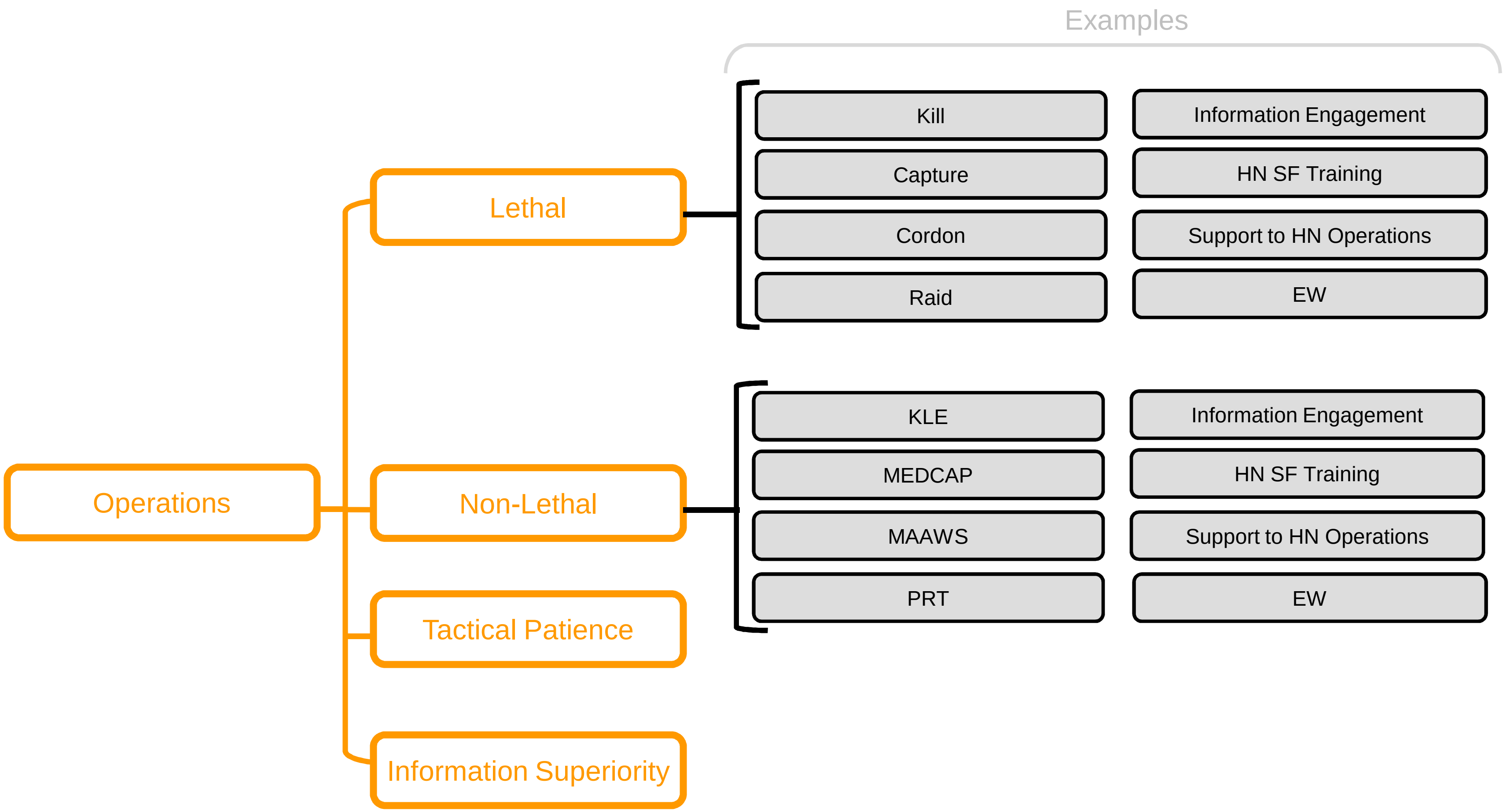
Consequence Planning

Crisis Action

Host Nation Legal Considerations

Prosecution Based Targeting

Warrant Based Targeting



Operations

- Lethal
- Non-Lethal
- Tactical Patience
- Information Superiority

Examples

Lethal:

- Kill
- Capture
- Cordon
- Raid
- Information Engagement
- HN SF Training
- Support to HN Operations
- EW

Non-Lethal:

- KLE
- MEDCAP
- MAAWS
- PRT
- Information Engagement
- HN SF Training
- Support to HN Operations
- EW

Engage the Networks

Support Friendly Networks

To support friendly networks is to provide material support, personnel, guidance, or public affirmation to network that is sympathetic to or cooperating in support of US interests.

Influence Neutral Networks

To influence neutral networks is to sway allegiance and support of the neutral network away from the threat network(s) and/or towards the friendly network.

Neutralize Threat /Adversary Networks

To neutralize threat/adversary networks is render ineffective a network that is in opposition to US interests.

Targeting

Targeting is the process of selecting and prioritizing targets and matching the appropriate response to them, while considering operational requirements and capabilities.

Targeting Guidance

Targeting guidance describes the desired effects of lethal and nonlethal fires. It is expressed in terms of targeting objectives (limit, disrupt, delay, divert, or destroy) or IO effects (destroy, degrade, disrupt, deny, deceive, exploit, or influence).

Theater Targeting Guidance

Theater targeting guidance is the general or specific parameters given by a combatant commander or theater commander to direct the activities, the decisions, or the desired outcomes of the a person or group that is executing the targeting process.

Commander’s Targeting Guidance

Commander's targeting guidance from a commander is the general or specific parameters given by the joint force commander to direct the activities, the decisions, or the desired outcomes of the a person or group that is executing the targeting process.

Host Nation/Partner Targeting Guidance

Host Nation/partner targeting guidance is the general or specific parameters given by a host nation or partner to direct the activities, the decisions, or the desired outcomes of the person or group that is executing the targeting process.

National Caveats

A national caveat is a limitation/restriction on the flexibility a commander has to prosecute targets. It can limit type of weapons, type of targets, or the targeting process by requiring additional coordination/approval.

Interagency Targeting Guidance

Interagency targeting guidance is the general or specific parameters given by the US government agencies to direct the activities, the decisions, or the desired outcomes of the a person or group that is executing the targeting process.

Engage the Networks

Prioritize Targets

To prioritize targets is to determine when operating with limited resources or time an order of precedence for targets.

Target Value Analysis

Target value analysis is a methodology which identifies potential high-value targets within a given tactical situation by producing a relative ranking on the worth of the target sets from the perspective of the enemy commander.

Target

A target is an entity or object considered for possible engagement or other action.

Deliberate Targeting

Deliberate targeting is a category of targeting that prosecutes planned targets. These are targets that are known to exist in the operational environment with engagement actions scheduled against them to create the effects desired to support achievement of JFC objectives.

Joint Targeting Cycle

The joint targeting cycle is an iterative, repeatable framework for targeting that is not time-constrained, and it occurs in 6 phases: end state and the commander's objectives; target development and prioritization; capabilities analysis; commander's decision and force assignment; mission planning and force execution; assessment.

Decide Detect Deliver and Assess (D3A)

Land and maritime force commanders normally use an interrelated process to enhance joint fire support planning and interface with the joint targeting cycle known as the decide, detect, deliver, and assess (D3A) methodology. D3A incorporates the same fundamental functions of the joint target cycle. The D3A methodology facilitates synchronizing maneuver, intelligence, and fire support.

Dynamic Targeting

Dynamic targeting is targeting that prosecutes targets identified too late, or not selected for action in time to be included in deliberate targeting.

Find Fix Finish Exploit Analyze and Disseminate (F3EAD)

Find, fix, finish, exploit, analyze, and disseminate (F3EAD), a subset of the targeting process, may be used in the AtN context to engage selected high-value individuals (HVIs) or activities (caches, bomb making facilities). It incorporates the same fundamentals of the joint target cycle and facilitates synchronizing maneuver, intelligence and fire support. F3EAD features massed, persistent ISR cued to a powerful and decentralized all-source intelligence apparatus. The goal is to find an HVI or activity (weapons cache, bomb factory) in the midst of civilian clutter and fix its exact location.

Engage the Networks

Find Fix Track Target Engage and Assess (F2T2EA)

F2T2EA the dynamic targeting process to find, fix, track, target, engage, and assess.

Effects Considerations

Effects considerations is the fore-thought given to the result, outcome, or consequences of targeting.

Direct Impact

Direct impact is a form of impact in which the target is affected by the agent of the targeting with nothing coming between the two in space or time.

Indirect Impact

Indirect impact is a form of impact in which the target is affected by the agent of the targeting through some second agent or effect.

AtN Operations

A series of strategic, operational, or tactical actions designed primarily to neutralize threat/adversary networks, support friendly networks, and/or influence neutral networks.

Lethal Force

Lethal force are actions that destroy targets through blast, penetration, and fragmentation.

Kill

Kill is to deprive of life; cause the death of.

Capture

To capture is to take into custody of a hostile force, equipment, or personnel as a result of military operations.

Cordon

A Cordon is an operation to encircle an area, to prevent entrance and exit, and to secure open areas.

Information Engagement

Information engagement is the integrated employment of public affairs to inform U.S. and friendly audiences; psychological operations, combat camera, U.S. Government strategic communication and defense support to public diplomacy, and other means necessary to influence foreign audiences; and, leader and Soldier engagements to support both efforts.

Host Nation Special Forces Training

The deliberate employment of host nation special forces in an ATN operation to render the enemy's personnel or equipment ineffective.

Support to Host Nation Operations

Support to Host Nation operations is providing material support, personnel or guidance to a host nationals planned operation.

Non-Lethal Force

Nonlethal force are actions explicitly designed and primarily employed to incapacitate personnel or material, while minimizing fatalities, permanent injury to personnel, and undesired damage to property and the environment.

Engage the Networks

Key Leader Engagement (KLE)

Commanders often interact directly with local populations and stakeholders through face-to-face meetings, town meetings, and community events highlighting counterinsurgent community improvements. These interactions give commanders additional opportunities to assess their efforts' effectiveness, address community issues and concerns, and personally dispel misinformation. These events often occur in the CMOC. Leader engagement must be included in the overall plan. Dissemination of information by leaders can be vital and help build credibility and Host Nation legitimacy. These meetings should include the media and key leaders within the population. This interaction should be an ongoing process, it may increase to support certain COIN efforts or to counter insurgent efforts.

MEDCAP

A combined medical and civil affairs program used during stabilization and support operations in which local civilians are provided free medical care. These operations are intended to influence neutral networks and support friendly networks by providing task organized medical assistance to the population.

Money as a Weapons System (MAAWS)

Money as a weapons System is used as leverage to positively influence the host nation populace (e.g. CERP).

Tactical Patience

Tactical patience is the intentional delay of the execution of an operation against a target to allow a more fully developed picture of the operational environment or network. Tactical patience requires balancing the operational risk of not acting now with opportunities for intelligence gain and greater operational effects in the future.

Information Superiority

The operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. See also information operations.

Consequence Planning

Consequence planning is identifying the possible consequences of proposed actions and develop plans to mitigate as necessary unintended effects.

Crisis Action Planning

Crisis action planning is one of the two types of joint operation planning. The Joint Operation Planning Process involving the time-sensitive development of joint operation plans and operation orders for the deployment, employment, and sustainment of assigned and allocated forces and resources in response to an imminent crisis.

Engage the Networks

Host Nation Legal Considerations

Host nation legal consideration is accounting for the laws and the jurisprudence of citizens of the host nation when planning for the prosecution of targets.

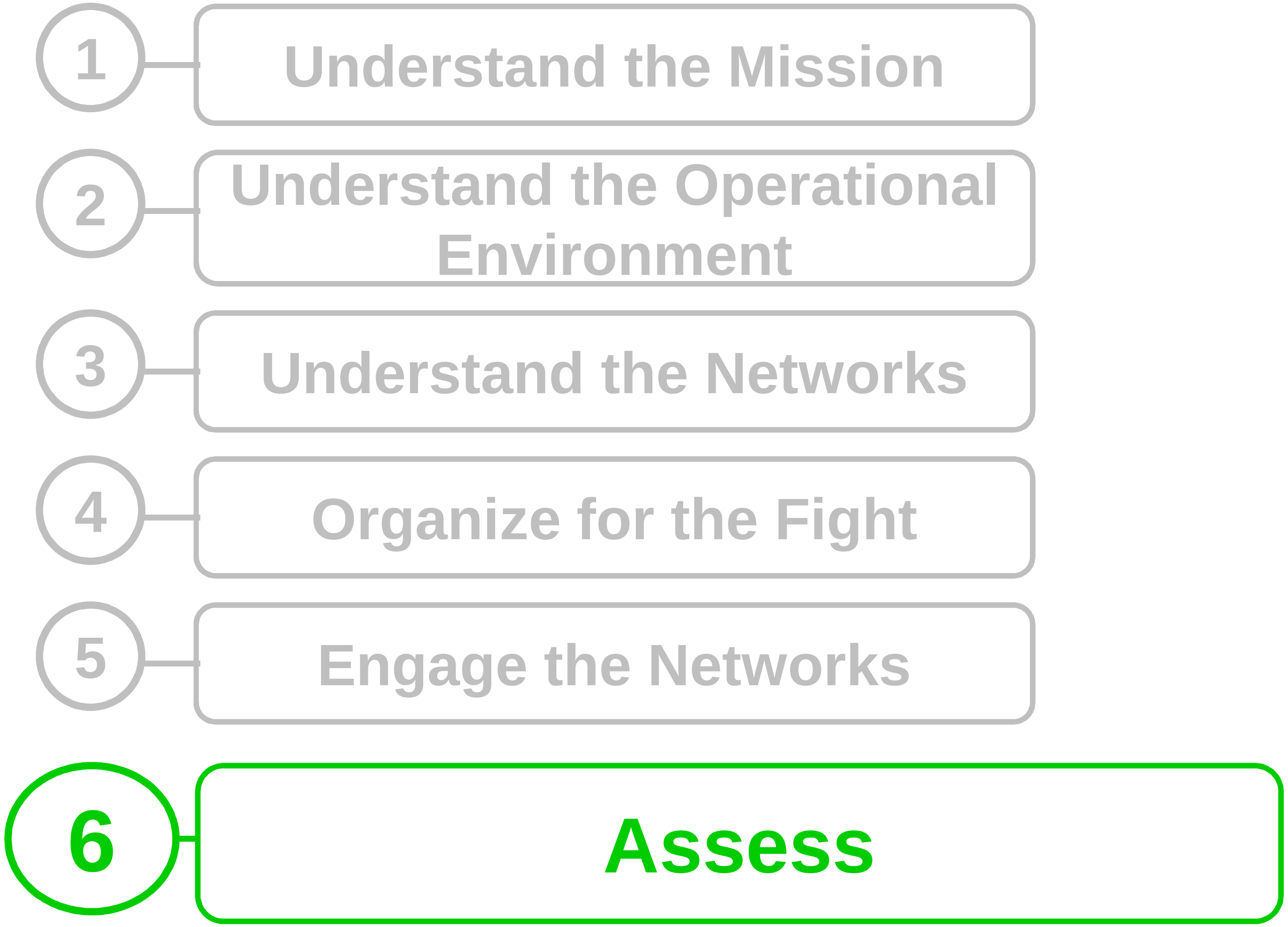
Prosecution Based Targeting

Prosecution-based targeting is a form of nonlethal targeting against an adversary by removing him from the battlefield by using intelligence collection and analysis to build a case that will effectively prosecute him in a host nation's criminal system.

Warrant Based Targeting

Warrant-based targeting is a form of nonlethal targeting against an adversary that uses intelligence in concert with hosts-nation law enforcement and judicial capabilities to generate a warrant against the adversary in order to arrest him and remove him from the battlefield.

Six pillars of Attack the Network:



1 Understand the Mission

2 Understand the Operational Environment

3 Understand the Networks

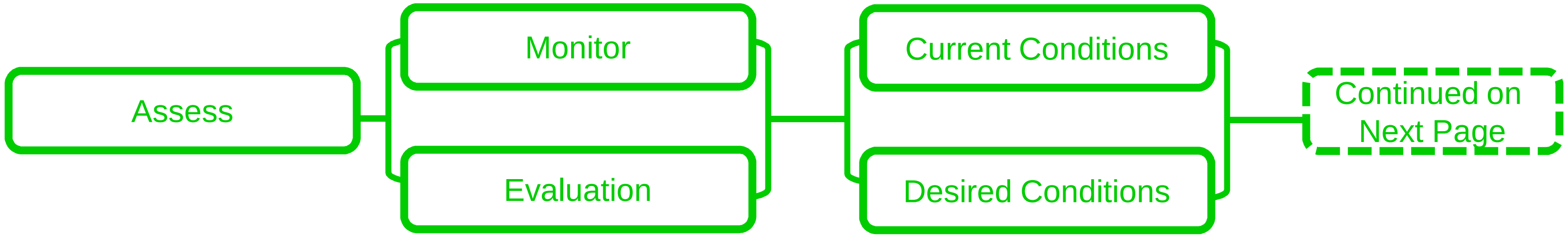
4 Organize for the Fight

5 Engage the Networks

6 Assess

6 ASSESS

To measure continuously the overall effectiveness of employing joint force capabilities during military operations.



Assess

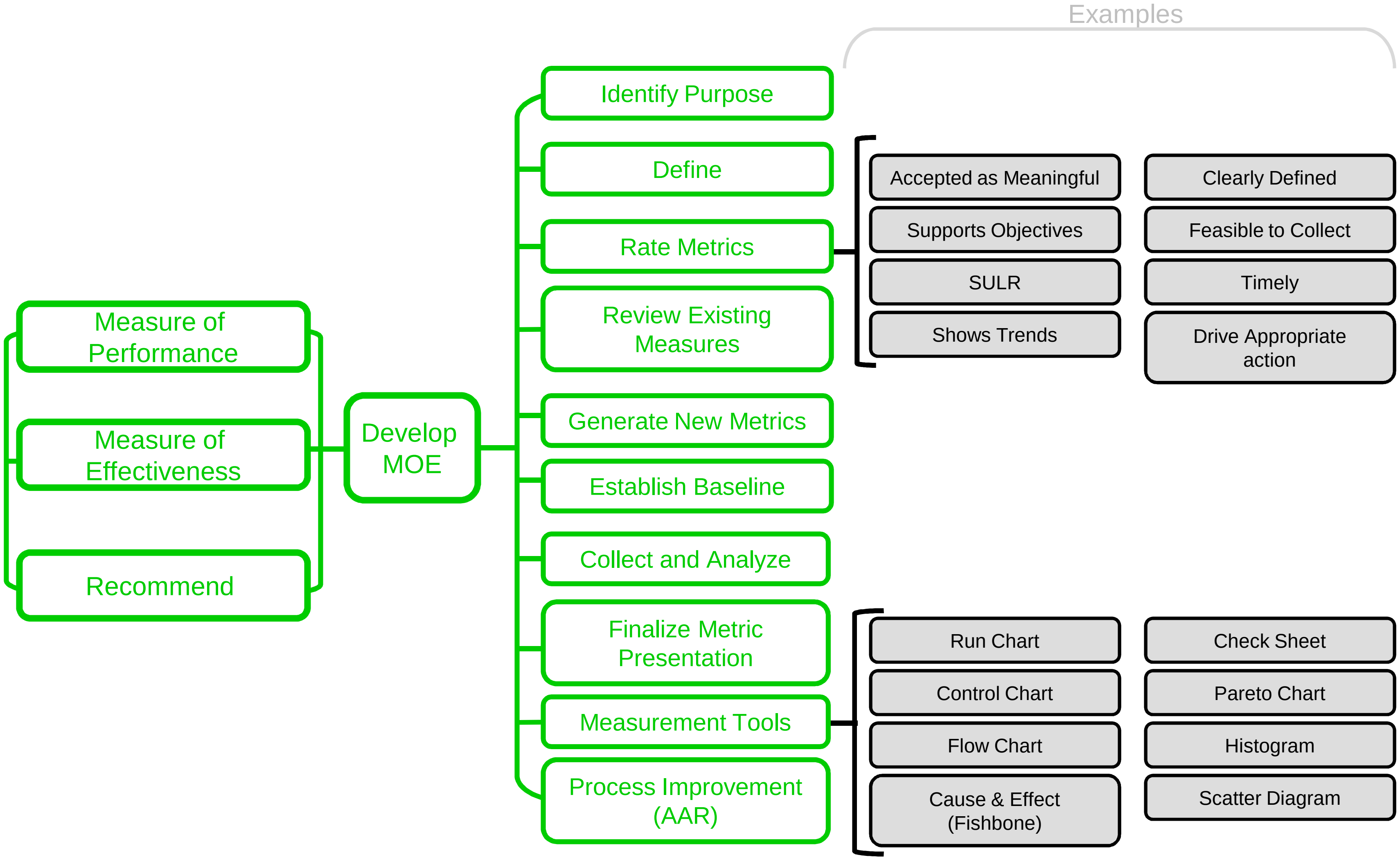
Monitor

Evaluation

Current Conditions

Desired Conditions

Continued on Next Page



Examples

Measure of Performance

Measure of Effectiveness

Recommend

Develop MOE

Identify Purpose

Define

Rate Metrics

Review Existing Measures

Generate New Metrics

Establish Baseline

Collect and Analyze

Finalize Metric Presentation

Measurement Tools

Process Improvement (AAR)

Accepted as Meaningful

Supports Objectives

SULR

Shows Trends

Clearly Defined

Feasible to Collect

Timely

Drive Appropriate action

Run Chart

Control Chart

Flow Chart

Cause & Effect (Fishbone)

Check Sheet

Pareto Chart

Histogram

Scatter Diagram

Assess

Monitor

To monitor is to watch and keep track of friendly network activities and the results on the neutral and threat networks.

Evaluation

Evaluation is the appraisal of the effectiveness (MOE) and performance (MOP) of the friendly network's actions.

Current Conditions

A description of a network's attributes prior to an action or operations designed to alter those attributes to a more favorable, or desired condition.

Desired Conditions

A description of a network's preferred attributes that a commander seeks to realize by undertaking an action or operation.

Measurement of Performance (MoP)

Measures of performance are criteria used to assess friendly actions that is tied to measuring task accomplishment.

Measurement of Effectiveness (MoE) Measures of effectiveness are criteria used to assess changes in system behavior, capability, or operational environment that is tied to measuring the attainment of an end state, achievement of an objective, or creation of an effect.

Develop Measures of Effectiveness

Through out an operation, a commander should create measures of effectiveness that are appropriate to his mission. Develop measures of effectiveness early and continuously refine them as the operation progresses. These measures should cover a range of social, informational, military, and economic issues. Use them to develop an in-depth operational picture. See how the operation is changing, not just that it is starting or ending. Typical measures of effectiveness include the following: percentage of engagements initiated by friendly forces versus those initiated by insurgents; longevity of friendly local leaders in positions of authority; number and quality of tips on insurgent activity that originate spontaneously; economic activity at markets and shops.

Identify Purpose

To identify purpose is to first align one's purpose with the organization's mission, vision, goals, and objectives. These should be inextricably linked to meeting the commander's needs and serve as a foundation for accomplishing and sustaining continuous, measurable improvement.

Define

Define is the who, what, when, why and how of this metric in sufficient detail to permit consistent, repeatable and valid measurement to take place. The operational definition starts with an understanding of the commander's expectations. You then "operationalize" the expectation(s) by defining characteristic(s) of the product, service, or process which are internally measurable and which, if improved, would better satisfy your customers' expectations.

Assess

Rate Metrics

Rate metrics assess a created metric against the eight characteristics of a good metric: meaningful to the customer; tells how well organizational goals and objectives are being met through processes and tasks; is simple, understandable, logical and repeatable; shows a trend; is unambiguously defined; is economical to collect; is timely; drives the "appropriate action."

Accepted as Meaningful

For a measure to be meaningful, it must present data that allow us to take action. It must be mission-oriented and support the meeting of one's organizational goals and objectives. Metrics foster process understanding and motivate action to continually improve the way we do operate.

Supports Objective

A metric must directly support the organization's goals or objectives because it is built from the strategy. All efforts to evaluate one's current situation and steps taken to improve one's processes will be in vain unless the end result is the advancement of the organization toward successfully meeting goals.

Shows Trends

To show trends is to demonstrate a measurement over time extending in a general direction.

Clearly Defined

A metric is clearly defined when it is unambiguously presented or explained.

Feasible to Collect

A metric is feasible to collect when it is economical (in dollars and manpower) to collect over time.

Timely

A metric is timely when it is appropriate for the mission or operation at hand or if it is useful at the moment.

Drive Appropriate Action

Metrics that drive appropriate action should be aligned to organizational objectives and identify which processes are targeted for improvement through their application.

Review Existing Measures

To review existing measures once the link to objectives and goals has been established, it is essential to determine if existing measures or other measurement systems exist that satisfy one's requirements. One should not reinvent the wheel, but use existing process measurements when they exist.

Generate New Metrics

One generates new metrics when measurements used in the past were not process oriented.

Establish Baseline

Baseline data is metric data that is captured at the beginning of an operation in order to compare it to metric data collected over time.

Assess

Collect and Analyze

To collect and analyze metrics is to continue to aggregate metric data over time, to examine trends. It also includes investigating common cause effects on the data and comparing the data to interim performance levels.

Finalize Metric Presentation

To finalize the metric presentation is to present the metric externally. The metric descriptors will provide enough information to communicate the appropriate details of the metric to your customer.

Measurement Tools

Measurement tools in metrics are the proper tools for analyzing and displaying your data.

Run Chart

Run chart is a graph of a process measurement over time.

Control Chart

Control chart is a tool used to analyze process variability over time. They measure the process in a time dimension and show movement toward or away from an average. Control charts have statistically calculated upper and lower control limits.

Flow Chart

Flow chart is a graphic, structured representation of all the major steps in a process.

Cause & Effect (fishbone)

Cause and effect diagram graphically illustrates the relationship between a given outcome and all the factors that influence this outcome. Also called a fishbone diagram (because of its resemblance to a fish skeleton) or Ishikawa diagram (after its inventor Dr. Kaoru Ishikawa).

Check Sheet

Check sheet is a simple form used to collect data in an organized manner.

Pareto Chart

Pareto Chart is a bar graph used to separate the "vital few" from the "trivial many." Based on the Pareto Principal which states that 10-20 percent of the problems have 80-90 percent of the impact.

Histogram

Histogram is a bar chart used to depict the average and variability of a data set.

Scatter Diagram

Scatter diagram is a type of graph used to reveal the possible relationship between two variables.

Process Improvement

In the context of metrics, process improvement is using the data to effect change within your organization.

Recommend

To recommend is to suggest changes within the organization based upon acceptable metrics, their collection, and analysis.

NOTES

NOTES

Prepared for the Joint Improvised Explosive Device
Defeat Organization by Toffler Associates under Air Force
Research Laboratory contract # FA8650-09-F-7955