AIR LAND SEA BULLETIN




Issue No. 2012-3 **Air Land Sea Application (ALSA) Center** *September 2012*

Attack the Network

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
SEP 2012		**00-00-2012 to 00-00-2012**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Air Land Sea Bulletin. Issue Number 2012-3. September 2012	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Air Land Sea Application (ALSA) Center,114 Andrews Street,Langley AFB,VA,23665-2785**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**36**	

ALSA Staff

Director

COL Bruce Sones, USA

Deputy Director

Col Robert C. Swaringen, USAF

Editor

Ms. Patricia Radcliffe, Civilian, USAF

Layout

Ms. Laura Caswell, Civilian, USN

Publications Officer

Maj Clayton Laughlin, USAF

Purpose: The ALSA Center publishes the *ALSB* three times a year. ALSA is a multi-Service DOD field agency sponsored by the US Army Training and Doctrine Command (TRADOC), Marine Corps Combat Development Command (MCCDC), Navy Warfare Development Command (NWDC), and Curtis E. LeMay Center for Doctrine Development and Education (LeMay Center). This periodical is governed by Army Regulation 25-30, Chapter 10. The ALSB is a vehicle to "spread the word" on recent developments in warfighting concepts, issues, and Service interoperability. The intent is to provide a cross-Service flow of information among readers around the globe.

Disclaimer: Since the ALSB is an open forum, the articles, letters, and opinions expressed or implied herein should not be construed as the official position of TRADOC, MCCDC, NWDC, Lemay Center, or ALSA Center.

Submissions: We solicit articles and reader's comments. Contributions of 1,500 words or less are ideal. Submit contributions, double-spaced in MS Word. Include the author's name, title, complete unit address, telephone number, and email address. Graphics can appear in an article, but a **separate computer file for each graphic and photograph (photos must be 300 dpi) must be provided**. Send email submissions to alsadirector@langley.af.mil. The ALSA Center reserves the right to edit content to meet space limitations and conform to the *ALSB* style and format.

Next issue: January 2013; Submission DEADLINE: COB 1 October 2012. The theme of this issue is "SOF and Conventional Force Integration".

Reprints: ALSA Center grants permission to reprint articles. Please credit the author and the *ALSB*. Local reproduction of the *ALSB* is authorized and encouraged.

Subscriptions: We continue to validate our subscriber's information and requirements. If you wish to **discontinue your subscription** of the *ALSB*, please send an email to alsa_alb@langley.af.mil.

ALSA Center Web Sites: The *ALSB* and MTTP publications are available at our public web site http://www.alsa.mil and our CAC-enabled web site: https://wwwmil.alsa.mil. For classified ALSA MTTP publications, visit http://www.acc.af.smil.mil/alsa

CONTENTS

Director's Comments 3

FEATURE ARTICLES

Expanding Attack the Network..... 4

Friendly, Neutral, and Threat Networks Show Comparable Engagement Value 8

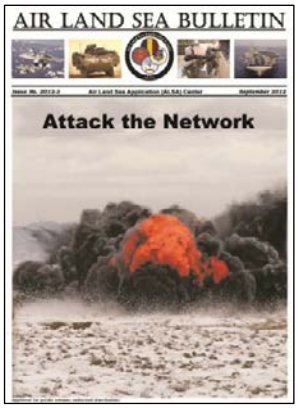
Networks in the Operational Environment ... How Can We Exploit Them?..... 14

Western Way of War is the Wrong Approach for Current Counterinsurgency 21

..... 26

IN HOUSE

Current ALSA MTTP Publications..... 30
SOF and Conventional Force Integration–Upcoming ALSB .. 33
ALSA Organization..... 34
ALSA Mission and Voting JASC Members 35
Online Access to ALSA Products..... 35



Cover photo—A mine-clearing line charge explodes during a route clearing mission in Paktika Province, Afghanistan. The charges are used to help clear routes of possible improvised explosive devices 10 February 2011. (Photo by SPC Zachary Burke, USA)

DIRECTOR'S COMMENTS

The Air Land Sea Application (ALSA) Center is experiencing its summer "changing of the guard" with personnel turnover. We would like to recognize and bid farewell to Lt Col Michael Woltman who retires after four years of service at ALSA and 28 years of total military service, and recognize and farewell Lt Col Andrew Frasch, who leaves us after two years, for assignment to the 421st Combat Training Squadron. We welcome their replacements, Maj Albert Denney and Lt Col (S) Joel Eppley, and also welcome aboard Col Robert Swaringen as the new deputy director for ALSA.

ALSA is currently working on 30 of the 35 multi-Service tactics, techniques, and procedures (MTTP) publications and expanding its use of information technology to reach more people in more innovative and efficient ways. This all supports our efforts to make MTTP more timely, relevant and compelling to meet the immediate needs of the warfighter

We invite you to visit our webpage at http://www.alsa.mil to get linked in to what ALSA is doing. At our webpage you can find all of the ALSA MTTP publications as well as our current and past editions of the Air Land Sea Bulletin (ALSB) in PDF format (downloadable to e-readers). Furthermore, we offer the option to view the ALSB online in Flash (SWF) format. To get an electronic notification of release dates for MTTP which are under revision, or the publication of the ALSBs send your organizational, military, or personal email addresses to: alsa_alb@langley.af.mil.

The intent of this ALSB is to explore the evolution of Attack the Network (AtN) from its inception as the improvised explosive device defeat mechanism, to where it is today: a holistic doctrinal approach to defeating all threat networks. The articles show the importance in retaining lessons learned and remembering basic mission analysis. Focusing efforts on all aspects of AtN and remembering the basics will help preserve the force and facilitate smarter, faster, more efficent enemy engagement across the range of military operations.

The first article, "Expanding Attack the Network", was authored by Scott Kinner of Marine Corps Training Operations Group. It addresses AtN from inception to its present status.

The second article, "Friendly, Neutral and Threat Networks Show Comparable Engagement Value", written by LTC Haimes Kilgore, Patrick Ryan, Mark Villegas, Jean-Yves Wood, and Michael Grant, expands on the future of AtN.

"Networks in the Operational Environment … How Can We Exploit Them?" was written by the Training Brain Operations Center and United States Army Maneuver Center of Excellence AtN Team, and further details various aspects of doctrinal AtN.

The next trio of writers, MAJ Zachary Basford, Lt Col Richard Freeman, and LCDR Michael Marquez wrote a point paper, "Western Way of War is the Wrong Approach for Current Counterinsurgency", for Joint Professional Military Education Phase II. This article contrasts counter-insurgency (COIN) aspects of AtN with traditional Western warfare techniques.

The last article is, "Role of Law Enforcement Professionals in Attack the Network Strategy", written by Richard Crawford and LtCol Adam Tharp. It details law enforcement in AtN.

Our next ALSB has a January 2013 publishing date. The topic is "SOF and Conventional Force Integration". To submit articles for consideration, email them to alsac2@langley.af.mil no later than 1 October 2012. As always, we value your feedback on our ALSB's and MTTP. Let us know how we are doing!

BRUCE V. SONES, Colonel, USA

Director

EXPANDING ATTACK THE NETWORK

US Navy Petty Officer First Class Travis Tellez, an explosive ordnance disposal (EOD) technician with EOD Platoon 815, inspects a device during a mission to safely remove, transport, and destroy explosives stored at an Afghan National Army (ANA) compound in Farah City, Farah Province, Afghanistan, 27 December 2011. ANA forces, Provincial Reconstruction Team Farah, and the EOD platoon worked together to safely destroy more than 250 weapons and more than 1,300 pounds of explosive material. (Photo by 1LT Mark Graff, USA)

By Scott Kinner

To many observers, Attack the Network (AtN) began, and is still most often associated with, counter-improvised explosive device (IED) efforts. Rather than spending time and energy in a classic competition between increasing or defeating armor; adding protection or increasing the size of IEDs; it became apparent that attacking networks that funded, created, planned, and implanted IEDs was more effective and economical.

… it became apparent that attacking networks that funded, created, planned, and implanted IEDs was more effective and economical.

Within the Marine Corps, operational forces and formal learning centers recognized the basic premise behind AtN applied in a far broader sense than merely that of the counter-IED fight. Marine Corps leaders were not alone in coming to this conclusion. As the Marine Corps worked with the Army on counterinsurgency doctrine, offensive and defensive tactics, and other efforts, both services recognized when it came to networks, the joint force "had been there before."

Indeed, from the birth of the nation, through the Indian Wars and Cold War, the joint force always possessed an interest in networks – command and control (C2), air defense, economic, social, political, information, etc. From its origins in World War I to present-day operations in Libya, Air Force planners sought to understand industrial, communications, economic, and transportation networks and how they could be pressured, degraded, and influenced. Navy and Marine Corps leaders sought to understand and affect trade, political, economic, military, and social networks by enlisting desert allies in the Barbary

Pirate Wars of yesteryear and conducting key leader engagements in Afghanistan today. In the Army's work as a frontier constabulary in the early years of this country, through modern-day involvement in the Philippines, Africa, the Balkans, Iraq, and Afghanistan, it has sought to mitigate or support various networks tied to the threat and local populace. From conventional adversaries to hybrid threats, formal networks and systems, to informal social and financial networks, AtN is well-trod joint ground. This means rather than a newly discovered concept, formally acknowledging AtN is, perhaps, evidence that something valuable has been lost. To ensure AtN is not lost and to expand it beyond merely defeating a particular tactic, the joint community must relearn the old, update it with the new, and formalize the framework for identifying and influencing networks.

The first requirement in accomplishing this is to demystify the academic jargon and network theory terminology that seem to surround any discussion of AtN. The fact is, we use, operate, live with, and within systems and networks all the time. We meet and talk with friends – our social network – and "network" at parties and conferences. Networks consist of people, things, and combinations of both. Simply using a cell phone to contact a group of friends to determine in which house a party will meet and figure out who is bringing what, is an example of a network.

We may use all manner of things to attack, defend, or influence networks. The Stuxnet virus damaged Iranian centrifuges processing nuclear materials in 2010. It was a cyber weapon that probably used a human network to enter an Iranian facility and a computer network to do its damage thereby influencing ancillary networks (e.g., political, organizational, security, and social).

Networks may be friendly, neutral, or enemy in nature. We must protect our networks, target those of the enemy, and influence neutral networks to either support us or at least not stand in our way. Every aspect of mission accomplishment for the joint force conducting foreign humanitarian assistance, for example, is affected by the force's understanding, or lack of understanding, of networks. The force must identify, work with, encourage, and influence networks of local governmental and security officials, allied nations, or nongovernmental organizations and identify and mitigate threat or potential threat networks. The joint force must engage with media and social networks in the information environment. Also, it must understand transportation networks and how they interact with deliveries of relief and those who will receive the relief (e.g., the joint force can get to a drop location, but can the populace get there?). It must understand the physical places and means that make up these networks – from cell phone towers and asphalt roads to fiber optic cables and electrical grids.

The AtN concept would not have seemed foreign to Soldiers, Marines, Sailors, or Airmen of yesteryear. What is new is the fact the joint world recognizes the need to name and codify AtN in doctrine and practice.

What is new is the fact the joint world recognizes the need to name and codify AtN in doctrine and practice.

This introduces the second requirement necessary to expand the concept of AtN: context. AtN is not operation specific. As seen in figure 1, it is always done in some manner and also applies across everything the joint force does across the conflict continuum and range of military operations. It applies to offense, defense, stability, and defense support to civil authorities in various balances or mixes. It is not people specific; the network and systems people use may be more important than the people themselves. AtN is not specific to any military domain. A network of narco-terrorists – those who use terrorist tactics in dealing illicit drugs – will occupy portions of land and space domains, the information environment, and even air and sea domains, depending on their operations.

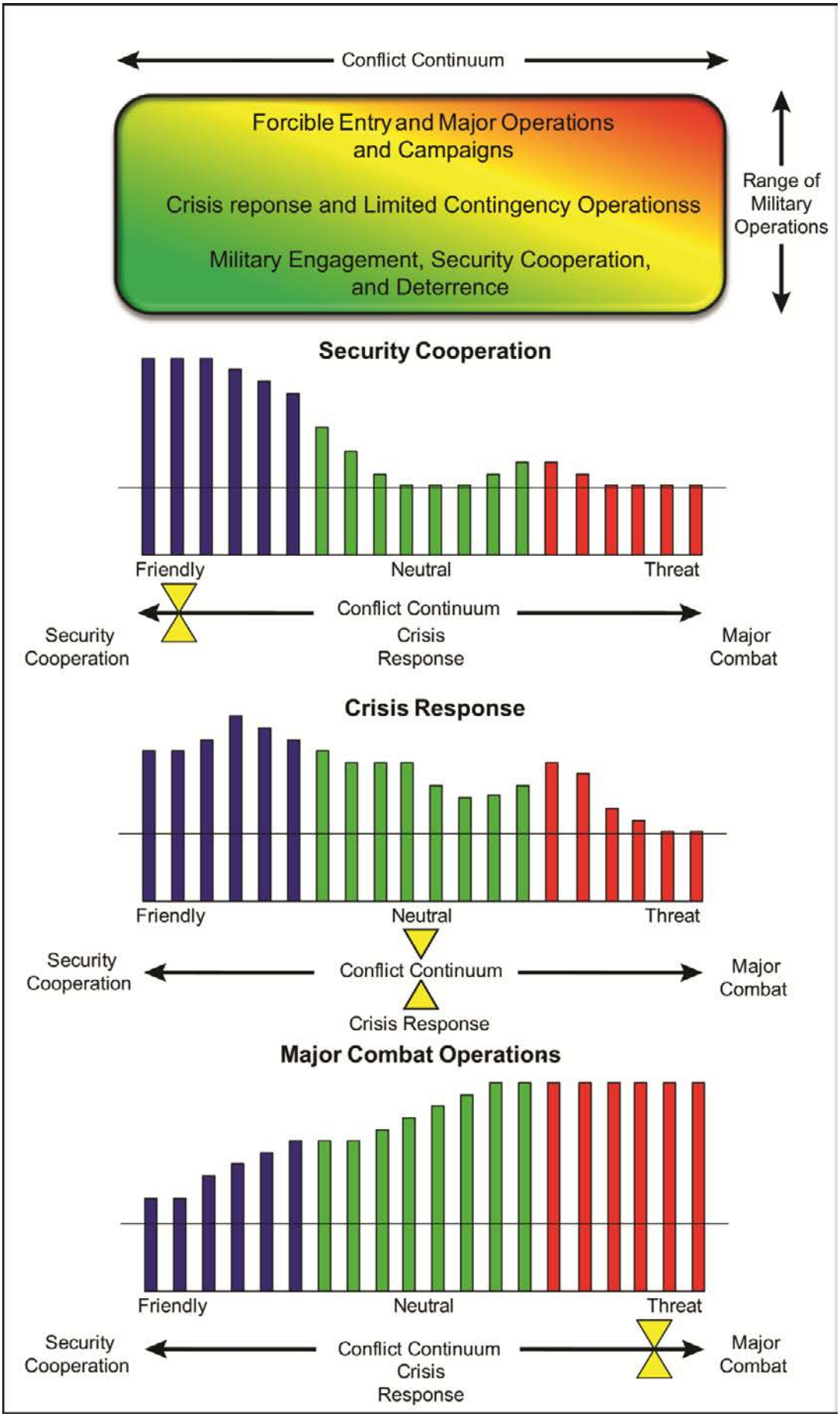


Figure 1. AtN Across the Conflict Continuum

The third requirement necessary to expand the concept of AtN is terminology, or language. "Network engagement" or "attacking the network" are fairly straight-forward concepts. Attacking a network consists of identifying it, determining whether it is important or not, and using the means at hand to defeat it. Engaging the network merely broadens the concept. We engage friendly networks by defending them, neutral networks by influencing or mitigating them, and threat networks by defeating or destroying them.

If the AtN concept is understood as something the joint force has always done, it applies across the conflict continuum and range of military operations and its language is not difficult to understand. Then the question is: "so what?"

By acknowledging AtN in a formal, doctrinal manner, the joint community can understand and recognize what it is once and for all without constantly having to relearn the concept. Instead of determining the requirement to learn the local network of political actors in the midst of an operation, an educated joint force that understands and has integrated AtN will determine that information and its relevance beforehand.

This does not mean the joint community needs to add another process or checklist, but it needs to recognize what it is already doing and institutionalize AtN as a framework that informs forces engaged in discussion and analysis. The AtN framework completely and seamlessly integrated into the intelligence preparation of the operational environment and intelligence preparation of the battlespace/battlefield processes is not as much something new as it is something newly labeled. This integration is something we have been doing, but need to do more consistently. There is no need for a new procedure to recognize the enemy's C2 network should be analyzed and targeted. A new staff process is not necessary to realize understanding local civic and social networks is important when conducting nation assistance. Another bloated paper drill is not required for the joint task force conducting a noncombatant evacuation operation to realize the local economic network is irrelevant, but the networks of armed, local nationalists are key information points.

In summary, AtN does not add steps to planning and execution as much as it serves to remind commanders and their staffs networks in the battlespace are present and need to be addressed. Identifying and attacking networks is nothing new for a worldwide deployable joint force. What is different from the network engagement previously conducted by this nation's armed services is AtN is evolving into a formal framework that names and organizes this knowledge. A formal, neatly integrated AtN approach prevents having to relearn recently regained information. Also, it prevents future commanders and their staffs from having to use discovery learning as the means to attack, defend, and influence the networks around them. It enables the joint force to better~~,~~ and more efficiently, solve the problems the nation and the world present it.

Identifying and attacking networks is nothing new for a worldwide deployable joint force.

FRIENDLY, NEUTRAL, AND THREAT NETWORKS SHOW COMPARABLE ENGAGEMENT VALUE

Soldiers with Alpha Company, 4th Brigade Special Troops Battalion, 4th Brigade Combat Team, 101st Airborne Division launch a mine clearing explosive line charge on a road in Paktika Province, Afghanistan, 10 February 2011. The route clearing procedure was used to destroy improvised explosive devices. (Photo by SPC Zach Burke, USA)

By LTC Haimes Kilgore, Patrick Ryan, Mark Villegas, Jean-Yves Wood, and Michael Grant

Attack the Network (AtN) focused on neutralizing the threat network, which caused commanders, in most instances, to overlook friendly and neutral networks. Network engagement changes the commander's focus from solely attacking threat networks to identifying, defining, and effectively engaging friendly, neutral, and threat networks, giving the host nation (HN) the capability to operate independently of United States (US) or North American Treaty Organization forces. The numerous adaptive networks pose varying threats to unified land operations. To neutralize threat networks, commanders must support and influence friendly and neutral networks where US Soldiers converse with citizens in a non-threatening manner. Accomplishing the aforementioned tasks require a unified approach to conduct network engagement as it is understood and internalized by commanders, staffs, and Soldiers. The Maneuver Center of Excellence, Fort Benning, Georgia is the proponent for the Army's network engagement (AtN) line of effort at the brigade level, and below.

To neutralize threat networks, commanders must support and influence friendly and neutral networks

WHAT IS A NETWORK?

A network is a series of direct and indirect ties from one entity to a collection of others. Network engagement delineates networks into three separate categories: friendly, neutral, and threat. Friendly networks share objectives that are aligned with US, coalition, and HN interests. They

generally support the commander's operational goals. A neutral network does not actively support or oppose US, coalition and HN interests or impact the commander's operational goals. Neutral networks are not generally considered to be a current threat or asset, but should be a significant focus for targeting resources to effectively influence them to support US, coalition and HN interests. A threat network has goals or objectives that actively oppose US, coalition, and HN interests and negatively impact the commander's operational goals and actions.

A successful network engagement program includes network analysis, template creating, and targeting. Understanding the three types of networks begins with a basic appreciation for their structure, characteristics, dynamics, and purposes. Although different from an analysis of a conventional military threat, the analytical process for describing networks and predicting their behavior is largely the same.

The network engagement operational approach rests on six pillars which comprise its backbone. These pillars are:

- Understand the mission.
- Understand the operational environment.
- Understand the networks.
- Organize for the fight.
- Engage the networks.
- Assess the current situation, evaluate progress toward the desired end state and recommend improvements.

UNDERSTANDING THE MISSION AND THE OPERATIONAL ENVIRONMENT

Understanding the mission is achieved by first understanding the commander's intent. It is essential to understand the network engagement mission in context with the larger, operational and strategic mission. Understanding the commander's intent is the key for creating detailed network engagement planning. It begins with the orders or initial guidance of the higher commander and is part of the military decision-making process (MDMP) found in the Army Tactics, Techniques and Procedures 5-0.1, Commander and Staff Officer Guide (chapter 5). Specifically, the MDMP steps of mission analysis (step 2), course of action (COA) development (step 3), and COA approval (step 6) are the most critical for network engagement operational planning. The output is the commander's selected COA, refined intent, and commander's critical information requirements and essential elements of friendly information.

Operational environment analysis is critical to network engagement. Figure 1 shows operational environments are composites of the conditions, circumstances, and influences that affect employing capabilities, and bears on the decisions of the commander. While they include all friendly, neutral, and threat networks, they also include an understanding of the physical environment, the state of governance, technology, local resources, and the culture of the local population. Outcomes are measured by the threat's capacity to conduct operations and the residual effect those actions have on the population.

THE NETWORK ENGAGEMENT OPERATIONAL APPROACH

The overall objective of network engagement is to increase the capability of the HN or civil authority while reducing the capability of threat networks to a level that is manageable by the friendly network. While neutral networks are a focus of network engagement, the decisive point occurs when the capabilities of friendly networks exceed those of threat networks as seen in figure 2.

The overall objective of network engagement is to increase the capability of the HN or civil authority

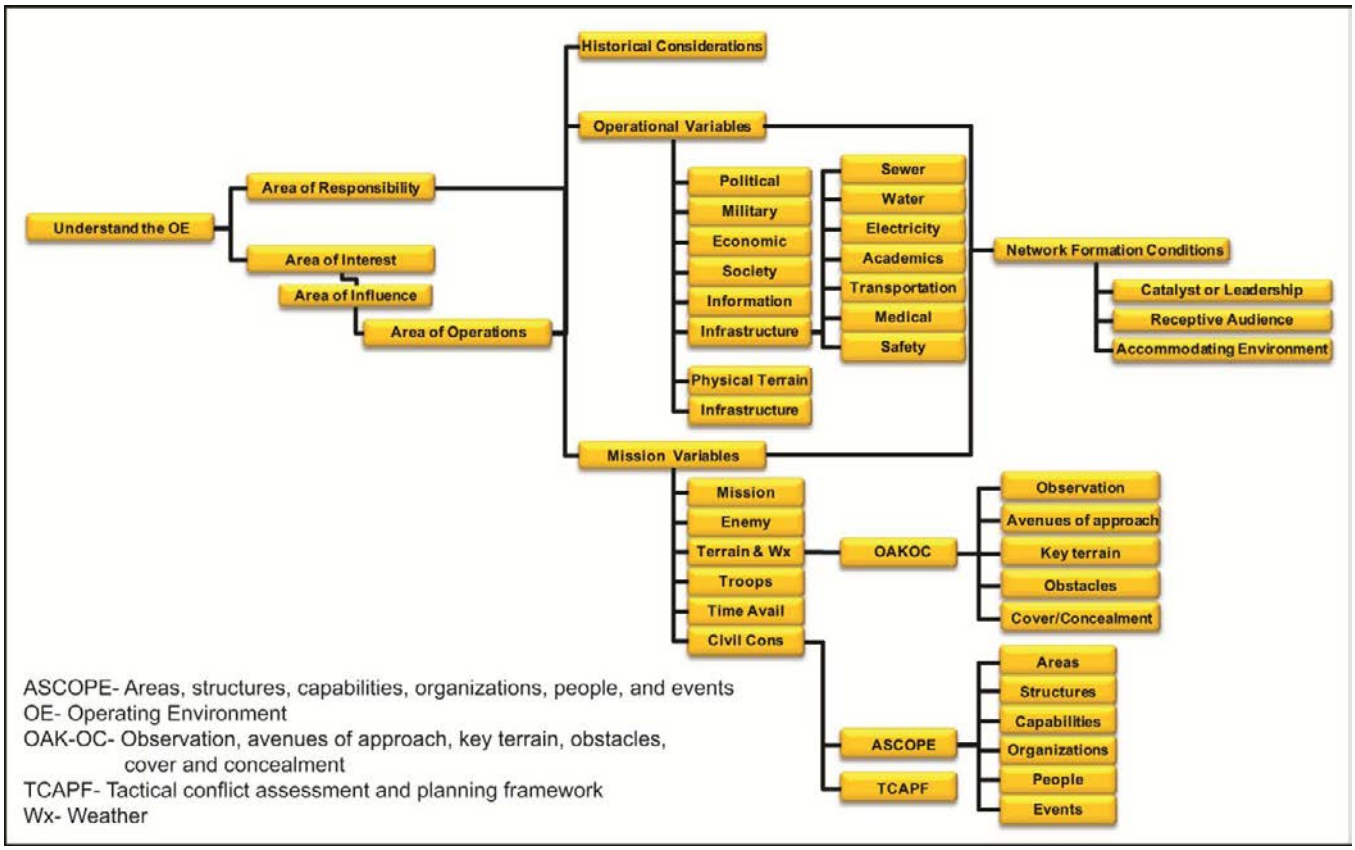


Figure 1. Network Engagement Operational Approach

The network engagement operational approach includes five lines of effort which:

- Support friendly networks as the decisive operation.
- Influence neutral networks as a shaping operation.
- Neutralize threat networks as a shaping operation.
- Protect the force as a sustaining operation.
- Inform and influence activities (IIA) as an all-encompassing shaping operation for the overall mission.

Critical factor analysis allows commanders to see the network and determine its center of gravity and identifies its critical capabilities.

The decisive operation for network engagement is supporting and enabling friendly networks to function effectively to manage the residual threats posed by other networks. At any moment, the main effort of an action may be something other than the decisive operation. Protecting the force or neutralizing threat networks may be an immediate need to create the ability to support friendly networks.

There are numerous analytical methods and tools available to identify network trends, links, associations, patterns and activities. Trend analysis, pattern analysis, pattern plot sheets, incident maps, time-event charts, link analysis and association matrices, activities matrices, and social network analysis can be used in network engagement. Critical factor analysis allows commanders to see the network and determine its center of gravity and identifies its critical capabilities.

Each network has a particular set of conditions, allowing it to function in a specific manner. Commanders must determine what the desired conditions and functions should be to support the overall operation. The unit staff uses the analytical methods available to identify COA that establish the commander's end state for each network or cell of interest. COA are planned through the targeting

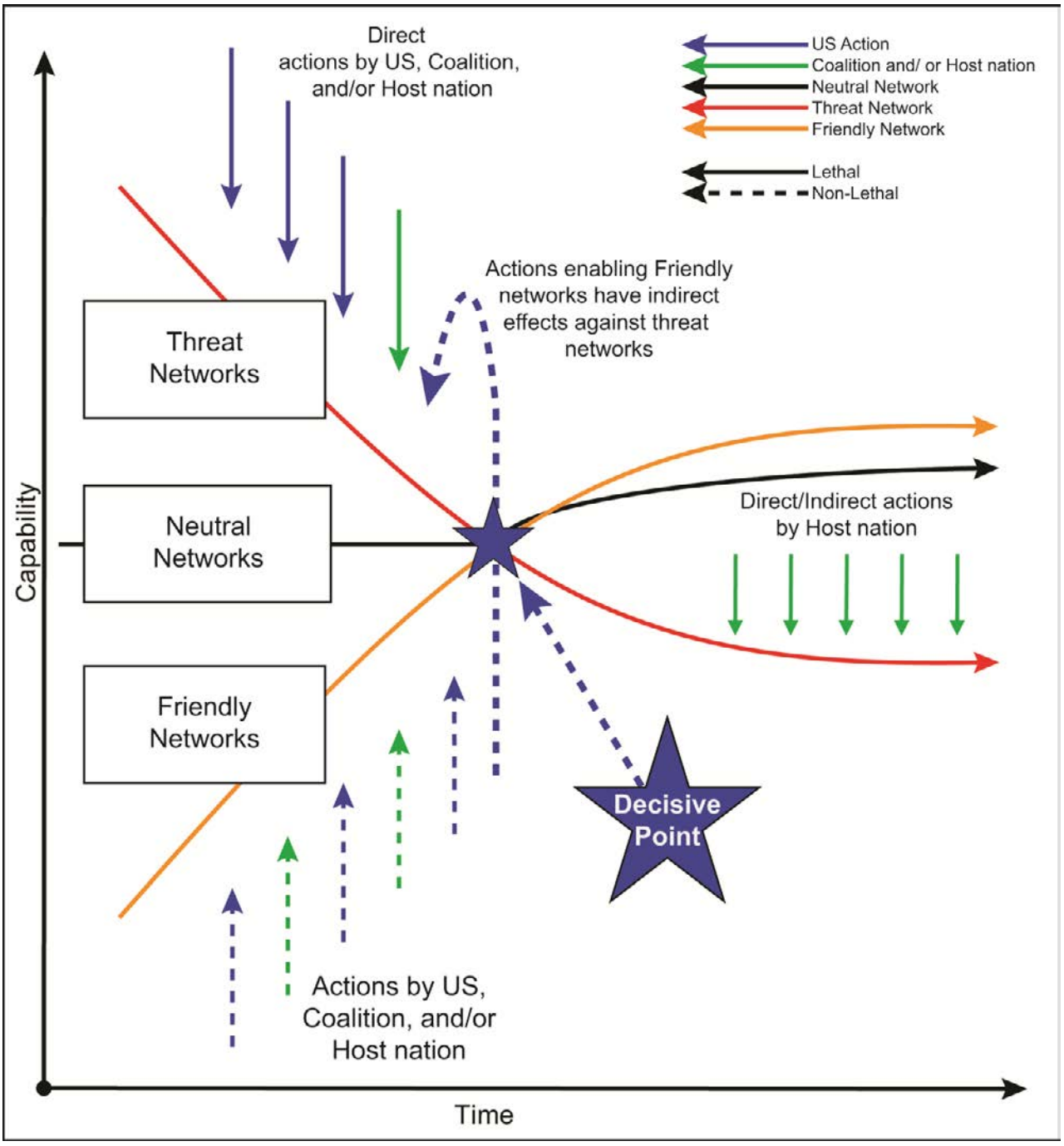


Figure 2. Attack the Network Concept

process and executed during operations. Targeting is the practice of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities (See Field Manual 3-60 for more information). In network engagement, the targeting process allows the commander and staff to synchronize intelligence, maneuver fire support systems, nonlethal systems, special operations forces, and other enablers. During network engagement operations, targeting is a resource and synchronization effort to achieve desired effects. Synchronizing lethal and nonlethal targeting actions is critical to network engagement. A target may be a person, place, process, organization, infrastructure, piece of equipment; capability, system, or function (a node). Friendly and neutral networks must be identified during the targeting process with nonlethal means to produce a friendly advantage as seen in figure 3.

Friendly and neutral networks must be identified during the targeting process …

The most significant measure of success in comprehensive network engagement operations is building and maintaining lasting relationships. The commander and staff understand this focus and build relationships rather than focus on short-term gains achieved from classic lethal targeting engagements. Considering the commander's goals within the operational approach, the network engagement mission should always be supported with inform and influence activities, and be aligned with the strategic communication plan.

Network engagement enablers are organizations with capabilities available to the commander that can be organic, attached, deployed within theater, or available through reach back. Understanding what these capabilities bring to the fight and integrating them into the commander's plan are critical. Enablers include a wide range of organizations and capabilities. The commander and staff determine which enablers are appropriate and available, and how to exchange information with the enablers. Some examples of enablers are the Counter IED Operational Integration Center, Counter Insurgency Targeting Program, law enforcement professionals, and operations research systems analysts.

Network engagement is best orchestrated with horizontal and vertical information coordination through working groups or cells

Network engagement operations are focused and conducted through forming unit working groups, or information cells, that gather intelligence, inform the commander, and perform targeting processes. At the battalion/brigade level, the formation of working groups may be driven by the commander's desire to task-organize by warfighting function. The overarching purpose of working groups is to collect and assess information needed by the commander for operational decisions that address the tactical problem.

Network engagement is best orchestrated with horizontal and vertical information coordination through working groups or cells, to assist the brigade staff in being as responsive, flexible, and adaptive as the networked threat it is opposing. Including

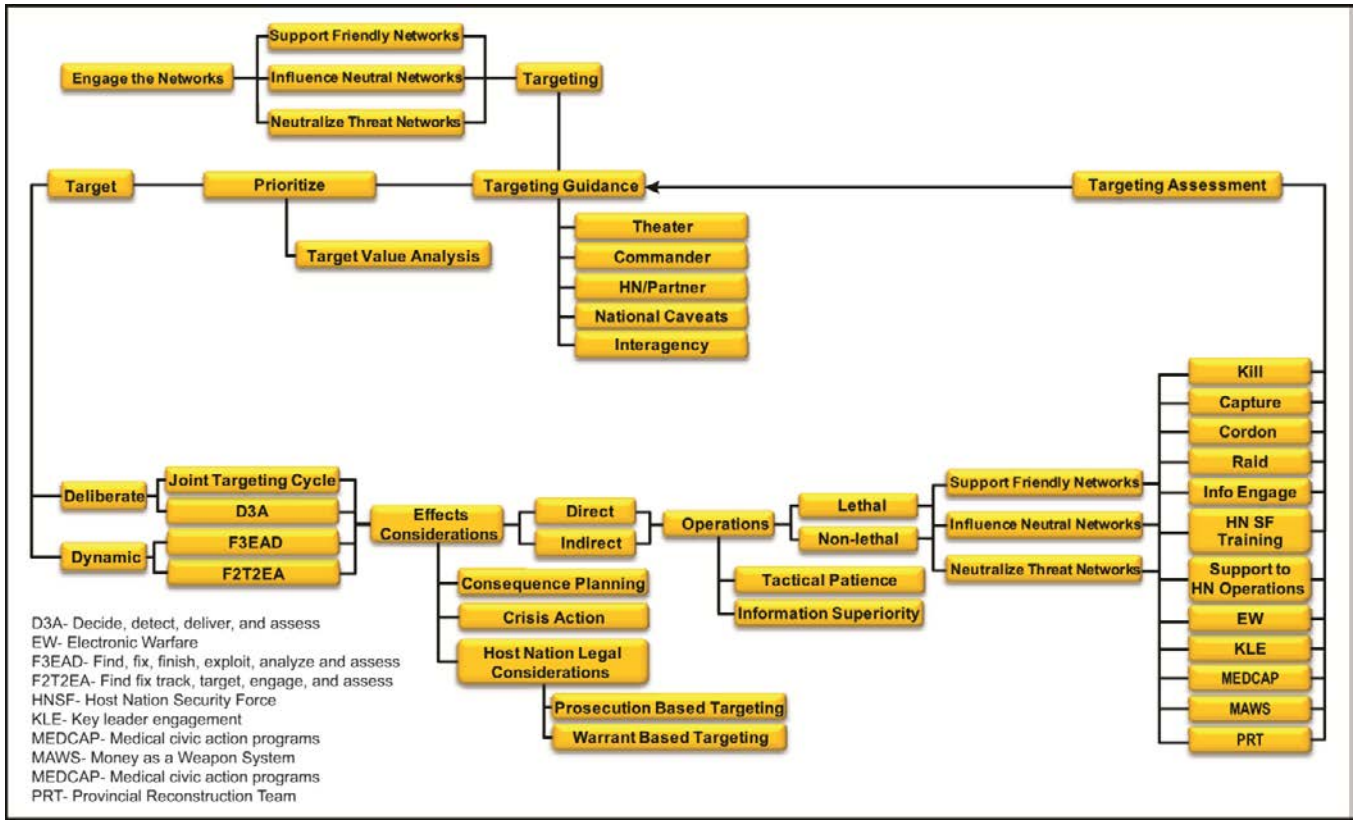


Figure 3. Human Network Engagement

A US Soldier, left, with 2nd Platoon, Alpha Troop, 3rd Squadron, 4th Cavalry Regiment, 25th Infantry Division, Task Force Raider, scans the thumb print of a local Afghan man, using a handheld interagency identity detection equipment at a checkpoint in the Nazyan District, Nangarhar Province, Afghanistan, 10 March 2012. (Photo by SPC Amber Leach, USA)

working groups or cells within the normal staff structure assists the commander in organizing and managing resource constraints, designing the network engagement construct to pool resources and clearly delineating staff section responsibilities so they perform complementary functions with minimum overlap.

Network engagement uses current doctrinal processes to identify and neutralize threat networks by mitigating their effects on operations while simultaneously supporting friendly and influencing neutral networks. Network engagement places an emphasis on not just neutralizing a threat with military power, but influencing neutral and friendly networks to act as force multipliers in defeating threat networks. The complexity of the brigade combat team's capabilities and systems requires an enhanced effort to address training and educational responsibilities across the force to execute network engagement effectively. It is imperative that Soldiers, units, and leaders are adequately prepared to engage networks and the threats they pose by incorporating network engagement processes as an integral effort in individual, collective, predeployment and deployed training. Units should train with a comprehensive network engagement strategy that focuses on addressing the causes behind networks, and their actions and impacts on US, coalition, and HN forces, and civilian populations.

The Maneuver Center of Excellence, Fort Benning, Georgia is the lead on network engagement. For additional information, contact LTC Haimes Kilgore at (706) 545-5989 DSN (835), haimes.a.kilgore.mil@mail.mil or Patrick Ryan at (706) 545-3532 DSN (835), patrick.h.ryan6.ctr@mail.mil.

AtN training materials can be located on the MCoE AtN Team Warrior University page: https://www.warrioruniversity.army.mil/training-wiki/-/wiki/Main/MCoE+Attack+the+Network Common Access Card is required to access this site.

Network engagement places an emphasis on not just neutralizing a threat with military power, but influencing neutral and friendly networks to act as force multipliers

NETWORKS IN THE OPERATIONAL ENVIRONMENT … HOW CAN WE EXPLOIT THEM?

Mark Covey, far right, of Systems Integration Modeling and Simulation for Joint Training Counter-Improvised Explosive Device Operations Integration Center (JTCOIC), demonstrates JTCOIC's capabilities for simulation for an unidentified colonel, left, Under Secretary of the Army Joseph W. Westphal, second from left, and LT GEN Mark P. Hertling, center, at the JTCOIC office in Newport News, Virginia, 16 July 2010. (Photo by SGT Angelica Golindano, USA)

By Training Brain Operations Center (TBOC) and U.S. Army Maneuver Center of Excellence Attack the Network Teams

"Context is king. Achieving an understanding of what is happening… comes from a truly integrated picture of an area, the situation, and the various personalities in it. It demands a layered approach over time that builds depth of understanding and context …"[1] **LTG Michael T. Flynn and BG Charles A. Flynn, *United States (US) Army***

The purpose of network analysis is to support planning for network engagement.

Most military personnel think of either computer network activities or lethal targeting operations when they hear the term "Attack the Network (AtN)", but kill/capture operations are just narrow elements within the AtN lines of effort, as currently defined. Among other things, AtN includes conducting actions and operations to support friendly, neutralize threat, and influence neutral networks. Furthermore, neither kill/capture operations, nor neutralizing threat networks represent the decisive effort within AtN. The decisive line of effort is often supporting friendly networks.

The purpose of network analysis is to support planning for network engagement. In this context, network engagement is comprised of five lines of effort and six pillars.[2] This article focuses on developing a better understanding of three of the five lines of effort and two of the six pillars. The lines of effort being considered are: support friendly networks, neutralize threat networks, and influence neutral networks. The two pillars are: understand the operational environment (OE) and understand

the networks. This does not imply the other lines of effort (i.e., protecting the force as a sustaining operation, and inform and influence activities as an all-encompassing shaping operation for the overall mission) and pillars (i.e., understand the mission, organize for the fight, engage the networks, and assess) are less significant. They're simply less relevant to the content of this short article.

The decisive point of network engagement is reached when threat networks are sufficiently degraded and friendly networks are sufficiently developed, so friendly networks can contain and manage any residual adaptive networked threats independently and in a sustained manner. Figure 1 shows successful network engagement is achieved at and beyond the decisive point.

Another important point shown in figure 1 is networks can be degraded indirectly. The effect of indirectly neutralizing threat networks through the support of friendly networks reinforces the concept that supporting friendly networks is often the decisive AtN effort.

Looking at two pillars of AtN, understand the OE and understand the networks, it becomes clear network analysis should be based on understanding the broader OE, because networks are an integral part of it. The more clearly the OE is understood, the more precisely its networks can be analyzed.

Understanding the OE is based on gathering and analyzing information in terms of the operational variables: political, military, economic, social, information, and infrastructure (PMESII). This allows commanders to understand the conditions and circumstances of the environment and influences the employment of capabilities that bear on the decisions of the commander.

The decisive point of network engagement is reached when threat networks are sufficiently degraded and friendly networks are sufficiently developed …

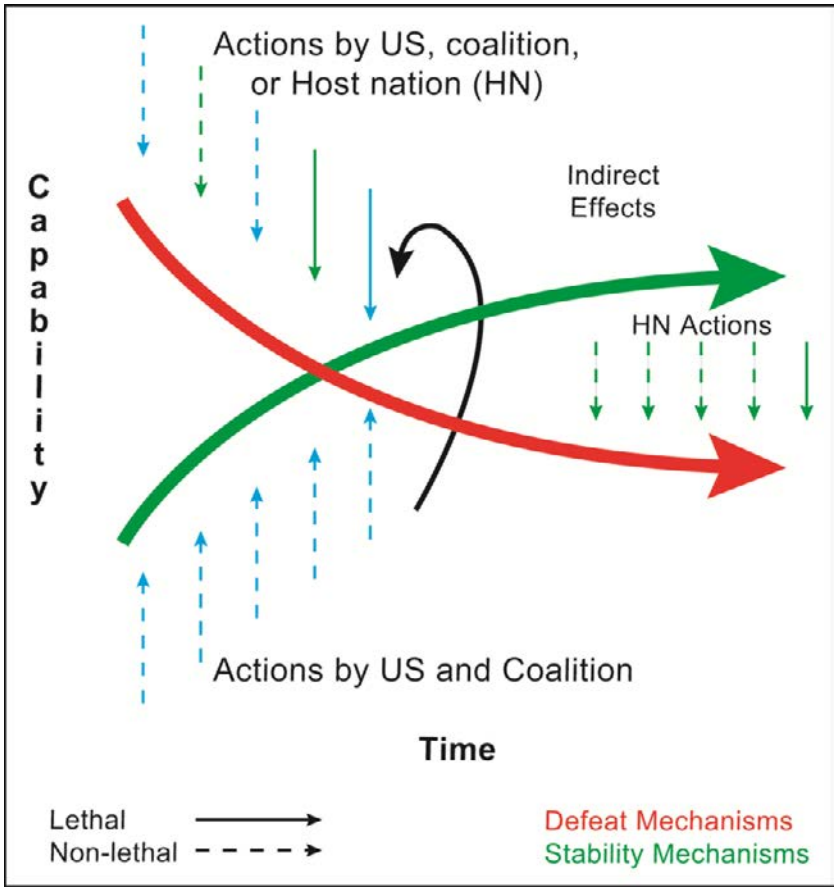


Figure 1. Network Engagement (AtN) Operational Concept

It is important to establish boundaries on how a staff describes the OE to maximize using limited time and resources. The doctrinal definition of OE is "a composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander."[3] The most significant part of the OE is almost always the people within it who belong to various networks. During the past ten years, the Department of Defense has increasingly viewed the people within the OE as a network of human networks. These networks include threat, friendly, and neutral networks which are interconnected. Analysts focus considerable time and effort on developing an understanding of the OE, human terrain, and networks operating within it. While human terrain is also considered key terrain, the OE is more than just human terrain or networks of people. The OE includes activities, interactions, influences, implications, processes, materials, and places affecting networks that subsequently bear on decisions of a commander.[4] Figure 2 shows that concept.

Identifying observables and signatures that are spawned by network activities and materials is an essential part of a comprehensive approach to effectively engaging networks.

The figure 2 concept is important because members of a network are often difficult to detect or identify and have intentions that are difficult to discern. The ability to detect network activities and materials can be enhanced with training on how to distinguish indicators that we can detect with our senses (i.e., observables) and indicators we can measure with our sensors (i.e., signatures). Identifying observables and signatures that are spawned by network activities and materials is an essential part of a comprehensive approach to effectively engaging networks.

The next pillar, understand the networks, is achieved through network analysis. Network analysis provides in-depth understanding of the people, places, processes, and activities within a network. The latest developments in how networks are analyzed include network templating (NT) and critical factors analysis (CFA), which are done at the same time to be mutually supporting. This is not to imply more traditional methods of analysis, such as pattern analysis and event matrices, are no longer relevant. Those analytical techniques remain completely relevant because they provide information on the basic elements of understanding networks – the 5Ws and H (who, what, when, where, why, and how).

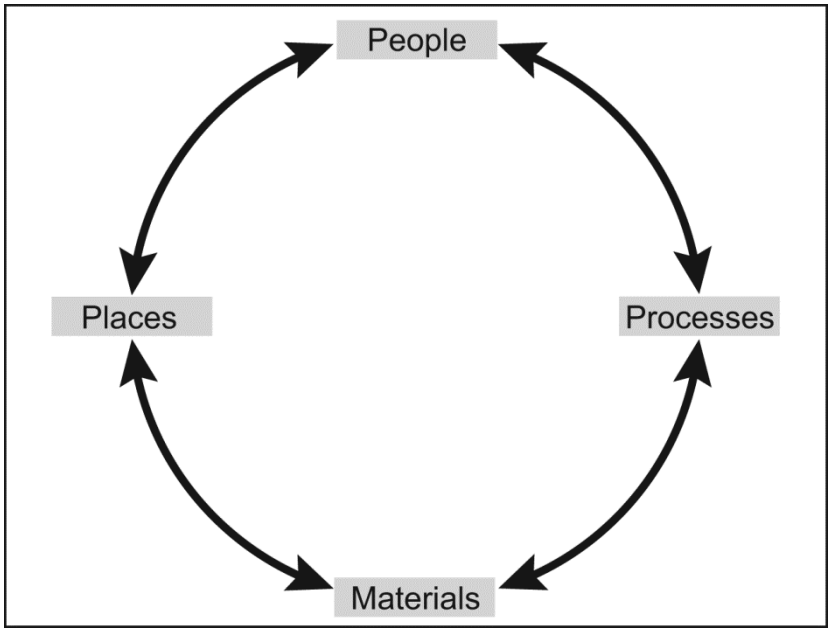


Figure 2. Comprehensive Approach to Networks

An unidentified American Soldier, right, Afghan, and coalition security forces await the arrival of CH-47, Chinook, helicopters after searching a compound for a Haqqani network leader responsible for acquiring and emplaceing improvised explosive devices and ambush attacks targeting Afghan security forces in the Sharan District, Paktika Province, Afghanistan, 9 June 2011. (Photo by PFC Troy Tippett, USA)

Correctly identifying the "who" within networks is challenging, and a significant development during the past few years is the application of social network analysis (SNA) to the targeting process. This is not intended to replace the use of standard link analysis diagrams, which represent the way most operational units analyze and understand networks. Applying SNA is intended to develop a deeper understanding of the relationships among entities within a social network. By augmenting standard link analysis with SNA, analysts can rapidly identify potential targets that would not otherwise be discoverable. SNA provides an understanding of the criticality of certain nodes based on how they fit into the network. Joint Publication 3-0 defines a critical node as a, "…point of influence within a network and a potential focal point for engagement of that network. Critical nodes represent central points of leadership communication, direction, or resourcing between nodes. These are vulnerabilities for lethal and nonlethal targeting against a particular network."

Analysts guided only by link analysis tend to identify potential targets based on hierarchical significance and basic evident relationships outlined in reporting. This type of network analysis is largely subjective while SNA provides additional options based upon potential targets and relational significance. SNA provides in-depth understanding of the network because it describes the nature of links in detail and assesses the significance of nodes based on their overall positions within networks, not just where they are positioned hierarchically.

… augmenting standard link analysis with SNA, analysts can rapidly identify potential targets

The staff would have to carefully consider not only the SNA, but the more subjective analysis provided by the link analysis diagram and the targeting recommendations of the analysts that developed them.

Network analysis is never complete. It is an iterative process that always has information gaps the staff

must strive to understand. Part of the art of network analysis is identifying gaps that can, and should, be filled by leveraging collection assets. Using information previously gathered and analyzed, NT provides the next level of in-depth understanding of networks. NT is a method of determining where best to focus collection assets to develop an understanding of unknown, but suspected portions of the network. It consists of five steps: (1) describe the network, (2) develop indicators, (3) identify named areas of interest, (4) determine collection capabilities required, and (5) make targeting recommendations. This process spans a wide berth within the operations process and connects elements of intelligence preparation of the battlefield, information collection and synchronization, and targeting.

... understanding the network must include knowledge of the basic activities involved within the network.

All previously described analytical efforts constitute step 1, describe the network. Step 2 is identifying indicators. Army doctrine publication 2-22.1 states: "An indicator, in intelligence usage, is an item of information which reflects the intention or capability of an adversary to adopt or reject a course of action (COA)."

An indicator is positive or negative evidence of threat activity or any characteristic of the area of operations that points toward threat vulnerabilities, the adoption or rejection by the threat of a particular activity, or that may influence the commander's selection of a COA. Indicators may result from previous actions or a threat's failure to take action. Indicators are the basis for situation development. The all source intelligence analyst integrates information from all sources to confirm indications of threat activities. Detection and confirmation will enable analysts to answer the commander's critical information requirements.

In more simplistic terms, indicators are those things we can detect with our senses (observables) and those things we can measure with our sensors (signatures) that indicate the type of activity we are looking for is occurring. That means understanding the network must include knowledge of the basic activities involved within the network. It is often helpful to begin the process of identifying network activities with a generic network model as shown in figure 3.[5]

A generic network model (figure 3) helps build a specific network template because it shows the basic functions and flow of commodities that need to be identified in the actual network being templated.

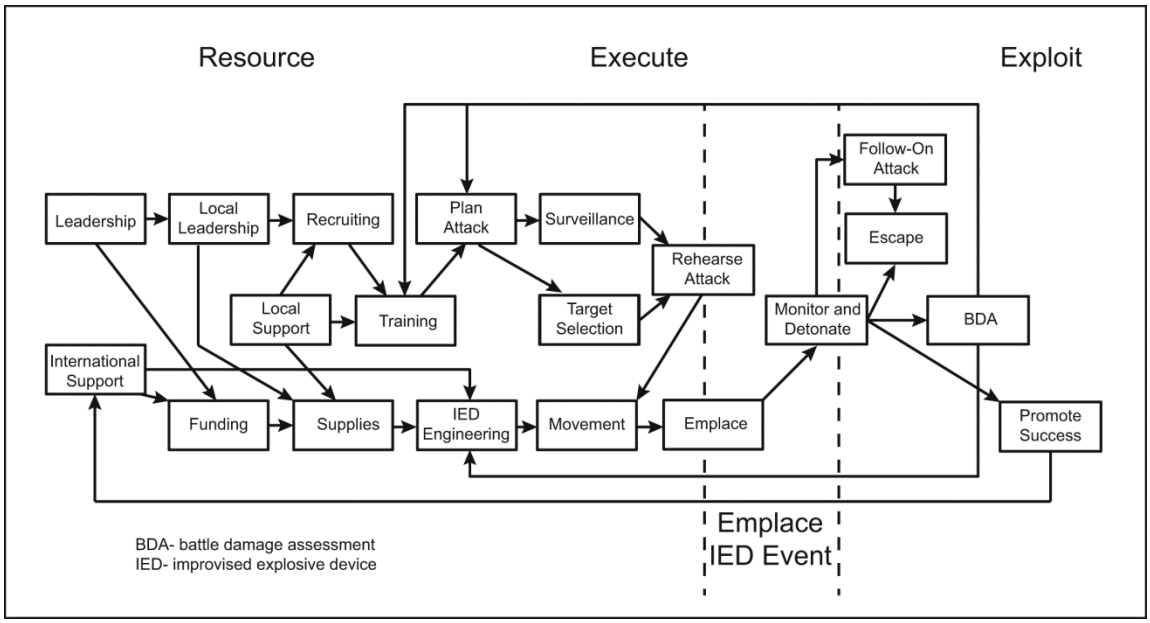


Figure 3. Adversary Improvised Explosive Device Activities

Rather than beginning from a blank white board and trying to imagine what activities to look for, the network model provides a broad range of functions and commodities and shows how they are generally interconnected. It equates to a doctrinal template, which is a model based on known or postulated adversary doctrine. Doctrinal templates illustrate the disposition and activity of adversary forces and assets conducting a particular operation unconstrained by the effects of the battlespace and represent the application of adversary doctrine under ideal conditions. Ideally, doctrinal templates depict the threat's normal organization for combat, frontages, depths, boundaries and other control measures, assets available from other commands, objective depths, engagement areas, battle positions, etc. Doctrinal templates are usually scaled to allow ready use with geospatial products.[6]

As this model is applied to reporting and analyses of a specific network, the network's unique patterns and sequence of activities emerge (figure 4). This enables analysts and operations personnel to develop potential indicators. The more clearly a network's sequence of activities is understood, the more robust a set of potential indicators can be developed. Throughout this process, specific activities need to be identified geographically. This is how

… the network model provides a broad range of functions and commodities and shows how they are generally interconnected.

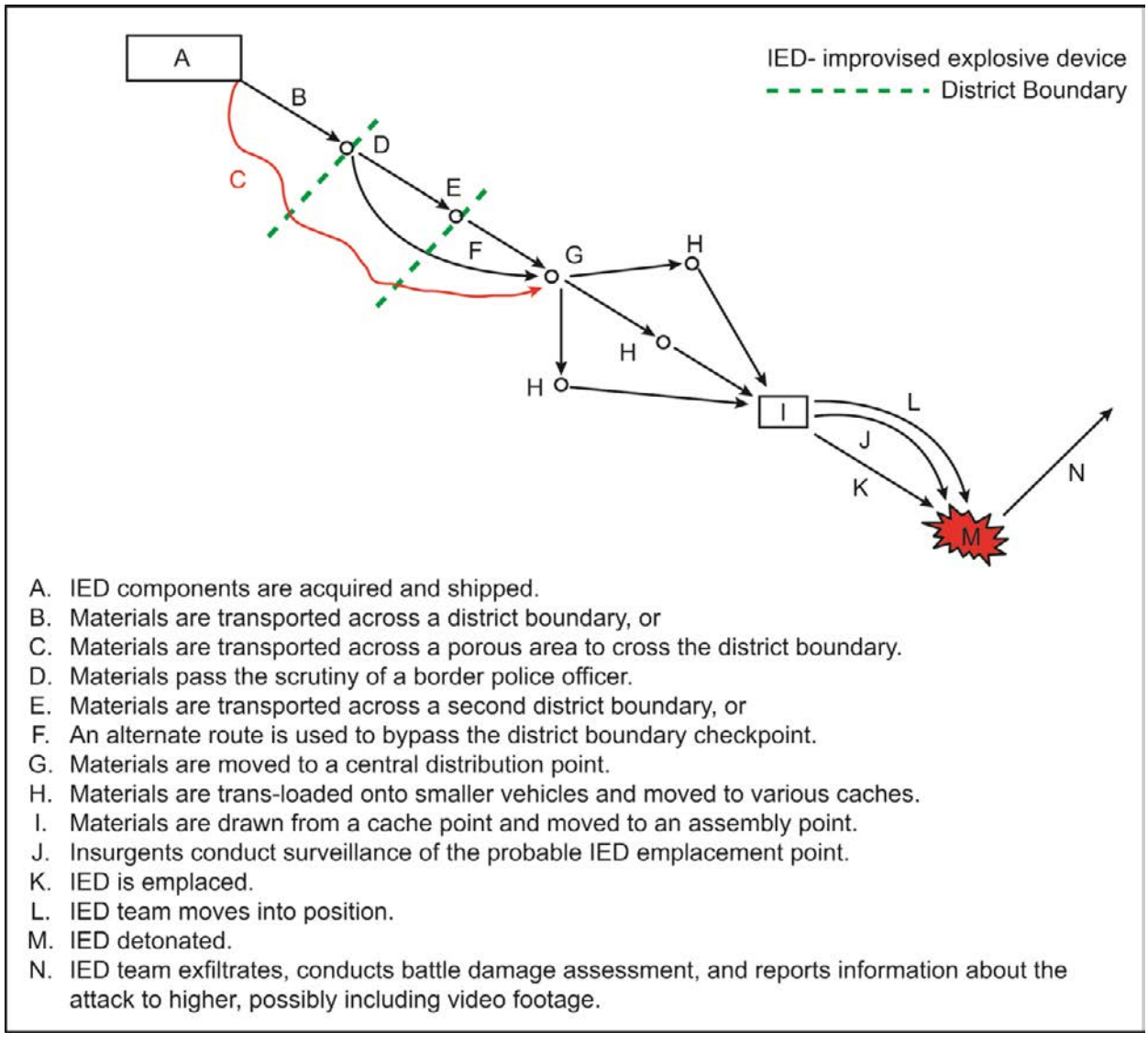


Figure 4. Network Analysis

named areas of interest (NAIs) are designated. NAIs provide areas on the ground at which information collection assets can be focused to identify indicators of activity. Multiple information collection assets are allocated against NAIs based on their capabilities to detect observables or signatures under various conditions.[7]

The final step in network templating is to make targeting recommendations, which include both lethal and nonlethal effects conducted against targets within threat networks, and the influencing effects within friendly and neutral networks. Making targeting recommendations requires drawing upon an understanding of the network and network analysis, and the commander's intent. Much experience has been gained in the last decade in applying CFA or center of gravity analysis and target systems analysis effectively against networks, but we lack the room in this brief article for those discussions. Network analysis and templating offer the analyst, and staff he or she is supporting, an important glimpse into the workings of the linked complex adaptive systems that exist within the commander's area of interest.

Network analysis and templating offer the analyst, and staff he or she is supporting, an important glimpse into the workings of the linked complex adaptive systems

This article briefly described both the context for and a means of conducting network analysis. While many units are using some of these principles to varying degrees, the recommended approach is to integrate the AtN methodology comprehensively. Doing so requires developing a comprehensive understanding of the AtN methodology and the ability to integrate it into staff processes and the unit battle rhythm. This effort will lead to a better ability to conduct successful AtN operations, which in turn will lead to more rapid and complete mission accomplishment.

END NOTES

[1] This quote is an excerpt from the article titled, "Integrating Intelligence and Information," written by Army LTG M.T. Flynn and BG C.F. Flynn, January-February 2012, Military Review.

[2] This concept of the broad approach to understanding networks and figure 2 were developed by Steve Duncan of the US Army Training and Doctrine Command (TRADOC) ISR TOPOFF Team.

[3] While the concept of network templating is doctrinally based, this particular approach to network templating was developed by the AWG and is explained in detail in the publication, Attack the Network Methodology Part 3: Network Modeling and ISR Synchronization, dated April 2009, pp 4-7. Hereafter cited as AWG AtN Methodology Part 3.

[4] Input related to draft Army Doctrine Publication 2-22.1 was provided by TRADOC Analysis and Production Division (G2) Senior Analyst, Jerry Leverich.

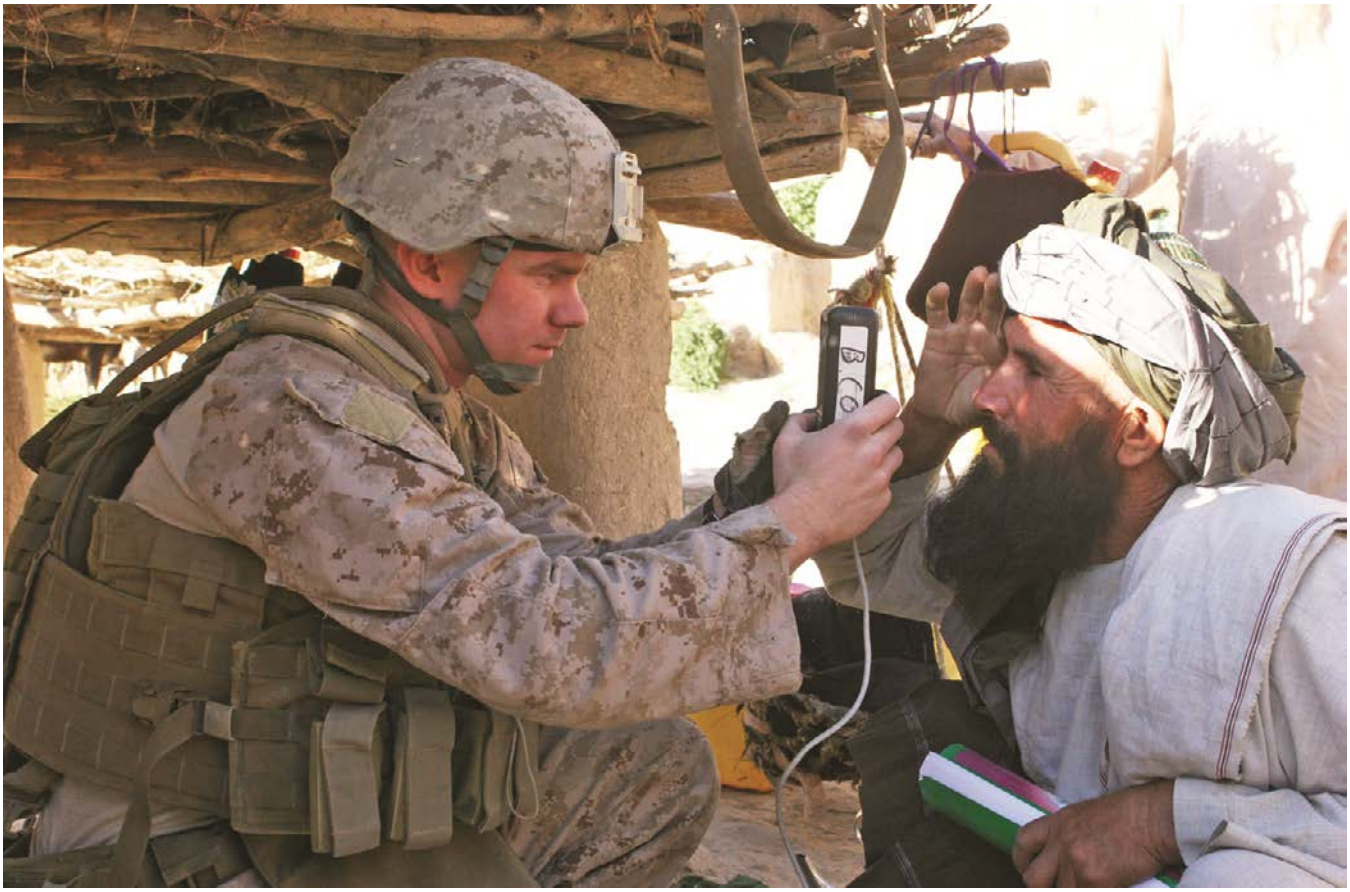
[5] This network model was provided by the TRADOC Intelligence Support Activity (TRISA) and is based on work done by a team at the Johns Hopkins University Applied Physics Lab under a Joint Improvised Explosive Device Defeat Operation contract.

[6] JP 2-01.3, Joint Intelligence Preparation of the Environment, dated 16 June 2009, pg. A-18.

[7] AWG AtN Methodology Part 3, pp 7-11.

This article represents a combined effort by TRADOC Intelligence (G2) (Training Brain Operations Center (TBOC)) and the US Army Maneuver Center of Excellence with support from TRADOC Intelligence Support Activity (TRISA and the ISR TOPOFF Team), and the Asymmetric Warfare Group. They endeavored to describe the latest methods used to analyze human networks, and how those methods fit into a broader methodology known as AtN. The AtN methodology demands network analysis and operations planning and, is based on understanding the mission and the operational environment (OE). Three pillars: understanding the mission, OE, and networks, provide the foundation for the AtN methodology.

WESTERN WAY OF WAR IS THE WRONG APPROACH FOR CURRENT COUNTERINSURGENCY



US Marine Corps Sgt. Michael B. Segaline collects biometrics data from a villager during Operation KALAWAL SUNRISE in the village of Faiscal, Sangin District, Afghanistan, 1 June 2011. Segaline is the team chief for the company level intelligence cell at Company B, 1st Battalion, 5th Marine Regiment. (Photo by Cpl Benjamin Crilly, USMC)

By Lt Col Richard Freeman, USAF, MAJ Zachary Basford, USA and LCDR Michael Marquez, USN

The United States (US) will fail in the current war in Afghanistan because of its tradition of fighting using the "Western way of war." History professor and author, Geoffrey Parker, characterizes the Western way of war as "a combination of technology, discipline, and aggressive military tradition with an extraordinary capacity to respond rapidly to challenges and to use capital rather than manpower to win."[1] There are five principle foundations of the Western method of warfighting. In addition to the first three mentioned in Parker's quote — superior technologies, superb discipline, and aggressive military tradition — there is also a challenge-and-response dynamic and the ability to mobilize resources. Victor Davis Hanson, a professor of Classics, put forth a similar delineation of the Western way of war.[2] Hanson described core qualities which parallel Parker's characterization of the five principle foundations. As stated by both authors, the Greeks conceived Western warfare which has developed over the centuries and evolved into an efficient professional combat force designed to destroy the adversary's combat fighting power. With advances in technology and the discipline of war, the Western way of war has become very effective for forces engaged in conventional warfare.

… the Greeks conceived Western warfare which has developed over the centuries and evolved into an efficient professional combat force …

The process of eliminating an adversary's combat forces is now done with increasing efficiency and

lethality. However, most adversaries realize they cannot fight a superior military force "toe-to-toe," and thus they employ insurgency-type operations which are becoming standard operating procedures for non-state actors. The principle foundations of the Western way of war have been used by nearly every Western nation conducting modern warfare. Historical examples include: the Prussians revolutionizing their Army through leadership training and instilling superb discipline in their Soldiers; German forces using railroads to mobilize resources during World War I; and the technological advance of the needle gun (a firearm with a needle-like firing pin) that was proclaimed as the "key to Prussian victory" at Königgrätz in 1866.[3]

Although historical examples show that military victories can be attributed to using the principle foundations of the Western way of war, these foundations may contribute to defeat in the current era of warfare. The reason for this is the battlefield and enemy has changed drastically from what they were just 50 years ago. Current battlefields and enemies are hidden within populations, and the dominant form of warfare for the US today is counterinsurgency (COIN). There are different principles of warfare that need to be applied to ensure success in COIN operations, such as in Afghanistan. Consequently, the US will be unsuccessful in Afghanistan because the fundamental principles in the Western way of war do not apply well to conducting COIN.

… the fundamental principles in the Western way of war do not apply well to conducting COIN.

Using superior technology is not the best way to gather information and fight the enemy in COIN operations. Technologically superior weapons and reconnaissance systems will work at the tactical level. However, the over-reliance on technology distracts coalition forces from focusing on the best method of gathering information and building trust and rapport with the local populace that will ultimately help us achieve strategic victory. The best method of gathering information in a COIN environment is through human intelligence (HUMINT) where information is gathered by talking to people and building trust and relationships. In a COIN environment, the enemy is not always easily identifiable. For example, one day a man may be farming his land and the next day the same man emplaces an improvised explosive device (IED) intended to kill coalition forces. This example highlights the predominant enemy coalition forces are facing in Afghanistan. The best way to identify this type of enemy is through people informing military or government authorities about suspicious or illegal activities. The US, and other countries, have used imagery to correlate pattern-of-life activities with vehicles planting IEDs and forensic evidence found at a detonation site to link people to such acts using biometric databases. The problem is: using technology does not prevent the enemy from acting, which renders superior technology of little use unless it can catch the enemy in the act. Catching the enemy in the act is extremely difficult to do. In addition, superior technology in weaponry may be good for risk mitigation by allowing standoff for friendly forces, but it does not allow for selective and precise targeting of individuals. There may be many individuals located at an objective, but not all are hostile combatants. Striking targets with smart weapons may cause collateral damage in the form of non-enemy deaths resulting in solidifying support against coalition forces from the relatives of casualties. In both cases, technology is doing what it was designed to do, but the enemy has already succeeded by carrying out its propaganda act or increasing support for its cause when coalition forces accidently kill neutral or friendly bystanders, thus denigrating superior technology contributions to strategic victory in a COIN environment.

Pictured is an F-22 Raptor departing Holloman Air Force Base, New Mexico on 29 February 2012. These aircraft should win tactical battles and give US forces the strategic advantage of air superiority. But this superior technology may not be the key to winning the hearts and minds of contested populations in current battlefields. (Photo by A1C Daniel Liddicoet, USAF)

Superb discipline and aggressive military action also result in unintended effects in COIN warfare. Parker defined discipline as "the ability to stand fast in the face of the enemy by suppressing the natural impulses of fear and panic, and to reinforce cohesion and combat efficiency by creating artificial kinship or fellowship."[4] The typical US Soldier speaks with authority, wears body armor with racks of magazines attached, carries a weapon with lasers and optics, and conceals his eyes with sunglasses. These characteristics are desirable in combat Soldiers, but make them unapproachable to those who are unaccustomed to military culture. Most civilians—local nationals in places like Afghanistan—are hesitant to talk to Soldiers because of these traits. US Soldiers, however, need local nationals to be willing to approach and talk to them. Western strategy is centered on the total defeat and destruction of the enemy. The objective of COIN warfare is not to militarily annihilate the enemy, but to win the population and thus take away support for the enemy's cause. Aggressive military action is desired during skirmishes but is, as a whole, an inappropriate approach to winning the strategic war through winning over the population.

Parker identified the challenge-and-response dynamic, as the West's "unique ability to change as well as to conserve its military practices as need arose and its power to finance those changes."[5] Parker stated the West has the capability to rapidly effect change without significantly affecting military doctrine. As such, the continuous and rapid innovation in weaponry was a response to the competitive nature of Western state systems. Hence, a less capable Western state would develop mechanisms to finance innovations, whether technological or training innovations, to gain an advantage against a competing state.[6]

Developing advanced mechanisms proved to be ineffective in COIN wherein the adversary is a non-state actor. The Western way of war directs the challenge-and-response

The objective of COIN warfare is not to militarily annihilate the enemy, but to win the population …

dynamic towards achieving a political goal, in support of Clausewitz's definition of war as an extension of politics by other means. Although insurgencies may also be an extension of politics, it is naturally employed by adversaries for social, cultural, and religious reasons as well.[7] COIN demands improving and developing the conditions of change to effectively mitigate the insurgents' social, cultural, or religious influences over the population. This aspect of COIN indicates slow and deliberate resourcing for population-based actions, hence, the challenge-and-response dynamic in the Western way of war is the wrong approach when conducting COIN.

A population-based action identifies the grievances and needs of the people, addresses those concerns, and elicits support of the people towards coalition and against enemy forces. The actions taken by General John J. Pershing during the Philippine Insurrection (1899-1902) demonstrated three critical principles in combating insurgency: restraint, perseverance, and the objective.[8] The application of force should never be restricted in COIN. Force should be deliberate but restrained. According to David Smythe, "restraint in the use of overwhelming power had a more profound influence on the population."[9] Plunk Mammoser, et. al., stated "perseverance is the way to develop the local connections and relationships necessary to influence the population and to achieve information superiority". The commander should focus the fire or effect in fulfillment of the objectives instead of being an end by itself. Given time, this tactic will neutralize support for the enemy and aid in winning the strategic war. If US forces are more proactive in seeking and addressing concerns of the population, US national objectives will be met sooner.

… "restraint in the use of overwhelming power had a more profound influence on the population."

The US needs fewer resources in Afghanistan to be more effective. For COIN warfare, "less is more." A fighting force can often obtain more desired effects with fewer resources because having too many resources can interfere with efficiency. A greater number of resources (units and assets) can take away effectiveness by making operations cumbersome, diluting messages through multiple variations of the messages, decreasing mobility, and causing competition for key assets and equipment. Just because the US has the ability to mobilize large amounts of resources and finances to wage war does not mean that the US should. For example, a few special forces and military information support operations teams could have a greater impact on the COIN fight because influencing—populations is their expertise. Also, conventional forces are bulky and expensive. They can hinder effective processes with restrictive rules of engagement and an overly-aggressive posture. Commanders need greater control to maintain order over larger numbers of forces. Additional control equates to additional rules that can restrict effectiveness.

There are two more negative aspects to the excessive mobilization of resources. First, surging equipment and personnel to the battlefield may help win the fight at the tactical or operational level of war, but may result in the US losing the strategic victory. The center of gravity in COIN—the one thing that is essential to ultimate victory—is winning the "hearts and minds" of the people. Massive amounts of equipment and personnel are usually perceived by a local population as occupation by a foreign nation. Occupation is always perceived negatively. Second, the US must consider its return on investment. Deploying more troops and equipment costs more money. If the US and allies can accomplish the mission at a lower cost they should do so.

The US is doomed to be unsuccessful in Afghanistan because it continues to apply the principle foundations in the Western way of war to the COIN fight. Although the principle foundations of this method of warfare have led to victory in the past, the modern battlefield environment has changed. No longer can superior technology be relied upon to win the war as it did with the advent "of ironclad warships, steam and rail transportation, and the telegraph" in the American Civil War.[10] Today's battlefield—COIN warfare—requires the ability to win the hearts and minds of the population. It does not require aggressive military action such as that used during World War I when the young men of armies and nations of Europe were indoctrinated "not simply to fight for their country, but to die for it."[11] The principle foundations of the Western way of war will win battles tactically by eliminating adversarial combatants, but they do not tend to win the hearts and minds of the contested populace—the goal of the actors in question. An example is contained in a letter intercepted by American intelligence personnel, sent by Usama bin Laden's deputy, Ayman al-Zawahiri to Abu Musab al-Zarqawi, a key leader of al-Qaida Arabian Peninsula. It stated, "I say to you: that we are in a battle, and that more than half of this battle is taking place in the battlefield of the media . We are in a media battle in a race for the hearts and minds of our Umma (Muslim peoples)."[12] It is evident the principles of the Western way of war are ineffective strategies to winning the hearts and minds of the population; and to ultimately, win the war in Afghanistan and other conflicts where COIN is being conducted.

END NOTES

[1] Geoffrey Parker, *The Cambridge History of Warfare* (Cambridge, UK: Cambridge University Press, 2009), n.p.

[2] Victor Davis Hanson & John Heath, *Who Killed Homer?: The Demise of Classical Education and the Recovery of Greek Wisdom,* (San Francisco, CA: Encounter Books, 2001), n.p.

[3] Dennis E. Showalter, "The Prusso-German RMA, 1840-1871," in *The Dynamics of Military Revolution: 1300-2050*, ed. MacGregor Knox and Williamson Murray (Cambridge, UK: Cambridge University Press, 2009), 110.

[4] Geoffrey Parker, *The Cambridge Illustrated History of Warfare*, (Cambridge, UK: Cambridge University Press, 2008), 3.

[5] Geoffrey Parker, *The Cambridge Illustrated History of Warfare*, (Cambridge, UK: Cambridge University Press, 2008), 3.

[6]Tony Corn, *From Mars to Minerva: Clausewitz, Liddell Hart, and the Two Western Ways of War,* (Small Wars Journal Foundation, 2011), 5.

[7] William Thomson, *All That Works Is Obsolete: The Shortcomings of US COIN That Must Be Addressed,* (e-International Relations, 2011), http://www.e-ir.info, (accessed May20, 2012).

[8] Plunk Mammoser, et.al., "Lessons from the Philippine Insurrection 1898-1915," Norfolk, VA: JFSC, September 10, 2004), 11.

[9] David Smythe, *Guerrilla Warrior: The Early Life of John J. Pershing,* (New York: Charles Scribner's Sons, 1973), 91.

[10] Mark Grimsley, "Surviving Military Revolution: The US Civil War," in *The Dynamics of Military Revolution: 1300-2050*, ed. MacGregor Knox and Williamson Murray (Cambridge, UK: Cambridge University Press, 2009), 77.

[11] Michael Howard, "Men against Fire: The Doctrine of the Offensive in 1914," in *Makers of Modern Strategy: from Machiavelli to the Nuclear Age*, ed. Peter Paret (Princeton, NJ: Princeton University Press, 1986), 522.

[12] *Al-Zawahiri's letter to al-Zarqawi,* www.readhunter.com, (accessed May 31, 2012).

"… more than half of this battle is taking place in the battlefield of the media . We are in a media battle in a race for the hearts and minds of our Umma (Muslim peoples)."

ROLE OF LAW ENFORCEMENT PROFESSIONALS IN ATTACK THE NETWORK STRATEGY

An Afghan boy walks through a dried poppy field, observing as a route-clearance team, with Special Operations Task Force-South, deploys and detonates a mine-clearing line charge during a clearing operation in Khakrez District, Kandahar Province, Afghanistan, 31 May 2011. The operation, led by Afghan commandos with the Afghan National Army's 3rd Commando Kandak, resulted in removing four suspected insurgents, and exploiting improvied explosive device-making materials and a weapon-sighting device. (Photo by SGT Daniel P. Shook, USA)

By Richard Crawford and Lt Col Adam Tharp, USMC

"The concept of embedding experienced law enforcement professionals as advisors and investigators with Marine headquarters at the RCT (Regimental Combat Team) and battalion level has proven effective and beneficial in the counter insurgency (COIN) fight. As the situation in Iraq has developed, the Law Enforcement Professional (LEP) Program evolved from providing Marines 'cop on the beat' training, to sensitive site exploitation and forensic training, to providing "detective" advice and expertise in developing evidence and reports that would support incarceration of insurgents and criminals. A significant part of the LEP program at the battalion level is the predeployment program (PTP) training of Marines by LEPs in 'cop on the beat' and community policing concept principles."

-Marine Corps Center for Lessons Learned (MCCLL) report on the Law Enforcement Professional Program, 2009

Lessons from the COIN campaigns in Iraq and Afghanistan highlighted initial Joint doctrinal and force capability shortfalls to meet intelligence requirements.

BACKGROUND

Lessons from the COIN campaigns in Iraq and Afghanistan highlighted initial Joint doctrinal and force capability shortfalls to meet intelligence requirements. Still operating in the "major combat operation" mindset, commanders futilely attempted to defeat insurgent groups using legacy Cold War intelligence

processes designed to target conventional militaries. The rise of the improvised explosive device (IED) as the insurgent weapon of choice combined with the loosely coupled decentralized command and control structure demanded developing new intelligence methods and capabilities.

Recognizing insurgent groups behaved more like criminal networks than conventional military forces, the services determined conventional intelligence collection tools and techniques were not sufficient to identify and target insurgent forces. A January 2006 Department of Defense study identified the applicability of United States (US) police capabilities to COIN operations. The study noted successful COIN required community interaction through dismounted patrolling, urban-police-department-styled gang suppression units, intelligence structures built around the target (vice the means of collection), and geospatial and crime mapping. The study recommended embedding advisors with law enforcement experience in ground combat element units, and hold resources and authorities at the lowest possible level (MCCLL, 2009).

From the study, the services (in coordination with the Joint Improvised Explosive Device Defeat Organization) instituted a proof of concept to embed experienced law enforcement advisors into tactical ground units and the battalion, regiment, division, and corps levels. The Marine Corps formalized this effort in 2009 as the LEP Program (HQMC, 2009).

THE ROLE OF LEPS IN ATTACK THE NETWORK STRATEGY

LEPs perform a number of roles in the Attack the Network strategy, depending on where they are embedded. From a law enforcement perspective, the strategy should be "linear", much the same strategy employed by the Drug Enforcement Administration (DEA) in the 1980s and 1990s in their efforts to dismantle the Cali cartel; attacking from the bottom (IED placers) to the top (cell leaders, bomb makers). Also included would be the disruption of the facilitators, by specifically disabling their financial networks.

BATTALION LEPS

Battalion LEPs play a significant role because they are with the "boots on the ground". Their primary job is emphasizing to ground units the critical need to collect biometric data. Biometrics is the key to a comprehensive intelligence picture and can identify potential actionable targets. They also ensure the evidence collected from the battlefield, especially weapons caches and IED events, is forwarded to the appropriate labs for exploitation, in an expeditious manner. Battalion LEPs work through their police mentoring teams with the local host nation security forces to assist their intelligence sections (S-2) in fully identifying IED cells in their area of operations.

… successful COIN required community interaction through dismounted patrolling, urban-police-department-styled gang suppression units, intelligence structures built around the target (vice the means of collection) …

REGIMENTAL/BRIGADE LEPS

Regimental/Brigade LEPs assist in developing the linear approach by moving information up to LEPs at higher headquarters (HQ) (i.e., division and corps or Marine Expeditionary Force) and down to LEPs at battalions. They assist their S-2 in developing a comprehensive intelligence picture of the IED threat. They can assist in ensuring biometric results from various labs are matched to IED events and thereby identify potential targets or areas for operations involving focused biometric collections. They work with the Police Mentoring Teams in developing more intelligence driven policing in the host country's security forces. In this way they can use the police to help fill intelligence gaps regarding IED cells. Regimental LEPs assist in disrupting financial networks by identifying key money exchanges and through interaction with signals intelligence (radio battalion). The S-2 identifies potential targets for the host country's security forces working with other US Government agencies

(e.g., in Afghanistan the Threat Finance Cell of the DEA working with the Afghans on court authorized wire intercepts).

HIGHER HEADQUARTERS LEPS

LEPs at higher HQ work with the various enablers (i.e., labs or other agencies) and "reach back" entities such as the Counter-IED Operations Integration Center or National Ground Intelligence Center to help complete the intelligence picture of the IED threat by requesting products such as biometric focused area studies, overlays of latents of value, and others. They ensure deoxyribonucleic acid (DNA) and latents of value lab results exploited from IED events are returned to the submitting units (in the field). Often these results are published to a theater-wide data base (e.g., the Combined Information Data Network Exchange) with which units in the field have limited or no connectivity.

When latent matches are made and bomb makers and IED placers are identified, the higher HQ LEPs assist by printing and distributing be-on-the-look-out (BOLO) messages to host nation security forces through the battalion LEPs. These are also placed in books to which units on the ground can have access while on patrols and during operations. The higher HQ LEPs act as catalysts in developing information on financial networks and dispersing it to the appropriate host nation enti-ties working in with other US agencies for further investigation and action.

CURRENT SUCCESSES, CHALLENGES, AND WAY AHEAD

Overall, the LEP program has enjoyed generally positive reviews in after-action reports and lessons learned summaries. LEPS support to connecting individual IED makers and placers through DNA and fingerprints, forwarding BOLOs, and encouraging units to collect biometric data in their area of operations, has been successful. However, challenges remain in realizing the LEP program's potential in Attack the Network operations.

The first challenge is the manpower requirement to fully develop the network picture. An LEP recently stated, "Attack the Network… is just too difficult without a dedicated squad of investigators."

A second challenge is ensuring processed information is available to the lowest units in a timely manner. Bandwidth issues and understanding where information is required remain problematic.

The third challenge is forensic lab capacity to process evidence. The same LEP noted, "the lab is backed up [with] some 400 DNA cases".

The fourth challenge is reliability of biometric collection tools. The LEP noted again "We had a lot of trouble with the Handheld Interagency Identity Detection Equipment today, and it just took too long to enter the 15 (people's data)".

With the recent withdrawal from Iraq and the impending drawdown in Afghanistan, many questions about the future of the LEP program emerge. Will LEPs become a formal capability set within service structure? Will it fade away with our redeployments? Can the LEP program fulfill its potential? Will it be needed in the future? Can it be applied to operations outside COIN?

While those questions remain, in the short term, doctrine, organization, training, and material development is progressing. ALSA (Air Land Sea Application) Center is preparing a multi-Service Tactics Techniques and Procedures publication on biometrics. Ground forces continue to form and train with LEPS. The industry continues to develop new and improved biometric equipment. For now LEPS continue to provide critical support to COIN operations.

… doctrine, organization, training, and material development is progressing. ALSA (Air Land Sea Application) Center is preparing a multi-Service Tactics Techniques and Procedures publication on biometrics.

REFERENCES

Marine Corps Center for Lessons Learned (MCCLLs), "Law Enforcement Professional (LEP) Program, Lessons and Observations from OIF, 2008", 4 June 2009

Headquarters, United States Marine Corps (HQMC), "Law Enforcement Professional (LEP) Program", CMC message 291526Z April 2009. MARADMIN 282/09.

ABOUT THE AUTHORS

Richard Crawford served two tours as a Regimental law enforcement professional. The first was in Fallujah, Iraq, and the second was in Northern Helmand Province, Afghanistan. He had a successful 25-year career as an agent for the Drug Enforcement Agency, focused on counternarcotics operations in South Florida. He is a former Marine Corps infantry officer who commanded Charlie Com-pany, 1st Battalion, Fifth Marines in Vietnam.

Lt Col Adam Tharp currently serves as doctrine development officer for Navy Warfare Development Command. He also served as Future Operations Officer, Regimental Combat Team-Two in support of OPERATION ENDURING FREEDOM from February 2010 to February 2011.

Taking a break during patrol, Orlando Montero, a law enforcement professional with 3rd Battalion, 5th Marine Regiment, interacts with local, 12 March 2011, during Operation Golden Shillelagh. The mission of the operation is to locate and interdict possible insurgent activity in the area. (Photo by Sgt Ryan Smith, USMC)

CURRENT ALSA MTTP PUBLICATIONS

AIR BRANCH – POC alsaa@langley.af.mil

TITLE	DATE	PUB #	DESCRIPTION / STATUS
AIRSPACE CONTROL *Multi-Service Tactics, Techniques, and Procedures for Airspace Control* **Distribution Restricted**	22 MAY 09	FM 3-52.1 AFTTP 3-2.78	Description: This MTTP publication is a tactical-level document, which helps synchronize and integrate airspace command and control functions and serves as a single-source reference for planners and commanders at all levels. Status: **Assessment**
AVIATION URBAN OPERATIONS *Multi-Service Tactics, Techniques, and Procedures for Aviation Urban Operations* **Distribution Restricted**	9 JUL 05	FM 3-06.1 MCRP 3-35.3A NTTP 3-01.04 AFTTP 3-2.29	Description: This publication provides MTTP for tactical-level planning and execution of fixed- and rotary-wing aviation urban operations. Status: **Revision**
DYNAMIC TARGETING (DT) *Multi-Service Tactics, Techniques, and Procedures for Dynamic Targeting* **Distribution Restricted**	7 May 2012	FM 3-60.1 MCRP 3-16D NTTP 3-60.1 AFTTP 3-2.3	Description: This publication provides the Joint Force Commander, the operational staff, and components MTTP to coordinate, de-conflict, synchronize, and prosecute DTs within any area of responsibility. Includes lessons learned, multinational and other government agency considerations. Status: **Current**
IADS *Multi-Service Tactics, Techniques, and Procedures for an Integrated Air Defense System* **Distribution Restricted**	1 MAY 09	FM 3-01.15 MCRP 3-25E NTTP 3-01.8 AFTTP 3-2.31	Description: This publication provides joint planners with a consolidated reference on Service air defense systems, processes, and structures to include integration procedures. Status: **Assessment**
JFIRE *Multi-Service Procedures for the Joint Application of Firepower* **Distribution Restricted**	20 DEC 07	FM 3-09.32 MCRP 3-16.6A NTTP 3-09.2 AFTTP 3-2.6	Description: A pocket-sized guide of procedures for calls for fire, CAS, and naval gunfire. Provides tactics for joint operations between attack helicopters and fixed-wing aircraft performing integrated battlefield operations. Status: **Revision**
JSEAD/ARM *Multi-Service Tactics, Techniques, and Procedures for the Suppression of Enemy Air Defenses in a Joint Environment* **Classified SECRET**	28 MAY 04	FM 3-01.4 MCRP 3-22.2A NTTP 3-01.42 AFTTP 3-2.28	Description: This publication contributes to Service interoperability by providing the Joint Task Force and subordinate commanders, their staffs, and SEAD operators a single, consolidated reference. Status: **Revision**
JSTARS (ATCARS) *Multi-Service Tactics, Techniques, and Procedures for the Joint Surveillance Target Attack Radar System* **Distribution Restricted**	16 NOV 06	FM 3-55.6 MCRP 2-24A NTTP 3-55.13 AFTTP 3-2.2	Description: This publication provides procedures for employing JSTARS in dedicated support to the Joint Force Commander. Describes multi-Service TTP for consideration and use during planning and employment of JSTARS. Status: **Revision**
KILL BOX *Multi-Service Tactics, Techniques, and Procedures for Kill Box Employment* **Distribution Restricted**	4 AUG 09	FM 3-09.34 MCRP 3-25H NTTP 3-09.2.1 AFTTP 3-2.59	Description: This publication assists the Services and Joint Force Commanders in developing, establishing, and executing Kill Box procedures to allow rapid target engagement. Describes timely, effective multi-Service solutions to FSCMs, ACMs, and maneuver control measures with respect to Kill Box operations. Status: **Assessment**
SCAR *Multi-Service Tactics, Techniques, and Procedures for Strike Coordination and Reconnaissance* **Distribution Restricted**	26 NOV 08	FM 3-60.2 MCRP 3-23C NTTP 3-03.4.3 AFTTP 3-2.72	Description: This publication provides strike coordination and reconnaissance (SCAR) MTTP to the military Services for conducting air interdiction against targets of opportunity. Status: **Revision**
SURVIVAL, EVASION, AND RECOVERY *Multi-Service Tactics, Techniques, and Procedures for Survival, Evasion, and Recovery* **Distribution Restricted**	20 MAR 07	FM 3-50.3 NTTP 3-50.3 AFTTP 3-2.26	Description: This publication provides a weather-proof, pocket-sized, quick reference guide of basic survival information to assist Service members in a survival situation regardless of geographic location. Status: **Revision**
TAGS *Multi-Service Tactics, Techniques, and Procedures for the Theater Air-Ground System* **Distribution Restricted/ REL ABCA**	10 APR 07	FM 3-52.2 NTTP 3-56.2 AFTTP 3-2.17	Description: This publication promotes Service awareness regarding the role of airpower in support of the Joint Force Commander's campaign plan, increases understanding of the air-ground system, and provides planning considerations for conducting air-to-ground ops. Status: **Assessment**

AIR BRANCH – POC alsaa@langley.af.mil

TITLE	DATE	PUB #	DESCRIPTION / STATUS
UAS *Multi-Service Tactics, Techniques, and Procedures for Tactical Employment of Unmanned Aircraft Systems* **Distribution Restricted**	21 SEP 11	FM 3-04.15 NTTP 3-55.14 AFTTP 3-2.64	Description: Establishes MTTP for UAS addressing tactical and operational considerations; system capabilities; payloads; mission planning; logistics; and, most importantly, multi-Service execution. Status: **Current**

LAND AND SEA BRANCH – POC alsab@langley.af.mil

TITLE	DATE	PUB #	DESCRIPTION / STATUS
ADVISING *Multi-Service Tactics, Techniques, and Procedures for Advising Foreign Forces* **Distribution Restricted**	10 SEP 09	FM 3-07.10 MCRP 3-33.8A NTTP 3-07.5 AFTTP 3-2.76	Description: This publication serves as a reference to ensure coordinated multi-Service operations for planners and operators preparing for, and conducting, advisor team missions. It is intended to provide units and personnel scheduled to advise foreign forces with viable TTP so they can successfully plan, train for, and carry out their mission. Status: **Assessment**
AIRFIELD OPENING *Multi-Service Tactics, Techniques, and Procedures for Airfield Opening* **Distribution Restricted**	15 MAY 07	FM 3-17.2 NTTP 3-02.18 AFTTP 3-2.68	Description: This is a quick-reference guide to opening an airfield in accordance with MTTP. It contains planning considerations, airfield layout, and logistical requirements for opening an airfield. Status: **Revision**
CF/SOF *Multi-Service Tactics, Techniques, and Procedures for Conventional Forces and Special Operations Forces Integration and Interoperability* **Distribution Restricted**	17 MAR 10	FM 6-03.05 MCWP 3-36.1 NTTP 3-05.19 AFTTP 3-2.73 USSOCOM Pub 3-33V.3	Description: This publication assists in planning and executing operations where conventional forces and special operations forces (CF/SOF) occupy the same operational environment. Status: **Revision**
CORDON AND SEARCH *Multi-Service Tactics, Techniques, and Procedures for Cordon and Search Operations* **Distribution Restricted**	25 APR 06	FM 3-06.20 MCRP 3-31.4B NTTP 3-05.8 AFTTP 3-2.62	Description: This publication consolidates the Services' best TTP used in cordon and search operations. This publication provides MTTP for planning and executing cordon and search operations at the tactical level of war. Status: **Revision**
EOD *Multi-Service Tactics, Techniques, and Procedures for Explosive Ordnance Disposal in a Joint Environment* **Distribution Restricted**	20 SEP 11	ATTP 4-32.16 MCRP 3-17.2C NTTP 3-02.5 AFTTP 3-2.32	Description: Provides guidance and procedures for employing a joint EOD force. It assists commanders and planners in understanding the EOD capabilities of each Service. Status: **Current**
Military Diving Operations (MDO) *Multi-Service Tactics, Techniques, and Procedures for Military Diving Operations* **Approved for Public Release**	12 JAN 11	ATTP 3-34.84 MCRP 3-35.9A NTTP 3-07.7 AFTTP 3-2.80 CG COMDTINST 3-07.7	Description: This MTTP publication describes US Military dive mission areas (DMA) as well as the force structure, equipment, and primary missions each Service could provide to a JTF commander. Status**: Assessment**
Military Deception *Multi-Service Tactics, Techniques, and Procedures for Military Deception* **Classified SECRET**	12 APR 07	MCRP 3-40.4A NTTP 3-58.1 AFTTP 3-2.66	Description: This MTTP facilitates integrating, synchronizing, planning, and executing of MILDEC operations. It serves as a "one stop" reference for service MILDEC planners to plan and execute multi-service MILDEC operations. Status: **Revision**
NLW *Multi-Service Tactics, Techniques, and Procedures for the Tactical Employment of Nonlethal Weapons* **Distribution Restricted**	24 OCT 07	FM 3-22.40 MCWP 3-15.8 NTTP 3-07.3.2 AFTTP 3-2.45	Description: This publication provides a single-source, consolidated reference on the tactical employment of NLWs and offers commanders and their staff guidance for NLW employment and planning. Commanders and staffs can use this publication to aid in the tactical employment of NLW during exercises and contingencies. Status**: Revision**
PEACE OPS *Multi-Service Tactics, Techniques, and Procedures for Conducting Peace Operations* **Approved for Public Release**	20 OCT 03 Change 1 incorporated 14 APR 09	FM 3-07.31 MCWP 3-33.8 AFTTP 3-2.40	Description: This publication provides tactical-level guidance to the warfighter for conducting peace operations. Status: **Revision**
TACTICAL CONVOY OPERATIONS *Multi-Service Tactics, Techniques, and Procedures for Tactical Convoy Operations* **Distribution Restricted**	13 JAN 09	FM 4-01.45 MCRP 4-11.3H NTTP 4-01.3 AFTTP 3-2.58	Description: Consolidates the Services' best TTP used in convoy operations into a single multi-Service TTP. It provides a quick reference guide for convoy commanders and subordinates on how to plan, train, and conduct tactical convoy operations in the contemporary operating environment. Status: **Revision**

LAND AND SEA BRANCH – POC alsab@langley.af.mil

TITLE	DATE	PUB #	DESCRIPTION / STATUS
TECHINT *Multi-Service Tactics, Techniques, and Procedures for Technical Intelligence Operations* **Approved for Public Release**	9 JUN 06	FM 2-22.401 NTTP 2-01.4 AFTTP 3-2.63	Description: This publication provides a common set of MTTP for technical intelligence operations. It serves as a reference for Service technical intelligence planners and operators. Status: **Revision**
UXO *Multi-Service Tactics, Techniques, and Procedures for Unexploded Explosive Ordnance Operations* **Distribution Restricted**	20 SEP 11	ATTP 4-32.2 MCRP 3-17.2B NTTP 3-02.4.1 AFTTP 3-2.12	Description: This MTTP describes hazards of UXO submunitions to land operations, addresses UXO planning considerations, and describes the architecture for reporting and tracking UXO during combat and post conflict. Status: **Current**

COMMAND AND CONTROL (C2) BRANCH - POC: alsac2@langley.af.mil

TITLE	DATE	PUB #	DESCRIPTION / STATUS
AOMSW *Multi-Service Tactics, Techniques, and Procedures for Air Operations in Maritime Surface Warfare* **Distribution Restricted**	17 NOV 08	NTTP 3-20.8 AFTTP 3-2.74	Description: This publication consolidates Service doctrine, TTP, and lessons earned from current operations and exercises to maximize the effectiveness of "air attacks on enemy surface vessels". Status: **Assessment**
BREVITY *Multi-Service Brevity Codes* **Distribution Restricted**	7 APR 10	FM 1-02.1 MCRP 3-25B NTTP 6-02.1 AFTTP 3-2.5	Description: This publication defines multi-Service brevity which standardizes air-to-air, air-to-surface, surface-to-air, and surface-to-surface brevity code words in multi-Service operations. Status: **Revision**
CIVIL SUPPORT (DSCA) *Multi-Service Tactics, Techniques, and Procedures for Civil Support Operations* **Distribution Restricted**	3 DEC 07	FM 3-28.1 NTTP 3-57.2 AFTTP 3-2.67	Description: The DSCA publication fills the Civil Support Operations MTTP void and assists JTF commanders in organizing and employing Multi-Service Task Force support to civil authorities in response to domestic crisis. Status: **Revision**
COMCAM *Multi-Service Tactics, Techniques, and Procedures for Joint Combat Camera Operations* **Approved for Public Release**	24 MAY 07	FM 3-55.12 MCRP 3-33.7A NTTP 3-13.12 AFTTP 3-2.41	Description: This publication fills the void that exists regarding combat camera doctrine and assists JTF commanders in structuring and employing combat camera assets as an effective operational planning tool. Status: **Revision**
HAVE QUICK *Multi-Service Tactics, Techniques, and Procedures for HAVE QUICK Radios* **Distribution Restricted**	7 MAY 04	FM 6-02.771 MCRP 3-40.3F NTTP 6-02.7 AFTTP 3-2.49	Description: This publication simplifies planning and coordination of HAVE QUICK radio procedures. It provides operators information on multi-Service HAVE QUICK communication systems while conducting home station training or in preparation for interoperability training. Status: **Revision**
HF-ALE *Multi-Service Tactics, Techniques, and Procedures for the High Frequency-Automatic Link Establishment (HF-ALE) Radios* **Distribution Restricted**	20 NOV 07	FM 6-02.74 MCRP 3-40.3E NTTP 6-02.6 AFTTP 3-2.48	Description: This MTTP standardizes high power and low power HF-ALE operations across the Services and enables joint forces to use HF radio as a supplement / alternative to overburdened SATCOM systems for over-the-horizon communications. Status: **Revision**
JATC *Multi-Service Tactics, Techniques, and Procedures for Joint Air Traffic Control* **Distribution Restricted**	23 JUL 09	FM 3-52.3 MCRP 3-25A NTTP 3-56.3 AFTTP 3-2.23	Description: This publication provides guidance on ATC responsibilities, procedures, and employment in a joint environment. It discusses JATC employment and Service relationships for initial, transition, and sustained ATC operations across the spectrum of joint operations within the theater or AOR. Status: **Assessment**
EW REPROGRAMMING *Multi-Service Tactics, Techniques, and Procedures for the Reprogramming of Electronic Warfare and Target Sensing Systems* **Distribution Restricted**	01 FEB 11	ATTP 3-13.10 MCRP 3-40.5A NTTP 3-51.2 AFTTP 3-2.7	Description: This publication supports the JTF staff in planning, coordinating, and executing reprogramming of electronic warfare and target sensing systems as part of joint force command and control warfare operations. Status: **Current**
TACTICAL CHAT *Multi-Service Tactics, Techniques, and Procedures for Internet Tactical Chat in Support of Operations* **Distribution Restricted**	7 JUL 09	FM 6-02.73 MCRP 3-40.2B NTTP 6-02.8 AFTTP 3-2.77	Description: This publication provides MTTP to standardize and describe the use of internet tactical chat (TC) in support of operations. It provides commanders and their units with guidelines to facilitate coordination and integration of TC when conducting multi-Service and joint force operations. Status: **Assessment**

COMMAND AND CONTROL (C2) BRANCH - POC: alsac2@langley.af.mil			
TITLE	**DATE**	**PUB #**	**DESCRIPTION / STATUS**
TACTICAL RADIOS *Multi-Service Communications Procedures for Tactical Radios in a Joint Environment* **Approved for Public Release**	14 JUN 02	FM 6-02.72 MCRP 3-40.3A NTTP 6-02.2 AFTTP 3-2.18	Description: This publication standardizes joint operational procedures for SINCGARS and provides an overview of the multi-Service applications of EPLRS. Status: **Revision**
UHF TACSAT/DAMA *Multi- Service Tactics, Techniques, and Procedures Package for Ultra High Frequency Tactical Satellite and Demand Assigned Multiple Access Operations* **Approved for Public Release**	31 AUG 04	FM 6-02.90 MCRP 3-40.3G NTTP 6-02.9 AFTTP 3-2.53	Description: This publication documents TTP that will improve efficiency at the planner and user levels. (Recent operations at the JTF level have demonstrated difficulties in managing a limited number of UHF TACSAT frequencies.) Status: **Revision**

January 2013 Air Land Sea Bulletin (ALSB)

Got a story? Want to tell it? Help us help you!

The Air Land Sea Application (ALSA) Center develops multi-Service tactics, techniques, and procedures (MTTP) with the goal of meeting the immediate needs of the warfighter. In addition to developing MTTP, ALSA provides the ALSB forum to facilitate tactical and operationally relevant information exchanges among warfighters of all Services.

There is no better resource for information than the people doing the jobs. Personal experiences, studies and individual research lead to inspirational and educational articles. Therefore, we invite our readers to share their experiences and possibly have them published in an upcoming ALSB.

The topic for the January 2013 ALSB is "Special Operations Forces (SOF) and Conventional Force Integration."

We want to take your lessons learned from Operations IRAQI FREEDOM, ENDURING FREEDOM, NEW DAWN, or any other multi-Service or multi-nation missions in which you have been involved, and spread that knowledge to others. Get published by sharing your experiences and expertise.

With the focus on SOF and conventional force integration, your article could concentrate on intelligence sharing; advising foreign forces; airfield opening; or survival, evasion, reisitence, and escape. Also, tactical employment of nonlethal weapons and dynamic targeting are among other possible considerations. There is a vast number of topics to be explored. Challenge yourself and submit an article for consideration.

Please keep submissions unclassified and in accordance with the instructions in the box on this page.

SOF and Conventional Force Integration

Submissions must:

- Be 1,500 words or less
- Be releasable to the public
- Be double spaced
- Be in MS Word format
- Include the author's name, unit address, telephone numbers, and email address
- Include current, high-resolution (300 dpi minimum), original photographs and graphics

Note: Article submissions and photos are due no later than 1 October 2012 for publication in the January 2013 issue.

Early submissions are highly encouraged.

Contact ALSA's Command and Control Branch at:
alsac2@langley.af.mil or
DSN:
575-0904/0903/0967/0854 or
Commercial:
(757) 225-0904/0903/0967/0854

ALSA ORGANIZATION

JASC
Joint Actions Steering Committee

Director
COL Bruce Sones, USA

Deputy
Col Robert C. Swaringen, USAF

NCOIC
TSgt Christal Jefferson, USAF

Support Staff
Cheryl Parris, Admin Support Asst
Sonya Robinson, Budget Analyst
Leila Joyce, Office Auto Asst

Publishing Staff
Patricia Radcliffe, Editor
Laura Caswell, Illustrator
Maj Clayton Laughlin, Publications Officer

Air
LTC Stephen Parker, USA
Lt Col Steve Lloyd, USAF
LTC Dana Smith, USA
Maj Clayton Laughlin, USAF
Maj Jeffrey Hughes, USMC

Land and Sea
LTC Troy Ewing, USA, USA
LTC Reginald Armstrong
Lt Col Richard Freeman, USAF
Lt Col William Wallis, USAF
MAJ Michael Saxon, USA

Command and Control
LTC Deidra Broderick, USA
Lt Col (S) Joel Eppley, USAF
LCDR Christian Goodman, USN
Maj Albert Denney, USAF

Airspace Control
22 May 09

Aviation Urban Operations
9 Jul 05

Dynamic Targeting
07 May 2012

Integrated Air Defense System (IADS)
1 May 09

Joint Application of Firepower (JFIRE)
20 Dec 07

Suppression of Enemy Air Defenses (JSEAD)
28 May 04

Joint Surveillance Target Attack Radar System (JSTARS)
16 Nov 06

Kill Box Employment
4 Aug 09

Strike Coordination and Reconnaissance (SCAR)
26 Nov 08

Survival, Evasion, and Recovery
20 Mar 07

Theater Air-Ground System (TAGS)
10 Apr 07

Tactical Employment of Unmanned Aircraft Systems (UAS)
21 Sep 11

Advising Foreign Forces
10 Sep 09

Airfield Opening
15 May 07

Conventional Forces/ Special Operations Forces Integration and Interoperability (CF/SOF)
17 Mar 10

Cordon and Search Operations
25 Apr 06

Explosive Ordnance Disposal (EOD)
20 Sep 11

Military Diving Operations (MDO)
12 Jan 11

Military Deception (MILDEC)
12 Apr 07

Nonlethal Weapons (NLW)
24 Oct 07

Conducting Peace Operations (PEACE OPS)
14 Apr 09 (CH1)

Tactical Convoy Operations (TCO)
13 Jan 09

Technical Intelligence (TECHINT)
9 Jun 06

Unexploded Explosive Ordnance Operations (UXO)
20 Sep 11

Air Operations in Maritime Surface Warfare (AOMSW)
17 Nov 08

Brevity Codes
7 Apr 10

Civil Support Operations
3 Dec 07

Combat Camera Operations (COMCAM)
24 May 07

Have Quick Radios
7 May 04

High Frequency-Automatic Link Establishment Radios (HF-ALE)
20 Nov 07

Joint Air Traffic Control (JATC)
23 Jul 09

Electronic Warfare Reprogramming
1 Feb 11

Internet Tactical Chat in Support of Operations (Tactical Chat)
7 Jul 09

Tactical Radios
14 Jun 02

Ultra High Frequency Tactical Satellite and Demand Assigned Multiple Access Operations (UHF TACSAT/DAMA)
31 Aug 04

MISSION

ALSA's mission is to rapidly and responsively develop multi-Service tactics, techniques and procedures (MTTP), studies, and other like solutions across the entire military spectrum to meet the immediate needs of the warfighter.

ALSA is a joint organization chartered by a memorandum of agreement under the authority of the Commanders of the, US Army Training and Doctrine Command (TRADOC), Marine Corps Combat Development Command (MCCDC), Navy Warfare Development Command (NWDC), and Headquarters, Curtis E. LeMay Center for Doctrine Development and Education. ALSA is governed by a Joint Actions Steering Committee (JASC) consisting of four voting and three nonvoting members.

Voting JASC Members

Maj Gen Thomas K. Andersen

Commander, Curtis E. LeMay Center for Doctrine Development and Education

RADM Terry B. Kraft

Commander, Navy Warfare Development Command

BGen (Sel) Eric M. Smith

Director, Capabilities Development Directorate, Marine Corps Combat Development Command

Mr. Kirby R. Brown

Acting Deputy to the Commanding General US Army Combined Arms Center

ALSA Public Web Site

http://www.alsa.mil

ALSA CAC Web Site

https://wwwmil.alsa.mil

ALSA SIPR Site

http://www.acc.af.smil.mil/alsa

JDEIS

https://jdeis.js.mil/jdeis/index.jsp?pindex=84

Online Access to ALSA Publications

ALSA CENTER
ATTN: ALSB
114 ANDREWS STREET
LANGLEY AFB VA 23665-2785

OFFICIAL BUSINESS

Scan Me

Air Land Sea Application Center

http://www.facebook.com/ALSA.Center

http://www.twitter.com/ALSA_Center