MARCH 2009

ATTACK THE NETWORK METHODOLOGY: PART 2 CRITICAL VULNERABILITIES AND TARGETING

ASYMMETRIC WARFARE GROUP

OVERVIEW:

This document facilitates discussion, training, and implementation of effective targeting methods at the Battalion and Brigade level. This paper discusses the *Center of Gravity analysis model* for identifying threat networks, Critical Capabilities, and Critical Vulnerabilities; use of the methodology to determine the Intelligence Surveillance and Reconnaissance (ISR) focus; and as a basis for understanding Attack the Network concepts.

BACKGROUND:

The discussion must start with understanding the insurgent networks' capability to influence or control the Center Of Gravity (COG). Typically, ***in a Counter Insurgency (COIN) environment, the COG is the population***. An adaptive threat will modify its Tactics, Techniques and Procedures to maintain control over the COG. Dr. Strange's COG model is extracted from the writings of Karl von Clausewitz, who emphasized that a COG must be identified by analyzing one's adversary; Dr. Strange extended the 19th century definition to include "the primary sources of moral or physical strength, power, and resistance" and further defined analytical elements (Critical Capabilities, Critical Requirements and Critical Vulnerabilities) necessary to enable practical operational use.[1]

COG analysis is a five-step process (discussed in detail within AWG's Al Qaeda and Associated Networks Vulnerability Analysis Workbook, Understanding the Threat Series, Volume 1, 1 JUN 2008). (See AWG SIPR / NIPR websites on final page)

- Identifying the COG.
- Identifying Critical Capabilities for the COG to function.
- Identifying Critical Requirements for each Critical Capability to support the COG.
- Determining the Critical Vulnerabilities (through attack, interdiction [or neutralization]) of each Critical Requirement.
- Developing plans that focus on exploiting Critical Vulnerabilities, which are in effect the development of our own Critical Requirements.[2]

This method allows us to see the network by highlighting the functional capabilities required to sustain the network. Each Critical Capability and Critical Requirement requires human interaction, management and support. These individuals are typically trusted agents capable of leading others. We identify these individuals as Tier II targets. They were also called "intermediaries" within the Asymmetric Warfare Group's Attack the Network Part I paper.

This is the second example within the Attack the Network series of papers that highlights the need to focus targeting efforts against something other than the threat's strength. Often our efforts focus on reacting to "Who conducted the IED attack that affected Coalition Forces on this date?" which leads to allocation of resources against the lowest tiered targets rather than key individuals within a network. The compartmentalization of an insurgent cell and the large pool of recruits available as replacements indicate that pursuit of low level insurgents does not have long term significant impacts on the COIN fight. Low level insurgents are relatively easy to replace, and targeting them only succeeds in creating a "refit/ reorganize cycle". ***Units that focus on attacking the vulnerabilities related to the enemy's Critical Requirements will have more impact on the leadership of the network, as well as, reduce the number of enemy attacks against them.*** For the purposes of this discussion, Critical Capabilities can be described as High Value Targets. The Multi-National Corps-Iraq Intelligence Officer (C2) recently described this in blunt terms, "Attacking the network is really about targeting High Value Individuals; the Counter-Insurgency fight is about key personalities that dominate the threat organization."[3] This paper demonstrates the linkage of key individuals to key functions within an insurgent network to determine which targets should be prioritized for finding, fixing and finishing the threat.

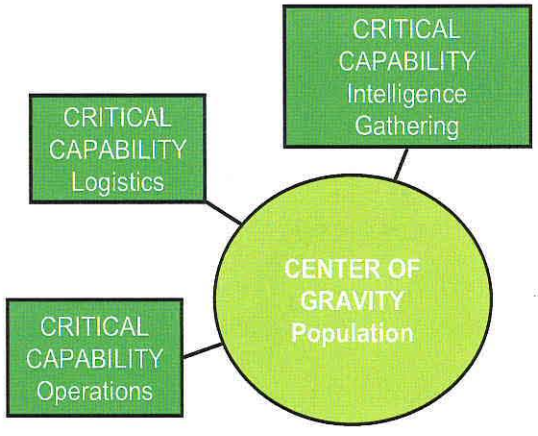
INSURGENT CAPABILITIES DESCRIBED THROUGH CENTER OF GRAVITY ANALYSIS:

Insurgents must be able to perform critical operations to control or influence the COG (the people) in the COIN environment. These operations, or *Critical Capabilities*, ensure key tasks are successful and can also be described as threat Warfighting functions. For example, a threat must have the following functions to be successful:

- Command and Control
- Intelligence Gathering
- Operational Capability
- Logistics
- Recruitment and Training

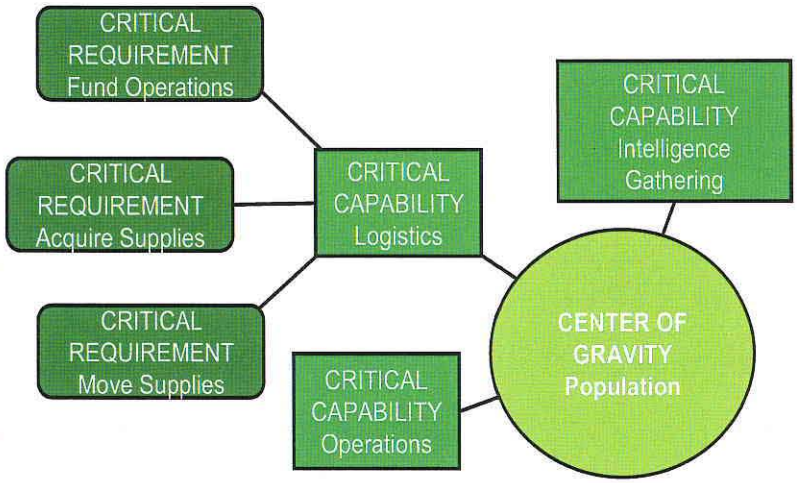
Each of these functions can be labeled as Critical Capabilities under the COG Analysis methodology. The MNC-I C2 indicated the importance of recognizing that in many insurgent organizations one key person is responsible for more than one function. An effort should be made to diagnose each insurgent organization's capabilities/ networks to determine their relative strengths and weaknesses. This will lead to an understanding of intersecting threat lines of operation and key leaders, and will help prioritize targeting efforts against networks and High Value Individuals (HVIs).

CENTER OF GRAVITY ANALYSIS – Critical capabilities



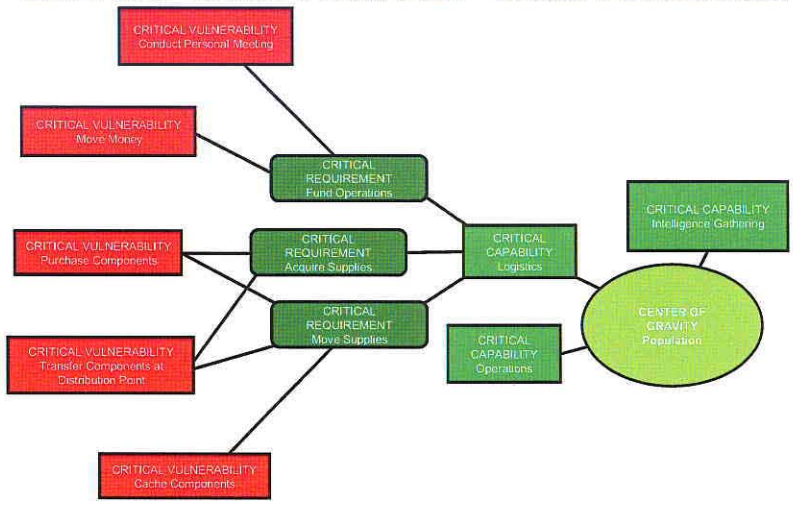
Required tasks within a Critical Capability that must be successfully accomplished to ensure the network functions are called *Critical Requirements*. Another way to describe the importance of requirements and capabilities is to think of the association of Battle Tasks to Collective Tasks. Collective Tasks form the basis of a unit's expected capabilities. The same holds true for insurgent organizations. For example, if the enemy has to ensure it receives adequate resupply to conduct attacks against Coalition Forces then it is required to *Fund Operations, Acquire Supplies* and *Move Supplies* (Critical Requirements). After this level of analysis, staff elements should be able to evaluate which threat capabilities are strengths and which are weaknesses to the enemy's organization. ***We should attack the threat's weaknesses and contain its strengths.***

CENTER OF GRAVITY ANALYSIS – Critical Requirements



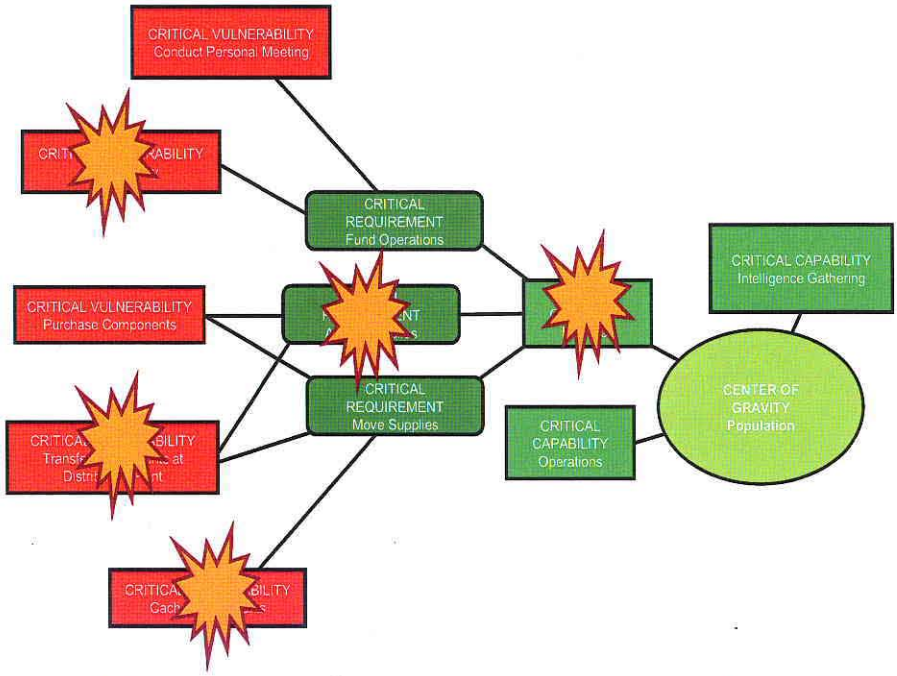
Threat actions that increase chances of detecting and capturing the threat are Critical Vulnerabilities. A series of individual tasks must be accomplished to constitute a collective task, just as collective tasks are combined to form the structure of a network. For analysis, it is not necessary to reinvent all associated tasks. Staffs that have already determined the insurgent's weaknesses, within the capabilities and requirements framework, can narrow their focus to those actions that can be observed with their internal ISR assets. Just as in our own training doctrine, where individual tasks are often common to various collective skills, threat Critical Vulnerabilities are typically common requirements in different networks. Our ability to detect the threat is increased because the tasks overlap or one key individual is responsible for more than one requirement. ***For example, if the Critical Capability is to provide logistics and one of the Critical Requirements that we believe is a weakness is to move those supplies, then possible vulnerabilities may include the following:*** transfer supplies from a cache to vehicle, distribute materials from large truck to multiple vehicles, or conduct a personal meeting to coordinate resupply. There will be several tasks associated with the Critical Requirement. A staff will have to understand their Operating Environment, the threat's previous actions, and their own capabilities to understand which of those individual tasks are most vulnerable to detection and action. **The purpose of identifying Critical Vulnerabilities is to focus ISR, provide intelligence to the commander so that he can make a decision on how to neutralize the threat, and then take action.**

CENTER OF GRAVITY ANALYSIS – Critical Vulnerabilities



Returning to the theme that a key element of the COIN fight is personality targeting, key insurgent individuals who perform tasks that are vulnerable to detection/exploitation or supervise the execution of Critical Requirements are those who should receive priority targeting. Individuals who perform tasks that are vulnerable to detection/exploitation and impact more than one Critical Requirement are a higher priority because of the role they play within the network. ***Multiple, near simultaneous attacks against Critical Vulnerabilities significantly reduce the capabilities of the network by shocking the system.*** Continuing with the earlier examples, a bomb maker that acquires supplies, coordinates meetings for delivering supplies, and also conducts reconnaissance of targets for future attacks deserves more priority for targeting than the insurgent that emplaced and triggered an IED. Combining actions to kill or capture this HVI as well as the cell leader responsible for planning and conducting the attacks both seriously degrades the Critical Requirement to resupply the network and critical capability to perform command and control; a shock to the network has been introduced by Coalition Forces. This is not easy to do, even with excellent intelligence, but using this strategy and analysis drives ISR planning and target development towards this goal.

CENTER OF GRAVITY ANALYSIS – Defeat the Network



CONCLUSION:

In Attack the Network – Part I, the Oil Spot model was modified to discuss insurgent operations for influencing the COG and developing various networks. The analysis helped to illustrate that mid-tier level insurgents (Tier II or 'intermediaries") are worth more targeting effort at the BCT level than low-level Tier III-type targets. In this paper, employing COG analysis to determine Critical Capabilities, Critical Requirements, and Critical Vulnerabilities shows that our ISR assets and targeting strategy need to be prioritized toward the enemy's weaknesses and NOT his strengths. Personality targeting is one of the keys to attacking an insurgent network. Units need to analyze both HVIs and the associated tasks performed to accomplish Critical Capabilities in order to have a significant impact on the enemy. Part III will continue the discussion by describing doctrinal templating of insurgent networks, ISR focus, and synchronization to the commander's intent and scheme of maneuver.

Look for Attack the Network Methodology: Part 3 Observable Indicators and ISR Synchronization

REFERENCES:

[1]Asymmetric Warfare Group, Al Qaeda and Associated Networks Vulnerability Analysis Workbook, Understanding the Threat Series, Volume 1: 1 JUN 2008; page vii.

[2]Asymmetric Warfare Group, Al Qaeda and Associated Networks Vulnerability Analysis Workbook, Understanding the Threat Series, Volume 1: 1 JUN 2008; page A-5.

[3]MNC-I C2, Multi-National Corps – Iraq, Personal Interview: 24 NOV 08.

[4] AWG Attack the Network Part 1: March 09

ATTACK THE NETWORK METHODOLOGY: PART 2
CRITICAL VULNERABILITIES AND TARGETING

ASYMMETRIC WARFARE GROUP

SIPR: http://army.daiis.mi.army.smil.mil/org/aawo/awg/default.aspx
NIPR: https://portal.awg.army.mil

Asymmetric Warfare Group
2282 Morrison Street
Fort George G. Meade, MD 20755
301.833.5258