FEBRUARY 2011

TACTICAL INFORMATION SUPERIORITY
ASYMMETRIC WARFARE GROUP

OVERVIEW:

This document facilitates discussion, training, and implementation of effective information superiority 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 threat vulnerabilities; and as a basis for understanding how to achieve Information Superiority.

INTRODUCTION:

The battalion commander instantly knew from looking at the map, with all of the red significant activities plotted on the overlay, that renewed operations in the valley would be rough. Almost every route into and out of the area had seen recent Improvised Explosive Device (IED) activity. Worse, it seemed that many of the villages in the valley were supportive of insurgent activity. The insurgents had recently stepped up their propaganda campaign in the area, as well, intimidating villagers, kidnapping elders, assassinating key figures, leaving behind strong warnings against cooperating with Coalition Forces, while also reinforcing their own message: the insurgents would prevail over the foreign forces because they were from the region, the insurgents would take care of the people that supported their activities, and they would continue to be in the area long after the Coalition Forces left.

The commander planned a deliberate clearing operation to regain control of the major routes in the area, deny insurgents traditional safe havens, and bolster Host Nation Security Forces and Government officials, but he also knew that if he entered the valley using too much force that he might further alienate the locals. The commander could not stay in the valley, holding the terrain against insurgent re-infiltration indefinitely—he would be forced to withdraw and plan for other operations, hoping the locals and Host Nation Security Forces would be willing and able to defend the area against the enemy.

How could the commander expect the villagers to aid his unit in denying the area as a support base for insurgents when there was no apparent common ground? How was he, as a Commander, supposed to communicate his intent to the local people, Host Nation officials, and to other key individuals?

His battalion's task organization included three Infantry Companies, an Anti-Tank Company, a Mortar Platoon, and a Scout/Sniper Platoon. Additionally, the commander's capabilities were augmented by a Tactical Military Information Support Team, a Military Source Operations (MSO) qualified Counterintelligence (CI) Team, and an Explosive Ordnance Detachment (EOD) Team. The commander also had new devices (including the Radio-In-The-Box or RIAB); some of these newly issued devices were pieces of

equipment his leaders and Soldiers had never seen or used before deploying into theater.

The commander had enough combat forces to clear, and temporarily hold the valley, but what then? The commander knew he would achieve immediate but limited security in the area and also reach his higher headquarter's directed end state. But how could he achieve longer term effects so that he would not have to repeat the mission again in just four months?

Lethal options in a Counter Insurgency (COIN) environment are only a portion of the necessary operations that must be successfully conducted at the tactical level. Non-Lethal options provide a balance to more kinetic operations, providing choices that can impact the threat and the population in longer term ways. Information Superiority, at the tactical level, is an essential requirement for successfully defeating insurgents in the COIN fight.

Joint Publication 3-13, Information Operations, defines Information Superiority as the operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same.[1] Further, FM 3-0, Operations, describes how information shapes, at every level, the operational environment. Information is a critical, and sometimes the decisive, factor in campaigns and major operations. Effectively employed, information multiplies the effects of friendly successes. Mishandled or ignored, information can lead to devastating reversals.[2]

Asymmetric Warfare Group (AWG) observations indicate that tactical level staff processes concerning Information Operations (IO) can be improved. There are no Silver Bullets, however, a stronger emphasis placed upon Situational Awareness (both the Threat Vulnerabilities and Friendly Capabilities), as well as increased use of Measures of Effectiveness can facilitate stronger IO by incorporating it into the overarching Concept of Operation of each mission and facilitate reaching the commander's end state.

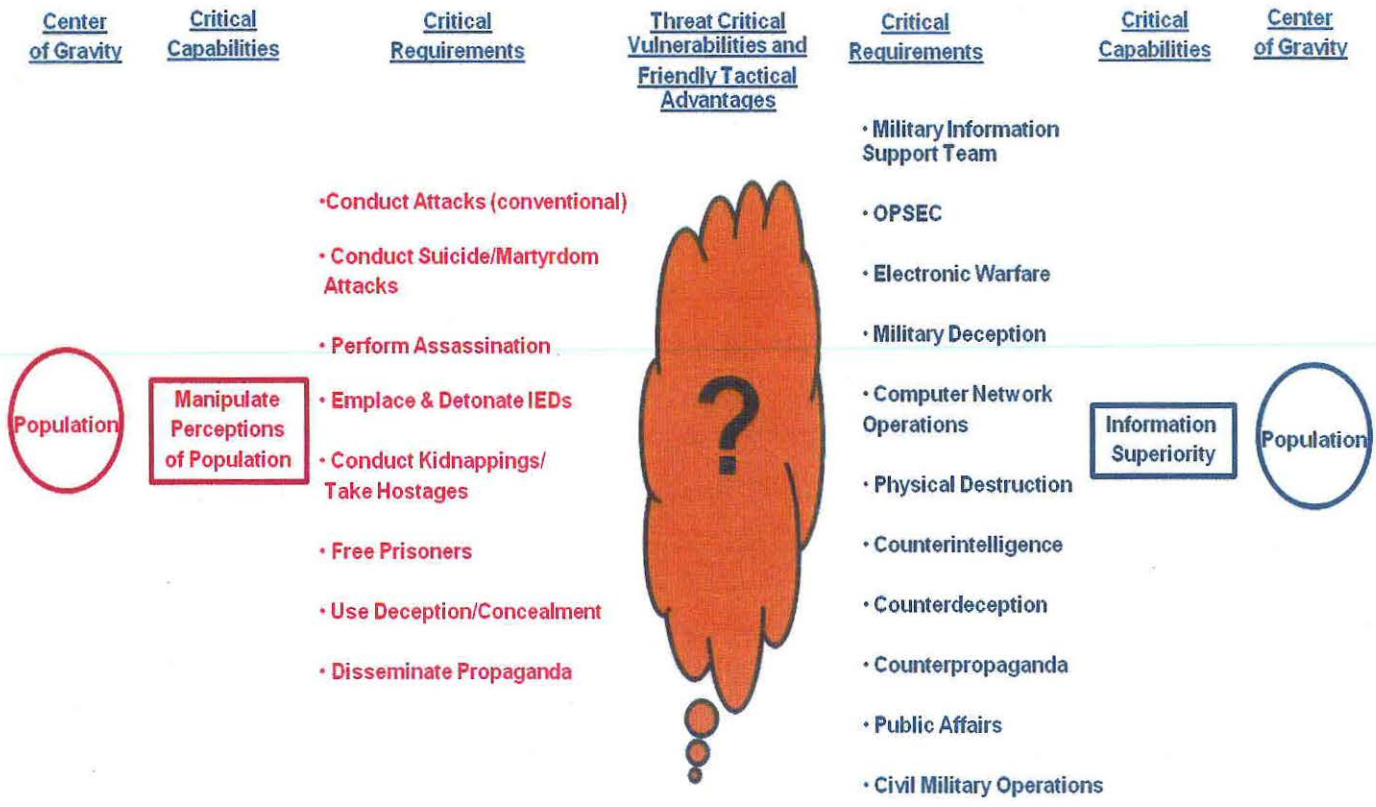
This document will highlight observed trends, and ways to achieve positive effects and mitigate negative effects at the tactical level in areas concerning IO. The paper will emphasize that understanding how the threat, friendly personnel, and population receive and transmit information is critical to gaining Information Superiority. Gaining Situational Awareness of the Information Environment (IE) allows the staff to leverage enablers (based on their capabilities and limitations) to shape the environment and achieve the commander's objectives. Finally, assessments of IO during all phases of operations are key to rapidly adapting plans and modifying 2nd and 3rd Order Effects.

IO SITUATIONAL AWARENESS:

Understanding the threat's, friendly's, and population's means of receiving and transmitting information is critical to gaining Information Superiority. However, IO Situational Awareness will not happen simply by templating threat and friendly locations. Staff officers must have a better understanding of the Threat's Capabilities and Vulnerabilities. For the sake of this discussion, a Threat Vulnerability is any threat activity related to IO that a friendly commander can identify and impact with his own organic capabilities. Friendly Capabilities are the tactical advantages that a commander can use to inform and influ-

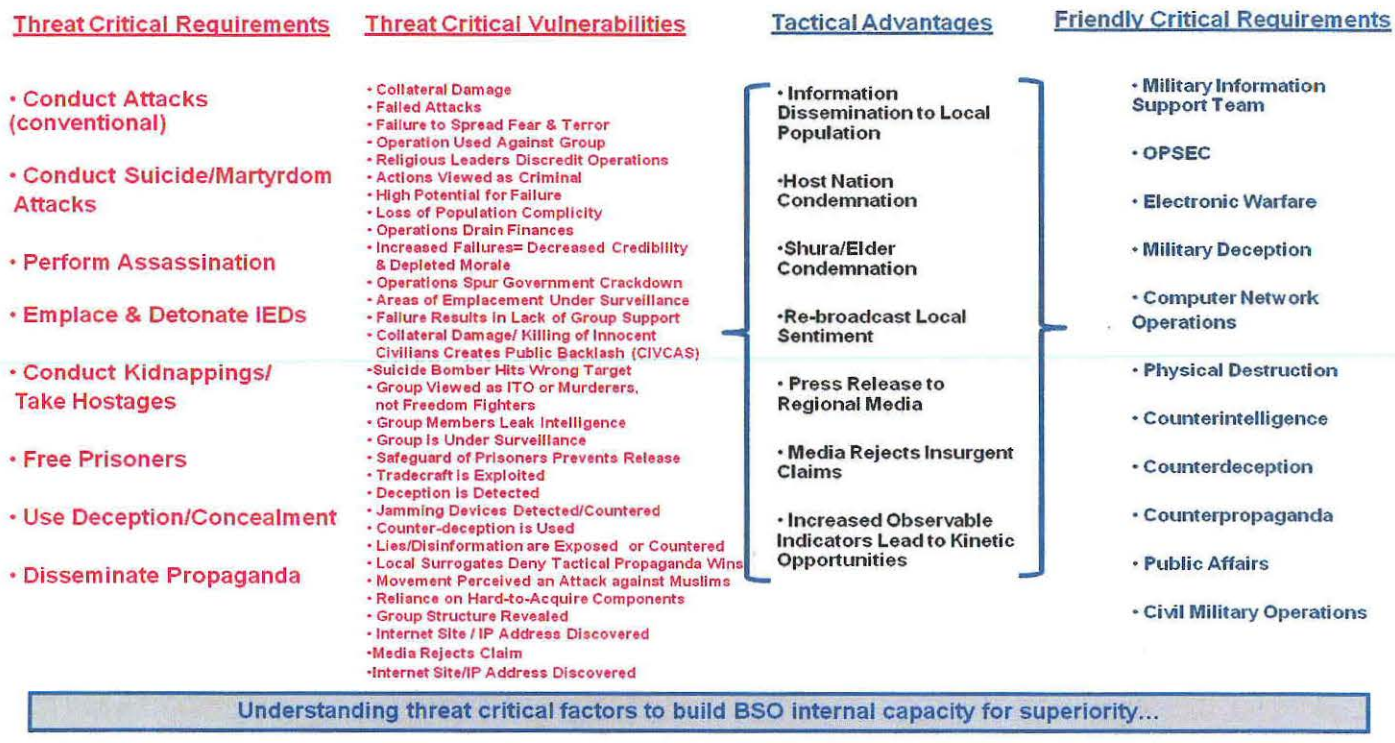
ence others within his operational environment and gain Information Superiority. See Figure 1.

Figure 1. Information Critical Capability-Requirement-Vulnerability Model



A staff can use the model depicted above to help them gain an understanding of the threat's strengths and weaknesses, as well as the friendly capabilities to take action. The example in Figure 1 was taken from an AWG Vulnerability Analysis Workbook; a staff can develop a more accurate model based on an understanding of their IE. The above example does help highlight one important issue, however. The threat's Critical Capability to manipulate perceptions of the population can often be considered their overarching tactical to strategic objective. The threat often identifies its Information objectives and then conducts kinetic and non-kinetic operations to achieve that objective. Conversely, we often think of Information Operations as an afterthought or a reaction to mitigate unintended consequences of kinetic operations. Because the threat often conducts operations to support his Information objectives, his process for affecting the population is much more streamlined than it is for friendly forces. To counter that disadvantage, the commander's staff will need to work together to determine what works best within their area of operation; there is too much analysis required for this to be the sole responsibility of any one staff officer. Information Superiority is the responsibility of the entire staff. There are too few resources at the tactical level to focus on all potential objectives (using IO as a non-lethal method of delivery); the commander's staff must identify the threat's vulnerabilities and match them with the unit's capabilities to take action. Figure 2 displays the threat critical requirements and vulnerabilities, and friendly tactical advantages and critical requirements based on the center of gravity (COG) being the populace and the critical capability being information superiority.

Figure 2. Information Center of Gravity Analysis and Tactical Advantages from Threat Vulnerabilities



Analysis of the threat's vulnerabilities and potential friendly advantages allows the staff to understand the fundamental concepts behind IO's integration in operations. More tools are needed, though, to increase Situational Awareness and develop multiple courses of action that balance lethal and non-lethal operations to achieve the commander's end state. The staff must accurately define the IE and describe the impact the environment has on the threat, friendly forces, and the population. The characteristics that should be defined are: terrain, civilian information infrastructure, media, civilian population, and third party organizations. When this information is combined with products and analysis developed by the intelligence staff, the commander better understands the Common Intelligence Picture and his potential courses of action.

Information environment characteristics analysis, represented graphically as the Combined Information Overlay (CIO), helps determine the combined effects of several different factors. For example, terrain analysis might show how the threat's lines of communication are canalized in a particular area. The restricted terrain may also indicate that only a series of strategically placed VHF repeaters allow the threat to communicate through a pass. Through civilian information infrastructure analysis and working with the Host Nation Partners, the staff will understand what key communications systems are used throughout the operational environment, as well as the content transmitted. Media analysis will highlight the bias or context of available outlets, the media's audience, and the various types of content presented. Civilian population analysis focuses on how the people in the operational environment communicate, what type of information the people need/want, and the cultural characteristics of the population. Finally, third party organization analysis identifies the Non-Governmental Organizations (NGO) operating in

the operational environment, their purpose and objectives, and what type of information the NGOs are willing to share. The usefulness of a CIO lies in its ability to highlight the enablers that will best deliver information to an audience, whether it is via social communication, radio, cell phone, television, or even the internet. It also allows the staff to anticipate threat actions and plan friendly actions.

In the example figures below, the staff might be able to discern that natural Lines of Communication move personnel and information through the northern portion of the environment, but that friendly Combat Outposts are not placed in the correct locations to control traffic that affects the majority of people in the north. The staff may also be able to determine that the threat's primary communication capability hinges upon a series of repeaters in the northeastern portion of the environment; denying, delaying, or disrupting the threat's ability to communicate with subordinate elements, as well as the population, is a critical component of Information Superiority. Additionally, a demographic/tribal analysis product helps the staff to see that the threat's influence over one tribe is less than another. All of these assessments, when combined with the rest of the staff's efforts, help the commander to prioritize his objectives. See Figures 3, 4, 5.

Figure 3. CIO Terrain Analysis

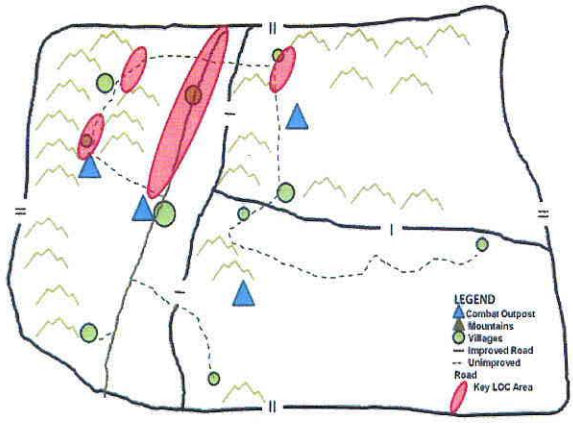


Figure 4. CIO Civilian Info/Infrastructure Analysis

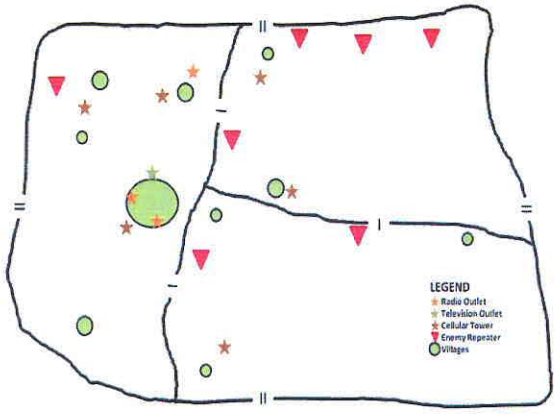
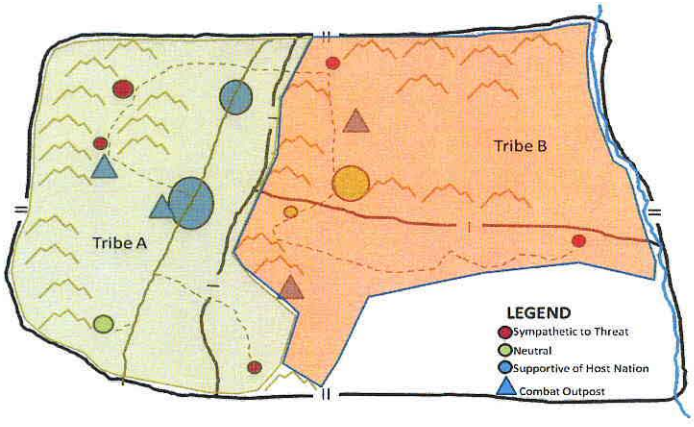


Figure 5. CIO Population Density/Tribal Affiliation Analysis



PLANNING:

Gaining IE Situational Awareness allows the staff to leverage enablers (based on their capabilities and limitations) to shape the environment and achieve the commander's objectives. The intended use of

enablers for Information Superiority starts with Situational Awareness, but tactical units must also develop solid plans to counter threat activity, mitigate some friendly actions, and determine Information objectives to establish an offensive mindset. The staff needs to look at the defined/described operational environment (through the CIO and written narratives supporting the IE) and identify the tactical advantages. Each tactical advantage should have a corresponding plan of action that the staff and subordinate units will use once an event occurs. This detailed planning does not equate to "making a unit reactionary" or "waiting for the threat to strike." Predicting threat activity and taking action, possibly before the enemy has the opportunity to strike, is pre-emptive in nature, and allows the friendly unit to gain momentum and information superiority. See Figure 6.

Figure 6. Pre-Planned Mitigation to Counter Threat Vulnerabilities

Activity	Critical Vulnerabilities	Tactical Advantages	Actions
IED near Village Stability Operation – damage to local shop: injuries/deaths	Actions Viewed as Criminal – vandalism, theft, sabotage	Information Dissemination to Local Population	Report truthful information immediately by all means showing the threats negative effects on the populace. Inventory damaged local property: Record statements of population impacted by event: Photos taken of scene: Record Host Nation Security Forces statements
	Collateral Damage/ Killing of Innocents	Shura/Elder Condemnation Host Nation Condemnation	Record statements of Elders condemning attack/confirming loss of innocent life: Host nation officials notified immediately: Record officials and locals statements condemning attack
	Lies/Disinformation are Exposed or Countered	Threat claims responsibility indicating success at killing Friendly Forces	Disseminate immediate Information Release stating facts: who involved: what happened: time and location incident occurred: others involved: Information confirms civilian casualties and damages.
	Media Rejects Claims	Re-broadcast Local Sentiment Media Rejects Insurgent Claims	Available media notified of event. Locals and Officials recordings and photos of incident reviewed. Media acknowledges threat is providing false information and airs facts of attack: media rejects future threat claims
	Areas of Emplacement Under Surveillance	Increased Observable Indicators Lead to Kinetic Opportunities	Temporary Checkpoint established at incident: Temporary Checkpoint/roving patrol established along likely infiltration route to incident: alternate infiltration routes templated, assigned NAIs/TAIs, and ISR tasked to watch for increased Observable Indicators: Local Reaction Force prepared to maneuver, investigate, and take appropriate action: Locals informed of increased security: Information disseminated of new security measures based on need to protect innocents from harm

The above model for mitigating actions is simple; actions in combat are often much more complex. As the staff becomes more accustomed to working through IE issues, they should begin to look at how each enabler can support their ability to gain Information Superiority by destroying, denying, disrupting, delaying, or countering the threat's ability to pass information. For example, when the threat carried out the IED strike intended for friendly forces but killed two locals and damaged a nearby shop, the actions in Figure 6 facilitated passing truthful information to the rest of the population as quickly as possible. The above model could also be used by reviewing each enabler to determine how they can assist in the efforts. Under the tactical advantage of "Threat claims responsibility of killing friendly forces," the staff could also request jamming support from higher headquarters against known/suspected enemy frequencies. Electronic Warfare is a core component of IO, and in this situation, could allow friendly forces the time needed to get the truth out before the threat is able to spread disinformation throughout the opera-

tional environment. It is normally a combination of enablers with desired effects that allows a unit to gain Information Superiority.

The same type of model can be used to prepare for Friendly Vulnerabilities. When an incident occurs that involves collateral damage, the staff must be ready to take immediate action. The Information Officer should be in the Tactical Operations Center during any planned operation; he should be ready to coordinate activities when a collateral damage incident occurs. A pre-determined "Call Chain" of key individuals, including Host Nation officials, who must be notified to rapidly disseminate facts about the incident, as well as a plan for releasing information to the population denying the threat the ability to take advantage of the situation must be a part of any tactical unit's planned operation. Utilize Host Nation Partners throughout the planning, development and dissemination.

The planning process should also focus on preparing forces for an operation by giving them the minimum information requirements that should be disseminated to the people. This information is designed to provide facts that reassure the population, prevent them from interfering with the operation, and could also facilitate obtaining additional intelligence. For example, a partnered operation, into a village to investigate reports of a cache, should have talking points already prepared that they plan to disseminate to the villagers. The tactical commander in charge of the operation, with support from the battalion staff, determines that the following information must be quickly put out: the reason the joint operation is being conducted, what the villagers need to do to remain safe during the operation, and how anyone with information about the location of munitions or insurgents can report it to the patrol safely. The commander realizes that this information can be put out by each Soldier as they engage the people, but there are also key individuals who will help spread the information quickly. These individuals include the village elder, members of the tribal council, and the local religious leader. By recognizing the importance of these individuals, the commander intends to garner the support of the village quickly, and set the conditions for the information to reach outlying areas after the operation is completed.

Taking this an additional step, tactical commanders can use forces to achieve an Information Superiority effect. The Commander wants to ensure that the population in his area knows that Host Nation forces can secure the area and protect the people. The commander determines that he can reinforce that concept by deliberate, visible actions that include partnered operations to drive out the enemy, kill or capture key insurgent leaders, and secure critical infrastructure projects. In this case, achieving the Information Superiority effect becomes the main effort of the unit, and kinetic and non-kinetic operations are conducted to support that main effort.

MEASURES OF EFFECTIVENESS:

Clearly defined and prioritized Measures of Effectiveness (MOE) confirm or deny Methods of Performance to rapidly change plans based on accurate Situational Awareness; MOE are the assessment phase to any operation and give the commander and staff the opportunity to adapt plans based on the restated objectives, current situation, and sentiments of the population. MOE are the criteria that focus Information Requirements to determine whether a desired effect was achieved; MOE are also questions the staff must ask itself during all phases of an operation to determine if 2nd and 3rd order effects were ac-

complished or if a plan must be changed. MOE and Specific Information Requirements must be closely linked in the COIN fight. Intelligence collection must support Information Superiority objectives and define what each collector can observe, providing indicators that answer the MOE. See Figure 7.

Figure 7. Measures of Effectiveness Linked to Information Requirements

Objective	Measures Of Effectiveness	Specific Information Requirement	Observable Indicators	Assigned Responsibility
Deny Threat Communication with Population in Valley X	Is the population of Village A. In Valley X. receiving night letters From insurgents?	When was the last night letter delivered within Village A? Is the threat still attempting to deliver letters to Village A?	Night Letters. new Anti-government graffiti. Movement on motorcycle During limited visibility	Host Nation Partner Units Local government Patrol CI UAV AWT
	Is the population's view of our ability to pass truthful info favorable?	What was the last radio broadcast most people in Valley X listened to? Who do the people believe is more credible?	More invitations to engage locals during patrols. more dialogue and tips passed during KLE. requests for more radios	MISO TM CI CMO PAO
	Has the number of friendly radio station listeners in Valley X increased by 25%?	How many radios were passed out over the last 6 months? How many listeners report they listen to the daily broadcast?	Cell phone /radio delivery increased. Security Force announcements on radio increased. tip line calls increased. reports actions by local security increased	SIGINT LEP PAO/CMO AS3
	Has the number of Tips to either Host Nation or Friendly Forces Increased or decreased since operations in Valley X?	How many tips did the Security Forces receive last week vs. week prior? How many tips did friendly forces receive last week vs. week prior?		

COMMANDER'S INFORMATION SUPERIORITY SCENARIO:

Taking the discussion a final step, the Information representative, with the assistance of the rest of the staff, should get to a point where they predict certain threat activities. Enablers supporting Non-Lethal operations do not have to be reactive; enablers can and should help the unit seize the initiative. The first thing the commander realizes is that nothing precludes him from disseminating facts, data, or instructional information. To reinforce this concept, the commander of all forces in Afghanistan has already declared that friendly forces must be first with the truth.

A commander may determine that his primary objective is to secure a valley and deny its use as a support zone for the threat. The commander also realizes he must gain short-term Information Superiority to be successful at clearing operations, and must sustain a Village Stability Operation in the heart of the valley for the next four months; the commander and staff realize they will not be able to maintain Information Superiority in the operational environment for four consecutive months, but the unit must be able to react and quickly re-take the initiative from the threat if an incident occurs. The staff decides to deny the threat the ability to communicate via Push-To-Talk within the valley for a short period of time to prevent the enemy from re-positioning forces or withdrawing from the valley. The staff requests Electronic Attack capabilities through their higher headquarters, but realizes that part of what they have accomplished also hurts the population in the valley because a majority of the information the people receive is through the threat (whether it is truthful information or not)—the information vacuum created

through Electronic Attack should be filled by friendly forces. The Military Information Support Operations (MISO) Team will be used to pass information to the locals about a new radio broadcast capability that will provide factual and timely information to the villagers. Additionally, the Counter Intelligence (CI) Team will be tasked with gaining information about what type of information the people expect, how they expect to receive it and whether the information they receive raises friendly force's credibility in the operational environment.

The staff uses pre-approved MISO messages from higher to start a broadcast campaign, suggests refined messages based on the target audience, and starts focusing on the villagers residing within the valley. The mayor condemns (via radio) the latest enemy attack that killed two civilians, damaged a shop, and disrupted movement of a village's produce to the market. The local police chief also goes on the air to announce new security measures taking place in outlying regions and explains the government's actions to halt threat activities. Both officials encourage listeners to contact the tip line about suspicious activity, including the emplacement of roadside bombs.

Daily, the commander meets with Host Nation officials and local media to confirm current events, reiterate his joint objectives, and to show the true partnering aspect of the operation. Staff members predicted the threat would not idly stand by and watch one of its key support zones be taken away. They predicted the enemy would try to intimidate the locals and disrupt Host Nation involvement in the operation by emplacing Improvised Explosive Devices (IEDs) near government buildings and on major routes into and out of the valley. Because friendly forces had disseminated information about their operation and followed up by taking action to protect the population in the valley, there were few infiltration routes left open to the enemy, and these were assigned NAIs and TAIs with a unit responsible for taking action when the enemy was observed.

When the enemy is detected, and kinetic operations destroy the threat, the information is quickly obtained and disseminated by Host Nation officials to the people inside the area of operation. This dissemination serves several purposes: friendly forces are informed of significant activity, the partnering force gains confidence that the threat can be defeated, the villagers feel they are a little more secure, and the threat realizes that the momentum has shifted out of their control. Additionally, severing the enemy's primary means of communicating, with each other and the populace, gains a victory in the tactical fight as well as achieving Information Superiority. The combination of many different aspects of Information Operations such as rapidly disseminating truthful information to the population, MISO, Electronic Warfare, and Counter Intelligence gains greater effects and helps achieve the commander's objectives.

CONCLUSION:

In the scenario, the commander knew he would face a hardened enemy in an area where he had never operated before. The commander assessed that he would have to fight the enemy in order to clear the area and establish initial security. He also knew, however, that he could not hold the valley indefinitely (without the support of the Host Nation and the local population). The commander needed to gain their support and willingness to fight the threat if he was to achieve any long term success. Information

Superiority is about effectively communicating your intentions to your subordinates, the partnered force, Host Nation officials and the local population, while denying the enemy the ability to effectively communicate his message. Information Superiority at the tactical level is a key to winning the COIN fight because it balances the more kinetic side of combat and helps achieve longer term objectives. Information Superiority should be integrated into the planning, preparation, and execution of ***all*** operations.

At the tactical level, the main areas to concentrate upon to obtain Information Superiority include: developing a better understanding of the Threat's Vulnerabilities; creating tactical advantages based on the unit's capabilities to take action; developing a better understanding of the Information Environment; developing detailed plans for mitigating and predicting threat activity; and establishing Measures of Effectiveness that are synchronized to the commander's objectives and information requirements. Lastly, commanders need to establish a climate where information dissemination is seen as critical to success—there must be an offensive mindset to winning the information fight and supporting the population.

Without the proper application of non-lethal and lethal operations, designed to achieve Information Superiority, the chances of gaining and maintaining Information Superiority dwindle. The commander and staff must realize that this critical piece to the COIN fight is not an afterthought to kinetic operations or the responsibility of any one staff officer, but a "finishing force" that achieves the commander's objectives in the COIN fight.

REFERENCES:

[1] Joint Publication No.3-13 (JP 3-13) *Information Operations*, 13 Feb 2006, pg 1-10.

[2] U.S. Army Field Manual No.3-0 (FM 3-0) *Operations*, U.S. Army, 27 Feb 2008, pg 7-1.

ADDITIONAL INFORMATION:

[1] Afghan Key Leader Engagement (KLE) Pocket Reference, GTA 90-01-019, January 2010.

[2] Information Operations into F3EAD Pocket Reference, GTA 90-01-027, December 2010.

TACTICAL INFORMATION SUPERIORITY
ASYMMETRIC WARFARE GROUP

SIPR: http://portal.awg.army.smil.mil/products/default.aspx
NIPR: https://portal.awg.army.mil

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