APRIL 2009

ATTACK THE NETWORK METHODOLOGY: PART 3 NETWORK MODELING AND ISR SYNCHRONIZATION

ASYMMETRIC WARFARE GROUP

OVERVIEW:

This document continues discussion on effective targeting methods (lethal and non-lethal) at the Battalion and Brigade level. It continues dialogue on Attacking the Network by further describing Center of Gravity and Critical Vulnerability analysis themes and their link to network modeling. This document also discusses the use of detailed, Observable Indicators to focus Intelligence Surveillance and Reconnaissance assets against the enemy's vulnerabilities. A modified Intelligence Synchronization Matrix (ISM) ensures integration and synchronization to the friendly course of action in a Counter-Insurgency environment. Using doctrinal and situational templates and a modified ISM helps the S2 understand the insurgent networks operating in his Area of Interest, focus assets against the known or suspected Critical Vulnerabilities, and synchronize ISR to give the commander the information he needs at the Decision Points.

BACKGROUND:

Part I of the Attack the Network Methodology series discussed the significance of understanding an ideologically motivated insurgent leader's approach to influencing the Center of Gravity (COG). The major point discussed within the first paper was the need for commanders and staffs at Brigade Combat Team (BCT) and below to understand the significance of targeting Tier II personalities, or "Intermediaries." Tier III targeting may result in immediate impacts to security, but are typically not long term gains. Tier II targeting severs the link between the ideologically motivated Tier I leadership and the Tier III cell members and develops longer term effects. Part II of the Attack the Network Methodology series focused on personality targeting as one of the keys to attacking an insurgent network. Units need to analyze the enemy's Critical Capabilities, Critical Requirements, and Critical Vulnerabilities. Analysts then identify HVIs and the associated tasks they perform in order to have a significant impact on the enemy. We need to attack the threat's weaknesses and contain its strengths. The final discussion focuses attention on "how" to identify the targets we determine are a higher priority for attack.

We can easily convince ourselves that detailed analysis of threats is not required because the situation is too fluid. Several published articles focusing on the strategic issues of intelligence and analysis in the Counter-Insurgency (COIN) environment have argued that we must be adaptive, that we must completely re-think our analytical processes. In some ways, they are correct; we have to continually adjust to new threat Tactics, Techniques and Procedures. More importantly, however, is the reality that analysis in a tactical COIN environment must be extremely detailed. After all, what is harder to find, a Motorized Rifle Regiment or a High Value Individual (HVI)?

When a commander uses an indirect approach to attacking a threat in his battle space he will have the intelligence staff, with assistance from other staff elements, identify those areas within the insurgency network that are most vulnerable. Once those Critical Vulnerabilities are identified, the

Modifying doctrinally sound processes for application in a COIN environment can work to successfully target and destroy enemy networks.

intelligence staff should start working diligently to find out who are the threat personalities within the network. That is a major challenge in the COIN fight. Imagine an S2 coming into theater for the first time, taking over a new area and understanding what needs to be done, but not knowing where to start. In the traditional Military Decision Making Process (MDMP), the S2 would start Intelligence Preparation of the Battlefield (IPB) by defining the battlefield environment, describing battlefield effects, evaluating the threat, and determining the threat Courses of Action (COA).[1] An intelligence officer would list out the threat's organization, capabilities, battle formations in a doctrinal template, and then plot known and suspected positions on a situational template based on reporting and sound tactical reasoning. He would then determine possible COAs based on the threat's COG, objective/intent, and capabilities and vulnerabilities. Why should that be any different in a COIN environment?

Using doctrinal and situational templates, as well as a modified Intelligence Synchronization Matrix (ISM) the S2 can better understand the insurgent networks operating in his Area of Interest, focus ISR assets against the known or suspected Critical Vulnerabilities, and synchronize ISR to give the commander the information he needs at the Decision Points.

NETWORK MODELS

The process starts by identifying the Critical Capabilities, Critical Requirements, and Critical Vulnerabilities of the threat within the battle space (the second paper in this series covers this topic in detail). Once the Critical Capability or Threat Network in the area is identified we must consider all of the actions that take place for the network to be successful. For example, if the Critical Capability is to provide logistics then there are several Critical Requirements that must be identified. We can use a simple wire diagram to describe the link between each of the Critical Requirements; this is a type of doctrinal template.

In the following example, a commander wants to neutralize the threat's ability to detonate Improvised Explosive Devices (IEDs) in his battle space. The staff knows the components are coming from a nearby country. They also know that caches are often used and the components must be brought to a centralized location for an expert to make the bomb. The intelligence staff begins work by describing each of the Critical Requirements associated with the threat operation. They can wargame the threat's actions from the point of detonation, and work backwards in time, or they can start with the initial action. In the example, the staff chose to start from the beginning. Each of the Critical Requirements was labeled with a "letter". The staff determined the following Critical Requirements had to occur for there to be a successful detonation: smuggle IED materials across an international border, distribute materials, cache materials, assemble materials into an effective IED, conduct reconnaissance, emplace IED, and detonate IED. Other requirements were added as the staff began to understand the tasks associated with the insurgent movement of lethal aid and bomb-making (see Figure 1).

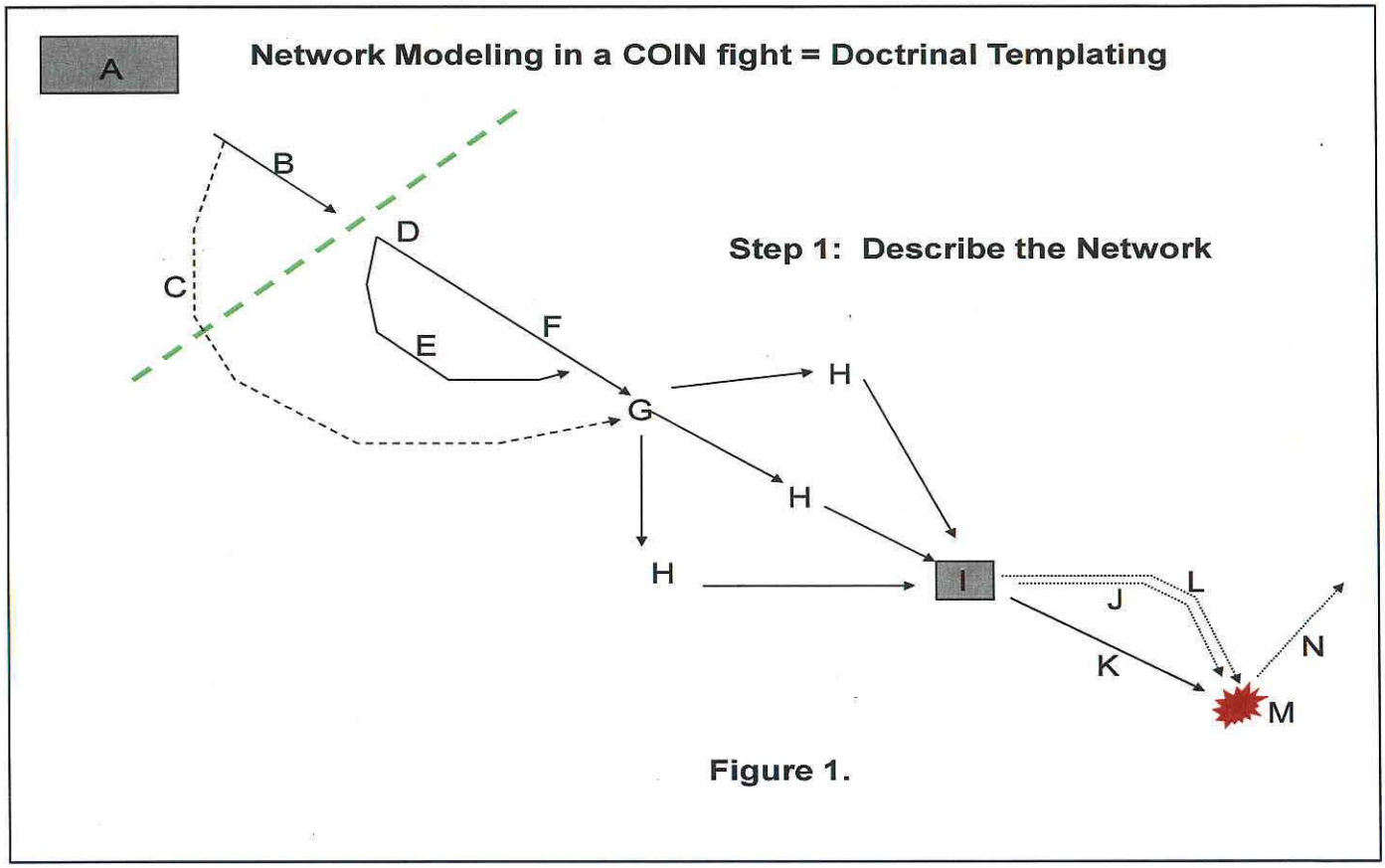

Figure 1.

A. IED Components are completely or partially constructed at a factory or warehouse in another country.

B. Materials are transported to an official international border crossing point OR…

C. Materials are transported across the porous border region using a smuggling route.

D. Materials pass the scrutiny of a border police officer.

E. Materials possibly undergo additional scrutiny in a secondary search area at the border point.

F. Materials are moved to a distribution point.

G. Materials are trans-loaded onto smaller, more maneuverable vehicles and moved to cache points/safe houses or directly to a bomb maker.

H. Materials are cached for future use.

I. Materials are drawn from a cache point and moved to an assembly point for use against Coalition Forces.

J. Insurgents conduct surveillance of the probable IED emplacement point.

K. IED is emplaced.

L. Trigger man moves into position.

M. IED detonated.

N. Trigger man leaves the scene, conducts Battle Damage Assessment, and reports information to his commander. This will likely also include turning over video recordings to be used as part of a media message and for Battle Damage Assessment.

This first step, Describe the Network, helps the staff understand the framework for insurgent activity surrounding the IED movement, but it does not provide the detail required to understand what the threat's vulnerabilities are or where the Brigade's assets should be focused. Further analysis is required.

The second step is a detailed analysis of each Critical Requirement. In theory, this would include listing each individual task associated with each requirement. However, this is unrealistic in a time constrained environment, and analysis should focus on potential Observable Indicators (see Figure 2). Observable Indicators are those things that could potentially be detected by friendly ISR assets.

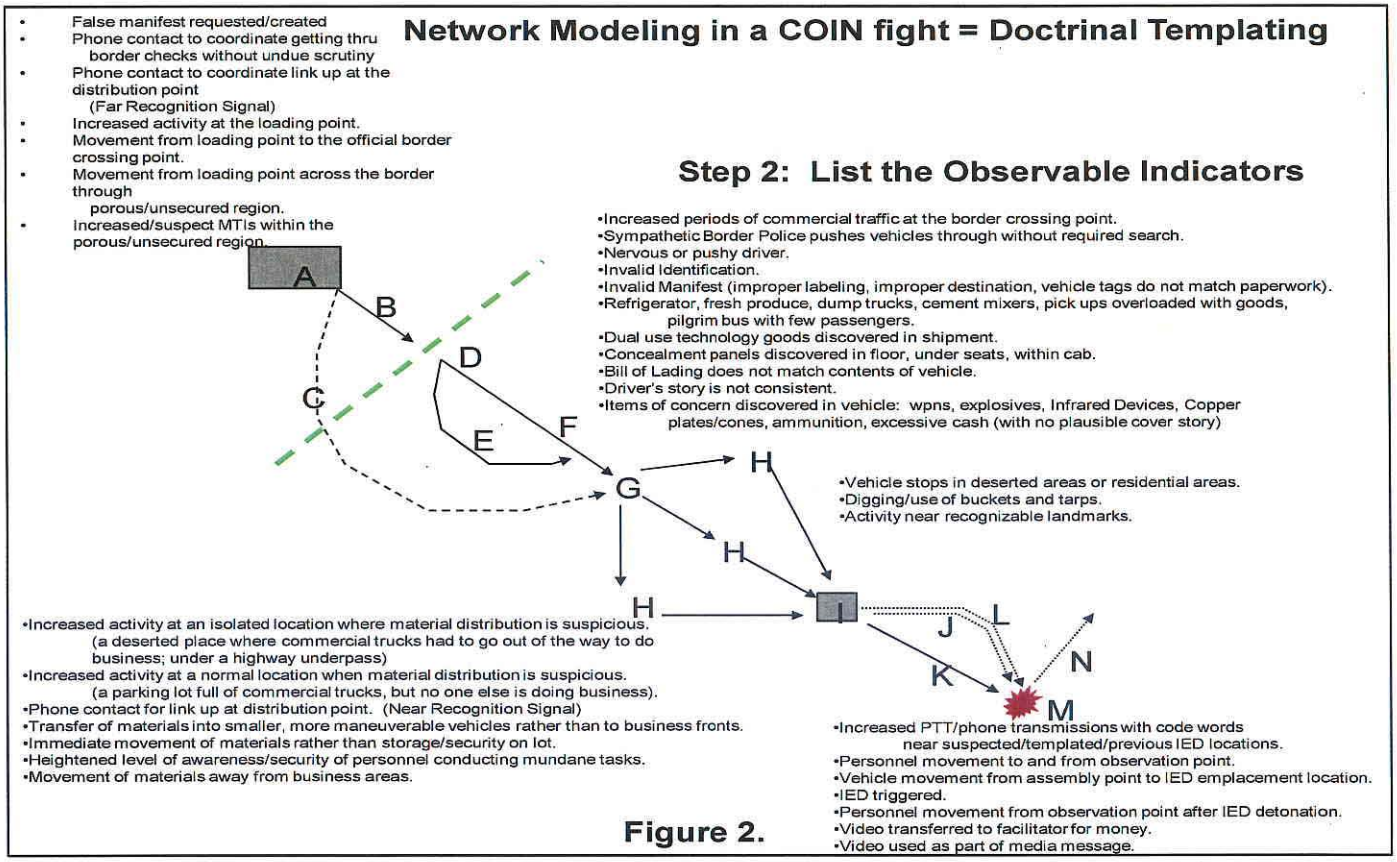

Figure 2.

It can help to list the Observable Indicators separately for each ISR asset manager to review and determine what could be detected (based on their asset's capabilities). The Observable Indicators in Figure 2 are:

1. False manifest requested/created.
2. Phone contact to coordinate getting thru border checks without undue scrutiny.
3. Phone contact to coordinate link up at the distribution point (Far Recognition Signal).
4. Increased activity at the loading point.
5. Movement from loading point to the official border crossing point.
6. Movement from loading point across the border through porous/unsecured region.
7. Increased/suspect MTIs within the porous/unsecured region.
8. Increased periods of commercial traffic at the border crossing point.
9. Sympathetic Border Police pushes vehicles through without required search.

10. Nervous or pushy driver.
11. Invalid Identification.
12. Invalid Manifest (improper labeling, improper destination, vehicle tags do not match paperwork).
13. Refrigerator, fresh produce, dump trucks, cement mixers, pickup trucks overloaded with goods, pilgrim bus with few passengers.
14. Dual-use technology items discovered in shipment.
15. Concealment panels discovered in floor, under seats, within cab.
16. Bill of Lading does not match contents of vehicle.
17. Driver's story is not consistent.
18. Items of concern discovered in vehicle: weapons, explosives, Infrared Devices, Copper plates/cones, ammunition, excessive cash (with no plausible cover story).
19. Increased activity at an isolated location where material distribution is suspicious (a deserted place where commercial trucks had to go out of the way to do business; under a highway underpass).
20. Increased activity at a normal location when material distribution is suspicious (a parking lot full of commercial trucks, but no one else is doing business).
21. Phone contact for link up at distribution point (Near Recognition Signal).
22. Transfer of materials into smaller, more maneuverable vehicles rather than to business fronts.
23. Immediate movement of materials rather than storage/security on lot.
24. Heightened level of awareness/security of personnel conducting mundane tasks.
25. Movement of materials away from business areas.
26. Vehicle stops in deserted area or residential area.
27. Digging/use of buckets and tarps.
28. Activity near recognizable landmarks.
29. Increased PTT/phone transmissions with code words near suspected/template/previous IED locations.
30. Personnel movement to and from observation point.
31. Vehicle movement from assembly point to IED emplacement location.
32. IED triggered.
33. Personnel movement from observation point after IED detonation.
34. Video transferred to the facilitator in return for payment for conducting the attack.
35. Video is posted on the internet/and or DVDs are created.

Another way for analysts to understand the COIN doctrinal template's significance is to reduce the clutter and use a number system, in conjunction with the lettering system described in Figure 1. The Observable Indicators are represented numerically and placed next to the most likely Critical Requirement. For example, at Critical Requirement G, "Materials are trans-loaded onto smaller, more maneuverable vehicles and moved to cache points/safe houses or directly to a bomb

maker", indicators 19 through 24 were associated with that activity and placed on the doctrinal template next to "G". This is a highly detailed analysis but it helps to determine the most important point of the discussion: what are the threat's Critical Vulnerabilities? Are they the places on the ground where insurgents can be killed or captured? Is it where we can influence him the most with our lethal and non-lethal methods? Is it where our ISR assets have the best possibility of detecting their activity?

For the sake of this example, and to drive home the point on ISR synchronization issues we will say **the threat's key Critical Vulnerabilities are those locations where friendly ISR assets can detect threat activity or personalities. Combining analysis of Critical Requirements, Observable Indicators, and Critical Vulnerabilities is the basis for a solid collection plan in the COIN fight** (See Figure 3).

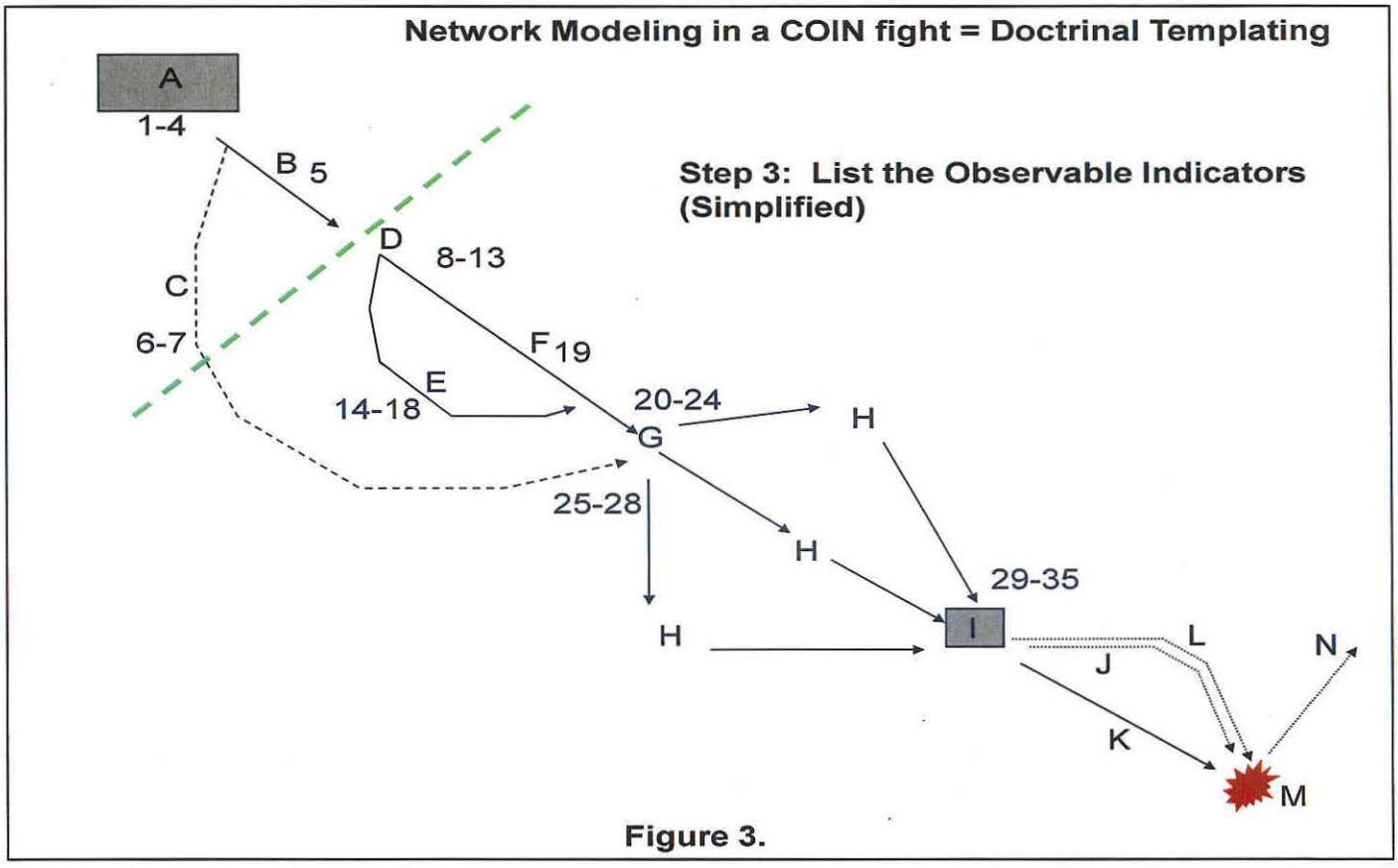

Figure 3.

The staff determined there were two primary locations where HVIs associated with the network would be most vulnerable to identification and attack: at the distribution point and the bomb maker's safe house (points G and I in Figure 3). Initial Named Areas of Interest (NAIs) were placed over locations G and I on the doctrinal template to focus ISR assets. Once enough information was gathered to confirm threat activity was taking place within the NAI the staff refined the location to a TAI and added additional NAIs to serve as triggers. On the doctrinal template, these new NAIs have to identify the location of the target before the commander has to make a decision. Placing these on a doctrinal template helps analysts understand the relationship of when ISR has to "see" the Observable Indicators and when the command has to make a decision to initiate a strike (see Figure 4). Though the figure indicates a relationship between ISR coverage and decision points based on distance it is just as important to realize the significance of time; there may not be an additional NAI forward of the Distribution Point or Safe House. If ISR coverage is sufficient at the Critical Vulnerability to provide triggers for the commander then there may not be a need for other NAIs.

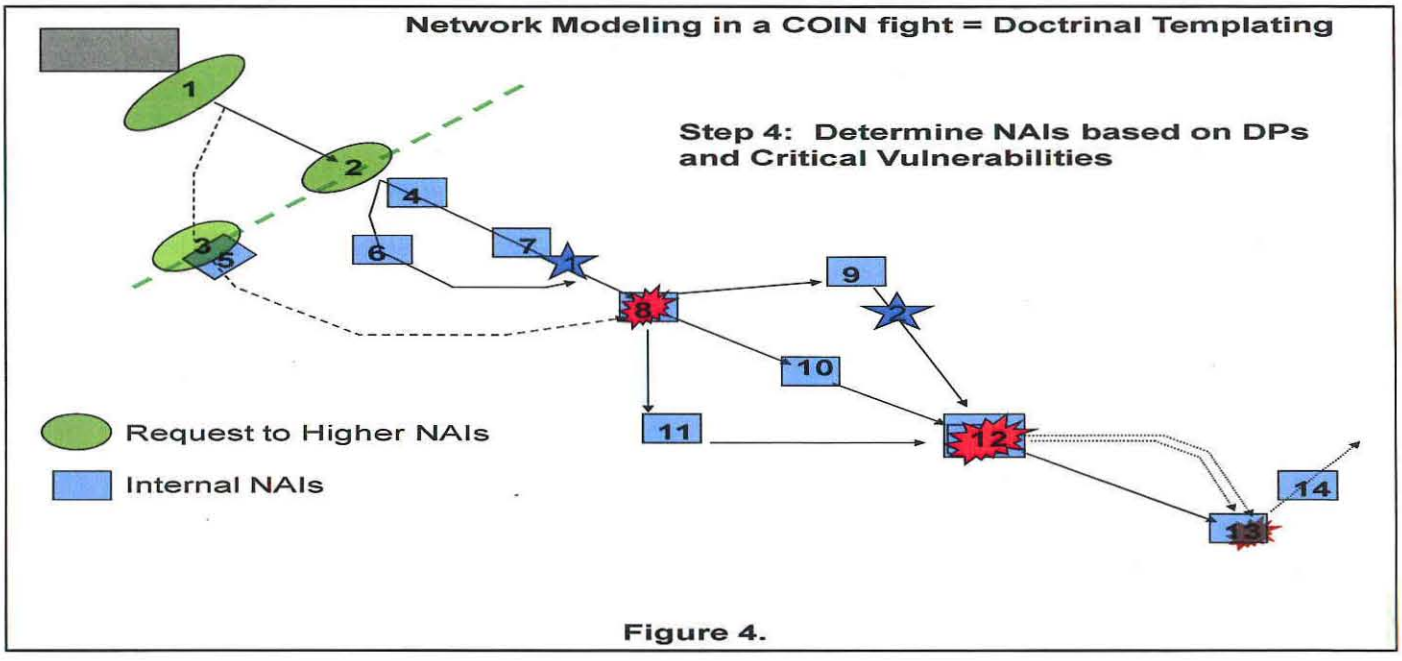

Figure 4.

A final process to assist in ISR integration is to combine the Observable Indicators template and Asset Manager input to develop an initial ISR plan. Not every Observable Indicator can or will be detected by the BCT's internal ISR assets. Combining the two assessments helps determine the best place to apply higher's assets since these platforms can be scarce commodities the BCT gets for only short periods of time. Intelligence Officers need to determine how to incorporate those external assets to best compliment the ISR Plan based, again, on Observable Indicators at the Critical Vulnerability locations. Other assessments should be incorporated to further refine and narrow the potential list of NAIs. The doctrinal and situational templates, observable indicators list, Imagery analysis, and Human Intelligence and Signals Intelligence reporting all help refine the Common Operating Picture. Combining all of these into one picture narrows the potential Critical Vulnerabilities down to those areas and/or persons the BCT has the best chance of detecting. In essence, we are **matching our ISR strengths to the threat's weaknesses and increasing our chances of identifying HVIs** (See Figure 5).

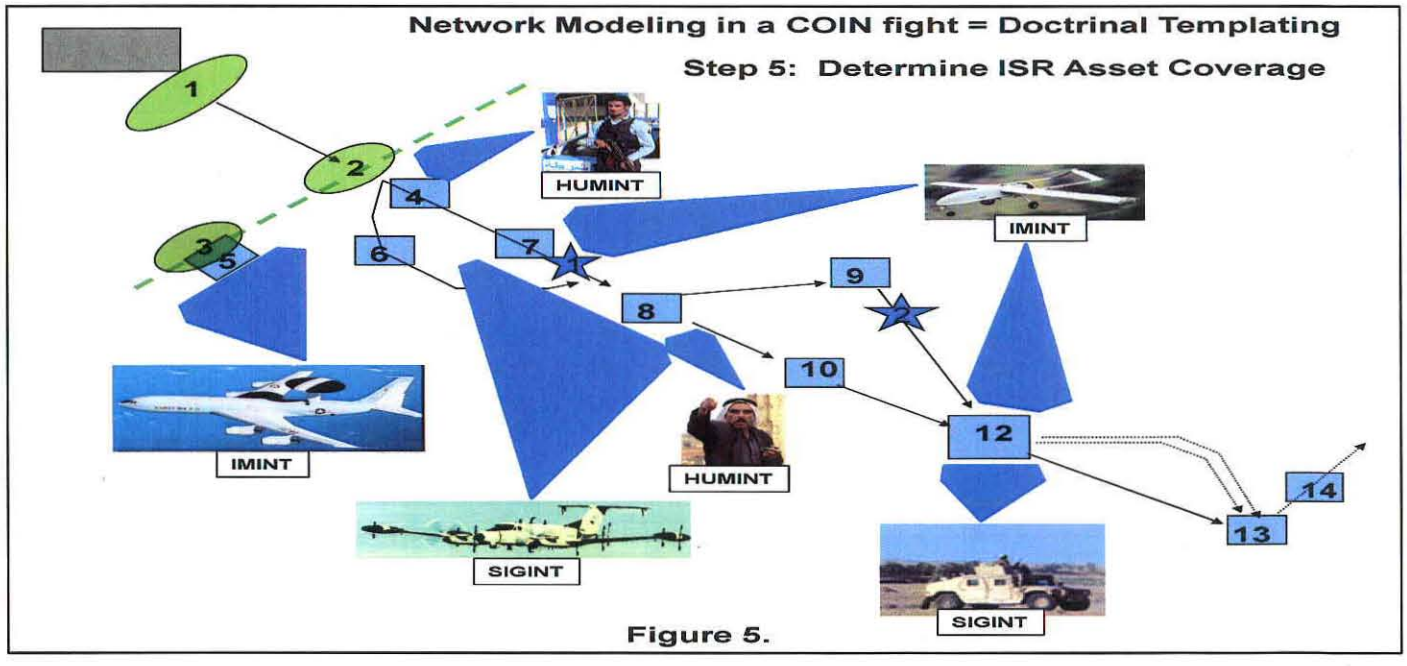

Figure 5.

This diagram depicts a general method for developing ISR coverage to detect indicators associated with insurgent movement of lethal aid and bomb-making. The S2 must ensure internal and available external ISR assets (HUMINT, SIGINT, and IMINT) are integrated and synchronized to the maneuver plan. For example, if the BCT's key task is to neutralize insurgent resupply activities within the Operational Environment, internal and external ISR assets must be aligned against the things they can detect at the right place and time to answer the Priority Intelligence Requirements.

Intelligence must give the Commander the information he needs to make a decision at the critical point in the battle whether in a COIN or Major Combat Operation environment.

In an IED resupply operation, what are the critical interdiction points? Where can the BCT take action against the enemy (at the border crossing, distribution point, cache point, safe house, bomb factory, or possibly the emplacement point)? In the example above, the commander determined he wanted to interdict threat activity by capturing associated Tier II HVIs at the Distribution Point (NAI 8) and the Safe House (NAI 12). Higher echelon ISR was requested to perform Early Warning and hand-off to BCT internal assets. If those assets were to be on station longer than needed then they can also be "stacked" against NAI 8 and NAI 12 to provide greater targeting fidelity. Internal assets were assigned the task of detecting the Observable Indicators at NAI 8 and NAI 12 (early enough for the commander and rest of the staff to take action). Assets were also tasked to continue collection until a decision was made on how to neutralize the enemy (via lethal or non-lethal means). **Multiple ISR platforms used against one target set significantly increase the chances of detecting HVIs and setting conditions for success.**

COLLECTION MANAGEMENT AND THE INTELLIGENCE SYNCHRONIZATION MATRIX (ISM)

It is not enough that all available ISR assets are integrated in the COIN fight; they must be synchronized to the friendly scheme of maneuver. In FM 34-2, Collection Management, it is the Collection Manager's (CM) responsibility to use assets in a way that ensures we satisfy Information Requirements (IR). According to FM 34-2, the CM is the key to intelligence synchronization. During the war gaming effort, the CM looks at each potential course of action (COA) and determines how to satisfy the IR with the available assets, focused on detecting the threat's indicators at the critical NAIs. With a blank ISM available during targeting meetings, the CM can track each asset's task and purpose, assigned NAI, and collection timeline.[2]

An ISM is compromised of the following required data:

- Time.
- Decision Points.
- Assets.
- NAIs assigned coverage.
- Cueing Requirements.
- Latest time information is of value (LTIOV) (See Figure 6).

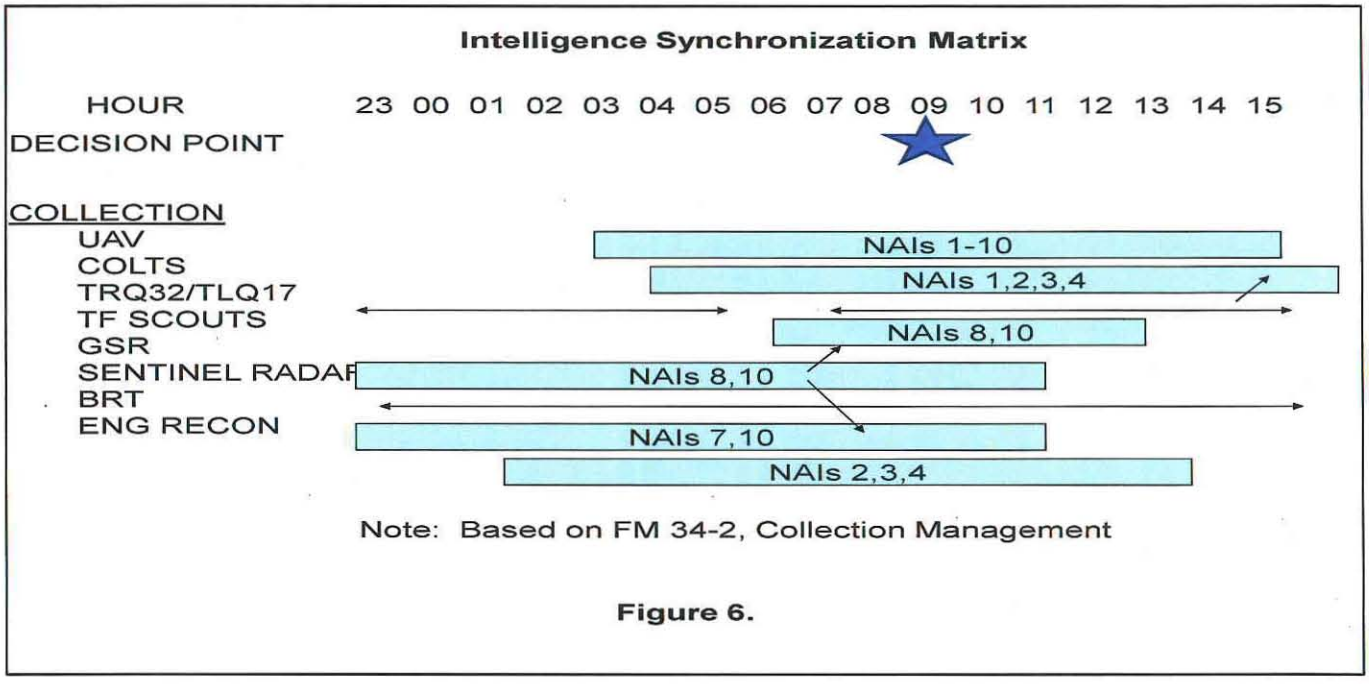

Figure 6.

Putting the brigade commander's Decision Points (DPs) on the matrix drives the development of Specific Information Requirements (SIR). By looking down the chart at the anticipated time for making a decision, the CM is able to verify that each asset is attempting to answer an SIR tied to the commander's DP. In the COIN fight, the commander's DPs are usually not tied to terrain, but to a threat Critical Capability and the indicators reflecting that activity. The ISM is a simple tool that ensures overall synchronization; however, it does not include the fidelity necessary to ensure ISR assets detect Observable Indicators, focus analytical efforts, or provide triggers for the actions of friendly forces. This is especially critical in a COIN environment where the dwell time of an asset or the window for detecting an indicator is extremely limited. The doctrinal ISM template often integrates and synchronizes ISR assets over a period of days. The modified ISM used in a COIN environment is adapted to integrate and synchronize ISR assets over a 24 hour period, providing the greater degree of fidelity necessary for Time Sensitive Targeting (TST).

MODIFIED ISM

The following information should be included in a modified ISM to achieve the required targeting fidelity in a Counter-Insurgency fight:

- BCT scheme of maneuver; this could include rows for each subordinate maneuver element. In the example, highlighted blocks were also added to indicate the Critical Vulnerabilities that we want to detect and attack.
- Commander's DPs.
- Situational Template/Threat Indicators focused on the network to be attacked.
- Focus of fires (including Air Weapons Teams (AWT).
- Asset location and assigned NAI(s).
- Collection focus for each intelligence discipline.

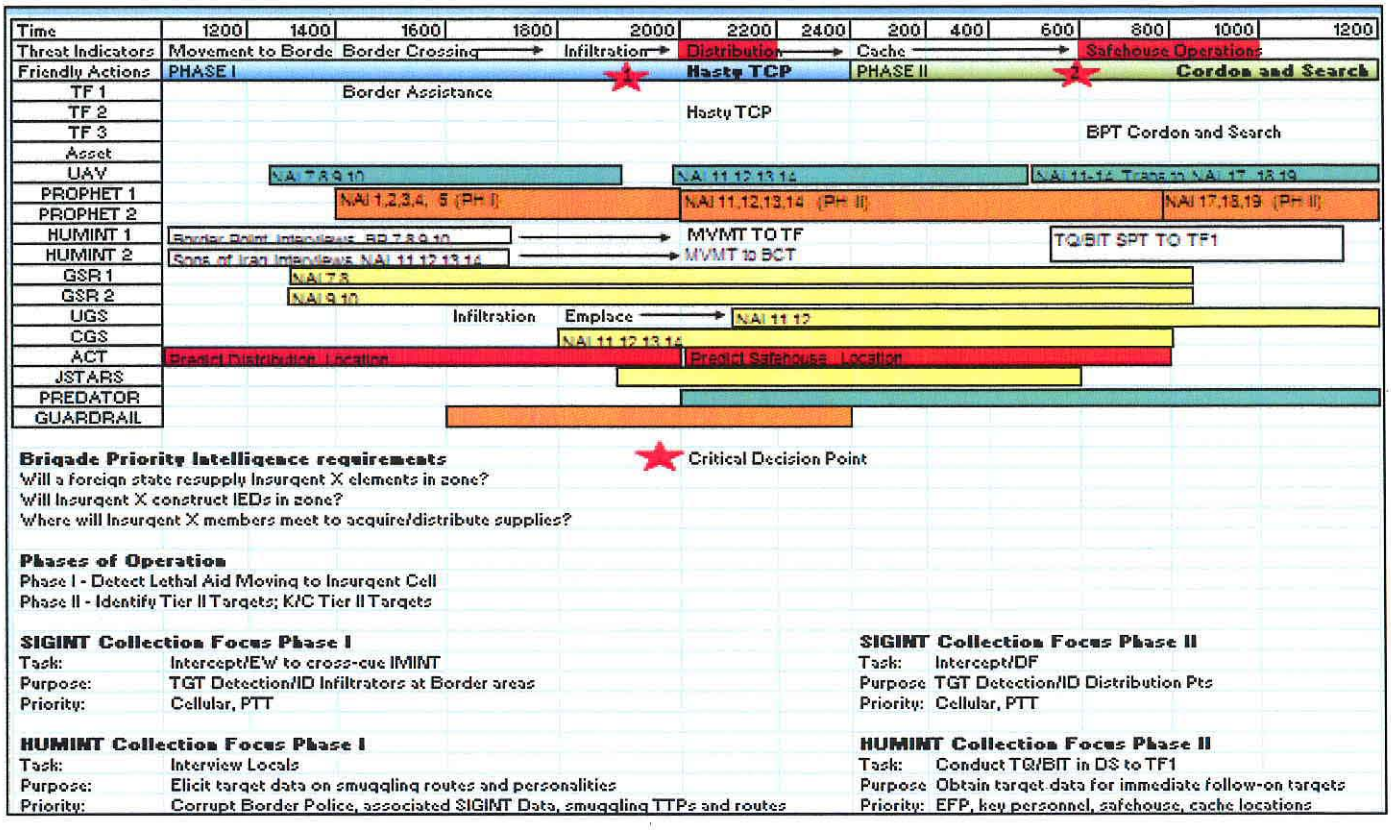

Figure 7.

Your imagination is the only limitation to the data that you put into the modified ISM to make it an efficient tool for your staff. The objective of developing a modified ISM is to ensure the staff provides answers to the Commander prior to him having to make a decision. The modified ISM also ensures proper allocation of ISR to provide sufficient targeting fidelity ("stacking" ISR against the Critical Vulnerability). The tool captures the staff's work to ensure massing of ISR assets against the correct NAI at the expected time of activity. It also provides guidance on the priority for each asset and which Observable Indicators the assets should report (See Figure 7 for an example of a 24 hour modified ISM). **The increased fidelity of data reflected within the modified ISM is critical to the complex and time sensitive task of targeting networks in a counter-insurgency.**

Using Figure 7 as an example, you can see each significant activity within the BCT scheme of maneuver; you should also be able to verify the focus of collection assets in support to the brigade. Phases of the Operation were used to delineate between the Find and Fix/Finish actions against the target. These phases were further used to indicate collection support and focus for SIGINT and HUMINT; the same level of fidelity should be done for all assets including the analytical section. This should assist units in focusing analysts on answering the IR in a timely manner. When the **staff** (not the S2 by himself) creates the modified ISM document during the targeting meeting, they have already developed the majority of the ISR scheme of support. The Commander's intent to neutralize the threat's ability to detonate IEDs in his battle space through analysis of the enemy's Critical Vulnerabilities, Observable Indicators, and ISR synchronization is, now, closer to being realized.

The usefulness of the modified ISM is not just in its ability to synchronize assets during the planning process; the modified ISM is also useful during the execution of intelligence operations. Asset managers, the S2, the BCT/BN Battle Captain, and Company Intelligence Support Teams (CoIST) should each have a copy of the modified ISM to verify that platforms and Soldiers are accomplishing their major tasks and purpose towards Attacking the Network. Analysts should also have a copy of the modified ISM to ensure their analysis is predictive rather than just reporting the

current enemy situation.

Subordinate elements like the CoIST and TST force use the modified ISM to link their combat operation SIR and ISR assets to the overall BCT plan; the matrix facilitates plans at all levels and ensures synchronization of both maneuver forces and intelligence assets. Finally, the modified ISM should be a major tool used during daily targeting meetings to ensure assets are synchronized to the identified network targets. The modified ISM also allows the brigade commander to see how his ISR assets are working to provide him with the information he needs to make the right decision at the right time. The main difference between the standard ISM and a modified version is the amount of detailed data included to ensure synchronization between collection assets, analytical effort, and operational elements.

CONCLUSION

In Attack the Network – Part I, the Oil Spot model was modified to discuss insurgent ideology for influencing the Center of Gravity and developing various threat networks. The analysis helped illustrate that Tier II insurgent targets (Intermediaries) are worth more targeting effort at the BCT level than Tier III targets (cell members). In Attack the Network – Part II, employing Center of Gravity analysis to determine Critical Capabilities, Critical Requirements, and Critical Vulnerabilities showed that our ISR assets and targeting strategy need to be prioritized towards the enemy's weaknesses and NOT his strengths. A key aspect of attacking a network is personality targeting; there needs to be analysis of both HVIs and the associated tasks performed to accomplish Critical Capabilities in order to determine which individuals have a significant impact on enemy operations. In this final paper, the value of network modeling (application of doctrinal templating in the COIN environment) was demonstrated using current threat methods for moving lethal aid into the battle space. It is not enough to ensure integration of ISR assets in the COIN fight; **ISR Synchronization**, where multiple platforms are used against one target set, is needed to set conditions for success. Just as important, the intelligence staff and CoIST analysts have to conduct detailed analysis to determine Observable Indicators for each asset and patrol element, as well as prioritize the analyst's priority of analysis.

Obviously, the real ISR struggle to detect Critical Vulnerabilities does not happen as easily as depicted in the examples highlighted in this series. The network modeling examples have to be used in conjunction with Significant Activity overlays. Known locations are plotted and suspect locations are templated on to the ISR overlay. NAIs are then placed over likely suspect locations to identify the Observable Indicators. This does not occur in a 24 hour period or in five easy steps (as depicted). It can take weeks or longer to identify the right Critical Vulnerabilities. The true impact of this concept is that no matter how inaccurate a staff's initial assessment of the network might have been, it will be continually updated and the ISR plan modified through the targeting process. The commander's PIR will be answered and precision targeting of HVIs will increase. It is also important to understand the relationship of planned ISR coverage to dynamic re-tasking in order to accomplish missions in an evolving and ever changing operational environment. A solid ISR plan cannot be so rigid that it is not adaptive to the fluid nature of the threat or the battlefield.

AWG SIPR website: http://hqinscom.portal.inscom.army.smil.mil/aawo/awg/default.aspx

REFERENCES:

[1]Field Manual 34-130, Intelligence Preparation of the Battlefield (Washington DC: Headquarters, Department of the Army; 8 July 1994), page 1-2.

[2]Tod A. Langley, Modified Intelligence Synchronization Matrix – A Technique for Brigade Combat Team Operations (Military Intelligence Professional Bulletin: Fort Huachuca, AZ; 1 JAN 2003), pages 1-3.

ATTACK THE NETWORK METHODOLOGY: PART 3
NETWORK MODELING AND ISR SYNCHRONIZATION

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