U.S. TRADOC G2 Intelligence Support Activity

Red Diamond

Complex Operational Environment and Threat Integration Directorate

Fort Leavenworth, Kansas Volume 3, Issue 9 SEP 2012

INSIDE THIS ISSUE

Red Diamond is produced monthly by the Complex Operational Environment and Threat Integration Directorate of the TRADOC G2 Intelligence Support Activity (TRISA). Send suggestions and feedback to Ms. Penny Mellies (penny.l.mellies.civ@mail.mil).

INSIDER THREAT HANDBOOK UPDATE

By H. David Pendleton, OEA Team

In late September 2012 TRISA published an updated version of its Insider Threat Handbook to reflect the numerous attacks against International Security Assistance Force (ISAF) Soldiers by Afghan National Security Force (ANSF) personnel in July and August 2012. The Handbook provides the latest information on "green-on-blue" attacks, analyzes the events for trends, and summarizes the inside attackers' tactics, techniques, and procedures (TTP). The Handbook also provides an annex with a summary of the 64 green-on-blue attacks from May 2007 to August 2012 available from open sources with the details of the attack; the type of attack, if known; and the results of the attack.

There are four types of insider attacks: co-option, infiltration, impersonation, and personal grievance. Co-option occurs when the insurgents pressure an already serving ANSF member to conduct an attack against ISAF by threatening the individual, his family, or through some sort of enticement such as money. Infiltration occurs when an insurgent purposely enlists in the Afghan National Police (ANP) or Afghan National Army (ANA) to conduct an attack. Impersonation occurs when an insurgent obtains an ANSF uniform and uses the disguise to get close enough to ISAF members to conduct an attack. Personal grievance is when a dispute between the ANSF member and an ISAF member precipitates the actual attack.

An analysis of the data from the 64 attacks provides some important trends. Over one-third (24/64) occurred in only two provinces—Kandahar and Helmand. Insider attacks doubled from 2010 to 2011 and have already doubled again in 2012 despite four months remaining in the year. While the majority of all attacks since 2007 have been against U.S. Soldiers, there was a drop in the percentage of attacks against Americans between mid-2011 and mid-2012. In July 2012, however, the attacks against U.S. Soldiers again rose while attacks against non-Americans dropped.

More attacks occurred in July and August each year while the fewest attacks occurred in June and September. The rise in the hottest months of the year could have been attributed to Ramadan when the increased fasting times may have increased irritability in ANSF members, which could have escalated an argument into a personal grievance attack. After the elimination of all insider attacks where the cause could not be realistically determined, 26 of the 29 remaining cases, or 89%, fell into the personal grievance category.

The Insider Threat Handbook Update provides additional details about trends and a concise but informative recap of each of the 64 attacks. Access to the Insider Threat Handbook Update is available through AKO.

THE M21 (M25/M14SEI/M21A5) SNIPER/DESIGNATED SQUAD MARKSMAN RIFLE

By Mike Spight, Training-Education-Leader Development

In an article appearing the in February issue of the Red Diamond, we featured the Dragunov SVD, which is the old Soviet, now Russian Army's equivalent of the M21 rifle. In this article, for the sake of comparison of these two venerable weapons, we'll focus on the M21, which was based on the U.S. Army's battle rifle of the late 1950s and early 1960s, the M14. Note that unlike the Dragunov SVD, which was designed and purpose built as a sniper rifle, the M21 system is a modification of a battle rifle that was never intended for that purpose, much like previous U.S. Army sniper rifles, the M1903-A4 (based on the 1903 Springfield) and the M1-C and M1-D (based on the M1 Garand).

Vietnam-Era M21 with Leatherwood ART Scope

Originally adopted by the U.S. Army in 1957, the M14 was the replacement for the M1 Garand, which had served as the main battle rifle for the U.S. Army and U.S. Marine Corps since WW2. But unlike the Garand, the M14 was chambered in 7.62x51mm, the standard battle rifle caliber adapted by all NATO nations for both rifles and light machine guns.

This changed in the early 60s when the U.S. was engaged in a counterinsurgency fight in the Republic of South Vietnam. There, the M14's shortcomings as a battle rifle became readily apparent. Heavy, oversized, and the fact that Soldiers and Marines were limited by the amount of ammunition they could carry in their Basic Load, all led to the eventual adoption of the M16 Assault Rifle as this nation's Tier 1 individual rifleman's weapon.

By the mid 1960s in South East Asia, the only modern, type-classified sniper rifle in use was the M40 (an arsenal and USMC armorer modified Remington M700 bolt action rifle) chambered in 7.62x51 NATO and used by the Corp's Scout/Snipers. Due to demand within the Army for a modern sniper rifle, a decision was made to take approximately 1,400 of the M14 National Match Grade weapons held in depots and armories at unit level, and convert them into sniper rifles which, with optics, could meet the accuracy demands of that profession. Initial offerings were dubbed the XM21 system, and were provided to snipers in South Vietnam in 1969. The XM21 featured a walnut stock, which was later replaced by a fiberglass stock that was much more resilient to the rainy, damp weather of South Vietnam, and less prone to losing zero due to swelling and contracting. The Rock Island Arsenal modified the 1400 selected M14 NM rifles by installing a specially tuned, 4.5 pound two-stage military trigger, and mounting a Leatherwood 3x-9x Variable Adjustable Ranging Telescopic (ART) sight. These rifles were initially fielded in South Vietnam in 1969 and some were also supplied with a Sionics suppressor. The rifle was eventually type classified as the M21 in 1975, and remained the U.S. Army's issue sniper system until adoption of the M24 SWS in 1988 (another specially built Remington 700 bolt gun). When combined with the newly developed M-118 (173gr Full Metal Jacket Boat Tail) match ammo in the mid 1960s, the M21 proved to be a deadly and capable weapon in the hands of the right Soldier, particularly since the Leatherwood ART scope was engineered to provide excellent performance with a rifle firing M-118 ammunition. This system was capable of relatively consistent, 500-750 yard accuracy.

M25 Sniper Rifle

As noted, the M21 was the U.S. Army issue sniper rifle until adoption of the M24 SWS in 1988. At that time, the M21s were returned for depot storage at installations around the U.S., or a few remained in the arms rooms of some Special Operations units. At about that same time, United States Special Operations Command (USSOCOM) indicated that they wanted to continue to use the M21 system for particular mission profiles (Army SF and Navy SEALs), but sought to improve the weapon. As a result of this program, the M25 system was developed, and was used extensively by both Army and Navy SOF during the 1st Gulf War. The M25 is essentially an improved M21 system featuring the following: rather than the GI fiberglass stock, the M25 is glass bedded in a McMillan polymer/glass stock; an improved gas piston system; improved scope mount and a new scope. Typically, the M25 came with a Bausch & Lomb 10x fixed power scope, but others were equipped with Leupold variable power scopes, and of course, all of them had a specially tuned 4.5 pound two-stage trigger installed. Also, the more modern Ops Inc. suppressor replaced the Sionics unit on these rifles. The M25 continued to serve both Army and Naval SOF as superbly performing semi-automatic sniper system during the 90s (SFC Randy Shugart, 1st SFOD-Delta, carried one in Mogadishu, Somalia) and the system has been used in both Iraq and Afghanistan even as the new SR25 (NAVSOC) M110 (USASOC) Semi Auto Sniper System (manufactured by Knight's Armament) was brought into service by USSOCOM.

For general purpose forces, the Global War on Terror revealed that although the U.S. Army did have many capable snipers fielding the M24 SWS, there were not enough of these Soldiers available to support the overall needs of a typical Infantry unit engaged in a counterinsurgency fight, particularly in urban areas. As a result the Designated Squad Marksman (DSM) or Squad Designated Marksman (SDM) program was developed by the Army. Soldiers identified by their chain of commands as superior riflemen were given advanced marksmanship training, and although this training was not up to the standards of the Army Sniper School, and did not result in the award of an Additional Skill Identifier, it did provide greater capability to either proactively engage or react to enemy direct fires at the squad/platoon level. Although initially equipped with scope (commonly a Trijicon ACOG of some type) sighted M16 rifles or M4 carbines, the typical engagement ranges encountered in rural areas of Iraq and particularly in Afghanistan, indicated the need for a more powerful rifle with the ability to make the hit at ranges typically greater than achievable by a DSM with a 5.56x45mm rifle or carbine.

This problem led directly to what is probably the final, most technically advanced and accurate model of the M21/25 family: the Smith Enterprises, Inc. (SEI) M21A5 aka M14SEI.

Specifically, in the spring of 2004, a Brigade Combat Team (BCT) of the 2nd Infantry Division was preparing to deploy from home station to Iraq. The BCT "owned" 110 NM M14s and M21 systems, but they were in very bad condition. Additionally, they needed new optics and mounting systems. Becoming aware of the work SEI had been doing on an improved M14NM/M21based sniper

M25A5/M14 SEI

system, the BCT was able to sole source a contract with SEI who then received the 110 rifles and began the conversion process. The rebuild process consisted of the following: detailed disassembly and inspection of all parts that would be reutilized; gas cylinder rebuilt and heat treated; operating rods refurbished; trigger groups rebuilt and set for 4.5 lbs; receivers inspected for cracks and damage; cryogenic treatment of receivers, bolts, and barrels; upgraded gas piston; laser aligned barrel installation; modern springs and pins throughout; magnesium phosphate black refinished; function checked and zero live fire certification at 100 meters; supplied with SEI M14DC suppressor and a modified gas lock front sight for mounting; SEI Vortex flash hider installed; heavy duty (tool steel) scope mounting rings; SEI proprietary scope mount; an extended bolt stop; a 22" medium-heavy profile 4140 chrome-moly steel barrel; Leupold Mark 4 3.5-10x40 variable power scope with illuminated reticle. Note that if in good condition, the SEI build utilizes the following on the supplied rifles:

receiver, bolt, operating rod, trigger assembly, metal furniture, rear sight assembly, fiberglass stock, and forearm.

The SEI variant is also chambered for and rifled at a 1:10 rate of twist in order to provide maximum accuracy with the standard 7.62x51mm sniper load in use by Army, Navy, and Marine snipers: M118 LR, which is loaded with the Sierra Match King 175gr boat tail bullet. With this loading or M852 (165gr Sierra Match King boat tail bullet), the M14SEI is capable of sub minute of angle (MOA) shot groups at 100 yards—groups that measure less than 1" in total size. This is an exceptional degree of accuracy from a semi-automatic sniper/SDM system, and far surpasses the accuracy capability of the Dragunov SVD (approximately 2 MOA at 100 yards). The 1:10 rate of twist will also provide acceptable accuracy with standard M80 Ball if M118 LR or M852 is not available for issue. Additionally, the SEI build seems to have solved one of the major faults associated with the M21/25 system over the years: the SEI rifle can produce excellent, consistent "cold bore" accuracy with its first shot, something that the M21/25 and other semi-automatic sniper systems have not always been able to do on a consistent basis. Additionally, the SEI variant maintains its zero once established better than the M21/25 variants. Bottom line, it gives general purpose (or SOF) shooters a rifle that is capable of reaching out and "touching" targets at ranges far greater than generally possible with the M4 system. And it offers superior barrier penetration over the 55 or 62gr 5.56x45mm projectile. It is an extremely capable system that has been tested at the U.S. Army Sniper School at Ft. Benning, GA and has produced verified 8-inch groups at 1,000 yards (sub MOA) with M118 LR ammunition.

Besides the 2nd Infantry Division, the SEI M21A5/M14SEI was also purchased by the 101st Airborne Division (Air Assault) and the 25th Infantry Division, and has seen extensive combat use in Iraq and Afghanistan. The system has been provided at a lower overall cost than purchasing new M110 systems for use by general purpose forces and designated marksmen. Realistically, this will probably be the last variation on a theme that has existed since 1957, but it will continue to provide our conventional Infantry units the capability to engage and destroy enemy troops at extended ranges of 500 yards and beyond.

CIVIL STRIFE IN MALI: OPPORTUNITY IN ACTION

By Laura Deatrick, OEA Team

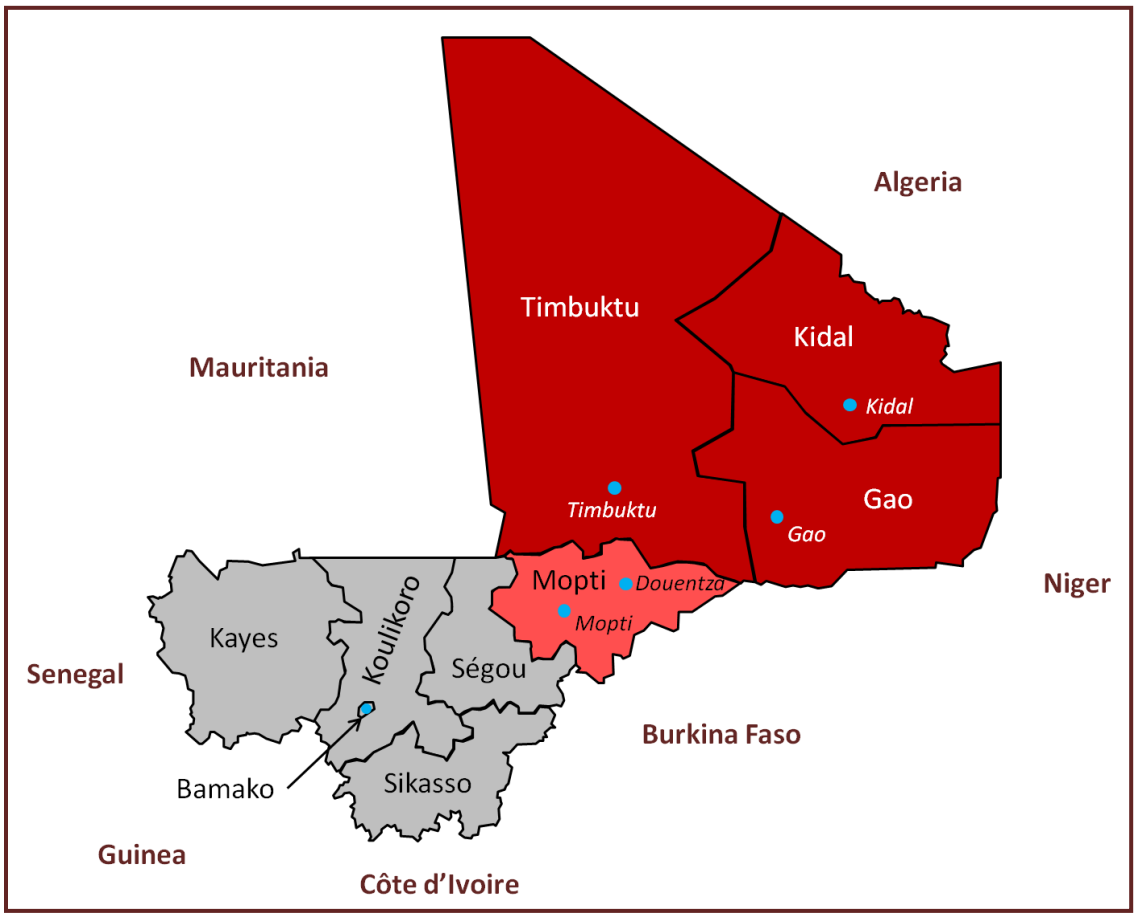
When Libya's Muammar Gaddafi fell in 2011, few considered the impact on African nations that did not share a common border with the country. However, ethnic Tuaregs who originated from northern Mali had been fighting with Libyan pro-government forces. With Gaddafi's downfall imminent, hundreds of these Tuaregs returned to their home country, over 530 miles southeast of Libya, and began a rebellion there that resulted in half of the country being taken over by militant Islamists. The upcoming new OEA Team Threat Report, Civil Strife in Mali: Opportunity in Action, examines the history of this rebellion to date, including key players, events, and implications of the current situation.

Mali is a large, sparsely-populated, landlocked nation located in western Africa. Relatively flat, the country consists mainly of desert in the north and tropical savanna in the south. It is home to 14-16 million people comprised of several ethnic groups, including the Tuaregs. The vast majority of people – around 90% – are Sunni Muslim, and the rest follow either indigenous beliefs or Christianity. Mali is very poor, with an annual per-capita GDP of only $1,100. Around two-thirds of the populace lives in rural areas and most people engage in agricultural activities such as farming, fishing, or nomadic herding.

A former colony of France, Mali achieved independence in 1960. A military coup in 1968 ushered in a two-decade period of military/single-party rule. This lasted until a subsequent coup in 1991 that led to a multi-party republic. The country is a member of the West African Economic and Monetary Union, sharing a common central bank and currency with six other West African nations. Mali maintains a small military and paramilitary security forces, numbering approximately 15,600, and has a military budget of less than $200 million annually. Tuareg rebels, feeling neglected by the

southern-based government, have staged two previous rebellions during the past twenty years.

During the latter half of 2011 it became clear that the Gaddafi regime would soon fall. Ethnic Tuareg fighters began returning home, bringing Libyan weapons with them in the process. The first sign of trouble occurred in October of that year, when Tuaregs attacked a government installation in Kidal province.



In mid-January 2012, Tuareg rebels attacked three towns in northern Mali in short succession. The towns were briefly retaken by the Mali Army, but the Tuaregs were in back in control within weeks. The fighting spread from there, with small towns falling to the rebels and local residents fleeing the area. Refugee and internally displaced person (IDP) numbers grew quickly, with estimates of 44,000 refugees and 60,000 IDPs by mid-February.

The Economic Community of West African States (ECOWAS), of which Mali was a member, was quick to condemn the rebel attacks and call for peace talks. Malians in Bamako held protests against the government for its perceived lack of support to the Army forces fighting in the north. Plans were soon made for a summit on the crisis, to be held in neighboring Algeria.

On 21 March, Malian Army troops stationed near the capital, Bamako, mutinied against their officers due to lack of weapons and opposition to potential peace talks. The action quickly ballooned to an attack on the presidential palace and an impromptu coup d'état. The coup leader, Captain Amadou Sanogo, suspended the Constitution and announced that the coup leaders would return the country to democracy once the rebellion had been put down. President Touré, who was due to step down after the upcoming election in April, went into hiding. Within twenty-four hours the African Union (AU), ECOWAS, and the European Union (EU) had condemned the coup, and both the World Bank and the African Development Bank had suspended aid.

It soon became clear that three separate groups were fighting government forces in northern Mali. The first was the National Movement for the Liberation of Azawad (MNLA), an ethnic Tuareg group whose main goal was to create an independent state – called Azawad – in the northern half of Mali. The second was Ansar Dine (aka Harakat Ansar al-Din), a militant Islamist group founded by known Tuareg rebel Iyad Ag Ghali. This group had close ties to al-Qaeda in the Islamic Maghreb (AQIM) and desired to institute Sharia (Islamic) law throughout the country. The third group, Movement for Unity and Jihad in West Africa (MUJAO), was another Islamist group desiring Sharia law in Mali.

Seizing the opportunity provided by the chaos in Bamako, the rebel groups quickly took the initiative. Having surrounding Kidal city, the MNLA, Ansar Dine, and MUJAO, working together, took over the cities of Kidal, Gao, and Timbuktu, as well as their associated military bases within a three day period. Malian forces

were ordered to withdraw from Kidal and Gao, citing the military's desire to avoid civilian casualties.

Divisions between the MNLA and the Islamist groups began to show at once. On 2 April, just one day after capturing Timbuktu, the MNLA was chased out of parts of the city, and aspects of Sharia law were instituted in parts of Gao, Kidal, and Timbuktu. MUJAO attacked the Algerian Consulate in Gao that same week, kidnapping the consul and six of his staff. By this time the number of Malian refugees had increased to 100,000 with an equal number of IDPs.

The MNLA declared the northern region of Mali to be the independent state of Azawad on 6 April. Though the group claimed to control the area, Islamist influence continued to dominate. The international community quickly condemned the announcement and refused to recognize the region as an independent nation. Ansar Dine stated that it was in a "holy war" and had no interest in dividing the country in two. Reports of foreign Islamists in northern Mali, including Afghans, Pakistanis, and members of Boko Haram, began to appear, as did reports of child soldiers.

In the meantime, coup leaders in Bamako had quickly become bogged down with forming a new government. The junta propagated a new constitution and again promised to restore democratic rule, but came under immense pressure from the international community. ECOWAS threatened sanctions against the country if the coup leaders did not return the country to democratic rule at once. Sanogo subsequently announced his intention to reinstate the constitution, but did not relinquish power and had no transition plan. The stated sanctions against Mali – including border closure, asset freezes, and denial of money transfers from the Central Bank (located in Senegal) to Malian banks – went into effect the next day.

The junta continued to face resistance, both internally and externally. A national meeting planned by Sanogo was cancelled because political and civil groups, claiming the junta was illegitimate, refused to attend. ECOWAS leaders began meeting to discuss military intervention against both the junta and the rebels. Four days after sanctions were imposed, coup leaders agreed to stand down in exchange for the lifting of sanctions and immunity from prosecution. Parliamentary Speaker Diouncounda Traoré would be made interim president, and would have 40 days to organize elections in accordance with the Constitution. Malian President Touré, who was still in hiding, officially resigned and Traoré was subsequently sworn in as President. Sanogo, apparently unwilling to disappear quietly, hinted that elections could not realistically be held so quickly and that he would have a say in the country's leadership structure after the 40-day period ended.

Though the MNLA had a presence in all three cities, MUJAO was firmly in charge of Gao and Ansar Dine controlled Timbuktu and Kidal. Despite protests by local residents, Sharia law continued to be enforced. Ancient mausoleums in Timbuktu and other locations were destroyed, non-Islamic ancient documents were removed from libraries, and "Islamic" standards of dress and behavior were enforced. Sharia-type punishments were meted out, to include whippings, cutting off hands, and stoning individuals for adultery. Residents protested regularly against the presence of armed groups and the imposition of Sharia law. By the end of April, refugee and IDP numbers were up to 270,000.

During April the junta continued to influence all decisions made by Mali's interim government. The military frequently arrested influential leaders in Bamako, who were usually released after several days' detention. Former President Touré and his family fled to Senegal in mid-April, and a counter-coup attack occurred in late April. The latter was precipitated by the junta's intent to arrest the leader of the anti-coup Presidential Guard. The junta defeated the Guard, killing several and arresting as many others as it could find. By this time Traoré had expressed willingness to negotiate with the MNLA and perhaps Ansar Dine, but not "foreign groups." ECOWAS had also determined that a military force of up to 3,300 troops must be sent to the country in order to stabilize the government and fight the rebels. Sanogo, however, refused to allow their deployment on Malian soil.

Due to the upcoming 40-day deadline on 21 May, ECOWAS insisted that Traoré be allowed to rule for a year in order to stabilize the country and allow time for elections to be held. Sanogo initially refused, but eventually agreed when appropriate perks – including a salary and a mansion – were offered. The very next day, Traoré was attacked by protesters and beaten unconscious. After recovering consciousness he was taken to France for cardiac tests and related medical treatment, where he remained for two months.

The MNLA and Ansar Dine reached an agreement to combine their movements and form an interim government in late May. Azawad was to be an independent state with Sharia as the basis for law.

However, within days of its signing the pact began to break down. MNLA leaders announced they were breaking the agreement, as it was not secular enough. Ansar Dine claimed the statements were not representative of the MNLA as a whole, and pronounced the agreement to be "irrevocable." By this time IDPs and refugees had reached 140,000 and 160,000, respectively.

Fighting between the MNLA and Ansar Dine broke out in Kidal city in early June, then between MUJAO and the MNLA in late June in Gao. By mid-July the two Islamist groups had driven the MNLA from all cities in northern Mali. At the beginning of August, MUJAO attacked and took over Douentza city in Mopti province. That same day the group killed one of the Algerian diplomats it had captured in early April, citing Algeria's refusal to release three MUJAO members from State custody. Refugee and IDP numbers continued to increase during this time, approaching 500,000 by the end of August.

Unwilling to deploy ECOWAS troops to Mali without a UN mandate, ECOWAS and the AU formally requested assistance from the UN Security Council in June. In August, the Malian government agreed to allow a few hundred ECOWAS troops to deploy in the north, but none in the south. By early September, Traoré had formally requested military assistance from ECOWAS, who was still awaiting a mandate from the UN Security Council. Representatives of the rebel groups and the Malian government have met at various times during the past several months to discuss the possibility of negotiations, but nothing concrete has developed yet. As of this writing, the Security Council has denied the request multiple times, each time citing "lack of details," and has scheduled a meeting on the issue for 26 September 2012.

Introducing groups such as the MNLA, Ansar Dine, MUJAO, and the junta in a training scenario can provide several benefits. Slow or weak reactions by authorities to events on the ground can open a window of opportunity to their opponents. Groups that are working together but are fundamentally at cross-purposes can quickly turn on each other, bringing effective government to a standstill. Ruling authorities that appear to be stable may be quickly overturned. The takeover of an area by persons with an ideology differing from that of local residents may lead to large public protests. The diplomatic process, while not without value, can be long, drawn-out, and complex, allowing opposition groups time to cement their positions. The number of refugees and IDPs can grow dramatically in a short time, presenting a humanitarian crisis that must be handled.

The Civil Strife in Mali: Opportunity in Action Threat Report provides information to the Army training community on the current situation in Mali. It contains a detailed review of events beginning in late 2011 and a discussion of the main players on the ground. In addition, it considers both current and future implications of the militant Islamist occupation of northern Mali, as well as training implications. You can find the report on AKO.

NETWORKS IN OPERATIONAL ENVIRONMENTS: FRIEND OR FOE?

This article represents a combined effort by TRADOC G2 (Training Brain Operations Center (TBOC)-led with support from TRADOC Intelligence Support Activity (TRISA), TRADOC G2 Analysis and Production Division, and ISR TOPOFF Team); The Asymmetric Warfare Group; and The Maneuver Center of Excellence (MCoE) to describe the latest methods used to analyze human networks and how those methods fit into a broader methodology currently known as attack the network (AtN). The AtN methodology demands that network analysis and operations planning be based on understanding the mission and the operational environment (OE). Three pillars – understanding the mission, understanding the OE, and understanding the networks – provide the foundation for the AtN methodology. Many of the concepts described in this article will be included in a forthcoming Army Training Publication to be titled "Network Engagement." The term Network Engagement will replace the term AtN as it is currently used because Network Engagement better captures the essence of what the term AtN currently represents.[1]

"Context is king. Achieving an understanding of what is happening – or will happen – 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."[2] *(LTG Michael T. Flynn, U.S. Army, and Brigadier General Charles A. Flynn, U.S. Army)*

Intuitively, most military personnel think of kill/capture operations when they hear the term attack the network

(AtN), but kill/capture operations are just one narrow element within the AtN lines of effort as currently defined. Among other things, AtN operations include conducting actions and operations to support friendly networks, neutralize threat networks, and influence neutral networks. Furthermore, neither kill/capture operations, nor neutralizing threat networks represents the decisive effort within AtN. The decisive line of effort within AtN is *supporting friendly networks*. Because of the dissonance between intuitive understanding of what the term AtN means and what the term has come to represent in the training realm, the term AtN will be changed to the term "Network Engagement" within emerging doctrine. The Maneuver Center of Excellence (MCoE), TRADOC's lead for AtN, will use the term **network engagement** to replace the current use of the term AtN in its forthcoming Training Circular 3-90.50, to be published no earlier than November 2012. The term AtN will also be used in the Army Training Publication ATP; however, it will represent only the line of effort against threat networks. The term **network engagement** will be used when the context implies the broad operational concept of lines of effort against the networks of networks. Figure 1 portrays this operational concept.[3]

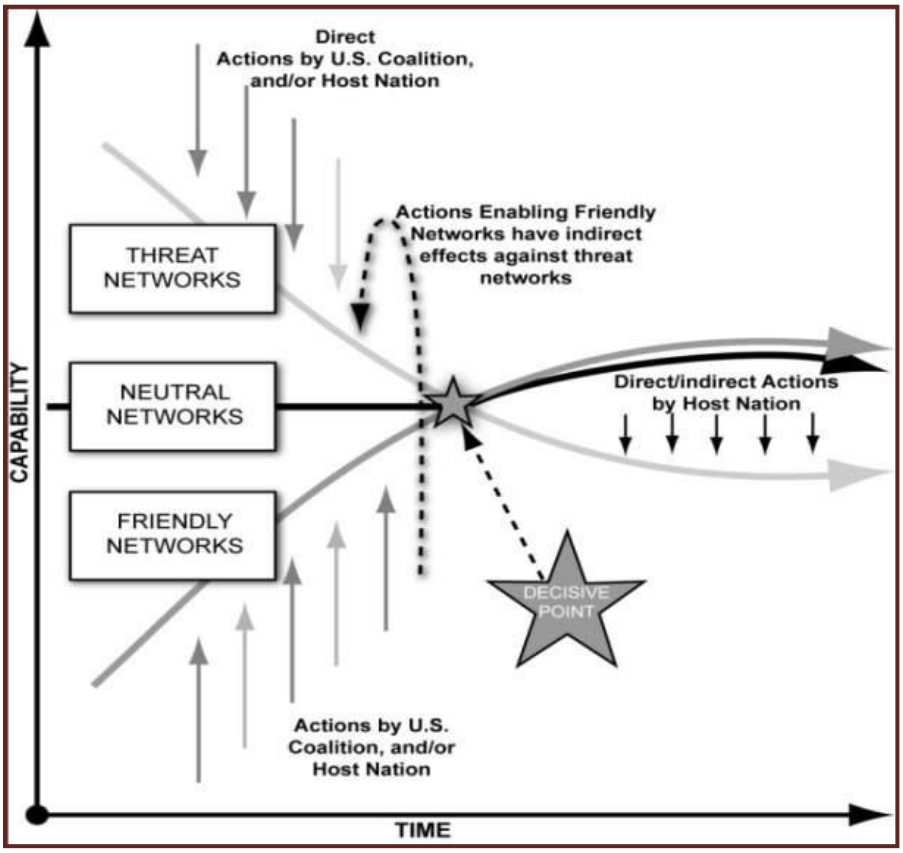


Figure 1. Network Engagement Operational Concept

Purpose

It is important to remember the purpose of network analysis which is supporting planning for network engagement. In this context, network engagement is comprised of five lines of effort and six pillars.[4] Unlike the soon to be published ATP 3-90.50, *Network Engagement*, this article focuses only on three of the five lines of effort of network engagement: support friendly networks, neutralize threat networks, and influence neutral networks. The theme of this article is that in order to support friendly networks, influence neutral networks, and neutralize threat networks, the most effective underlying analysis incorporates a variety of concepts, methodologies, and analytical techniques, which are represented by Figures 1-11 below.

The key point of Figure 1 is that successful network engagement is achieved at and beyond the decisive point, when threat networks are sufficiently degraded and friendly networks are sufficiently developed so that they can contain and manage any residual networked threats independently and in a sustained manner. Another important point related to Figure 1 is that networks can be degraded indirectly. As stated in draft ATP 3-50.90:

> Threat network capabilities can be neutralized through a combination of direct or indirect actions. Neutralizing a threat network is conducted through focused and synchronized lethal and nonlethal action such as kill/capture activities (lethal), electronic warfare (nonlethal), and influence and inform activities (nonlethal). Threat networks can be neutralized indirectly through specific or direct actions by U.S., coalition, or host nation (HN) forces that increase the capabilities of friendly networks (government, security forces, police, business leaders, social leaders, and the population). Indirect actions can have enduring positive effects that greatly reduce the threat networks capabilities.[5]

The effect of indirectly neutralizing threat networks through the support of friendly networks, as described above, reinforces the concept that supporting friendly

networks is generally the decisive effort. This is not intended to preclude individual unit analyses from concluding that other lines of effort may be of higher priority for specific phases of actual operations.

The six pillars of network engagement are shown below:

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

Looking closely at two of the pillars of network engagement, *understand the OE* and *understand the networks*, it's clear that network analysis should be based on understanding the broader OE, because networks are an integral part of the broader OE. The more clearly the OE is understood, the more precisely networks can be analyzed.

Understand the OE

By Department of Defense (DOD) definition, an OE is "a composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander" (JP 3-0). This definition applies to an OE for a specific operation, at any level of command, and any level of analysis. Multiple OEs can and do exist.

The framework for thoroughly and systematically analyzing and understanding any potential OE and all the challenges and opportunities inherent in it consists of the eight variables: **political**, **military**, **economic**, **social**, **information**, **infrastructure**, **physical environment**, and **time**. The memory aid for these variables is PMESII-PT.

Army forces apply the PMESII-PT variables to the specific OE in which they are conducting or plan to conduct operations. Use of the framework by Army commanders and staffs at all levels to analyze and understand their OEs:

- Enables lower commands to use their higher command's analysis of its own OE and just add details to capture the nature of variables and sub-variables in their own specific OE, which is part of that higher-level OE or the strategic environment.
- Enables higher commands to assimilate into their own OE analysis the relevant information developed by their subordinates.
- Facilitates a common operational picture (COP) at all levels of command.
- Provides compatibility with the PMESII framework used at joint level and in the Interagency Conflict Assessment Framework (ICAF).

The PMESII-PT variables are fundamental to development of a comprehensive understanding of an OE for planning and decision-making at any level, in any situation. These variables and their interrelatedness determine the nature of an OE and how it will affect or be affected by an operation.[6]

Networks in an OE

One of the most significant parts of an OE is the people within it who belong to various networks. During the past ten years, DoD has increasingly viewed the people within the OE as a network of human networks. These networks include threat, friendly, and neutral networks all of which are interconnected. Analysts focus considerable time and effort on developing an understanding of an OE to include the human terrain and networks operating within it.

This is an important concept 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 *processes* and *materials* can be enhanced with training on how to detect indicators that we can see with our eyes, *observables*, and indicators that we can measure with our sensors, *signatures*. Identifying observables and signatures that are spawned by network activities and materials is part of a comprehensive approach to understanding any potential OE.

Understanding an OE is challenging because of its dynamic nature, and is driven in large part by interaction among the PMESII-PT variables and the fact that human networks within OEs are dynamic, complex, adaptive systems. This implies that they are constantly adjusting to myriad internal and external factors that force them to adapt. As a result, understanding an OE is a constant effort, which requires analysts to continually identify and anticipate changes, update information, refine or adjust collection, and assess their

understanding of the OE. Understanding of an OE may not be achieved in a timely manner to allow fully informed decisions, however, operational units must strive to maintain a comprehensive understanding of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander.

Effective network analysis is undermined by the dynamic and complex nature of an OE because analytical products provide only a snapshot of the OE and its networks. The most accurate possible snapshot today will become stale over time as external and internal factors interact among the variables of the OE and networks change and adapt in order to survive in the environment. This implies that a running intelligence estimate is essential for the commander and staff to maintain the most accurate understanding. Secondly, it implies that analytical products do not show the complete picture, they can only capture a portion of an OE and the networks. While it is critical to identify second and third order effects of our operations and decisions, there is always the potential for unknown elements that will result in some degree of unexpected consequences for blue force actions.

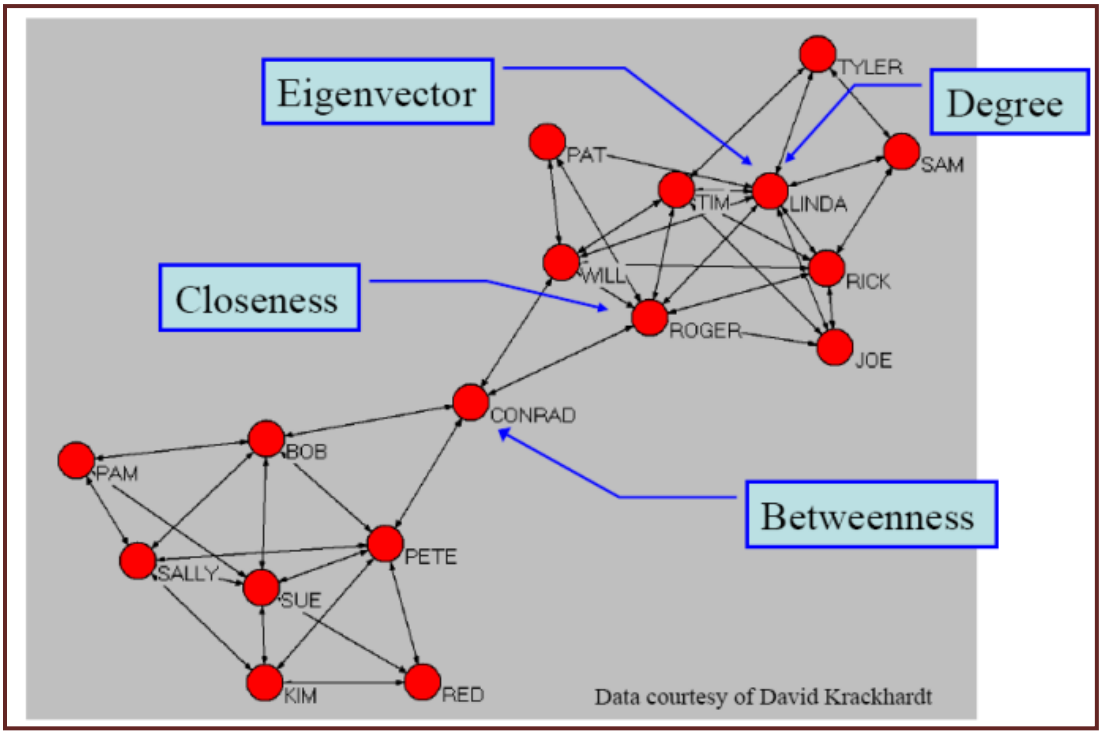


Figure 2. Centrality Measures[7]

Understand the Networks

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 in parallel so as to be mutually supporting. This is not to imply that the 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). For example, pattern analysis provides information on the "what" and "when," and event matrices provide information on the "who" as well as the "what" and "when."

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. Rather, 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 critical vulnerabilities for lethal and nonlethal targeting against a given 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.

Social network analysis tools speed identification of network members who possess high degrees of centrality. Nodes that are high in betweenness centrality (BC) are candidates for maximizing disruption of the network because of their relational position within the network. In the same manner, nodes that are high in other types of centrality are candidates for achieving other specific, desired effects on networks.

In the notional network in Figure 2, for example, Conrad is high in BC because he connects major elements of the network. Depending on the desired effect that U.S. and coalition forces might want to impose upon the network, Conrad's high BC could be significant.[8]

For example, if U.S., coalition, or host nation forces were attempting to disrupt this network, Conrad would potentially represent a critical node. The staff would have to also carefully consider not only the SNA analysis, but also the more subjective analysis provided by the link analysis diagram and the targeting recommendations of the analysts that developed it.

The diagram in Figure 3 demonstrates how link analysis can be used as a foundation for SNA. It was produced by importing a standard link analysis diagram into the Organizational Risk Analyzer (ORA) software application. After the link analysis diagram is imported, ORA is then used to rapidly produce multiple views of the network, including views based on each of the measures of centrality. In each case, the red circles represent people, and the diameter of each circle represents the degree to which people possess the particular measure of centrality being assessed at that time.

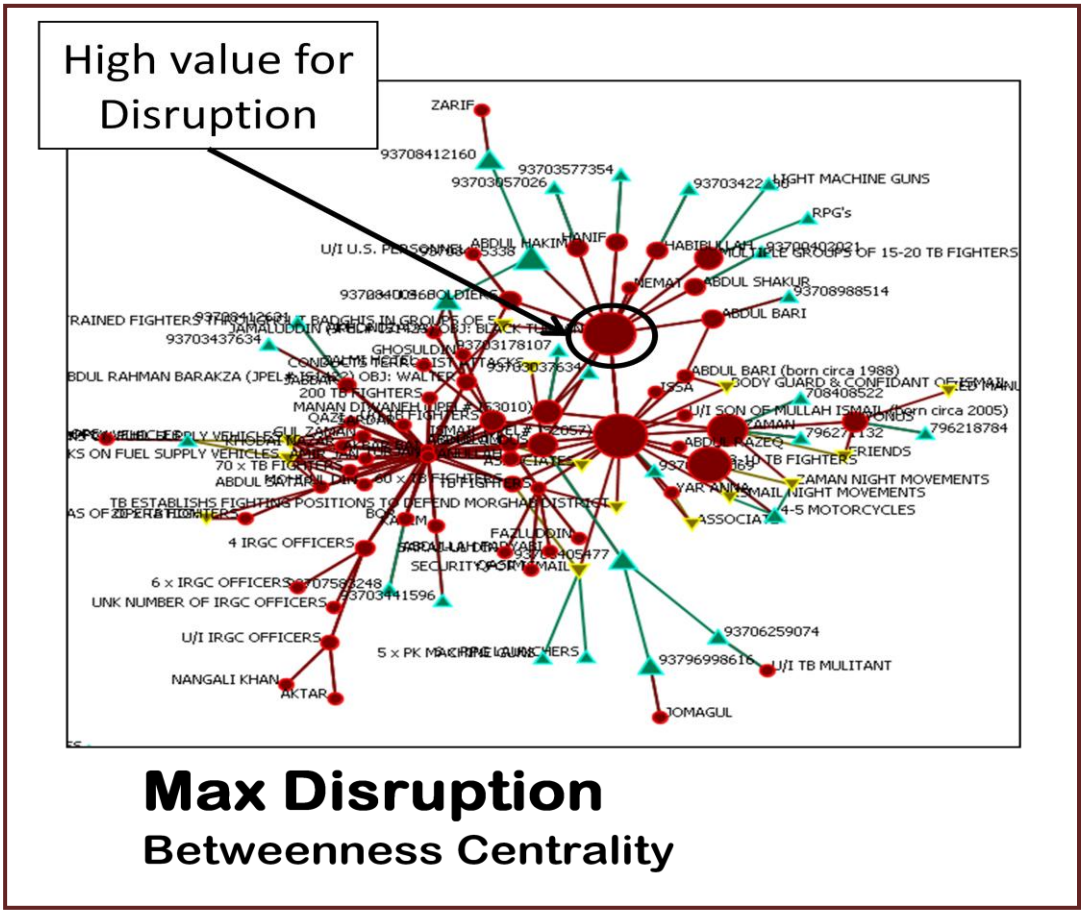


Figure 3. ORA Output[10]

Network analysis is never complete, rather, it is an iterative process that always has information gaps that staff must strive to understand. Part of the art of network analysis is identifying those information gaps that can and should be filled by leveraging collection assets. Using information previously gathered and analyzed, network templating provides the next level of in-depth understanding of networks.[9] Network templating is a method of determining where best to focus collection assets in order 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 (IPB), information collection and synchronization, and targeting.

All previous analytical efforts described above constitute step 1, describe the network. Step 2 is

indentifying indicators.[11] Draft ADP 2-22.1 provides this definition:

"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 (JP 2-0). An indicator is positive or negative evidence of threat activity or any characteristic of the AO that points toward threat vulnerabilities, the adoption or rejection by the threat of a particular activity, or that confirm indications of threat activities. Detection and confirmation of indicators enable analysts to answer CCIRs (PIRs and friendly force information requirements)."

In more simplistic terms, indicators are those things we can see with our eyes (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

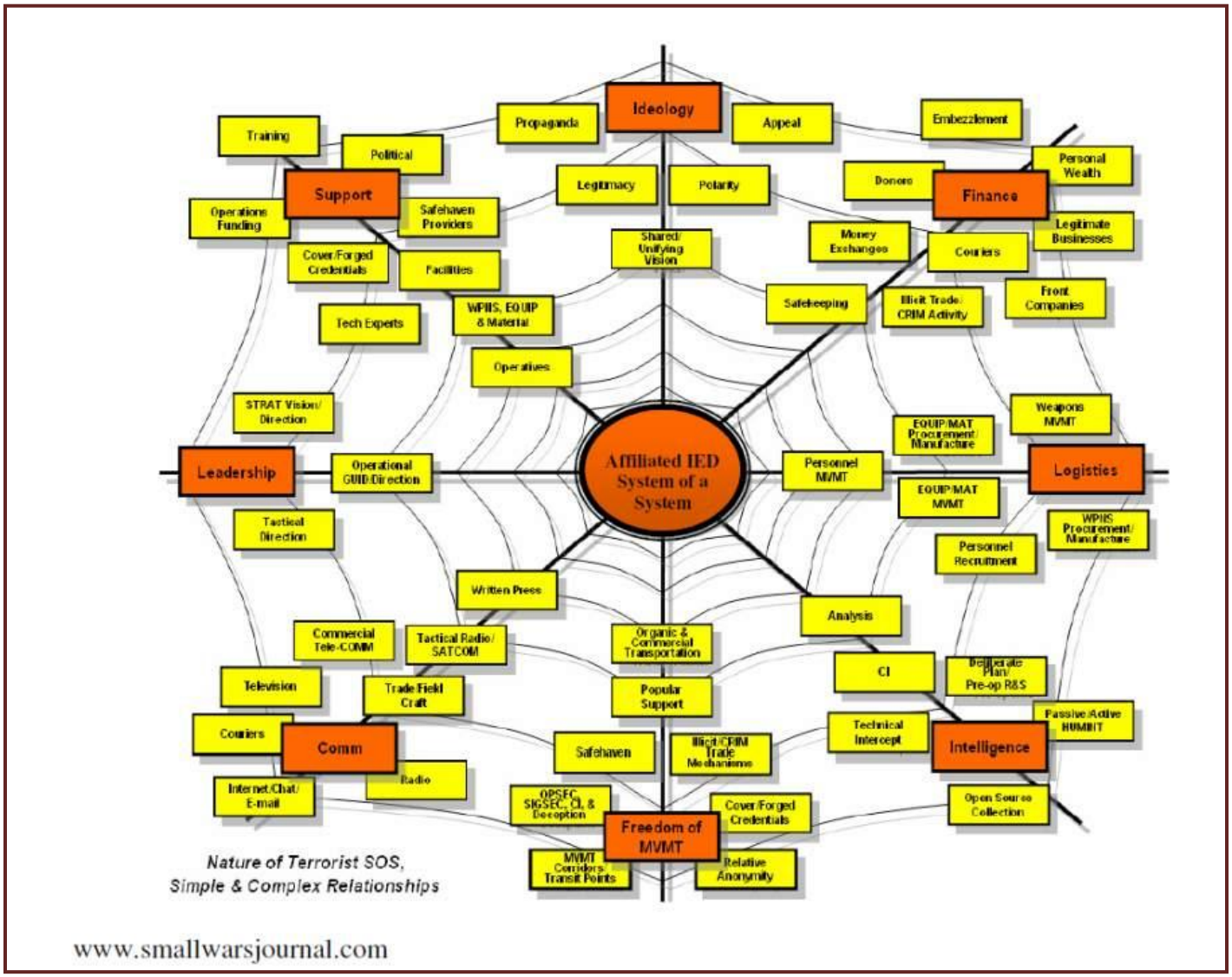


Figure 4. Network Model

may influence the commander's selection of a COA. Indicators may result from previous actions or from threat failure to take action. Indicators are the basis for situation development. The all-source intelligence analyst integrates information from all sources to knowledge of the basic activities the network is involved in. It is often helpful to begin the process of identifying network activities with a generic network model as shown in Figure 4.[12]

A generic network model (Figure 4) 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. Rather than starting with 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. Doctrinal templates illustrate the disposition and activity of adversary forces and assets conducting a particular operation unconstrained by the effects of the operational environment 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, and so forth. Doctrinal templates are usually scaled to allow ready use with geospatial products.[13]

When this model is applied to reporting and analyses of a specific

Operation (Action)	1st Order Effect	2nd Order Effect	3rd Order Effect
Medical mission providing medical training to providers followed immediately by service to local residents	Local residents receive immediate increase in medical care and attention	Locals residents see providers receiving professional training and perceive an immediate benefit	Locals see Afghan doctors and ANSF working with CF and CF assisted but main effort is Afghan. Increases confidence in GIRoA.
Medical mission providing medical service to local residents	Local residents receive immediate increase in medical care and attention	Local medical providers lose business to CF and are marginalized	GIRoA medical providers are discredited and delegitimized in the eyes of the populace

Figure 6. Source: FM 4-23.2

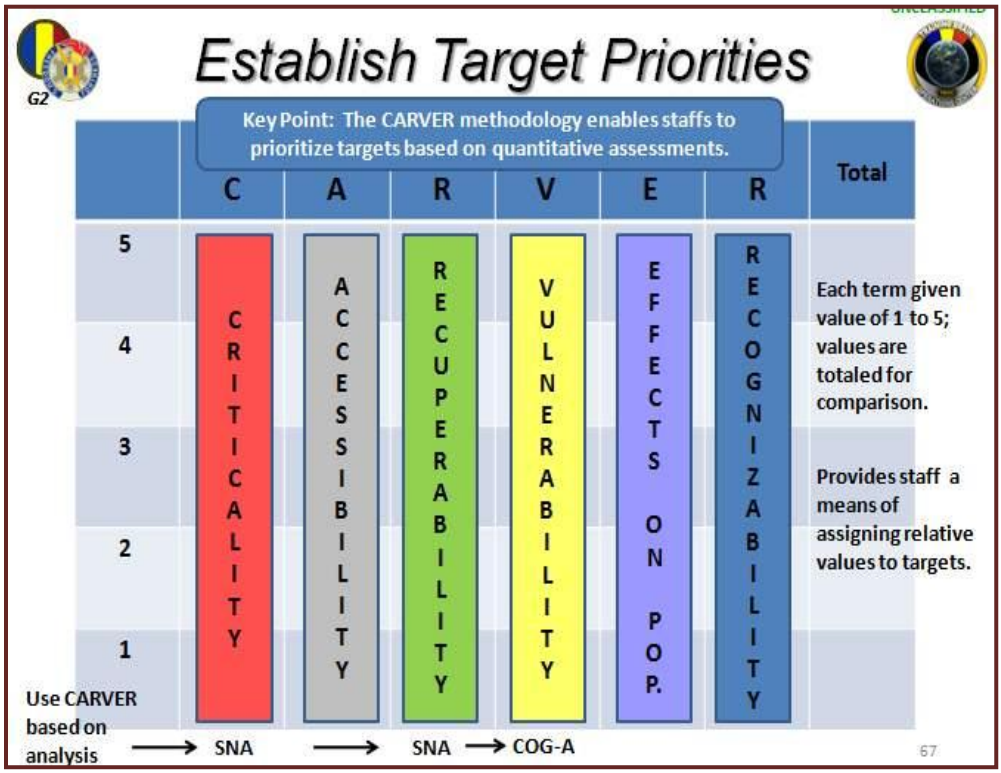


Figure 7. CARVER Analysis

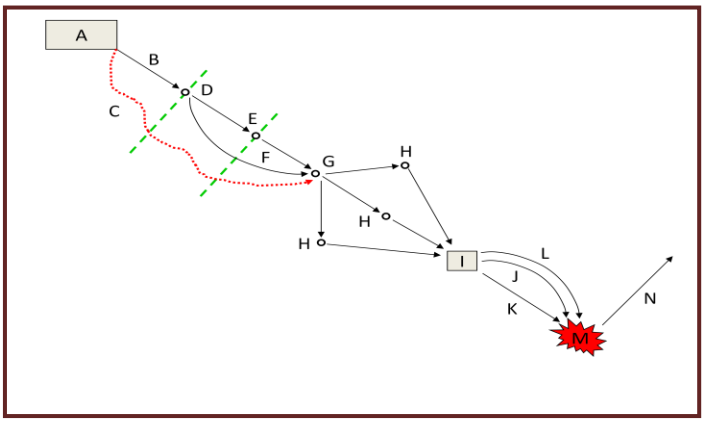


Figure 5. Network Template

network, that network's unique patterns and sequence of activities emerge (Figure 5). This enables analysts and operations personnel to develop potential indicators. Obviously, the more clearly a network's sequence of activities is understood, the more robust set of potential indicators can be developed. Throughout this process, specific activities need to be identified geographically. This is how 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 each NAI based

on their capabilities to detect observables or signatures under various conditions.[14]

The final step in network templating is to make targeting recommendations. Targeting recommendations include both those lethal and nonlethal effects desired 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, as well as the commander's intent.

Unit commanders and staffs can prioritize the potential targets they are considering by analyzing a network's capability, accessibility, recuperability, vulnerability, effects on populace, and recognizability (CARVER). CARVER analysis assigns a quantitative value to targets based on subjectively rating these six criteria.[15] Each of these elements is assigned a numerical value which collectively equates to the quantitative value of each potential target. Operational units must keep in mind that lethal and nonlethal targeting should be done as part of a single targeting process. Often, lethal and nonlethal targeting processes are done as separate and distinct efforts, which undermines unity of effort and discounts considerations of how targeting single networks affects the overall network of networks. In the example below, two different approaches are used by coalition forces to provide medical support to a host nation. The differences were that in course of action (COA) 1, the support is first provided to HN medical personnel, then to the populace. In COA 2, medical support is provided immediately to HN local residents. Although the first order effects are the same, second and third order effects are far different.

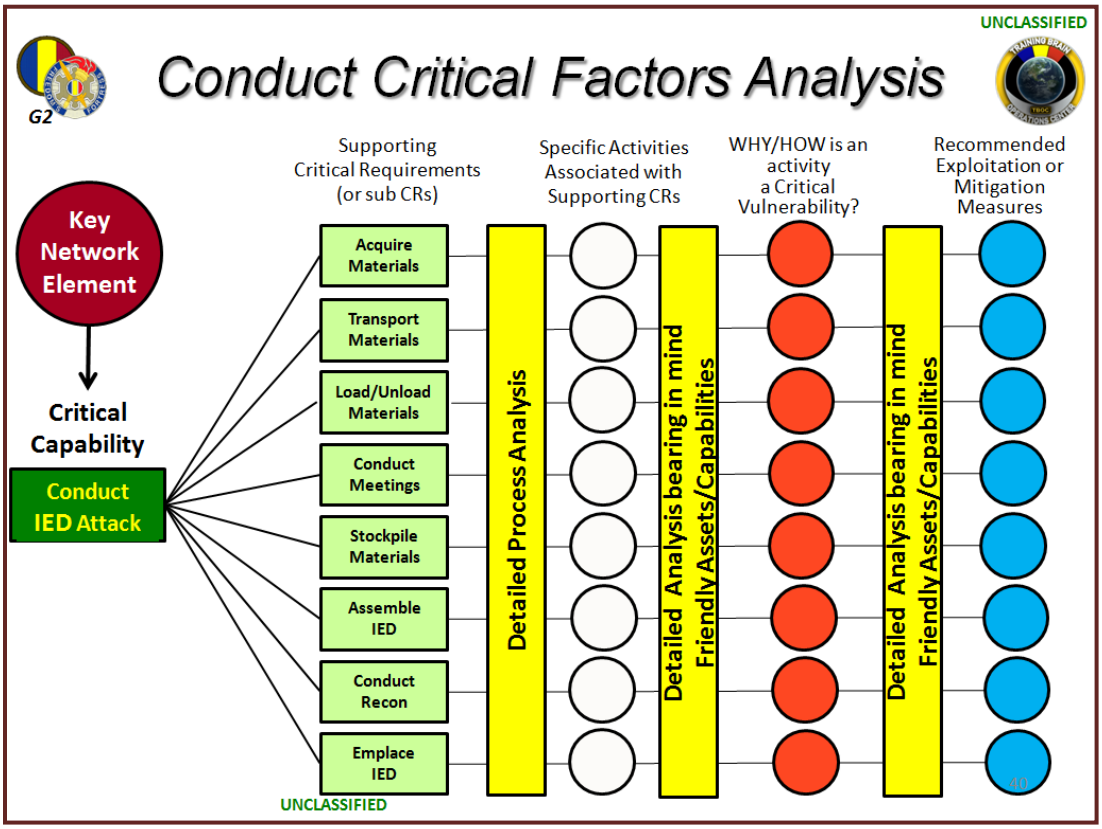


Figure 8. Critical Factors Analysis (CFA)

Network templating must be done in parallel with another means of analysis – critical factors analysis, which is also known as center of gravity analysis. As shown in Figure 8, critical factors analysis (CFA) is a method of determining a network's critical vulnerabilities. CFA can be applied to exploit threat network vulnerabilities or to mitigate friendly network capability gaps, depending on what type of network is being assessed and which AtN line of operations is being pursued.[16]

CFA enhances the network templating process by further defining which collection assets should be employed against critical network vulnerabilities in order to better understand network activities. CFA represents the thought process that guides network templating. In the example above, analysis of the critical requirement "Transport Materials" may reveal that a specific member of the red network is tasked with transporting IED components from two locations. By analyzing this process, it is determined the individual only travels to the second stop, to pick up explosive materials, if he visits the Internet café on Main Street. The transport of explosive materials is critical since the majority of the other components can be easily acquired. This represents a critical vulnerability to the red network. Friendly assets/capabilities could be leveraged to detect

observables and signatures associated with this activity for the purposes of disrupting the shipment.

networks and key aspects of the OE. The better a unit understands its OE and the networks within it, the more

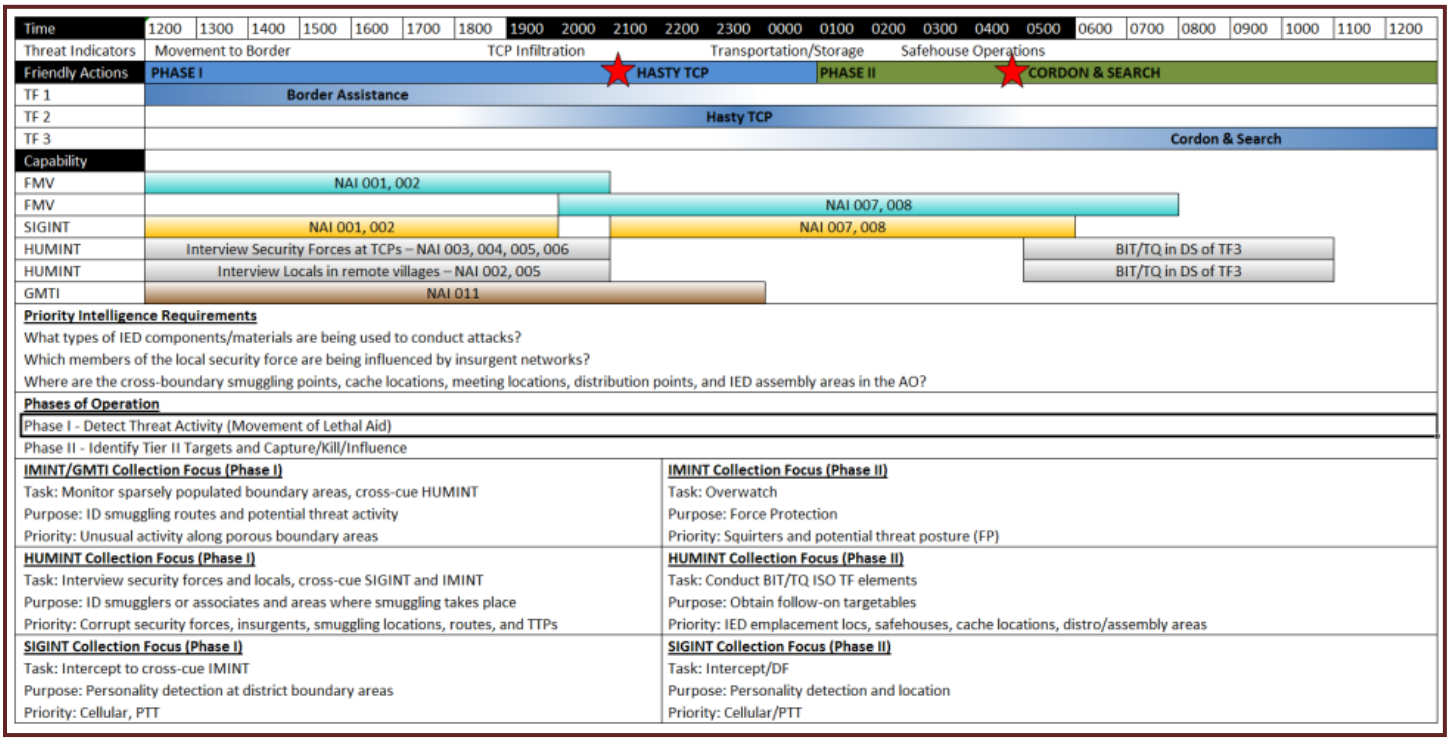


Figure 9. Staff Synchronization Matrix

The result of the combined efforts of network templating and CFA is a staff synchronization matrix (SSM) such as in Figure 9.[17] The SSM combines the information collection synchronization matrix with the scheme of maneuver in order to provide the commander and staff a single perspective that facilitates oversight of both. The SSM guides commanders and staffs during the execution of AtN operations.

Summary

This article described both the context for and a means of conducting network analysis. While many units are utilizing some of these principles to various degrees, the recommended approach is to integrate the AtN methodology comprehensively. Doing so requires comprehensive understanding of the AtN methodology and the ability to integrate it into staff processes and the unit battle rhythm. I Corps has done exactly that during their ongoing deployment as the Warfighter for Operation ENDURING FREEDOM. The result has been the ability to conduct successful AtN operations.[18]

The ability to conduct successful AtN operations is the ultimate context for network analysis. Network analysis provides the foundation for understanding the likely it will succeed in accomplishing its mission.

Endnotes

1 This discussion of the term "Network Engagement" and subsequent information related to it are derived from draft Army Training Publication (ATP) 3-90.50, Network Engagement, as provided to the TBOC on 27 April 2012 by the MCoE AtN Doctrine Team. Hereafter cited as Draft ATP 3-90.50.

2 This quote is excerpted from "Integrating Intelligence and Information" by LGEN M.T. Flynn and BGEN C.F. Flynn, January-February 2012 Military Review.

3 This quote is taken from the latest draft version of ATP 3-90.50, provided by the MCoE AtN Doctrine Team on 24 April 12.

4 Six pillars of AtN are taken from the latest draft version of ATP 3-90.50. These pillars represent a portion of the overall AtN Framework, which is addressed at length in the ATP.

5 Draft ATP 3-90.50, Paragraph 2-13

6 The concept of the PMESII/ASCOPE matrix is explained well and placed into a broader context in the AWG publication, An Introduction to the Vulnerability Assessment Method A Practitioner's Handbook Coordinating Draft, 17 August 2010, pages 2-1 through 2-7. Cited hereafter as "VAM".

7 This diagram, in which the data are attributed to Mr. David Krackhardt, was provided by LTC Ian McCulloh (PhD) during 2010, while he was serving as a member of the United States Military Academy Network Science Center (USMA NSC).

8 FM 3-24, COIN, Dated December 2006, Appendix B, page B-14 includes the following definition of Betweenness Centrality: *Betweenness centrality* indicates the extent to which an

individual lies between other individuals in the network, serving as an intermediary, liaison, or bridge. A node with high "betweenness" has great influence over what flows in the network. Depending on position, a person with high betweenness plays a "broker" role in the network. A major opportunity exists for counterinsurgents if, as in group C of figure B-6 (page B-11), the high betweenness centrality person is also a single point of failure which, if removed, would fragment the organization.

9 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.

10 This diagram represents output derived using a methodology titled Advanced Network Analysis and Targeting (ANAT), which was developed by then Major Ian McCulloh (PhD) and Maj Tony Johnson (PhD) of the USMA NSC. It is developed by importing a link analysis diagram into the Organizational Risk Analyzer (ORA) software suite. ORA was developed and is continually refined by Dr. Kathleen Carley and a team at Carnegie Mellon University.

11 Input related to draft ADP 2-22.1 was provided by TRADOC G2 Senior Analyst, Mr. Jerry Leverich.

12 This network model was provided by the TRADOC Intelligence Support Activity (TRISA) and is based on work done by a team at johns Hopkins University Applied Physics Lab under a JIEDDO contract. It is part of the TRISA IED Reference Set, hosted on the TBOC/JTCOIC SIPR website.

13 JP 2-01.3, Joint Intelligence Preparation of the Environment, Dated 16 June 2009, pg A-18.

14 AWG AtN Methodology Part 3, pp 7-11.

15 FM 34-36, Appendix D.

16 Figure 8 and TBOC's development of Critical Factors Analysis is based in large part on interaction with Dr. Joseph Strange of the Counter-IED Operations and Intelligence Integration Center during 2010.

17 AWG AtN Methodology Part 3, pp 10-11.

18 The following email was received from Mr. Steve Duncan of the TRADOC G2 ISR TOPOFF Team, while serving in Afghanistan on 1 April 2012, sent an email describing a conversation with a Major assigned to I Corps. An excerpt follows: "He remembered the AtN and Signatures training and was extremely complimentary and enthusiastic about the event. When they arrived in theater, they created an entire program around it and had some significant successes."

SYRIAN SOCIAL MEDIA

By Rick Burns, OEA Team

Social media is a reality on the modern battlefield and is ignored at a commander's peril. The ubiquitous nature and relatively low cost of social media requires serious consideration of its implications. Recent history has shown how an obscure video, in the hands of a few provocateurs, can inflame the passions of large numbers of people. Anticipating friction points and events will require familiarity and proficiency with all kinds of social media.

The power of social media to organize, rally, and inform government opposition reached new and unparalleled proportions during the Arab Spring. Most visibly, social media inflamed popular support and amassed protests in Egypt's Tahrir Square in 2011, leading to the downfall of the Mubarak regime. In the same year, Iran faced the largest uprisings since the 2009 elections, fueled in large measure by social media. As social media technology becomes more easily accessible and user friendly, it will become a more integral tool for planning, organizing, and inflaming opposition to entrenched governments.

The Syrian conflict is seeing an evolving social media environment with new twists. Opposition forces have been using social media to garner support outside of Syria using YouTube, Facebook, and Twitter. Uploading videos of atrocities carries emotional impact on those far from the battlefields. To counter this, a pro-Assad regime group of young computer-savvy zealots formed the Syrian Electronic Army (SEA) to push a different message. Additionally, the Syrian government has used measures such as false Facebook pages to identify opposition protesters. The battle in Syria now rages on the Internet as well as on the ground.

In addition to instantly publishing videos of what is happening on the ground, some have taken it upon themselves to track events in real time. The Web site *Syria Tracker*, for example, relies on eyewitness reports submitted via the Internet to track, document, and map such things as Syrians missing, killed, arrested, etc. Collating data and then plotting it on a map allows for analysis and accountability that was unavailable even a few years ago.

The Syrian Social Media Threat Report describes ways in which social media is affecting the ongoing conflict in Syria. The evolving nature and increasing availability of social media technology will require serious consideration of its bearing on future conflicts. Social media will continue to be a curse and a blessing and used by both sides in current and future clashes.

For more details, see the TRISA Threat Report "Syrian Social Media" on AKO.

ISRAEL'S IRON DOME (MOBILE SHORT RANGE ADA SYSTEM)

By Kris Lechowicz, OPFOR Doctrine Team

The Iron Dome is short range air defense artillery (ADA) system developed by Israel as a supporting system for the "lower level threat" for Israel's multi-layered missile defense. The system is a mobile short range (up to 2.5 and 45-mile engagement radius) ADA system that was supplemented with U.S. funding. This system can engage and negate improvised indirect threats such as mortars and rockets that are common to groups like Hamas and Hezbollah (see WEG Sheet on Improvised Rocket Launchers following this article).

Top: Mini Raz MMR (EL/M-2084)
Bottom: Interceptor System

The Indirect Threat

These short range rockets are easily manufactured by threat groups and proliferate worldwide. These recurring indirect short range mortar/rocket threats are similar to what U.S. soldiers faced in Iraq and currently experience in Afghanistan.

Mission

The Iron Dome can engage multiple simultaneous short range threats from rockets or artillery rounds. The development of the Iron Dome started in 2007 and it was deployed in 2011.The system reports a success rate of between 70-79% (overall 75% in 2011). An estimate from Israel indicates that 10-15 batteries would be sufficient to defend most of Israel's urban population centers. The Iron Dome is being considered for export to a number of countries including South Korea, Singapore, and India. Based on the success rate of the system, more countries may invest in the Iron Dome. Israel has current plans to upgrade and develop the functionality of the system in the near future.

The Battery Functions

One Iron Dome Battery includes:

- Multi-mission capable radar, or the Mini Raz MMR (EL/M-2084)
- Mission command center, or the "Battle Management & Weapons Control (BMC)"
- "Interceptor" system (3 systems per battery) with 20 Tamir "interceptor" rockets in each system (60 rockets in battery)
- The Tamir rocket has electro-optic sensors and steering fins that allow the rocket to be highly maneuverable

Operating Environment

The Iron Dome is reported to be able to maintain operational effectiveness day or night in all types of inclement weather which includes cloud cover, rain, dust storms, and/or fog. The system is reported to be highly mobile and can be moved around the battlefield and set up within hours in different locations.

How the System Works

The main mission of the Iron Dome is to protect highly populated areas from indirect threats. The Iron Dome carries out this mission by using its radar to identify and "backtrack" threat trajectories from rockets or artillery rounds. The radar sends the data to the BMC for trajectory analysis and potential impact projection (risk assessment). If the threat is deemed actionable, the "interceptor" rocket is launched to negate the indirect threat. After launch, the BMC continues to track the threat providing the interceptor rocket with updates on target location. The BMC can send a message with the point of origin to aircraft or artillery within an estimated 25 seconds of detecting a potential threat. The interceptor rocket tends to engage the threat over "neutral area" with less population density, which greatly reduces the threat of collateral damage.

Battle Management and Weapons Control (BMC)

Negative

- The system cannot successfully engage targets within a shorter range, which leaves towns on the Gaza border vulnerable to indirect fire.

- An Iron Dome battery is estimated to cost 50 million USD, with each Tamir interceptor rocket to be $50,000 in additional cost.

- Mass attack from multiple rockets could potentially overwhelm the system.

Positive

- LTC Shabtai Ben-bocher (head of the Lower Layer Wing of Israel's Shield Administration) states that the Dome System will continue to upgrade and improve intercept capabilities.

- Open source reporting indicates that the Iron Dome has been reasonably successful in engagement rates.

The Israeli Iron Dome appears to be a successful ADA system that has been tested under fire. On a tactical level, U.S. soldiers may deploy to areas that have Iron Dome systems and should be aware of such ADA capabilities. The Iron Dome in the near future may also be used in conjunction or integrated with U.S. ADA systems. Improvised indirect rockets remain a useful tool for militant groups worldwide and will continue to be a threat for U.S. forces no matter where they are deployed.

WEG HIGHLIGHT: IMPROVISED ROCKET LAUNCHERS

The *Worldwide Equipment Guide (WEG)* was developed to support OPFOR equipment portrayal across the training community. The WEG is not a product of the U.S. intelligence community. The WEG is a TRADOC G-2 approved document. Annual WEG updates are posted on AKO.

Improvised Rocket Launchers

Insurgent prepares rockets against U.S. base in Ramadi, Iraq (AP Photos)

Afghani IRL improvised from aerial rocket laucher

Hamas improvised rockets and launchers used 2000-04

Improvised rockets and lauchers can be fabricated using different levels of improvisation. The more common and successful approach is to acquire existing rockets of various types, such as artillery MRL rockets (107/122/130/132mm) and aerial rockets (57/68/80/81/122-mm), and to fabricate launchers. Launchers are fabricated using tubes, angle iron, or boards, which can be quickly erected at the launch site. Because these rockets are very imprecise, launchers may be moved within a few hundred meters of the target (such as the **Donkey Cart MRL** -see next page). When the goal is harassment, or the target is a large area, such as a base or city, the launcher may be 20 km away. Some launchers are set for remote detonation using electronic timers, RF triggered detonators, or pyrotechnic fuze. Timers or command detonation permit the launchers to maximize losses. Although electronic communications are not necessary, organized cells can employ observers with cell phones to monitor the targets and launch area to increase possibility of target vulnerability and to assure launch security. Additional multiple launchers or booby-trapped launchers with trip wires may be used to initiate a second attack in order to target military investigation/EOD teams.

SYSTEM: Kassam or Qassam-1, 2, or 3
Date of Introduction: 2000 for Kassam
Proliferation: Used in Palestine by the Hamas, and similar to hand-fabricated rockets employed by insurgents elsewhere. In the period 2000-2003 more than 140 Kassam rockets were launched.

Launcher: Sighting is based on tilt and pointing the launch ramp. Accuracy is inversely related to range. Targets are towns or cities, rather than specific buildings or point targets.
Type: Metal ramp, although boards or other surfaces could be used.
Number of Tubes: 1
Crew: 1-4 or more
Emplacement Time (min): 2-30 depending on configuration
Launch Rate: 1-5 minutes for launch salvo, one salvo per location

AMMUNITION
A Kassam rocket is made from available tubes with a variety of warheads. One source claimed that the Kassam or Kassam-1 is fired by a mortar. Propellant for the rocket is a locally blended formula, with sugar, oil, alcohol, and fertilizer. Rockets are hand-fabricated of steel tubes with welded fins in "workshops". A 120-mm Kassam-2 weighs about 11 kg, is 1.8 m in length, with 6-10 kg of warhead and a PD fuze. Above mixture yields a 3-m hole on impact.

Range is 4-6 km for Kassam-1 and 5-10 km for Kassam-2. It has been claimed that an extended range version (15-17 km), possibly Kassam-4 was successfully test launched. However, the increased range is expected to increase targeting error 200-300%.

SYSTEM: Anti-Iraqi Forces (AIFs) Fabricated Rocket Launchers.
Date of Introduction: 2004, examples date from earlier conflicts, with AIF distributing counter-US TTP from the Vietnamese War
Proliferation: AIFs have fabricated field-expedient 122mm rocket launchers using sheet metal in Al Anbar Province and are firing these rockets against US Bases in Ramadi.

Launcher: See launcher data noted at left. For other data needed for simulation of indirect fires, use 9P132/BM-21P (pg 6-36).

AMMUNITION
Caliber, Type, Name: The following are examples of widely disseminated rockets which can be used with improvised launchers.

68-mm SNEB French-designed aerial rocket HEAT, see pg 13-2
Range (m): <1aimed

68-mm SNEB French-designed aerial rocket Frag-HE, see pg 13-2
Range (m): 14 maximum

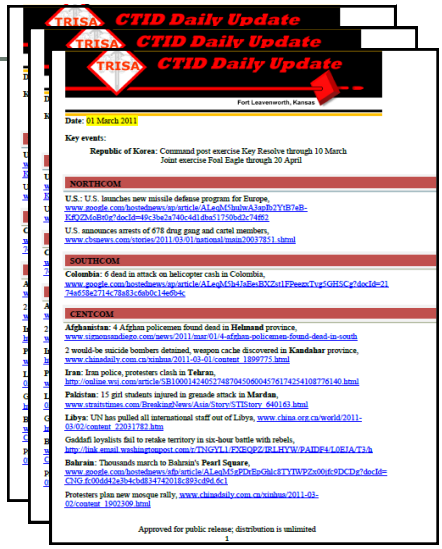
107-mm Frag-HE, Chinese Type 63 MRL rocket, see pg 6-37
Range (m): 8.1 km

122-mm Frag-HE, 9M22M (6-ft rocket, see pg 6-36)
Range (m): 0-10,800

122-mm Frag-HE, 9M22U (9-ft rocket, see pg 6-38)
Range (m): 0-20,380

NOTES Munition/warhead alternatives include: gun rounds, air-to-surface rockets, mortar rounds, RPG-7V grenades, C-4 , or improvised explosives.

MONTHLY WRAP-UP OF CTID DAILY UPDATES



CTID analysts produce a daily *CTID Daily Update* to help our readers focus on key current events and developments across the Army training community. Available on AKO, each *Daily Update* is organized topically across the Combatant Commands (COCOMs). This list highlights key updates during September 2012. The *Daily Update* is a research tool, and an article's inclusion in the *Update* does not reflect an official U.S. Government position on the topic. Also, CTID does not assume responsibility for the accuracy of each article.

NOTE: Due to operational requirements, the CTID Daily Update was published intermittently this month.

04Sep—**Social Media**: Tweeting jihadists: The next generation of militants

04Sep—**Colombiantry**: 'Godmother of Cocaine,' Griselda Blanco, gunned down in **Medellin**

05Sep—**Syria**: 44 insurgents killed in clashes with Syrian gov't troops in **Homs**

05Sep—**India**: India and America's growing partnership

06Sep—**Central African Republic**: Ugandan military closes in on senior LRA commander in CAR

06Sep—**Mali**: Mali rules out deployment of foreign troops into combat

07Sep—**Arctic Issues**: As sea ice fades, the Arctic becomes a nautical highway

07Sep—**Russia**: Thousand of Russian Soldiers are being killed and the Kremlin has no idea what to do

24Sep—**East China Sea**: China surveillance ships enter waters near disputed islands

24Sep—**Nigeria**: 35 suspected Boko Haram killed in **Damaturu** since Sunday: army

25Sep—**Yemen**: Oil pipeline in southeast Yemen bombed

25Sep—**Iran**: Iran test-fires missiles at target near U.S. naval drills

Disclaimer: CTID does not assume responsibility for the accuracy of each article shown on this page. Also, the views and opinions expressed in Red Diamond articles are those of the authors and do not necessarily reflect the official policy or position of any Department of Defense or government entity.

Director, CTID DSN: 552
Mr Jon Cleaves FAX: 2397
jon.s.cleaves.civ@mail.mil 913.684.7975

OE & OPFOR Doctrine & Training Lit.
Senior Analyst CTID: Dr Don Madill 684.7926
donald.l.madill.civ@mail.mil

OPFOR Doctrine Team
SME: Mr Rick McCall 684.7960
richard.g.mccall.civ@mail.mil

Intelligence Specialist
SME: Mr Kris Lechowicz 684.7922
kristin.d.lechowicz.civ@mail.mil

Intelligence Specialist
SME: Mr Jerry England 684.7934
jerry.j.england.civ@mail.mil

Worldwide Equipment Guide (WEG)
SME: Mr Tom Redman BAE 684.7925
thomas.w.redman.ctr@mail.mil

Threats Terrorism Team (T3) Integration
SME: Mr Jon Moilanen L3-MPRI 684.7928
jon.h.moilanen.ctr@mail.mil

Operational Environment Analysis
SME: Ms Penny Mellies 684.7920
penny.l.mellies.civ@mail.mil
SME: Angela Wilkins L3-MPRI 684.7929
angela.m.wilkins7.ctr@mail.mil

Training-Education-Leader Development
SME: Mr Walt Williams 684.7923
walter.l.williams112.civ@mail.mil

National Training Center - OPFOR
SME: LTC Terry Howard USAR 684.7939
terry.d.howard.mil@mail.mil

Joint Readiness Training Ctr - OPFOR
SME: Mr Marc Williams BAE 684.7943
james.m.williams257.ctr@mail.mil

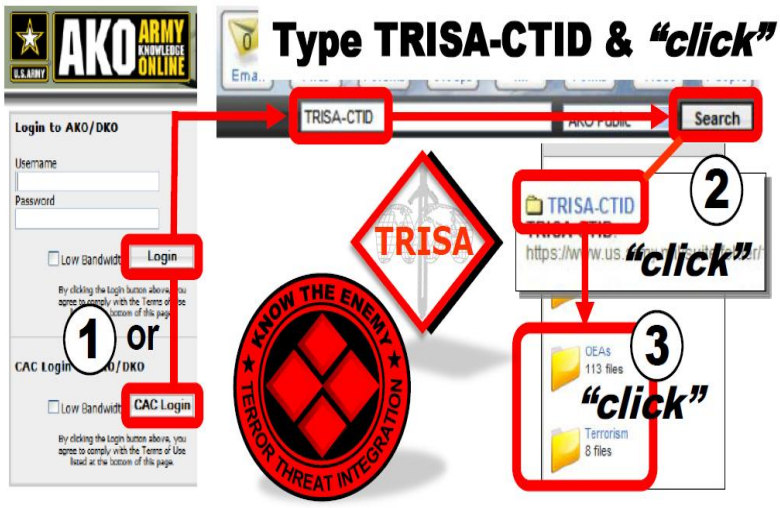
Joint Maneuver Readiness Ctr - OPFOR
SME: Mr Mike Spight BAE 684.7974
michael.g.spight.ctr@mail.mil

Mission Command Training Program - OPFOR
SME: Mr Pat Madden S3 Inc 684.7997
patrick.m.madden16.ctr@mail.mil

Threats Website-Support Operations
SME: Mr Charles Christianson 684.7984
charles.e.christianson.civ@mail.mil

YOUR Easy e-Access Resource

AKO *Three "Click"* Drill-Down



Find Your Topic – Do Your Research

What We Do for YOU

- ***Determine OE Conditions***
- ***Publish Operational Environment Assessments (OEAs)***
- ***Publish OE Threats in FSO***
- ***Publish Army OPFOR Doctrine***
- ***Assess Threat-Enemy & TTP***
- ***Support Terrorism Awareness***
- ***Produce the Decisive Action Training Environment (DATE—previously Full Spectrum Training Environment)***

All CTID products can be found on AKO. Check out all of our products at:
www.us.army.mil/suite/files/11318389