U.S. ARMY TRADOC G2 Intelligence Support Activity

TRISA

Red Diamond

Contemporary Operational Environment
and Threat Integration Directorate (CTID)

Fort Leavenworth, Kansas Volume 2, Issue 12 December 2011

INSIDE THIS ISSUE

This end-of-the-year issue features selected encore articles from 2011 Red Diamond *issues. Thanks to all our readers for spreading the word about our newsletter. Suggestions are always welcome. Happy holidays!*

INSURGENTS AND GUERRILLAS—THE HEART OF THE HYBRID THREAT

From the February 2011 Red Diamond*, learn about elements and examples of hybrid threats plus tactics for dealing with them.*

By Michael Spight, Training, Education, and Leadership Development Team

What is a hybrid threat? What does it typically consist of and what are its capabilities? According the *TC 7-100: Hybrid Threat,* a hybrid threat is the diverse and dynamic combination of regular forces, irregular forces, and/or criminal elements all unified to achieve mutually benefitting effects. A hybrid threat consists of at least two of the following five elements:

- A conventional regular force
- A professional military force or a force comprised of a professional cadre and conscripts
- A paramilitary forces (state police, internal security troops, border protection forces, etc.)
- Criminal elements
- Insurgent groups (typically rely on subversion and violent acts [terrorism] to force political change) and guerrilla units (irregular, homegrown forces operating in occupied territory, they may or may not be uniformed, organized, and equipped like a regular force)

In addition, TC 7-100 Hybrid Threat also defines insurgents and guerrillas:

- **Insurgents**: An insurgency is “the organized use of subversion and violence by a group or movement that seeks to overthrow or force change of a governing authority” (JP 3-24).
- **Guerrillas**: A guerrilla is “a combat participant in guerrilla warfare” (JP 1-02). Guerrilla warfare is “military and paramilitary operations conducted in enemy-held or hostile territory by irregular, predominantly indigenous forces” (JP 3.05.1).

History is replete with examples of active hybrid threats. Some of the more notable are:

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

- 1754 to 1763: regular British and French forces fought each other amidst irregular Colonialists fighting for the British and American Indians fighting for both sides.
- The American Civil War: Bloody Kansas (Quantrill and “Bloody Bill” Anderson).
- 1814: Peninsula War ended after the combination of regular and irregular allied forces from Britain, Portugal, and Spain prevented France from controlling the Iberian Peninsula.
- World War II: On the Eastern Front, Soviet partisans tied down approximately 10 Wehrmacht and Waffen SS divisions in the invading German Army’s rear areas. These units later took part in the Red Army’s counter offensive by supporting Red Army in conventional formations.
- 1954 to 1976: Viet Cong and People’s Army of Vietnam combined irregular and regular forces in fighting the French and U.S. forces. Viet Cong would organize into conventional and unconventional units.
- 2006: Hezbollah mixed conventional capabilities (such as anti-armor weapons, rockets, and command and control networks) with irregular tactics (including information warfare, non-uniformed combatants, and civilian shielding). The result was a tactical stalemate and strategic setback for Israel.

And the trend continues in Iran, North Korea, and China with each possessing robust conventional capabilities with a significant irregular capability.

We can expect any future adversary to be aware of the successes the hybrid threat, particularly irregular forces, have had against U.S. forces of the past 10 years. When competently led, irregular forces add an amazing level of complexity to the tactical problems BLUFOR must plan for and respond to on the battlefield.

> **Irregular forces add an amazing level of complexity to tactical problems that BLUFOR must plan for and respond to on the battlefield.**

This article will focus on insurgents and guerrillas (irregular forces as part of the OPFOR) and how Combat Training Centers (CTCs) can best replicate their capabilities against Rotational Training Unit (RTUs-BLUFOR) in a manner that supports conventional OPFOR formations and provides a real challenge for the RTU during a Full Spectrum Exercise (FSX).

Tactics

Although the hybrid threat may conduct strategic and operational level planning and operations, this article will focus on the tactical level and its practical application within scenario planning and execution at a CTC.

***INFOWAR*:** INFOWAR is a key weapon system that will be used with great skill by irregular force elements. Specifically, they will seek to degrade/deny BLUFOR communications capabilities and use specific incidents (injuries/deaths of civilians) to their advantage by leveraging the Internet, local, and international media sources. Additionally, capabilities to interfere with BLUFOR GPS-based systems or their IT systems are not outside the bounds of reality, and BLUFOR must be prepared for such attacks, as OPFOR’s irregular forces and conventional forces must be set to act if an opportunity presents itself.

***Systems Warfare*:** Irregular forces will attempt to locate, identify, isolate, attack and degrade/destroy BLUFOR critical systems. Critical systems consist of the primary system and associated sub-systems; it may be possible to degrade/destroy the ENTIRE critical system by merely attacking a key sub-systems rather than the system in its entirety. C4I, logistical nodes, and critical infrastructure being used by BLUFOR and/or the indigenous population, are examples of potential targets for irregular force elements.

***Functional Tactics (Action Functions vs. Enabling Functions)*:** The hybrid threat will utilize specific assets/capabilities it assesses as most capable of accomplishing a given mission against the BLUFOR. That asset or assets are known as the Action Element. If the mission is to conduct an attack, then the mission is performed by the attack element. If the mission is to conduct the main defensive effort, that mission would be performed by the main defense element. But, a force that supports the action element by conducting a separate operation in support of the action element is the enabling element. An example of this could be conduct of an operation in an area designed to draw the BLUFOR away to respond, thus leaving the area (the OPFOR’s actual objective) vulnerable to an OPFOR action element attack. Simultaneous (Enabling) functions by irregular forces—attacks on BLUFOR critical nodes, particularly logistical, C4I or indirect fire capabilities—will enable the hybrid threat’s conventional force as it conducts combat operations against BLUFOR infantry and armor units.

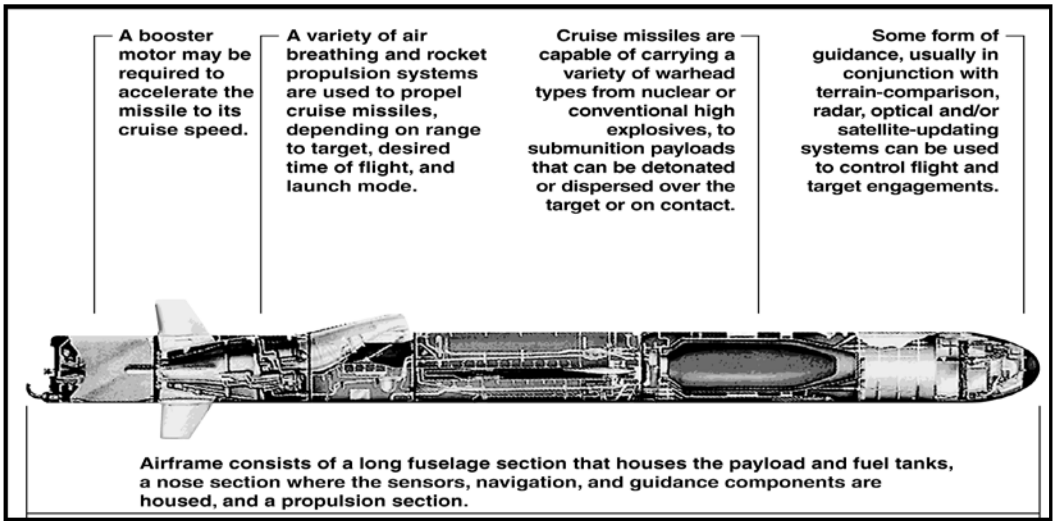
How can insurgents and guerrillas be most effectively replicated on a CTC? Focus on INFOWAR—this is a critical piece to ensuring OPFOR success, as seen in recent initial full spectrum operations (FSO) exercises at CTCs. The ability to leverage information to OPFOR or BLUFOR advantage, and to do so quickly and efficiently, thus forcing your opponent to react to the information you release is critical, and the importance cannot be overemphasized. ◆

THREATS TEAM: INTRODUCTION TO CRUISE MISSILES

This April 2011 Red Diamond summary highlights increasing use of this economical and accurate delivery system for these weapons, which are increasingly being used as land attack missiles.

By Kristin Lechowicz, OPFOR Doctrine Team

Many countries in the global arena, including potential threats to the US, are procuring cruise missiles (CMs) as an inexpensive alternative to ballistic missiles and aircraft. CMs are an economical and accurate delivery system that can be used for conventional, nuclear, chemical, and biological warheads. CM proliferation poses an increasing threat to U.S. national security interests. As the technology matures, both state actors and non-state actors are becoming increasingly able to acquire CMs and effectively employ such capabilities.


A booster motor may be required to accelerate the missile to its cruise speed.
A variety of air breathing and rocket propulsion systems are used to propel cruise missiles, depending on range to target, desired time of flight, and launch mode.
Cruise missiles are capable of carrying a variety of warhead types from nuclear or conventional high explosives, to submunition payloads that can be detonated or dispersed over the target or on contact.
Some form of guidance, usually in conjunction with terrain-comparison, radar, optical and/or satellite-updating systems can be used to control flight and target engagements.
Airframe consists of a long fuselage section that houses the payload and fuel tanks, a nose section where the sensors, navigation, and guidance components are housed, and a propulsion section.

This article—a follow-up to the article: Introduction to Theater Ballistic Missiles in the February 2011 *Red Diamond*—provides a basic introduction to CMs and these critical categories:

- What is a CM?
- What are the basic components?
- What are CM capabilities, ranges, and guidance system?

What is a CM?

Cruise missiles are basically unmanned, precision guided, subsonic weapons that are propelled by either rocket motors or jet engines. A CM assumes a non-ballistic flight path remaining within the atmosphere (air breathers), while ballistic missiles travel above the atmosphere. Modern CMs offer flexibility in payload and multiple launch configurations, including air, sea (surface and subsurface), and ground capabilities.

CM's small size (as opposed to most ballistic missiles), programmable delivery course, and low terrain-hugging capability make them an excellent delivery system and difficult to counter. The more modern CMs can take roundabout routes to engage their targets. CMs have the ability to circumvent known defenses and engage targets from suspected gaps in radar and surface-to-air missile coverage. The majority of CMs are anti-ship missiles, however, the new land attack missiles are becoming more sophisticated.

CM Basic Components

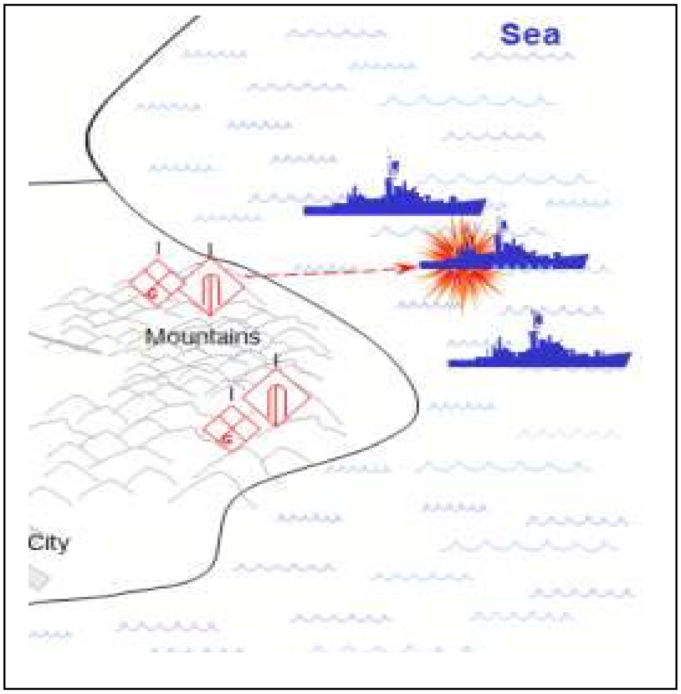
The four main components of CMs are a propulsion system, guidance and control system, airframe, and the payload. CMs are designed to have the booster rockets fall off after the fuel is depleted. After this action, the turbofan engine or jet engages and the tail fins, air inlet, and wings unfold. The diagram above breaks down and illustrates the main components of a typical turbo fan cruise missile. On target impact the missile explodes and it is destroyed.

CM Capabilities

CMs are relatively mobile and easy to conceal. Even after launch, most missiles can avoid detection by traveling at low altitude, under many radar horizons and using terrain masking until the CM reaches the target. Newer CMs present even greater challenges to aircraft and air defense assets by integrating stealth features that make them even less visible to radar and infrared sensors.

The OPFOR, or a real-world threat, could use CMs to target CONUS or OCONUS population centers, forward deployed military bases, naval assets, airfields and other fixed and mobile targets. The example on the next page shows the OPFOR using mountainous terrain>

to launch cruise (anti-ship) missiles at vessels. This example is similar to the attack that Hezbollah perpetrated against an Israeli corvette, INS Hanit, during the 2006 Lebanon war. The Israeli ship was heavily damaged and was rendered combat ineffective. This was the first time that a non-state actor had shown such a capability. The OPFOR could use CMs and the natural terrain as chokepoints to snare naval assets, logistics enablers, or targets of opportunity.



CM Ranges

The ranges of cruise missiles vary greatly from 50 miles (the French Exocet anti-ship missile) to 2,200 miles (the Russian AS-15 Kent). For naval assets, 50 miles would allow a naval ship to attack another vessel that would not be visible on the ocean horizon. In theory, a Russian AS-15 Kent has the range to be launched from Moscow and reach Tehran. Great disparity in missile ranges does not affect the weapon's lethality.

CM Guidance Systems

The overall sophistication of CMs has increased greatly with technological advancements. This is especially true with regard to guidance systems in the era of more capable Global Navigation Satellite Systems (GNSS) like GPS, Russian GLONASS, Chinese Beidou, and the European Galileo. These advanced guidance systems, in combination with autonomous onboard systems, have allowed CMs to become more accurate in acquiring targets. The basic CM guidance controls consist of one of four different systems that direct the missile to its target: Inertial Guidance System (IGS), Terrain Contour Matching (TERCOM), GNSS (GPS), and Digital Scene Matching Area Correlation (DSMAC). Most newer CMs use a combination of systems to provide redundancy and precision in a combat environment.

- IGS tracks detected acceleration via accelerometers from missile movement compared against a known first position, usually the launch position, to determine current location.
- TERCOM uses a radar that compares terrain features while in route to a pre-stored (loaded on the missile) 3-D mapped terrain database.
- GNSS, like GPS, uses satellites and an onboard GNSS receiver to verify the missile's position.
- DSMAC uses a camera and an image correlator to identify the target (good for use with moving targets).

Conclusion

As CMs become more sophisticated, their proliferation represents a clear and challenging threat to the U.S. The likelihood of these weapons falling into the hands of radical non-state actors was realized as witnessed by the 2006 Lebanon war. These weapons are viewed by many as reasonably economical, accurate delivery systems that can launch a number of different payloads, which provides a deep strike capability. The U.S. will likely face the challenging threat put forth by CMs in the future. ◆

OEA TEAM: MERCENARIES AS A TRAINING AID AND FUTURE COMBAT CHALLENGE

In this encore story from the June 2011 Red Diamond, find out how including mercenaries in training events can add both complexity and challenges for U.S. Army training events.

By Justin Lawlor, OEA Team

In a recent book by Parag Khanna, *How to Run the World*, the author suggests that the impending future global situation is not so much unprecedented as it is a return to the conditions of 12th century. Among the parallels to the 12th century will likely be a shift of military power from nation states to other actors within the strategic environment. As we have seen in the last decade, the U.S. Army must be ready not only to meet and defeat state actors, but non-state actors as well. Between the obvious state and non-state actors exists a third challenge, that of professional for-hire soldiers, or mercenaries. The rise of importance of mercenaries will present challenges on a variety of levels, and can potentially cause significant change to how the U.S. Army trains for operations in the future.

Mercenaries have been a fixture of warfare for practically the entire history of armed combat. Starting in the aftermath of the Thirty Years War (1618-1648) in Europe, international legal strictures on the use of mercenaries started to gather steam. As the force of international law became more universal, the acceptable use of mercenaries declined, though their existence continued, especially in more remote areas like Africa.

Recent events in Libya have highlighted the current and future roles of mercenaries because of their loyalty to the regime and willingness to operate aggressively against regime enemies.

Recent events in Libya have highlighted the current and future role of mercenaries. As the Libyan regime came under significant threat, its leader, Muammar Gaddafi, reportedly put out the call for foreigners to fight for his regime. This highlights the value of mercenaries or other foreign-sourced units for internal policing duties, due to their loyalty to the regime and willingness to operate aggressively against regime enemies.

Mercenaries are described in TRADOC Handbook 1.08, *Irregular Forces* using the Geneva Convention definition. The primary definitional element of mercenary is combatants who are not citizens of the nations involved in the conflict. This definition is itself somewhat problematic. First, the U.S. has been dealing with “foreign fighters” in Iraq and Afghanistan for nearly a decade. However, the vast majority of foreign fighters are overwhelmingly ideologically driven versus being economically motivated. As such, they fall outside common use of the term mercenary. Second, while the Geneva Convention definitions appear at first glance to be fairly descriptive, determining precise motive and sponsorship in specific cases can be difficult.

Past, Current, and Future Employment

Africa has long been the global epicenter for mercenary use. The combination of persistent conflict, demand for combat enablers, lack of international visibility of the conflict, and the general weakness of state actors set the conditions for the almost inevitable employment of mercenary actors. Unsurprisingly, a tour through the last 20 years of conflict in Africa shows Russian pilots manning combat aircraft in Sudan, Ethiopia, and Eritrea; Europeans in the Comoros, Equatorial Guinea, and Sierra Leone; and former South African National Defense Force serving even former adversaries in Angola.

Most recently, the wide-scale employment of mercenaries has been most obvious in Libya, as the Libyan regime seeks to strengthen its forces in its current civil war. Mercenaries—sourced from Africa and potentially Belarus, Serbia, and Russia - provide a combination of both poorly or untrained troops and elements of technically capable enablers. Similar reports of foreigners being employed as internal security forces are coming from the recent Iranian uprising and unrest in Syria, as well. It is likely that the grouping of conditions that drove Libyan, Iranian, and Syrian employment of mercenaries will be replicated as other regimes face similar challenges to their rule. For nations interested in discreet or economical intervention, mercenaries can be used as a deniable means of power projection or influence, especially for resource-constrained nations.

The current era of persistent global conflict demonstrates the increasing likelihood of U.S. forces encountering mercenaries in any potential OE. Understanding the complications of mercenary employment represents a new challenge for the Army training environment.

Training Implications

To completely replicate the growing dynamic nature of potential OEs, trainers can use mercenary enablers to >

provide fidelity and stress visiting units. Mercenaries can provide both low-end mass and high-end combat enablers to the opposing force (OPFOR), providing an OPFOR with the ability to meet U.S. units at parity in certain key elements:

Mercenaries add a highly variable component to the information environment of an OE—even if they're not in that specific OE.

- Politically, many nations have used mercenaries in the past as deniable forces to intervene in conflicts where it might be politically undesirable or impossible to do so. The engaging or handling of such individuals in the detainee environment could give interesting and nontraditional challenges to deploying and training units. Mercenaries are likely to be very loyal to the retaining nation, versus having loyalty to subnational elements like tribes or ethnic groups in an OE.
- Militarily, mercenaries with training and experience from militarily advanced nations can effectively and innovatively operate even basic or obsolete military equipment through a combination of training and experience. Mercenaries can provide the "software" to either effectively employ advanced Tier I capabilities, train local forces in the latest TTP, or innovatively employ even obsolete equipment in an effective fashion.
- Economically, the introduction of mercenaries can place unique burdens on an OE, through both expense to the retaining nation and the creation of economic incentives to the mercenary to continue fighting.
- Socially, mercenaries will likely be employed as they were in Iran and Libya, due to their lack of empathy with rebellious populations, and the lack of a social and political constituency, other the government, in the nation at war. Trainers should be attuned to the differences and similarities between mercenaries and foreign fighters as encountered in OIF and OEF.

In the information warfare (INFOWAR) realm, mercenaries from nations with advanced militaries are apt to be trained in the latest deception techniques, will provide insight into the most effective perception management efforts, and can offer effective information and computer attack capabilities. In the case of perception management and computer/information warfare, mercenaries do not even have to be in the specific OE to present tactical and operational impacts. Mercenaries can provide a highly variable component to the information environment of an OE, as their employment can render traditional Blue intelligence preparation of the battlefield (IPB) obsolete or difficult. Mercenary knowledge of other intelligence INFOWAR disciplines can effectively negate even advanced Army capabilities.

Conclusion

The introduction of mercenaries into training events has the potential to add complexity to our current training models. Mercenaries are a realistic, dynamic, and potentially capable threat. The current and expected future global economic conditions and their resultant effects on both state and individual finances are likely to inject more competencies into the international military marketplace, and make even the untrained more willing to fight for money and personal financial security. This complexity will require trainers and deploying units to be even more knowledgeable about the social, economic, and political variables of an OE, to include neighboring countries and regions critical for deploying forces. ◆

ULTRALIGHTS: IN USE ON OUR BORDER; CAN THEY BE USED IN COMBAT ZONES?

This July 2011 Red Diamond article considers the growing worldwide popularity of unmanned aerial vehicles and how they might become part of tomorrow's hybrid threat.

By Marc Williams, Training, Education, and Leadership Development Team

> Put simply, America's most likely and most lethal enemies for the foreseeable future are **adaptive, ruthless, networked, and committed**. These adversaries seek to foster conditions of fear, uncertainty, and instability. Ranging from violent extremist organizations to insurgencies to **criminal networks** and potent, adaptive mixes of each, these enemies are **unrestrained by international laws or norms of behavior and will flow to areas of vulnerability or weakness**.
>
> -Maj. Gen. David A. Morris, U.S. Army
> *Irregular Adversaries and Hybrid Threats, An Assessment-2011*

TC 7-100 *Hybrid Threat* defines a hybrid threat as "the diverse and dynamic combination of regular forces, irregular forces, and/or criminal elements all unified to achieve mutually benefitting effects." Most military training addresses the regular and irregular opponents the U.S. could face, but seldom replicates the criminal elements that could challenge our operations. Criminals operate with one primary objective: make money. And more is better. With such a motivation, the successful ones learn to operate as transparently as possible while implementing the latest technologies available.

The current situation on the U.S. southwest border has been called "America's third war" by some commentators. The criminal networks involved in wholesale drug smuggling, human trafficking, and illegal weapons transfer are well funded and operate with agility and adaptability. As the Customs and Border Patrol (CBP) intensifies its patrolling and surveillance activities, the criminals have resorted to numerous alternatives. Mexican drug trafficking organizations (DTO) have dug elaborate tunnels that employ electric lights and fresh air pumps. Some have captained pleasure and fishing boats and trained to avoid CBP patrols. The latest of these alternatives, which is increasing in use, is smuggling with light-sport aircraft, more commonly known as ultralights.

Ultralights are a popular choice for drug smugglers. The Department of Homeland Security reported 228 confirmed events involving ultralight aircraft in 2010 and 71 during the first four months of 2011.

The Federal Aviation Administration defines a light-sport aircraft as an aircraft with a maximum gross takeoff weight of not more than 1,320 pounds (600 kg) for aircraft not intended for operation on water; or 1,430 pounds (650 kg) for aircraft intended for operation on water; a maximum airspeed in level flight of 120 knots (220 km/h; 140 mph); a maximum stall speed of 45 knots (83 km/h; 52 mph); either one or two seats; fixed undercarriage and fixed-pitch or ground adjustable propeller; and a single electric motor or reciprocating engine, which includes diesel engines and Wankel engines. DTOs have gone so far as to put small motors on hang gliders.

Ultralights successfully fly under radar and evade most attempts to intercept them. These aircraft have been modified with all-terrain wheels for bumpy landings, extra seats removed to lower weight, and carry 150 to 250 pounds of drugs—depending on the weight of the pilot. Some are painted black and may have dark tarps covering the cargo, which is usually hanging in metal baskets attached to the bottom of the framing, to make for a stealthier landing or easier drops. CBP is working to procure a radar solution specifically designed to detect ultralight aircraft.

What began with a few flights in Arizona in 2008 is now common from Texas to California's Imperial Valley and, most recently, San Diego, where at least two ultralights suspected of carrying drugs were detected flying over Interstate 8. According to the Department of Homeland Security, during FY 2010 there were 228 confirmed events with ultralight aircraft, with 22 narcotics seizures, 12 arrests, and 5 ultralight aircraft seized. Seventy-one have been detected in this fiscal year through April, according to border authorities.

Incursions with ultralights have happened, with near-midair collisions and pursuits by CBP Blackhawk helicopters and USAF F-16 jet fighters. The trend has grown so much that Arizona Representative Gabrielle Giffords introduced legislation to stiffen penalties for criminal ultralight pilots (H.R. 5307-Ultralight Smuggling Prevention Act of 2010). Of course, not all pilots are successful. Numerous crashes take place as >

pilots receive minimal training, fly into wires and power lines, or simply land too hard.

Implications for Hybrid Threats

The implications of this technique are numerous in hybrid threat scenarios. Unmanned aerial vehicles (UAV) have become exceptionally popular worldwide and at our combat training centers. But there are times when an enemy will want to infiltrate Blue areas of operation with "eyes on." This could be with either expendable personnel to test Blue defenses or highly trained personnel as part of reconnaissance missions or for an infiltration attack. Ultralights can also be used to surreptitiously resupply small units without having to land and without alerting major air defenses as they move under the radar or through it with minimal signature. ◆

Ultralight crashes like this one are common as pilots receive minimal training, fly into wires and power lines, or simply land too hard (Photo courtesy of U.S. Customs and Border Protection).

THREATS TEAM: ORDERS OF BATTLE & THE DECISIVE ACTION TRAINING ENVIRONMENT

Initially printed in the July 2011 Red Diamond, this article focuses on how to use the Orders of Battle from the Decisive Action Training Environment (previously called the Full Spectrum Training Environment).

By Richard McCall, OPFOR Doctrine Team

This article is an extract from the Decisive Action Training Environment (previously called the Full Spectrum Training Environment) Introduction to Section 4: Orders of Battle. It provides simple instructions on how to select, use, develop, and apply OPFOR task organizations for combat for use in the DATE and other training environments.

Section 4: Orders of Battle is comprised of four appendices. Appendix A: Orders of Battle contains the administrative force orders of battle of Ariana, Atropia, Minaria, Gorgas, and Donovia. Organizational equipment tables of selected units are in an online version of Appendix B. Appendix C provides instructions on how to task organize OPFOR units for combat. Appendix D consists of the OPFOR equipment tier tables from the Worldwide Equipment Guide (WEG).

All five countries of the DATE/FSTE have an administrative force structure (AFS) to manage their military forces in peacetime. This AFS is the aggregate of various military headquarters, facilities, and installations designed to man, train, equip, and sustain the forces. In peacetime, forces are commonly grouped into divisions, corps, or armies for administrative purposes. The AFS includes all components of the Armed Forces—not only regular, standing forces (active component), but also reserve and militia forces (reserve component). Normally, these administrative groupings differ from the country's go-to-war (fighting) force structure which are task-organized to meet the combat situation. Organizations not contained in Appendix A or those units lower than brigade level can be found in FM 7-100.4, Opposing Force Organization Guide, Administrative Force Structure, Volumes I thru IV. [***Note 1.*** All of the OPFOR organizations listed in the AFS organizational directories are constructed using Microsoft Office® software (MS Word®, MS PowerPoint®, and MS Excel®). The use of these commonly available tools should allow trainers and planners to tailor and/or task-organize units individually or collectively to meet specific training and/or simulation requirements.]

You can download the updated Decisive Action Training Environment (formerly the Full Spectrum Training Environment) on AKO.

Appendix B: Organizational Equipment Tables, contains select tables of equipment by type and echelon of organization. Each unit contains a comprehensive detailed listing of organizations, personnel (by officer, NCO, and enlisted), and equipment (by nomenclature) of its subordinate units in an MS Excel® chart. Totals are also provided by parent and subordinate unit. Equipment in FM 7-100.4 is Tier 2. However, it can be easily modified to represent any tier necessary for training. As time permits, example Tier 1 and Tier 3 tables will be added. Detailed information on individual items of equipment can be found in the Worldwide Equipment Guide (WEG), Volumes I through III.

[Note 2. OPFOR equipment is broken into four tiers in order to portray systems for adversaries with varying levels of ability. The tier tables provide a convenient means for military trainers to replicate the OPFOR's equipment capability. Tier 2 (default OPFOR level) reflects modern competitive systems fielded in significant numbers for the last 10 to 20 years. See the WEG Vol 1, Chap 15 and Vol II, Chap 7 for additional information.]

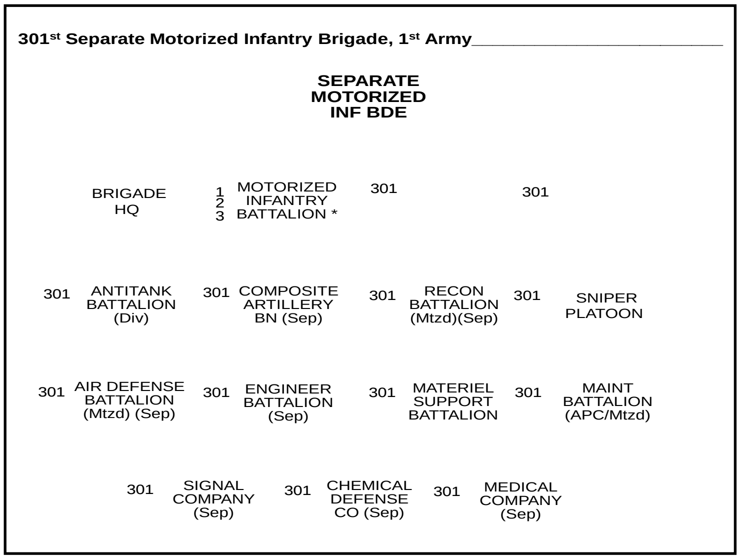
Appendix C: OPFOR Task-Organizing for Combat, describes how each of the five countries must task organize its forces from their AFS into the appropriate war-fighting orders of battle (ground, air, and naval). In order to properly task-organize, senior OPFOR commanders of each country will analyze their own strengths and weaknesses as well as those of their enemies. They will also consider how best to counter or mitigate what the enemy has (or it's capabilities) and/or how to best exploit their own advantage(s).

The mitigation or exploitation may be by means of equipment, tactics, or organization—or more likely all of these. However, the process generally starts with the proper task organization of forces with the proper equipment to facilitate appropriate tactics, techniques, and procedures**. OPFOR commanders must consider where the assets required for a particular task organization are located within the AFS and how to get them allocated to the task organization that needs them, when and where the assets are needed**. >

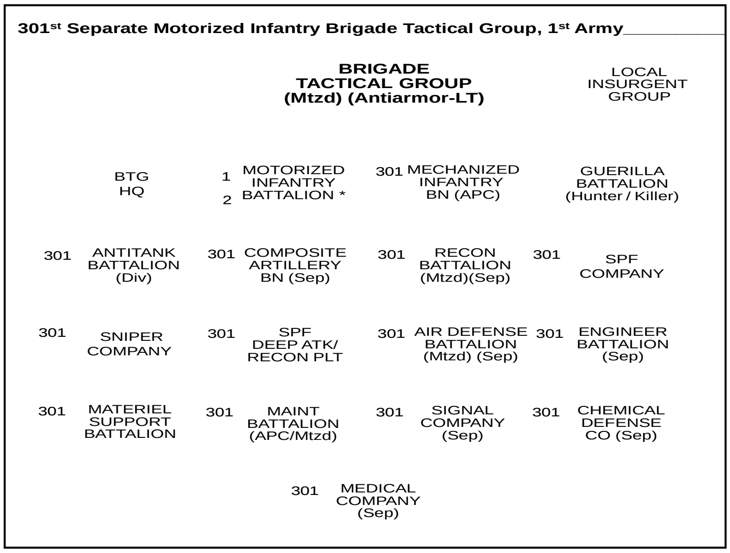
ORDERS OF BATTLE AND THE DECISIVE ACTION TRAINING ENVIRONMENT *(continued)*

Detailed information on task-organizing OPFOR units to meet U.S. training requirements and METL can be found in FM 7-100.4, Chapter 2, and FM 7-100.4, Appendix B. Also see TC 7-101, Exercise Design, for assistance in designing and executing a training exercise and producing an OE that achieves desired unit training objectives while fielding a challenging OPFOR consistent with Hybrid Threat OPFOR doctrine as described in the TC 7-100 series. Appendix D: divides the OPFOR's equipment into four Tiers in order to portray threat systems for adversaries with varying levels of ability. The tier tables provide a convenient means for military trainers to replicate the OPFOR's equipment capability. The tables also provide the U.S. military's training community with an instrument to create a flexible and challenging technological threat in an ever-changing operational environment.

The following examples illustrate the conversion of the 301st Separate Motorized Infantry Brigade, 1st Army of Ariana (AFS) into the 301st Separate Motorized Infantry Brigade Tactical Group (BTG) (task organized for combat). The red highlights AFS units in the 301st not applicable to impending combat operations and are therefore either removed or replaced in the conversion to the BTG. The yellow in the BTG shows gained organizations/capabilities needed to successfully complete the combat. ◆


301st Separate Motorized Infantry Brigade, 1st Army
SEPARATE MOTORIZED INF BDE
BRIGADE HQ
1 2 3
MOTORIZED INFANTRY BATTALION *
301
301
301 ANTITANK BATTALION (Div)
301 COMPOSITE ARTILLERY BN (Sep)
301 RECON BATTALION (Mtzd)(Sep)
301 SNIPER PLATOON
301 AIR DEFENSE BATTALION (Mtzd) (Sep)
301 ENGINEER BATTALION (Sep)
301 MATERIEL SUPPORT BATTALION
301 MAINT BATTALION (APC/Mtzd)
301 SIGNAL COMPANY (Sep)
301 CHEMICAL DEFENSE CO (Sep)
301 MEDICAL COMPANY (Sep)

Admin Force Structure: Separate Motorized Infantry Brigade


301st Separate Motorized Infantry Brigade Tactical Group, 1st Army
BRIGADE TACTICAL GROUP (Mtzd) (Antiarmor-LT)
LOCAL INSURGENT GROUP
BTG HQ
1 2
MOTORIZED INFANTRY BATTALION *
301 MECHANIZED INFANTRY BN (APC)
GUERILLA BATTALION (Hunter / Killer)
301 ANTITANK BATTALION (Div)
301 COMPOSITE ARTILLERY BN (Sep)
301 RECON BATTALION (Mtzd)(Sep)
301 SPF COMPANY
301 SNIPER COMPANY
301 SPF DEEP ATK/ RECON PLT
301 AIR DEFENSE BATTALION (Mtzd) (Sep)
301 ENGINEER BATTALION (Sep)
301 MATERIEL SUPPORT BATTALION
301 MAINT BATTALION (APC/Mtzd)
301 SIGNAL COMPANY (Sep)
301 CHEMICAL DEFENSE CO (Sep)
301 MEDICAL COMPANY (Sep)

Task Organized for Combat: Brigade Tactical Group

OEA TEAM: REVISING TALIBAN ATTACKS IN KANDAHAR, SPRING 2011

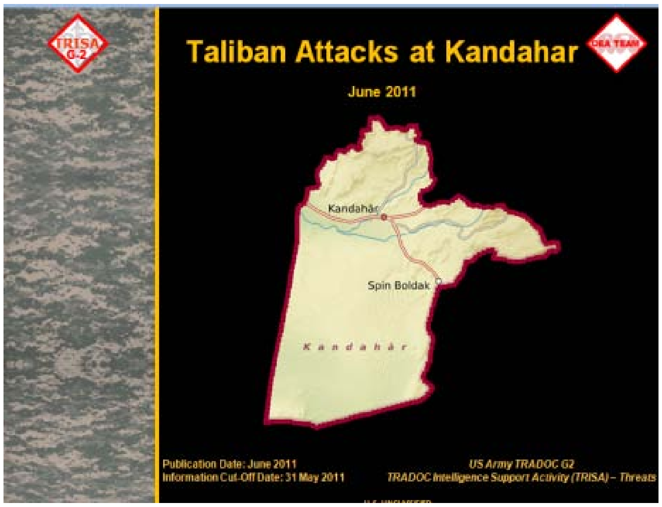
This summary from the July 2011 Red Diamond revisits the details of recent attacks in Kandahar.

By Angela Wilkins, OEA Team

This spring the Taliban launched aggressive attacks in Afghanistan, as Coalition forces predicted. Although attacks were expected, it was not known how the attacks would play out until they occurred. The Taliban's attacks during the spring months demonstrated multiple weapons and tactics for each show of aggression. The OEA Team threat report, *Taliban Attacks at Kandahar*, details the nature and motivation of the spring attacks.

Multiple attacks occurred throughout Kandahar province beginning in February, with the primary targets typically police buildings and other government locations. The majority of the casualties that stemmed from these attacks were Afghan police. Clearly, the Taliban's goal was to demonstrate their strength over the local police. On all occasions, though, the Afghan police, sometimes with limited assistance from U.S. and other forces, stymied the attackers, often killing or capturing all of them within a matter of hours. Although a goal of the Taliban was to demonstrate that local security forces, in the wake of dwindling support by other Coalition forces, would be unable to successfully thwart the attacks, the relatively low casualty numbers refuted that goal. For instance, an attack in February resulted in 19 people killed (only 2 civilians), and an April attack left 6 people dead (all Afghan police). An incident in April aided the Taliban in massing larger numbers of attackers, though, which did in fact allow them to conduct numerous attacks throughout the city of Kandahar in May. On 24 April, around 500 prisoners escaped from Kandahar prison through a tunnel that took five months to dig. The escape took an estimated five hours, and included numerous Taliban field commanders. Analysts assert those commanders played an important role in the Kandahar attacks in May.

Although the timing of Osama bin Laden's death caused speculation that these attacks were retributive in nature, the Taliban claimed that was not the case.



Taliban Attacks at Kandahar

June 2011

Publication Date: June 2011
Information Cut-Off Date: 31 May 2011

US Army TRADOC G2
TRADOC Intelligence Support Activity (TRISA) – Threats

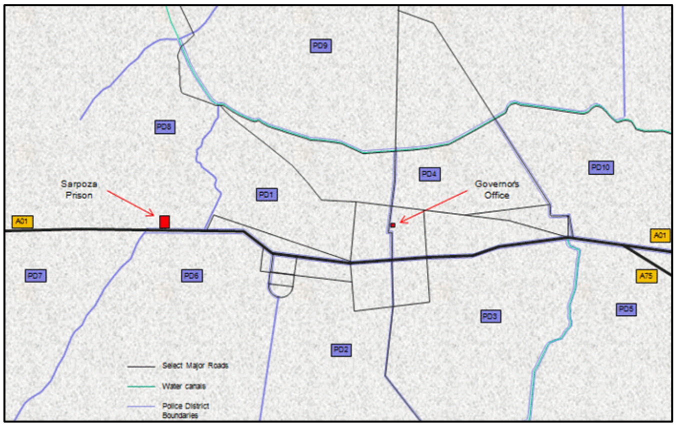
The serious, two-day-long attack on 7 and 8 May showed considerable planning on the part of the Taliban. Multiple attacks occurred at critical sites throughout the city, such as the governor's (Tooryalai Wesa's) compound, police stations, and the National Directorate of Security (NDS) office, among others. Taliban operatives managed to get close to such installations by dressing as security guards and taking over nearby buildings, such as a hotel close to the governor's compound. The weapons used were hand grenades, machine guns, vehicle borne improvised explosive devices (VBIEDs), and suicide vests. An effective part of the Taliban's strategy was to attack multiple locations at once, causing Afghan security forces to spread thin in response. An estimated 50 or more Taliban operatives killed approximately six people, only one or two of whom were civilians, and wounded dozens. By the end of the event, NATO claimed that all attackers were killed or captured.

Although the timing of Osama bin Laden's death caused speculation that these attacks were retributive in nature, the Taliban claimed that was not the case. Indeed, even Coalition forces acknowledged that the Kandahar attacks had likely been in the planning stages long before bin Laden was found and killed. Nonetheless, the Taliban capitalized on OBL's death as a means of motivation for their followers, stating, "The martyrdom of Sheik Osama bin Laden will give a new impetus to the current jihad against the invaders. The forthcoming time will prove this both for the friends and the foes." >

REVISITING TALIBAN ATTACKS IN KANDAHAR, SPRING 2011 *(continued)*

Despite the obvious planning on the part of the Taliban, U.S. and Coalition force leaders assessed the local Afghan forces' response as satisfactory, and the Taliban's ability to meet its goals as weak. ANSF, with only minimal support from Coalition forces in the form of perimeter security, stopped several VBIEDs, and limited the duration of the attacks to 36 hours. This is not to say that the Taliban's show of force was weak, though. The disruption caused throughout the city increased the level of fear and concern for local Afghan citizens, and that effect alone is significant. Additionally, the Taliban continued with attacks in Kandahar and several other areas of the country throughout May, relentlessly attacking every few days with the police, hospitals, and construction sites as primary targets.

The *Taliban Attacks at Kandahar* threat report provides information to deploying units, trainers, and scenario developers of the Taliban's recent attacks in Kandahar and surrounding areas. It portrays the Taliban's TTP and motivation in execution of the attacks, and discusses the related events both before and after the main attack in Kandahar. ◆



City of Kandahar, governor's office and Sarpoza Prison

A must-read for military and security experts...
Foreign Military Studies Office
OPERATIONAL ENVIRONMENT WATCH
This Edition: A special look at "Information" in the OE
Foreign News & Perspectives
IN THIS ISSUE

OEA TEAM: HANDBOOK, INTEL HELP MINIMIZE INSIDER THREAT

This article from the October 2011 Red Diamond highlights the growing concern surrounding insider attacks against U.S. forces in Afghanistan. The Center for Army Lessons Learned (CALL) is using this publication in its forthcoming Insiders Threat Handbook.

By H. David Pendleton, OEA Team

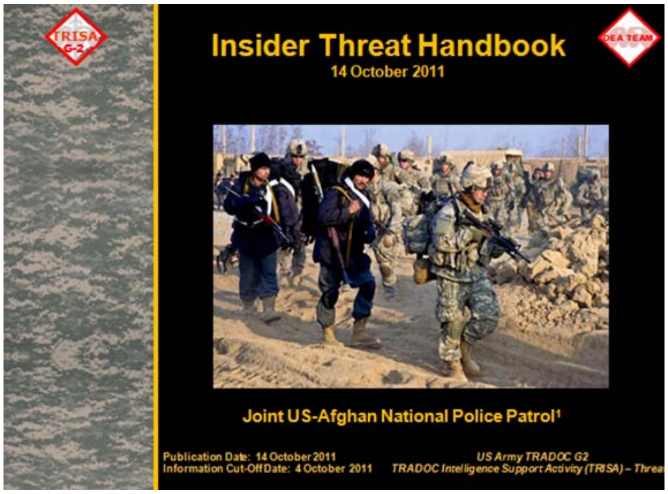
At least 34 cases of "insider" attacks against International Security Assistance Force (ISAF) soldiers by Afghan National Security Force (ANSF) personnel have taken place over the last five years. In April 2011, the number of attacks, also known as "green on blue" attacks, rose so rapidly that the ISAF Commander directed that a Red Team political and military behavioral scientist conduct a study to determine any commonalities between the attacks and possible means to identify attackers before they strike. Additional details of the insider threat can be found in the *Insider Threat Handbook* recently published by the TRISA-Threats OEA Team.

While the Taliban continues to claim that their agents successfully infiltrated both the Afghan National Police (ANP) and the Afghan National Army (ANA) with the sole purpose of launching these attacks, the evidence does not support the claim. In fact, at the time of the study's completion in May 2011, investigators could not find one valid case where a Taliban member infiltrated the ANSF to launch an attack. Almost half of the attacks occurred in only three of Afghanistan's provinces: Helmand, Kabul, and Kandahar. Many of the other provinces did not contain a single green on blue incident.

Of the five broad categories, disgruntled ANSF members or individuals who recently faced a personal disagreement with an ISAF soldier accounted for 40% of all the attacks studied. About 15% of the attacks were by an ANSF member co-opted by the Taliban through threats against the individual or his family, blackmail, or bribery. Taliban members who disguised themselves as ANP officers or ANA soldiers accounted for about 10% of the attacks. In about 35% of the attacks, the evidence could not substantiate the exact reasons for the attack. Prior to 12 May 2011, investigators could not attribute even a single insider attack to a Taliban who infiltrated into the ANSF.

Disgruntled Afghan National Security Force members or individuals who recently faced a personal disagreement with an International Security Assistance Force soldier accounted for 40% of all the attacks studied.

Despite the lack of evidence of Taliban infiltration, the ANSF implemented a more stringent screening process for all Afghans who wish to join an ANSF unit.


Insider Threat Handbook
14 October 2011

Joint US-Afghan National Police Patrol[1]

Publication Date: 14 October 2011
Information Cut-Off Date: 4 October 2011

US Army TRADOC G2
TRADOC Intelligence Support Activity (TRISA) – Threa

First, a village elder, mullah, or government official must vouch for the ANSF applicant. Second, the recruit must submit to a recording of his basic biometric information: retinal scan, fingerprinting, height, weight, and age. Third, the ANSF compares the information against the available databases of known insurgents. As another preventative measure, the ANA almost doubled the size of its counter-intelligence (CI) forces to 478 in the past year, with over 73% of the Afghan CI personnel having received ISAF or NATO training.

Even though the Taliban made erroneous claims for many of the attacks, the insurgents may increase their ANSF infiltration efforts for several reasons. First, the Taliban may no longer possess the strength and capability to directly confront ISAF forces or the increasingly capable ANSF units. Second, the Taliban may hope insider attacks initiate an INFOWAR campaign demonstrating that foreigners possess no safe havens anywhere in Afghanistan while the insider attacks sow mistrust between ISAF soldiers and the ANSF personnel they train. Third, green on blue attacks offer a cheap and effective method for the Taliban to target senior ISAF or ANSF leaders. Lastly, the imperative for the ANSF to increase its size by over 141,000 personnel by 2014 may allow the Taliban more opportunities to infiltrate if the ANSF lowers its vigilance.

OEA Team: Handbook, Other Intel Help Minimize Insider Threat *(continued)*

Many of the insider attacks occurred because of an actual or perceived slight by an ANSF member against an ISAF soldier, often based on a lack of cultural understanding by both sides. Jeffrey Bordin, the social scientist who conducted the study, discovered nine complaints that came from more than 50% of the various ANSF focus groups he surveyed. More culturally-sensitive ISAF members may reduce the number of ANSF complaints against ISAF soldiers. The top nine complaints included the use of ISAF personnel to conduct night raids instead of ANSF members; ISAF soldiers not respecting the privacy of Afghan females; ISAF setting up needless roadblocks that slowed traffic; ISAF not allowing any vehicles to pass slow-moving convoys, to include ANSF vehicles; ISAF members shooting indiscriminately in firefights; ISAF personnel causing too many "accidental" civilian and ANSF casualties; ISAF personnel cursing constantly; ISAF soldiers exhibiting extreme arrogance and refusing to heed any ANSF advice; and ISAF personnel humiliating ANSF personnel by searching ANA and ANP in public as the Afghan units entered a joint base.

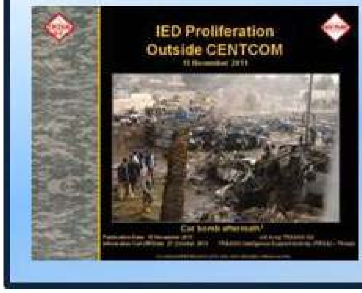
Actual or perceived slights as well as cultural sensitivities can increase the likelihood of insider attacks. Training to understand cultural differences can help minimize such attacks.

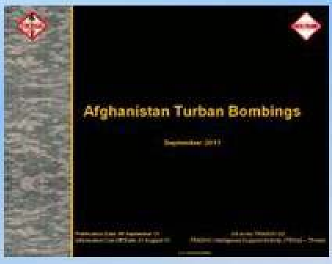
While Bordin made 58 recommendations in his study, most of these fall into one of five broad categories. First, ISAF personnel need to understand the cultural differences between the Afghans and themselves in an effort to stop or reduce the number of things they do that the Afghans find offensive. Second, ISAF needs to plan ahead to eliminate or at least mediate those actions ISAF must do for force protection reasons that go against Afghan cultural norms. Third, both ANSF and ISAF must receive training about the other's culture in order to gain more mutual respect for their differences. Fourth, ISAF members need to build bridges between the ANSF and themselves, not walls. Lastly, improved communication between ISAF and ANSF personnel would eliminate much of the anger, frustration, and disrespect for the other side.

While difficult, the Asymmetrical Warfare Group (AWG) has developed three categories of possible observable indicators for ISAF personnel and actions to take in each case. If an ISAF soldier observes category I actions by an ANSF member, the ISAF soldier needs to closely monitor the situation. If the actions become category II, the ANSF member should receive counseling and/or have his name passed onto the appropriate counterintelligence (CI) agency. Any ISAF member who observes category II actions by an ANSF member needs to take immediate action to refer the individual to the chain of command and CI personnel, take the ANSF member's weapon away, and even possibly detain the individual. The AWG also developed a force protection decision matrix and recommended actions if an ANSF member's actions label him a potential, moderate, high, or extreme risk as a possible insider attacker.

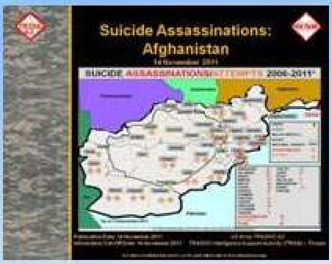
The available evidence indicates that few commonalities exist between the insider attacks over the last five years in Afghanistan. While the Taliban may claim responsibility for the attacks, most of the green on blue attacks occurred after a confrontation between an ANSF and ISAF member. Many of the disagreements occurred because of lack of cultural understanding by both sides, but often the ISAF soldier either finds himself ignorant of the Afghan lifestyle or refuses to modify his own cultural norms as a sign of respect for the other side. A two-track approach of vigilance by ISAF members for the observable indicators and the improvement of trust between both sides will most likely serve as the best way to prevent future insider attacks by ANSF personnel. ◆

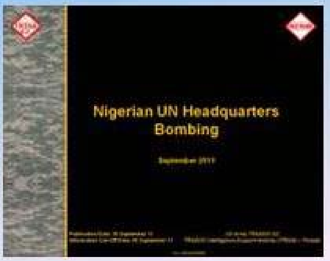
More TRISA-CTID threat reports at **www.us.army.mil/suite/files/25549573**


IED Proliferation Outside CENTCOM


Afghanistan Turban Bombings

September 2011


Suicide Assassinations: Afghanistan


Nigerian UN Headquarters Bombing

September 2011

THREATS TEAM: ELEMENTS OF AN INSURGENT ANTITANK AMBUSH

From the October 2011 Red Diamond, learn how these attacks work so you can help decrease the likelihood that your unit will become a target.

By Jon Moilanen, OPFOR Doctrine Team

Functional Organization of Elements to Conduct an Antitank Ambush

An *ambush* is a surprise attack from a concealed position, used against moving or temporarily halted targets. In an ambush, enemy action determines the time of attack, and the Opposing Force (OPFOR) chooses the place of attack. This example of an OPFOR antitank grenade launcher (ATGL) ambush has three elements:

- **Ambush element.** The assault element is comprised of a RPG-7V grenadier/cell leader.
- **Security elements.** Two security elements, each armed with automatic weapons, provide early warning of any approaching enemy forces. They protect the ambush element.
- **Support element.** The ammunition bearer/assistant grenadier remains near the grenadier, and is a videographer to record and transfer the audio and video coverage to an insurgent INFOWAR cell.

Background Situation

This example of an antitank (AT) ambush by an OPFOR insurgent organization uses the RPG-7V ATGL with the significant tank-killing capability of a 105-mm high-explosive antitank (HEAT) warhead. (See Chapter 1 of TRADOC G2 *Worldwide Equipment Guide, Volume I* for more information on infantry antitank weapon systems.)

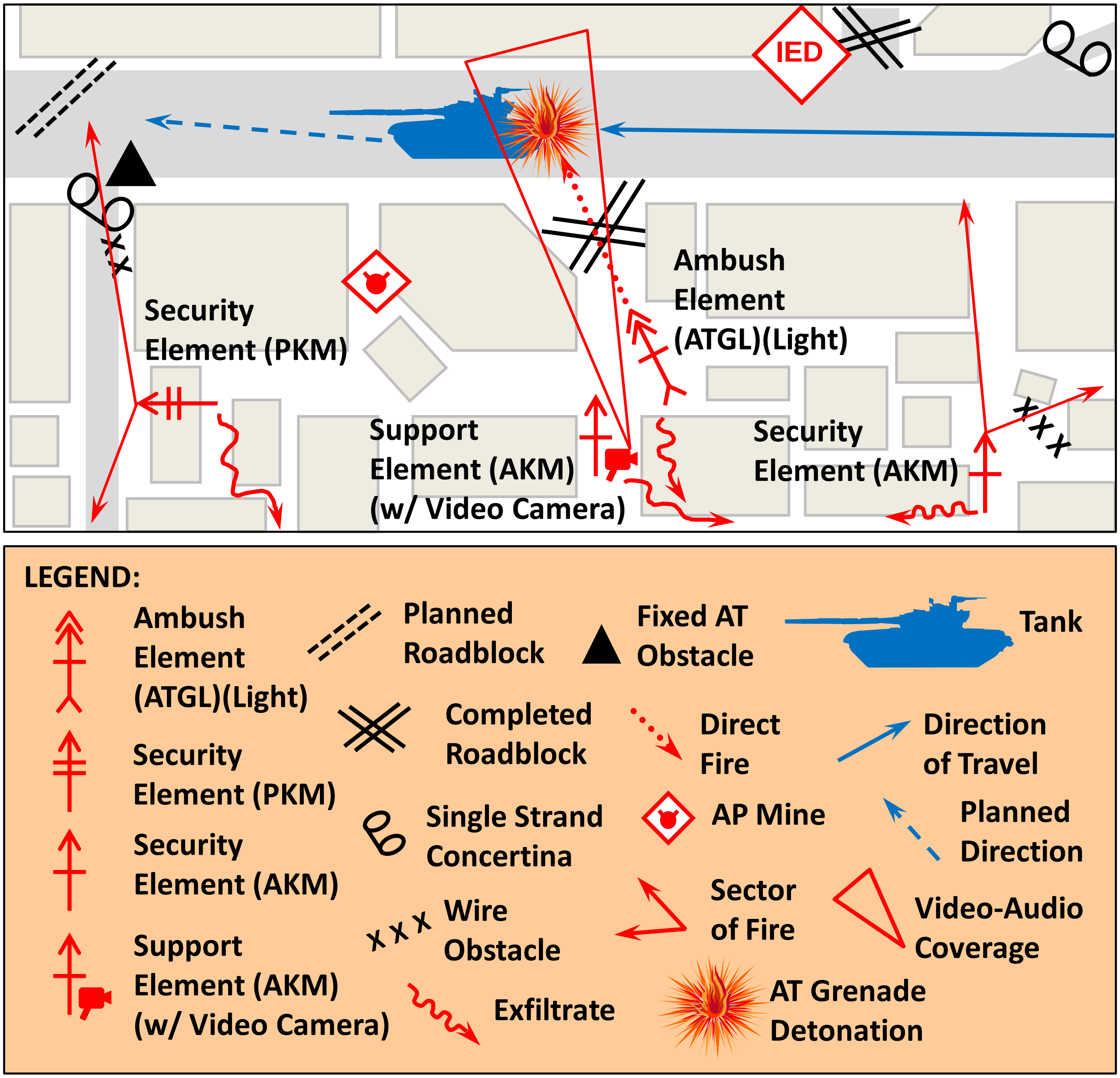
The enemy enters the network of streets and buildings. The local insurgent organization has already assigned neighborhoods as defensive areas to subordinate insurgent leaders. A direct action cell occupies an ambush position that is integrated with other direct action cells in the urban neighborhood. This cell example is one ATGL grenadier, an ammunition bearer/assistant grenadier, an insurgent with a PKM machinegun, and an insurgent with an AKM assault rifle. Obstacles channel the enemy into kill zones. Attacks separate enemy infantry from supporting armored vehicles. Insurgents command detonate improvised explosive devices (IED) to block streets with rubble and prevent any withdrawal of enemy columns. A number of other insurgents in basements, ground level positions, and rooms or rooftops of surrounding buildings coordinate for simultaneous attacks on the enemy. The cell leaders use cellular telephones to maintain situational awareness of friendly forces and the enemy. >

As part of an antitank ambush, insurgents often detonate IEDs to block streets with rubble and prevent withdrawal of enemy columns.

Insurgent's view in an RPG-7V ambush (example)

The RPG-7V Ambush on a Tank

The insurgent AT ambush is ready. The cell leader monitors reports from other cells to the local insurgent leader. A “keyhole” firing position conceals the ATGL grenadier from being observed. Security elements emplace hasty obstacles to slow and channel any dismounted enemy approach. A wire obstacle and camouflaged antipersonnel mine support early warning along an approach that cannot be observed by either security element. The videographer prepares to record the attack and remain clear of the back blast area of the ATGL. The cell leader receives a report that one tank has escaped a nearby ambush and is headed toward his kill zone. ◆



RPG-7V antitank ambush (example)

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

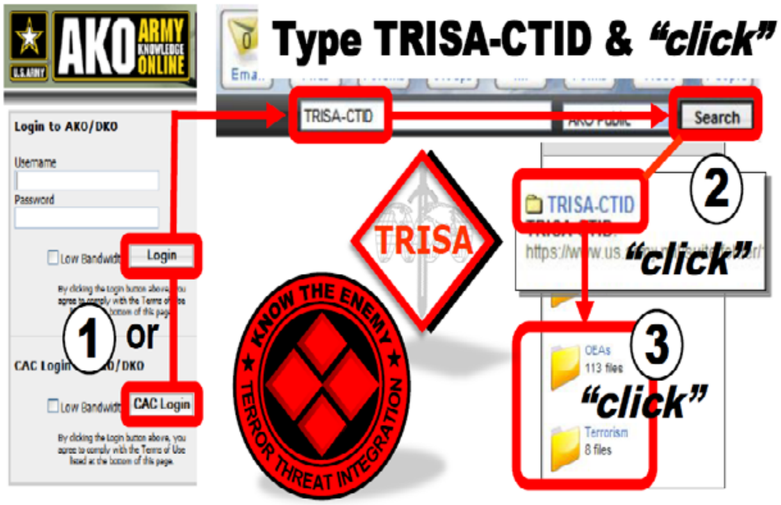
Joint Maneuver Readiness Ctr - OPFOR
SME: Mr Mike Spight BAE 684.7974
michael.g.spight.ctr@mail.mil

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

Disclaimer: 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 Army or government entity.