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 7 July 2011

Orders of Battle and the Full Spectrum Training Environment

by Richard McCall

This article is an extract from the *Full Spectrum Training Environment (FSTE)*, 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 FSTE 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. The Donovian orders of battle are currently under construction and will be added to the FSTE when available. 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 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.]

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.

NEWSLETTER DISTRIBUTION UNLIMITED

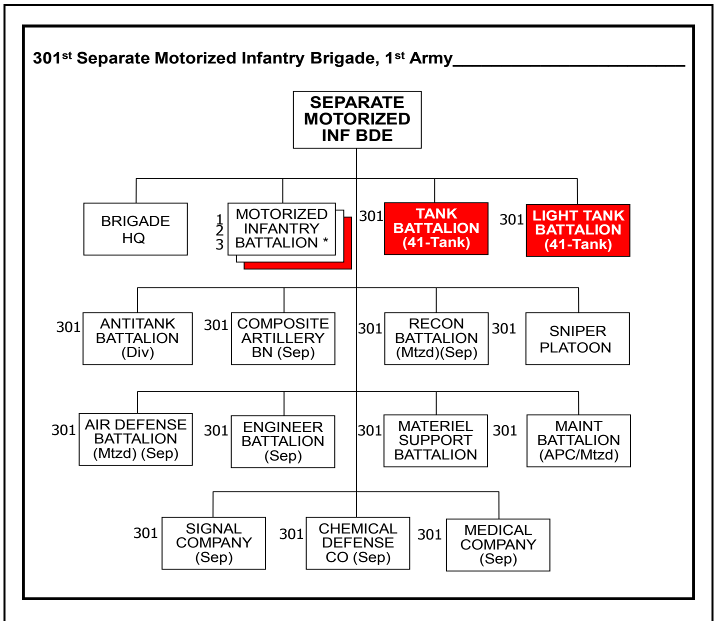
[Note 2. OPFOR equipment is broken into four tiers in order to portray systems for adversaries with varying levels of ability. The tier tables provide a convenient means for military trainers to replicate the OPFOR's equipment capability. Tier 2 (default OPFOR level) reflects modern competitive systems 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-Organizating 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).

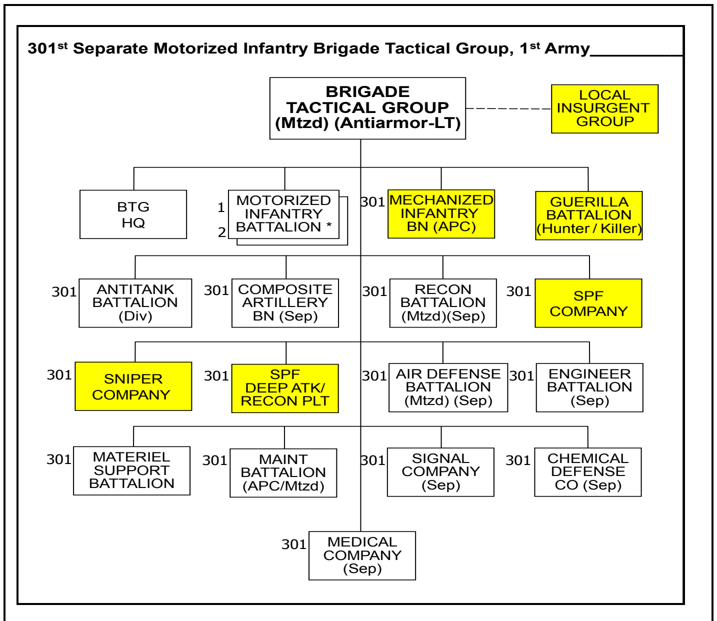
The mitigation or exploitation may be by means of equipment, tactics, or organization—or more likely all of these. However, the process generally starts with the proper task organization of forces with the proper equipment to facilitate appropriate tactics, techniques, and procedures**. OPFOR commanders 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**.

Detailed information on task-organizing OPFOR units to meet US 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 US 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 mission.


301st Separate Motorized Infantry Brigade, 1st Army
SEPARATE MOTORIZED INF BDE
BRIGADE HQ
1 2 3 MOTORIZED INFANTRY BATTALION *
301 TANK BATTALION (41-Tank)
301 LIGHT TANK BATTALION (41-Tank)
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.

Ultralights: In Use on Our Border; Can They Be Used in Combat Zones?

by Marc Williams

> *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**.*
>
> -MG David A. Morris, USA
> *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 US 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 US 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.

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.

Training and Education Team

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.

Crash site. (Photo courtesy of US Customs and Border Protection).

Implications for Hybrid Threats

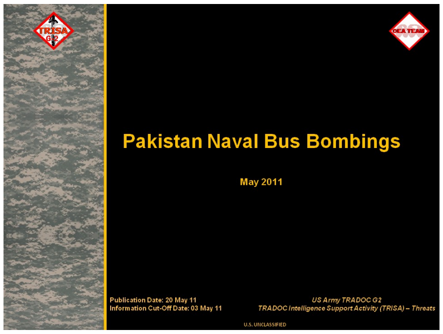
The implications of this technique are numerous in hybrid threat scenarios. Unmanned aerial vehicles (UAV) have become exceptionally popular worldwide and at our combat training centers. But there are times when an enemy will want to infiltrate Blue areas of operation with “eyes on.” This could be with 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.

OEA Team

Pakistan Naval Bus Bombings

by Laura Deatrick

Karachi is a city of major importance in Pakistan. The former capital is both Pakistan's largest city and the economic capital of the country. A seaport town, Karachi contains numerous military installations such as the Pakistani Navy's main base. It is also the chosen location for recent insurgent attacks in the form of bombings against naval busses. *Pakistan Naval Bus Bombings*, a new OEA Team threat report, examines these attacks in detail.



Pakistan Naval Bus Bombings

May 2011

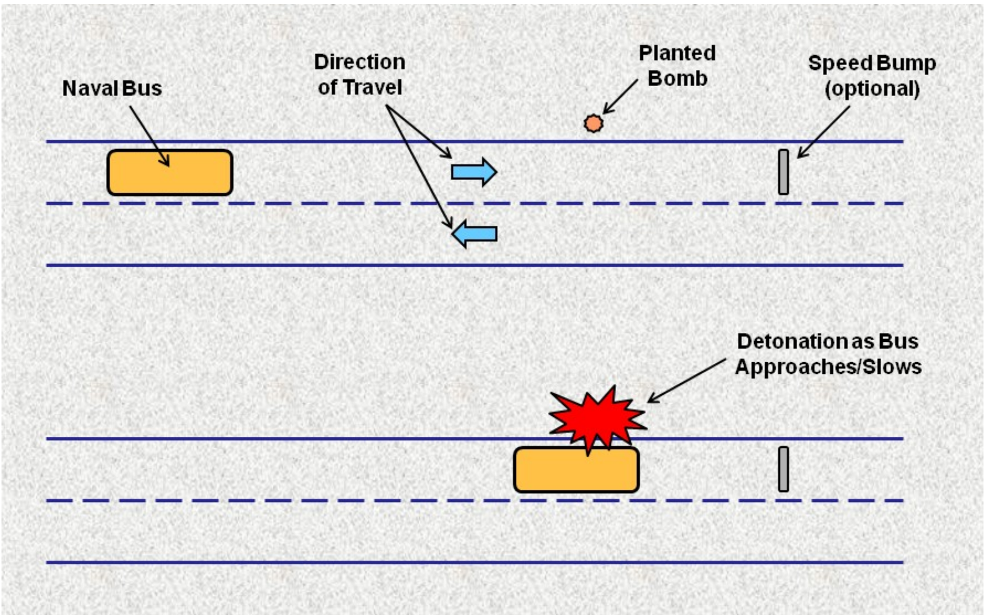
Publication Date: 20 May 11
Information Cut-Off Date: 03 May 11

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

U.S. UNCLASSIFIED

During April, there were three bomb attacks on Pakistani naval busses and one related bomb discovery in Karachi in the course of three days. Two bombings and the bomb discovery occurred on Tuesday, 26 April, and the third bombing happened on Thursday, 28 April. All three blasts occurred between 7:30 a.m. and 8:15 a.m. local time against busses carrying Pakistani naval personnel to work. The bombs had been planted beside major roads, some of them near speed bumps, and were detonated by remote control as the busses passed by. Total casualties included nine dead (eight navy personnel and one civilian), and approximately 71 wounded.

The Tehrik-i-Taliban Pakistan (TiTP) claimed responsibility for the blasts (though not the discovered bomb) and threatened additional attacks. The group's declared motive was two-pronged: force the Pakistani government to cease operations against militants in the northwestern part of the country; and punish the government for supporting the US in its fight against terrorism. Though not stated outright, the TiTP's announcement implied that the group found the Navy indistinguishable from the rest of the Pakistani military, therefore making it a legitimate target despite the Navy's lack of direct involvement in anti-militant operations.



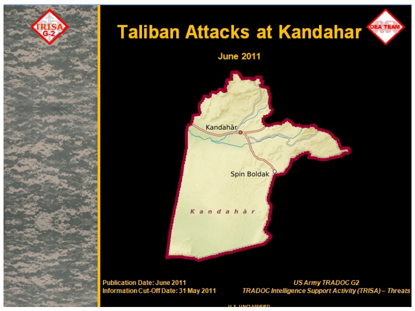
TTP used for naval bus bombings.

The *Pakistan Naval Bus Bombings* threat report provides information to deploying units, trainers, and scenario developers of the emerging threat against Pakistani naval forces. It contains a detailed review of the three naval bus bombings and one additional bomb discovery, and the TTP used. In addition, a discussion on threats and security, responsible parties and motives, and the likelihood of additional attacks is contained in the report.

OEA Team

Taliban Attacks in Kandahar, Spring 2011

by Angela Wilkins

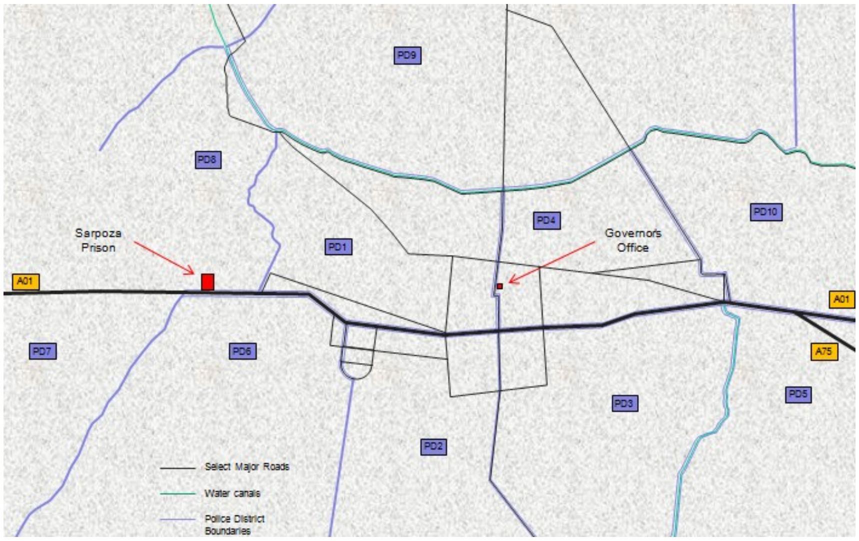

TRISA G2
Taliban Attacks at Kandahar
OEA TEAM
June 2011
Kandahar
Spin Boldak
Kandahār
Publication Date: June 2011
Information Cut-Off Date: 31 May 2011
US Army TRADOC G2
TRADOC Intelligence Support Activity (TRISA) – Threats
U.S. UNCLASSIFIED

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 US 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.

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."



City of Kandahar, governor's office and Sarpoza Prison.

OEA Team

Despite the obvious planning on the part of the Taliban, US 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.

Terrorism T3 Advisory

US Army Training and Doctrine Command G2

TRADOC G2 Intelligence Support Activity
Threat Terrorism Integration

Terrorism

T3 Advisory

Irregular OPFOR Tactics & Techniques...?!

Do YOU Know? OPPOSING FORCE TTP

OPFOR TC 7-100.3 ...Coming Soon!

Tasks: ○ Plan ○ Practice ○ Perform ○ Produce

Results

Conduct broad target analysis and general intentions.
Conduct reconnaissance and surveillance.
Select specific target and resources.
Refine target surveillance and intelligence.
Rehearse plan and contingencies.
Attack.
Exploit effects.
Target
Recon
Select
Refine
Ready
Act
ATK
Exploit
Continuum of planning -- execution -- evaluation -- lessons learned -- application

GUERRILLA -- INSURGENT OE and Affiliates ?

TRISA

We are at WAR on TERROR

Find our products on Army Knowledge Online
Access AKO with password.
Enter: https://www.us.army.mil/suite/files/11318389

AKO

JUN 2011

Terrorism TTP—Threats Terrorism Team (T3)

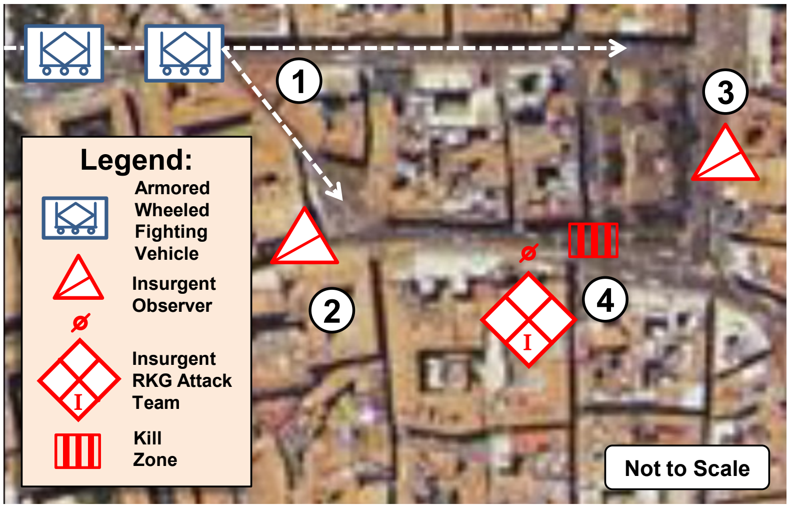
Reconnaissance Attack—Point Ambush

by Jon Moilanen

Planning and Preparation for Reconnaissance Attack

This example of an OPFOR reconnaissance attack-ambush illustrates the planning and preparation for the attack along one of several regularly traveled enemy lines of communication (LOC). The target is a small armored wheeled fighting vehicle patrol conducting LOC security and visible presence in an urban community. This section of the city has been coerced by **local gangs** working in conjunction with a local **insurgent** group. However, increased host nation law enforcement presence in the markets and main streets has started to obtain some active reporting to local police on insurgent activities by local citizens.

The OPFOR insurgents decide to demonstrate their ability to strike paramilitary forces of the host nation in neighborhoods claimed to be under control of insurgent militia. Attacking host nation forces is expected to counter increasing indications that the citizenry may be shifting support to city authorities and increased security measures. **OPFOR reconnaissance and surveillance** in roving patrols and observation posts monitor primary routes [①] through the area that are used regularly by security force dismounted teams and vehicle patrols.



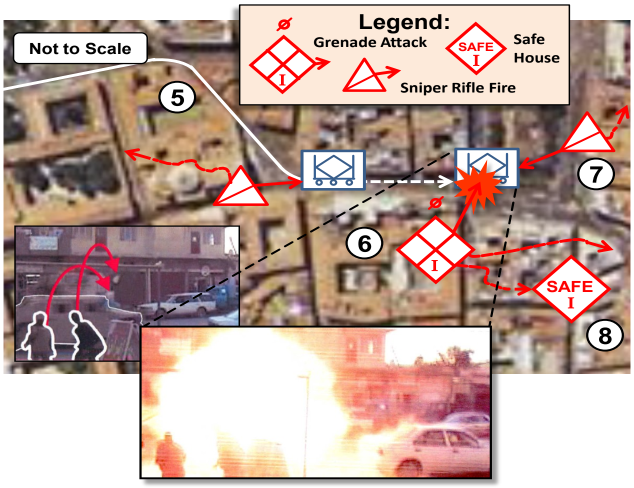
Planning and preparation for the ambush.

The assault is planned for a sudden hand grenade attack on an armored wheeled fighting vehicle and immediate suppression of vehicles with small arms fire in order to allow the assault element to disengage and exfiltrate from the area. The insurgents conduct **rehearsals** by timing the speed and distance between vehicles as they turn into the canalized street and approach the kill zone and market place. Cellular telephones relay code words within a ruse of a normal business conversation.

Terrorism TTP—Threats Terrorism Team (T3)

Conduct of the Reconnaissance Attack

An OPFOR **security element** consists of two observers who provide early warning and security. One observer is in a two-story room vantage point [②] that provides good visibility if a patrol takes a route southeast toward the market place. Another observer is on the sheltered roof of a three-story building [③]. This location provides early warning of any military force or law enforcement to the east of the kill zone at the market place. Both observers are armed with a 7.62-mm Mosin/Nagant sniper rifle. Two insurgents comprise the **assault element** and pose as pedestrians in an alleyway [④] that exits into the market square. Each of the two insurgents in the assault element is armed with a RKG-3 grenade as a shaped charge weapon.



Conduct of the Point Ambush.

The observer reports the two-vehicle patrol moving down the street [⑤] toward the market. The assault team and the other observer acknowledge the alert. The observer announces when the first vehicle turns left below his vantage point. Based on previous rehearsals, the assault team knows when to emerge from the alley to lob both RKG-3 grenades to detonate on the vehicle.

Throwing the grenades in a high angle arc and the grenade's parachute make effective contact with the vehicle and explode [⑥] with one detonation on the vehicle hood and one on the right front side near the door. The lead vehicle veers to the left and crashes into a store front and blocks the street. The trail vehicle stops abruptly due to the blocked passage. Security elements [⑦] engage the lead and trail vehicle with small arms rifle fire to fix the trail vehicle and both crews while the insurgent assault team [⑧] **exfiltrates** through a series of buildings and into the general population. Both observers hide their rifles in prearranged caches inside the buildings and exfiltrate along separate routes. The videographer moves quickly to a **safe house** near the market, hides the video camera, and assumes the role of an interested neighbor in viewing the emergency response to the attack. His observations of response times and types of medical or tactical response forces are added to the commentary and lessons learned that accompany the videotape of the attack.

Terrorism TTP—Threats Terrorism Team (T3)

Assessment

In this example, the OPFOR located a target with aggressive reconnaissance, provided early warning as the target entered one of several designated kill zones, and isolated and temporarily fixed the enemy in a kill zone. One vehicle was severely damaged and at least three host nation police officers were wounded with one officer dying at the attack site. One insurgent was wounded slightly by grenade effects. Configuration of the attack team included a two person **assault element**, **security elements**, and a **support element** consisting of the two security observers when they provided suppressive small arms fire immediately after the grenades exploded. A videographer was a member of the support element. Using two grenadiers as an attack team improved the probability of effective damage by the grenades in a sudden point ambush. The attack team did not plan for appropriate cover after throwing their grenades.

Note 1. The **RKG-3**, *Ruchnaya Kumulyativnaya Grenada,* is a hand-thrown, parachute-stabilized, high-explosive, shape charge, antitank grenade. After removing the safety pin and throwing the grenade, a spring deploys a parachute to assist in achieving a vertical angle of descent and shape charge detonation upon contact with the target.

Note 2. The **OPFOR Tactical Task List** "Reconnaissance Attack" is posted in TC 7-101, *Exercise Design*, Appendix B, Task 4.0.

New OEA Team Update

Update to Suicide Attacks: Afghanistan

https://www.us.army.mil/suite/doc/33441059
link added 08 Nov 2011

OEA Team has recently updated the threat report Suicide Attacks: Afghanistan. The threat report is constantly updated to:

- To inform deploying units, scenario developers, and trainers of the threat from suicide attacks in Afghanistan
- To provide examples of tactics, techniques, and procedures employed by suicide bombers in Afghanistan
- To identify trend in suicide attacks occurring in Afghanistan.

Suicide Attacks: Afghanistan

18 July 2011

Remains of an SVBIED, Paktia Province, FOB Gardez

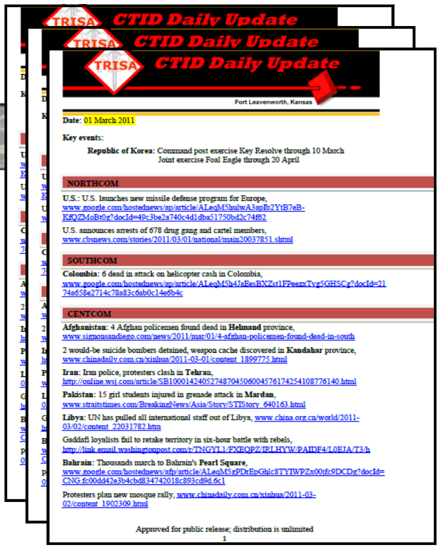
(U.S. Army photo, 24 September 2010)

Publication Date: 18 July 2011
Information Cut-Off Date: 18 July 2011

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

Monthly Wrap-Up of CTID Daily Update

CTID analysts produce a *Daily Update* to help focus our readers on key current events and developments which may be of interest across the Army training community. Each *Daily Update* is organized topically across the Combatant Commands (COCOMs). The following list is a highlight of developments in July 2011. CTID does not assume responsibility for the accuracy of each article. The *Daily Update* is a research tool and an article's inclusion in the *Update* does not reflect an official US Government position on the topic. The *CTID Daily Update* is posted daily on AKO.



TRISA CTID Daily Update

Fort Leavenworth, Kansas

Date: 01 March 2011

Key events:

Republic of Korea: Command post exercise Key Resolve through 10 March
Joint exercise Foal Eagle through 20 April

NORTHCOM

U.S.: U.S. launches new missile defense program for Europe, www.google.com/hostednews/ap/article/ALeqM5hulwA3apIb2YtB7eB-KfQZMoBt0g?docId=49c3be2a740c4d1dba51750bd2c74f62

U.S. announces arrests of 678 drug gang and cartel members, www.cbsnews.com/stories/2011/03/01/national/main20037851.shtml

SOUTHCOM

Colombia: 6 dead in attack on helicopter cash in Colombia, www.google.com/hostednews/ap/article/ALeqM5h4JaEesBXZst1FPeezxTvg5GHSCg?docId=2174a658e2714c78a83c6ab0c14e6b4c

CENTCOM

Afghanistan: 4 Afghan policemen found dead in **Helmand** province, www.signonsandiego.com/news/2011/mar/01/4-afghan-policemen-found-dead-in-south

2 would-be suicide bombers detained, weapon cache discovered in **Kandahar** province, www.chinadaily.com.cn/xinhua/2011-03-01/content_1899775.html

Iran: Iran police, protesters clash in **Tehran**, http://online.wsj.com/article/SB10001424052748704506004576174254108776140.html

Pakistan: 15 girl students injured in grenade attack in **Mardan**, www.straitstimes.com/BreakingNews/Asia/Story/STIStory_640163.html

Libya: UN has pulled all international staff out of Libya, www.china.org.cn/world/2011-03/02/content_22031782.htm

Gaddafi loyalists fail to retake territory in six-hour battle with rebels, http://link.email.washingtonpost.com/r/TNGYL1/FXEQPZ/IRLHYW/PAIDF4/L0EJA/T3/h

Bahrain: Thousands march to Bahrain's **Pearl Square**, www.google.com/hostednews/afp/article/ALeqM5gPDrEpGhlc8TYIWPZx00jfc9DCDg?docId=CNG.fc00dd42e3b4cbd834742018c893cd9d.6c1

Protesters plan new mosque rally, www.chinadaily.com.cn/xinhua/2011-03-02/content_1902309.html

Approved for public release; distribution is unlimited
1

July 5: Arctic Issues: The New Hydrocarbon Frontier.

July 5: Mexico: The War Next Door: How survivors of drug violence are fighting back. (includes video)

July 5: Persian Gulf: Secret Gulf firefight video. (*Analyst comment: The title is misleading. This is not a firefight, it is warning shots from a British warship. However, it appears to show the Iranians attempting to provoke a response*.)

July 5: Iran: Iran showcases homegrown arms in war games.

July 6: Canada: Lists TTP as a terrorist organization.

July 6: Iraq: "Flying Bombs" return killing 6.

July 6: China: Chinese perceptions of US engagement in the South China Sea.

July 7: Department of Homeland Security announces Maritime Operations Coordination (MOC) plan.

July 7: Iran: Busting Iran's new missile bunkers.

July 7: China: China develops military drones for Pakistan.

July 8: Cyber Security: 4000 hacked by *News of the World*.

July 8: Hezbollah in Latin America: Implications for US Homeland Security. (PDF)

July 8: Syria: Syrian security forces kill 13.

July 8: South China Sea: Dangerous Waters: Exercise caution. (CSIS PDF)

July 11: Afghanistan: SOF captures IMU explosives expert.

July 11: China: Pictures of the Type 99A2 tank?.

July 11: Russia: North Caucasus low-grade insurgency continues to simmer.

July 12: Cyber Security: How digital detectives deciphered Stuxnet, the most menacing malware in history.

July 12: Nigeria: Thousands flee Nigerian city hit by Islamist attacks.

July 12: China: China's "eye in the sky" near par with US.

July 13: Arctic: Russia in the Arctic. (SSI PDF)

July 14: The Haqqani nexus and the evolution of al-Qaida. (Combating Terrorism Center PDF)

July 15: Afghanistan: Foreign snipers: Another threat to US forces in southern Afghanistan.

Director, CTID DSN: 552
Mr Jon Cleaves FAX: 2397
jon.cleaves@us.army.mil 913.684.7975

OE & OPFOR Doctrine & Training Lit.
Senior Analyst CTID: Dr Don Madill 684.7926
donald.madill@us.army.mil

OPFOR Doctrine Team
SME: Mr Rick McCall 684.7960
rick.mccall@us.army.mil

Intelligence Specialist
SME: Mr Kris Lechowicz 684.7992
kristin.lechowicz@us.army.mil

Intelligence Specialist
SME: Mr Jerry England 684.7934
jerry.england1@us.army.mil

Worldwide Equipment Guide (WEG)
SME: Mr Tom Redman BAE 684.7925
tom.redman@us.army.mil

Threats Terrorism Team (T3)
SME: Mr Jon Moilanen L3 MPRI 684.7928
jon.moilanen@us.army.mil

Operational Environment Analysis
SME: Ms Penny Mellies 684.7920
penny.mellies@us.army.mil
SME: Ms Angela Wilkins L3MPRI 684.7929
angela.m.wilkins.ctr@us.army.mil

Training-Education-Leader Development
SME: Mr Walt Williams 684.7923
walter.williams@us.army.mil

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

Joint Readiness Training Ctr - OPFOR
SME: Mr Marc Williams BAE 684.7943
james.marc.williams@us.army.mil

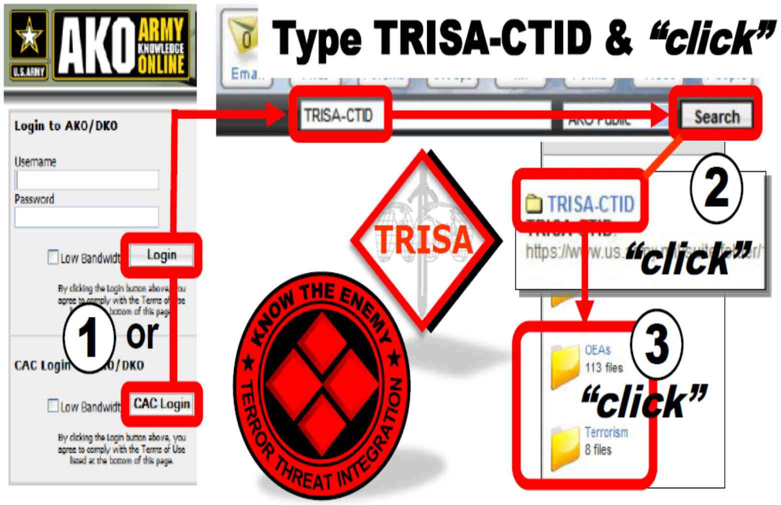
Joint Maneuver Readiness Ctr - OPFOR
SME: Mr Mike Spight BAE 684.7974
michael.spight@us.army.mil

Mission Command Training Program - OPFOR
SME: Mr Pat Madden S3 Inc 684.7997
patrick.madden@us.army.mil

Threats Website-Support Operations
SME: Mr Charles Christianson 684.7984
charles.christianson@us.army.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***

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