U.S. TRADOC G2 Intelligence Support Activity

Red Diamond

Complex Operational Environment and Threat Integration Directorate

Fort Leavenworth, Kansas Volume 3, Issue 10 OCT 2012

INSIDE THIS ISSUE

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

TRADOC G-2 Publishes New OE Estimate

The Operational Environments to 2028: The Strategic Environment for Unified Land Operations (August 2012)

The TRADOC G-2 has recently published an update to the 2009 OE White Paper, "Capturing the Operational Environment." The current paper, "**Operational Environments to 2028: The Strategic Environment for Unified Land Operations**" has been signed by General Robert W. Cone, TRADOC Commanding General and approved for widespread distribution. The paper is commonly referred to as the OE Estimate.

The OE Estimate presents a fresh look at the current and future strategic environment, key variable conditions, adversarial strategies, as well as a detailed look at the implications to leader development, training, concept development and experimentation. The OE Estimate also presents an analytical framework with which to capture the conditions of any potential OE across the globe at any level of analysis. This framework will be discussed in further detail in the forthcoming FM 5-02, *Operational Environment*.

"This strategic environment will serve as the foundation to build, train, and educate the U.S. Army. The intent of this document is not to predict what America's next war will look like. It is to provide potential future environments for commanders, staffs, instructors, and combat developers to use as the basis of training, leader development, education, and capabilities development. Our future success is dependent on building an operationally adaptable force capable of effectively operating in any environment." - GEN Cone

The Army does not have the luxury of focusing on any one potential adversary or any one mission type across the range of military operations. Instead, leaders and Soldiers must be exposed to the multiple conditions representing threats that exist

across the globe. Potential threats will range from standing conventional and unconventional forces, to irregular militias and paramilitaries, to terrorist groups and criminal elements. Training, education, capabilities development, and concept development should reflect this reality.

Currently, in the midst of a global recession, the Army finds itself at a strategically important crossroad as it tries to determine where to wisely invest its limited training, personnel, and materiel resources. The strategic environment (SE) to 2028, with its combination of tough enduring problems and newly developed conditions and characteristics, will add complexity to this challenge.

To help unravel the complexities of current and near-term challenges, the OE Estimate provides a description of the key conditions manifesting across the SE through 2028. Adversarial strategies based on these conditions are also addressed. The concluding chapter explores the military implications of both the conditions and potential adversarial strategies. We know that the current and future strategic environment will be characterized by uncertainty, complexity, and increasingly nuanced relationships. The conditions of the strategic environment must be understood, captured, and factored into Army decision-making. Only then can realistic training, the correct mix of systems and capabilities, and the proper approaches to leader development and education be identified and implemented across TRADOC and the Army in general.

The strategic environment is defined, in the context of this estimate, as the set of global conditions, circumstances, and influences that affect the employment of all elements of U.S. national power. The SE contains multiple potential operational environments (OEs), which are defined as any areas in which U.S forces may operate, from a locale as small as a village to entire regions of the globe.

The strategic environment remains as it has always been: complex. The interaction of the many variables within the environment, including human behavior, assures both fog and friction. The current strategic environment seems more ambiguous, presenting multiple layers of complexity and challenging the Army with requirements beyond traditional warfighting skills and training. Capturing the key strategic conditions is fundamental to understanding current and future military operations. Strategic conditions will be analyzed through the lens of eight OE variables—political, military, economic, social, information, infrastructure, physical environment, and time (PMESII-PT). The resulting conditions are listed below and explained in detail in Chapter 2 of the OE Estimate.

POLITICAL CONDITIONS

- Changing International Distribution of Power
- Decline of Global Governance
- Shortfalls in State Governance

MILITARY CONDITIONS

- Global Military Expenditure Rates
- Wide Range of Potential Missions and Adversaries
- Rise of Private Security Organizations (PSOs)
- Weapons of Mass Destruction (WMD) Proliferation
- Importance of the Global Commons
- Continued Vulnerability of the U.S. Homeland
- Emerging and Proliferating Military Technologies

ECONOMIC CONDITIONS

- Economic Shifts
- Income Inequality
- Economic Interdependence

SOCIAL CONDITIONS

- Demographic Transition
- Population Growth
- Persistent Youth Bulge

INFORMATION CONDITIONS

- Proliferation of Information and Communications Technology (ICT)
- Transparency across Societies
- Actor Empowerment
- Controlling the Strategic Narrative
- Technological Vulnerability

INFRASTRUCTURE CONDITIONS

- Urbanization
- Expanding Physical Infrastructure

PHYSICAL ENVIRONMENT CONDITIONS

- Competition over Natural Resources
- Climate Change
- Special Cases

TIME CONDITION

- Cultural Perception of Time

Implications of the Conditions

The current and future strategic environment will be—as the above conditions reflect—characterized by multiple actors, adaptive threats, chaotic conditions, and advanced-technology-enabled actors seeking to dominate the information environment. The Army must be operationally adaptive to defeat these complex challenges and adversaries operating within this environment.

Through 2028, the Army will face many unique OEs and simultaneous decisive action operations will be the norm within these environments. Training for sequential operations with clearly defined phases will not suffice. Conflict, post-conflict/failed state, humanitarian, disaster relief, and support and reconstruction operations will occur simultaneously. Such operations will require increased coordination/integration with a range of civilian organizations, both domestic and international. U.S. forces will be required to interact with and to protect nongovernment organizations (NGOs), private voluntary organizations (PVOs), and humanitarian organizations more than ever before.

Long-term implications of the SE conditions are uncertain and can lead to a multitude of potential alternative security futures (ranging from some variant of the status quo, to a more violent world, to a less brutal outlook marked by greater cooperation and more effective international institutions). Future conflicts, moreover, will primarily:

- Require simultaneous operations of varying kinds (combat and reconstruction) vs. sequential, phased operations
- Be identity- (ethnic, religious) and/or deprivation-based
- Occasionally rise to the level of genocide and/or mass atrocity
- Be asymmetric and irregular rather than symmetric (involving at times states but also various types of non-state actors, e.g. terrorist groups, criminal organizations, guerrillas, etc.)
- Occur increasingly in complex terrain to mitigate perceived technological advantages
- Require better cultural understanding to avoid broadening or deepening the conflict

Potentially Contentious OEs and Related Missions

Focusing on OEs likely to see increasing tension or conflict can help us understand the types of environments, conditions, missions, and adversaries we might face. The OEs of Iran, China, Yemen, North Korea, Pakistan, and Nigeria will be presented to highlight types of possible environments.[1]

The strategic environment is essentially the sum of all the OEs in which commanders and units could find themselves conducting decisive action. Adversaries take the means provided to them in the strategic environment and use those means in conceptually enduring ways to achieve their ends. That is adaptive strategy. Adaptation, broadly defined, is the ability to learn and to adjust behaviors based on learning, and is closely linked to one's environment and its variable conditions.

Ways – The Methods of Adaptive Strategy

Success goes to those who master the skills necessary to act, react, and adapt with speed and creativity. Enemies learn quickly and can change, although sometimes haphazardly and incompletely, making the "new" skills difficult to counter. Adversaries will continue to be adaptive in terms of using all available sources of power at their disposal. The methods of adaptive strategy are as follows: **conduct preclusion, control tempo, attack will, neutralize technological overmatch, change the nature of conflict, allow no sanctuary,** and **employ shielding**.

Means – The Human and Physical Capital of Adaptive Strategy

While, conceptually, adaptive strategy is the use of available means in the strategic environment to achieve goals, these activities occur in specific OEs. Inside these OEs, the means vary widely. U.S. national interest will also vary widely across the various OEs. The components that exist from which to build an improvised explosive device (IED) in South Asia are not the same as those available in Central Asia or Central America. The means are what change from year to year and OE to OE. However, given our analysis of the strategic environment, we know the means adversaries will need to accomplish their goals and the means available to them. This allows us to draw basic conclusions about the threats that will exist in the strategic environment during this period.

Hybrid Threat

The hybrid threat components of adaptive strategy include two or more of the following:

- Military forces
- Nation-state paramilitary forces (such as internal security forces, police, or border guards)
- Insurgent organizations (movements that primarily rely on subversion and violence to change the status quo)
- Guerrilla units (irregular indigenous forces operating in occupied territory)
- Criminal organizations (such as gangs, drug cartels, or hackers)

The tactical manifestation of an actor using a hybrid strategy is a hybrid threat.

Hybrid threats will use a strategic capability that forces any intervening power to adjust operations (WMD, special-purpose forces [SPF], etc). This capability may not be fully developed or developed at all. This will not affect the transition between regular and irregular operations, and the threat of the capability still provides a tool for manipulating the intervening force (e.g. Iraq's WMD capability circa 2001). **All components of a hybrid threat will use cyber**

operations to either degrade U.S. mission command capabilities, or to conduct global perception management campaigns.

Hybrid threats have the ability to combine and transition between regular, irregular, and criminal forces and operations and to conduct simultaneous combinations of various types of activities that will change and adapt over time. Such varied forces and capabilities enable hybrid threats to capitalize on perceived U.S. vulnerabilities. Perhaps even more confusing will be when those combinations of threats are uncoordinated and simply seek to maximize their own organizational goals rather than any overarching objective.

Tactical Designs

At the tactical level, hybrid threats will employ four key designs that specifically adapt resources available in the strategic environment for use against the U.S. and its partners.

- Exploit Regular/Irregular Synergy
- Employ Range of Technologies
- Information Warfare as Key Weapon System
- Employ Complex Battle Positions and Utilize Cultural Standoff Capabilities

Adversarial challenges will require that the Army be prepared for a wide range of missions over the forecast period. The leader development, training development, capabilities and concepts development implications are significant.

Military Implications

The conditions and strategies highlighted in **Chapter 2, Conditions of the Strategic Environment**, reveal the implications for leader, training, capabilities, and concepts development as well as several implications across Army Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, and Facilities (DOTMLPF).

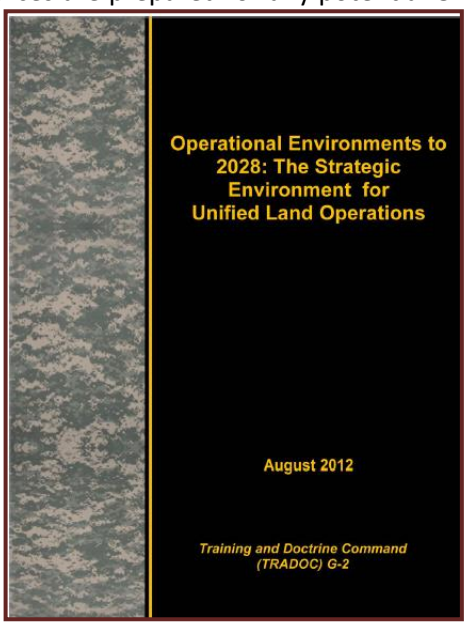
Development Implications

- Leader Development: Leaders must be able to deal effectively with the complexity and uncertainty of potential OEs, be culturally aware, understand the information environment, master consequence management, and be prepared to conduct decisive actions.

- Training Development: Training venues must reflect an understanding of the influence of various cultures and actors present in potential OEs, must continue the tradition of providing an arena that allows free play, and must adapt to new methods and mediums for training. Current and future Soldiers will demand that the Army keep pace with ICT developments for training.
- Capabilities Development: Capabilities development must anticipate the operational needs of commanders and incorporate the adaptability inherent in “off-the-shelf” technology to support the near future.

- Concepts Development: Accounting for adaptive adversaries requires scenario-based concepts that are informed by collaboration from ongoing operations but look well beyond the current fight.

Conditions across the strategic environment indicate future conflict will not be confined to one simple category. It will range in scope from major conventional fights to humanitarian support and nation-building missions. Very capable adversaries will continue to challenge U.S. interests globally, while rising military powers, coupled with existing militaries, will work to advance their regional and global interests. Training and preparation against these changing conditions will drive adaptation and flexibility within the Army and ensure U.S. forces are prepared for any potential OE and any potential mission:



- Increasing Challenge of a Wide Range of Threats
- Increasing Multiplicity of Actors across Potential OEs
- Increasing Importance of Gaining a Holistic Understanding of each OE
- Increasing Degree of Uncertainty
- Increasing Occurrence of Simultaneous and Continuous Engagements
- Prepare for Decisive Action
- Increasing Importance of the Information Environment
- Increasing Likelihood of a WMD Event and Consequence Management Activities
- Prepare for Homeland Security/Defense Missions
- Prepare to Defend Access to the Global Commons
- Prepare for Humanitarian Assistance/Disaster Relief Operations
- Prepare for Reconstruction Operations
- Prepare to Counter Threat Anti-Access Capability

Clearly, this estimate of the strategic environment to 2028 demonstrates that any future oe will be complex and demanding. Key themes emerging from analysis of se conditions and adversaries are proliferation of wmd, hybrid threats, advancements in technology, and an explosion of ict capabilities among actors of all types. Adaptation will be rampant among adversaries, so we must train and prepare for a multitude of these conditions on a wide array of oes. Only through these measures will the U.S. Military be able to successfully navigate any future OE.

1. Likely OEs based upon the TRADOC Intelligence Support Activity Top 10 Project February 2012. The Top 10 Project was created to provide the Army training community with a list of the operational OEs most likely to require Army brigade operations in the near- to mid-future. The list was not an attempt to determine the next location for U.S. ground troop deployment, nor is it predictive analysis reflective of a specific political policy. Instead, the Top 10 is an aid to inform the training community on the range of potential OE conditions that U.S. ground forces are liable to encounter, thus allowing commanders and trainers to focus and tailor their efforts in these areas.

OPERATIONAL ENVIRONMENT (OE) POSTERS

by Walter L. Williams, Training, Education, and Leader Development Team

Training developers often look for various media or devices to enhance student learning. More important are their efforts of determining the best method of getting key points of the desired training or education message disseminated to learners. Recently, the Training Education and Leader Development (TELD) Team received inquiries from our various customers for the location of current OE Posters that could be used at their respective facilities.

The TELD Team was able to retrieve an OE poster (below) developed by the U.S. Army School of Music at Virginia Beach, Virginia as a quick reference guide for students to understand the OE. The poster is divided

into four parts. The first part discusses the definition of an OE. The second area contains a brief discussion of the operational variables. The third area discusses the mission of Army Bands in various OE's. Finally, the fourth area provides a graphic overview of the locations of Army Bands around the world.

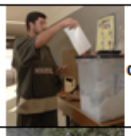
An electronic version of this poster is available and can be downloaded and adapted and printed for use.

Operational Environment

The operational environment is a composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander. (JP 1-02)

Operational Variables (PMESII-PT)

Operational variables are those aspects of an operational environment, both military and nonmilitary, that may differ from one operational area to another and affect operations.



P — POLITICAL
The political variable describes the distribution of responsibility and power at all levels of governance.

M — MILITARY
The military variable includes the military capabilities of all armed forces in a given operational environment.

E — ECONOMIC
The economic variable encompasses individual and group behaviors related to producing, distributing, and consuming resources.

S — SOCIAL
The social variable describes societies within an operational environment.

I — INFORMATION
The information environment is the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. (JP 1-02)

I — INFRASTRUCTURE
Infrastructure compromises the basic facilities, services, and installations needed for a society's functioning.

P — PHYSICAL ENVIRONMENT
The physical environment includes the geography and man-made structures in the operational area.

T — TIME
Time is a significant consideration in military operations. Analyzing it as an operational variable focuses on how an operations' duration might help or hinder each side.

Mission of Army Bands in Multiple OEs

United States Army bands provide music throughout the spectrum of operations to instill in our forces the will to fight and win, foster the support of our citizens, and promote America's interests at home and abroad.

- Live performances in parades, concerts, and other public appearances represent the Army and promote our national interests at home and abroad.
- Army bands provide concurrent music support at home station and while deployed for ceremonial and morale support within unified land operations to sustain warriors and inspire leaders.
- Deployed bands are capable of reinforcing positive relations with unified action partners in the joint, interagency, and multinational environment.
- Army bands support the recruiting mission, provide comfort to recovering Soldiers, and contribute to a positive climate for Army families.

Army Bands Around the World

Korea
8th U.S. Army Band
2nd Infantry Division Band

Japan
U.S. Army Japan Band

Europe
USAREUR Band and Chorus

Operation Enduring Freedom
Afghanistan

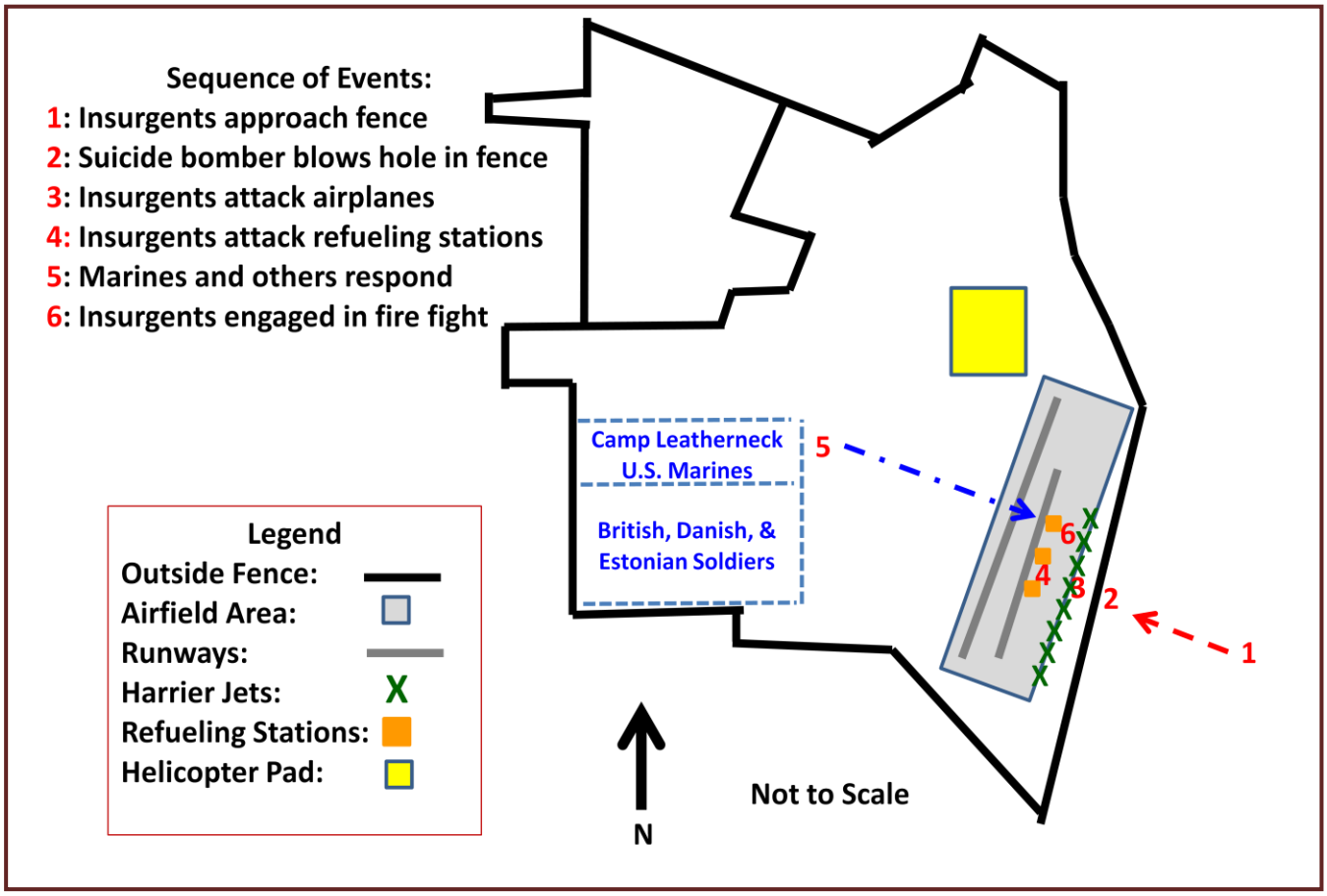
INSURGENTS ATTACK CAMP BASTION

by H. David Pendleton, OEA Team

On the night of 14-15 September 2012, fifteen insurgents dressed in a collection of mismatched, outdated, and ill-fitted American uniforms launched a successful assault on Camp Bastion in Afghanistan that destroyed six Harrier jets and damaged two other planes. U.S. Marines and British security forces responded to the raid and eventually thwarted it, killing fourteen of the attackers and capturing a lone survivor.

helicopter base also operates out of Camp Bastian. In total, over 600 flights take off and land there each day.

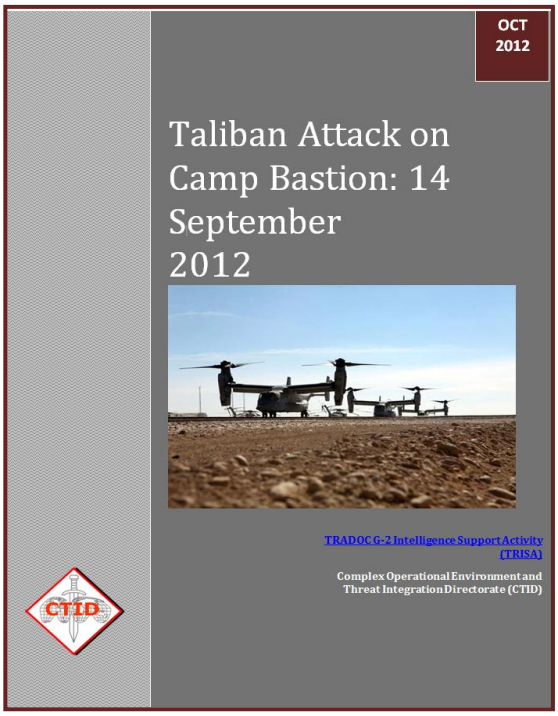
ISAF chose Camp Bastion to build a major logistics base in Afghanistan because of its perceived secure location. First, it is out in the middle of the desert, so there is a long distance line-of-sight in any direction. In addition, ISAF established three additional concentric rings of security. The outer ring consists of a 30-foot high fence



Camp Bastion is located in Helmand Province in the southern part of Afghanistan. Before the United States began military operations in the country, there was only one airstrip at the location that measured just 300 feet long. Now there are two runways, the longest measuring 11,481 feet, which are capable of accommodating almost any plane flown by ISAF forces. The camp houses over 28,000 Soldiers, civilians, and contractors from the United States, Great Britain, Denmark, and Estonia. In addition to the runways, a

topped with 6-foot high coils of concertina wire. The inner ring, also called the inner concrete blast wall, is also 30 feet high and is more than 24 miles in circumference. On the inner wall, armed Soldiers man watch towers equipped with search lights. Between the two 30-foot fences is a layer of razor wire six feet in height. In addition, ISAF uses a combination of radar, cameras, and motion sensors to detect movement on the ground and in the air as far as 20 miles away from the base.

The fifteen insurgents conducted a well-planned and -rehearsed attack. Wearing local clothing and carrying no weapons, the attackers passed several checkpoints in pick-up trucks without drawing any undue attention to themselves. Somewhere near Camp Bastion, the insurgents found a cache of weapons and other supplies, placed there earlier by either the intruders themselves, or their supporters. The attackers changed into uniforms that resembled the American military, strapped on suicide vests, and gathered up the weapons left for them. The insurgents then approached the logistics base through a series of wadis (dry river beds that run throughout the desert terrain) without drawing any notice from Camp Bastion's electronic surveillance devices or human security teams.



At approximately 2215 hours, an explosion occurred along the eastern exterior wall, possibly caused by one of the attackers detonating his suicide vest in order to open a gap in the outer perimeter. The other insurgents rushed through the opening and divided into three five-man teams, revealing a degree of precision only obtainable by repeated rehearsals. The insurgents, through sheer luck, careful reconnaissance, or possibly insider information, chose one of the most unsecured areas of the base, far away from where most ISAF defenders slept. The teams immediately began the systematic destruction of the USMC aircraft with RPGs and possibly other explosive devices. After initially targeting the lined-up Harrier airplanes, the insurgents changed their focus to the refueling stations and the temporary aircraft shelters along the runway. Some reports even state that the attackers received mortar support during the attack.

ISAF personnel, primarily U.S. Marines and British force protection elements, responded to the explosions and began engaging the attackers with small arms fire. The firefight lasted from 2½ to 5 hours, depending on the source consulted, with the ISAF personnel containing the attackers within the vicinity of the runway area, and away from the base's sleeping quarters. With the assistance of American helicopters, the ISAF personnel killed fourteen of the insurgents and captured a fifteenth after he was wounded. Two U.S. Marines, including the Harrier squadron commander, were killed during the firefight and nine other ISAF personnel – including one civilian contractor – received minor wounds.

The attack inflicted significant monetary losses on Camp Bastion. At approximately $30 million for each Harrier, the loss of six jets and the damage of two more was the most expensive one-day loss of coalition equipment since OEF began. In addition, three fueling stations were destroyed or heavily damaged; three to six soft aircraft shelters were destroyed or partially ruined; and one maintenance tent was damaged, in addition to the damage done to the perimeter's infrastructure.

After the attack, the Taliban released various messages about the reason for the attack. One message stated that the attack was in retaliation for the anti-Muslim video that had recently caused riots throughout the Middle East. Another statement claimed that the insurgents launched the attack because Prince Harry of Great Britain was stationed at the camp. Shortly after the attack, the Taliban released a video that supposedly showed the attackers training for the mission.

Despite the attack, ISAF issued a statement saying that the raid would not interrupt ground or air operations at Camp Bastion. The runways became operational later in the day. Within a week, two replacement Harrier jets had already arrived at the base and four additional planes were in route to serve as replacements. The Marine Corps also redeployed the two damaged planes to the United States for repair.

This insurgent attack demonstrates that no static facility is ever totally secure, especially against an attacker who is willing to die in the assault. The success of the raid also demonstrates that good reconnaissance, detailed planning, and extensive rehearsals increase the likelihood of success. The wearing of the American

uniforms shows that the insurgents do not obey the Law of Land Warfare or other international treaties in regards to the conduct of war. Lastly, the failure of electronic surveillance devices or lapses in human security can cause significant damage and loss of life.

The TRISA Threat Report, "Taliban Attack on Camp Bastion: 14 September 2012" provides additional details on the attack, graphics of the assault, and the training implications of this daring raid.

INSURGENT ASSAULT ON A TCP – TACTICS, TECHNIQUES, AND PROCEDURES (TTP)

by Jon H. Moilanen, EdD

Insurgent organizations attack typically with small cells that can comprise as few as two to eight insurgents but can mass up to several hundred insurgents temporarily for a particular combat mission. These types of attacks can have insurgents supporting an assault as planners, trainers, observers, videographers, or other support elements.

Insurgents conduct direct and indirect tactical level offensive actions against an enemy. The typical forms of offensive tactics at the local insurgent organization level and sometimes in conjunction with a higher insurgent organization and/or other affiliated elements in an operational environment (OE) are generally as follows:

- Assault
- Ambush
- Raid

Assault

An *assault* is an attack that destroys an enemy force through firepower and the physical occupation and/or destruction of his position. An assault is a basic form for tactical offensive combat. Other types of offensive action may include an element that conducts an assault to complete the mission; however, that element is typically given a designation that corresponds to the specific mission accomplished. For example, an insurgent cell that conducts an assault in the completion of an ambush would be called the ambush element.

Functional Organization for Assault

The insurgent leader will locate himself where he can best command the mission. Whenever possible, an insurgent assault incorporates three elements:

- Assault element
- Security element
- Support element

Assault Element

The assault element is the action element. This element maneuvers to and seizes the enemy position and destroys any enemy forces in the position.

Security Element

The security element provides early warning of approaching enemy forces and may also have the task to prevent the enemy from reinforcing the assaulted enemy unit. The insurgent leader can accept risk and employ a security element that provides early warning but is not expected to halt or repel enemy reinforcements.

Support Element

The support element provides the assault element and security element with capabilities that can include the following functions:

- Supporting direct fire
- Supporting indirect fire
- Logistics
- Information warfare (INFOWAR)
- Mission Command
- Guides to assist in insurgent exfiltration

Execution of Insurgent Assault on a TCP

The local insurgent organization has had a traffic control point (TCP) under surveillance for several weeks. The local insurgent organization leader selects this TCP for

destruction by direct action cells because the TCP is manned by policemen of the governing authority and coalition military policemen. Audio and video coverage of the insurgent assault will add to the negative psychological effect on the relevant population. An insurgent videographer identifies the best vantage point for video and audio coverage of the assault and occupies a position ① in the third floor of a nearby building.

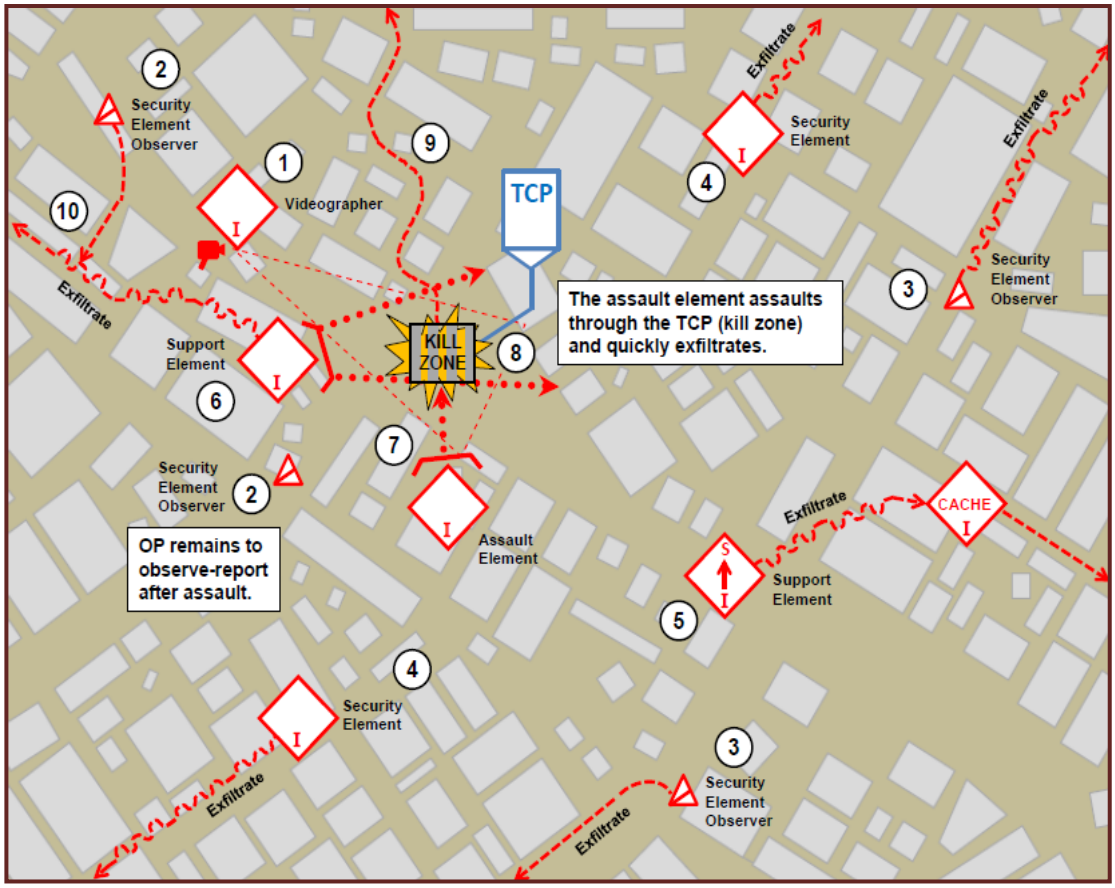
A security element observer ②occupies a position in the vicinity of the videographer to provide early warning to the videographer if his hide position appears compromised. Other security element observers ③ locate themselves at critical intersections to provide regular information updates to other insurgents as they occupy their positions. All insurgents appear to be noncombatant civilians in order to blend into the daily activities of the neighborhood. They use cellular telephones to maintain regular contact among themselves.

Security elements ④ report that they are in their positions and update the local insurgent organization leader that community activities appear to be normal. Support elements consisting of a sniper cell ⑤ and a direct action cell ⑥ with automatic small arms occupy positions to assist the assault element ⑦ when it assaults the TCP.

The local insurgent organization leader orders the assault. The support element ⑥ initiates direct small arms fire (SAF) at the TCP and draws the immediate return SAF from law enforcement officers at the TCP. As the TCP officers take cover and orient to counter this initial threat, the assault element ⑦ surprises the TCP officers from a flank with additional SAF. The overlapping SAF of the insurgent support and assault elements suppresses return SAF from the TCP. The assault element rushes the TCP ⑧ with all cell members assaulting abreast and firing their weapons. The support element lifts its SAF as the assault element reaches the TCP vehicles.

The assault element confirms four law enforcement officers are dead next to their vehicles or in the TCP booth and kill a fifth policeman who is wounded and attempting to crawl into a nearby building. The assault element moves quickly through the kill zone, throws a grenade inside each police vehicle, and continues to run along a preplanned ⑨ exfiltration route.

Once the assault element clears the kill zone and is away from the open intersection, support elements exfiltrate along preplanned routes. The sniper ⑤ does not engage anyone. One insurgent sniper places his weapon and ammunition in a cache as both insurgents of this element quietly exfiltrate to the southeast.



Insurgent Assault on a TCP (Example)

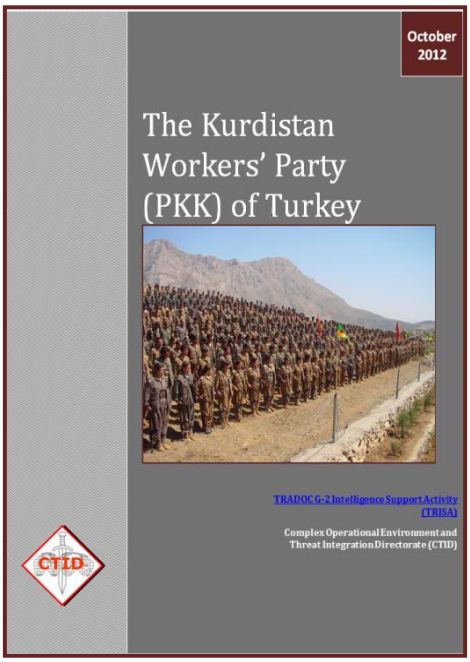
Security elements disperse and individually exfiltrate. The security element observers exfiltrate and rendezvous at designated safe havens with one exception. One security element observer ② near the videographer remains nearby to provide protection while the videographer remains in position to record the aftermath of the successful assault on the TCP. The videographer and security element observer exfiltrate ⑩ together. The videographer gives his video-audio coverage of the assault to an INFOWAR cell representative. The cell representative uses the video and audio coverage in an INFOWAR media release and later as a visual aid in training insurgent recruits.

The assault was a complete success. The action took only six minutes from the first insurgent SAF to the assault element clearing the TCP and kill zone. The videotape of the incident was released within hours for posting on the Internet and to regional media news outlets for the evening television and radio news cycle. The governing authority was embarrassed and openly criticized as inept by local community leaders. Coalition forces revised how they conducted stability operations in conjunction with governing authority police forces. The relevant population witnessed the growing authority of the insurgent movement and would be much more cautious in any active support to local civic or coalition authorities.

THE KURDISTAN WORKERS' PARTY OF TURKEY

by Jim Bird, PhD

An upcoming OEA Team Threat Report will focus on the Kurdistan Workers' Party of Turkey (PKK). This group, known by several names but most commonly referred to as the PKK, has been waging an on-again, off-again guerrilla war since the late 1970s, with the primary goal of establishing an independent Kurdish state within the present boundaries of Turkey. As members of the world's largest ethnic group (roughly twenty-five million people) deprived of a national homeland, the Kurds have long cherished dreams of establishing their own country. The PKK has sought to capitalize on this desire, universally popular among Kurds, by portraying itself as the only legitimate path toward national independence.



Besides claiming to be the sole standard bearer in the fight for a Kurdish state, the PKK is part personality cult as well as a political machine ideologically committed to Maoist doctrine. The "father" of this movement is Abdullah Öcalan, a one-time student in Ankara's School of Political Science, who by 1979 had abandoned his academic pursuits in order to direct all his time and energy to ending what he regarded as Turkish exploitation of ethnic Kurds. Öcalan's followers often refer to him as "Apo," the Kurdish word for "uncle," and to themselves as "Apocos," or "Apoists," to underscore the centrality of the PKK leader to their own destinies. Because Öcalan advocated the violent overthrow of the Turkish government, he predictably became a public enemy with a price on his head. The state he envisions is a Marxist-oriented workers' paradise populated by citizens of a worker-peasant alliance, whose initial task is to provide manpower support for the Kurdish revolutionary struggle. Counting the casualties on both sides, the PKK's war for Kurdish national independence so far has cost between 30,000 and 40,000 lives.

Violence has always been the hallmark of the PKK. It began its existence during the Cold War at a time when Lebanon's Beqa Valley was still under Syrian occupation. As a proxy of both Syria's Ba'athist regimes and the Soviet Union, the PKK remained a constant thorn in the side of Turkish authorities throughout the closing decades of the twentieth century. Kidnappings, hijackings, suicide bombings, and small unit tactical operations targeting Turkish army and security forces have long been a part of the PKK portfolio. For a

number of years Turkey's foreign policy has rested on the premise that anyone who supports the PKK is Turkey's enemy. PKK Cross-border raids from Syrian safe havens into Turkey during the late 1990s became so flagrant that Turkey mobilized its armed forces and threatened war if the provocations continued. The Adana Protocol, named after the Turkish city that hosted peace talks between Syria and Turkey in 1998, ushered in a period of relative calm between the two antagonists, and created a unique combination of circumstances that led to Öcalan's expulsion from Syria and his subsequent capture, trial, and incarceration by Turkish authorities. Although serving a life sentence for treason, he continues to exert considerable influence and authority in PKK circles from his prison cell.

In October 2006 Öcalan declared a unilateral PKK "cease-fire" in the organization's ongoing terrorist campaign against civilian targets, while still reserving the prerogative to act in "self defense" against Turkish army and security forces. Any cease-fire in the PKK's campaign against noncombatants apparently ended on 12 May 2007 when a bomb exploded in the port city of Izmar, in Turkey's Aegean Region, killing one person and injuring 14 others. Ten days later, on 22 May, an explosion occurred in the capital city of Ankara, at a major shopping center located near the Turkish parliament building. These and other attacks on popular tourist sites often preferred by Westerners were in apparent retaliation for European authorities apprehending PKK suspects implicated in international drug trafficking operations. The PKK is notorious for using profits garnered from the drug trade to support its infrastructure and terrorist activities inside Turkey.

The "Arab Spring" of 2011 was a game-changer in Turkish policy relative to the PKK, and also with regard to Turkey's relations with its neighbors. Early in the Syrian uprising, Turkish Foreign Minister Ahmet Davutoglu visited Damascus to caution Bashar al-Asad against taking extreme measures that world public opinion might condemn as too heavy handed. The Syrian regime spurned the Turkish overture, sent tanks to quash the uprising in Hama shortly after Davutoglu departed, and once again allowed PKK militants to reestablish enclaves on Syrian soil. Meanwhile Iran also buried the hatchet with Kurdish rebels within its borders, freeing the PKK to focus exclusive attention on undermining the Turkish state. In part for that reason, many Turkish citizens perceive the PKK threat inseparable from the crisis unfolding in Syria. Efforts to overthrow the regime of Bashar al-Asad have breathed new life into Kurdish national aspirations, while Turkey is highly unlikely to tolerate any diplomatic solution that would condone an independent Kurdish state within its own territory.

An important dimension of the Syrian uprising often masked by current news headlines is that any military countermeasures taken by Turkey in response to its border disputes with Syria could reignite the decades-long guerrilla war fomented by the PKK. The Amanos Mountains span the porous Syrian-Turkish border, contain inhospitable key terrain highly familiar to the ethnic Kurds who inhabit them, and offer the PKK an inviting avenue of approach deep into the Turkish interior. This harsh reality could have important strategic implications for U.S. response options planned in support of Turkey, its lone NATO ally in the region. It could also impact the rules of engagement adopted for any brigade deployed to this operational environment.

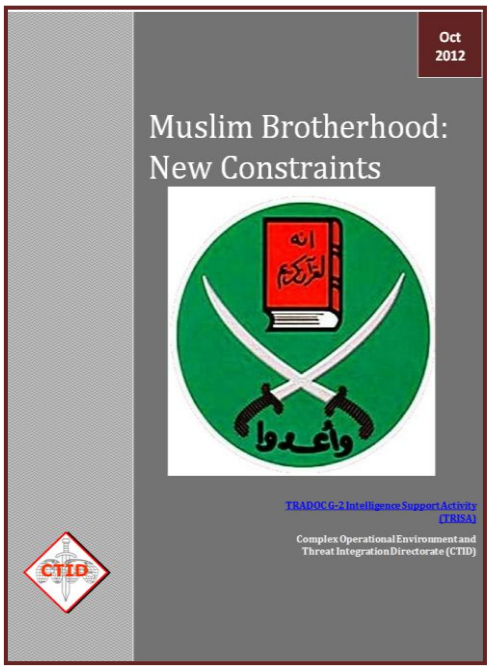
MUSLIM BROTHERHOOD: NEW CONSTRAINTS

by Rick Burns, OEA Team

In 2012 the Muslim Brotherhood (MB), after decades of working in the shadows of government, won overwhelming victories in the People's Assembly (the Egyptian Parliament) and saw one of its own become president of Egypt, Mohamed Morsi. This unprecedented change of events came on the heels of a revolution that saw the end of the Mubarak regime's decades' long rule. MB success in the relatively free and transparent elections was the payoff for many years of patient political and social networking in the People's Assembly and in small communities where it supplemented and expanded on social service needs unmet by the Mubarak government. The overwhelming victory during the 2011-2012 elections is a testament to

the broad organizational reach developed by the MB over decades.

The MB rise to power has caused a degree of consternation within some circles. The MB is seen as a moderate Islamist organization advocating for eventual Sharia law through political means. It is too early to determine how the MB will govern. Assuming a leadership role in the government requires a different kind of accountability and visibility than does operating outside the ruling government. The revolution is relatively easy compared to the need to manage the post-revolution expectations for delivery of improve d public services and more transparent and effective governance. The MB is now moving into the new realm of the criticized as opposed to its traditional role of the critic.



It is clear, however, that the MB will operate with at least three constraints. First, young members of the MB were the first to step into the revolutionary fray. Older and more cautious members of the MB came to the revolution only after success of the revolution became clearer. Some younger members are not as interested in dogma and are more concerned with freedoms that may come into stark contrast with a conservative interpretation of Islam. Second, pressures from the ultra-conservative Salafists will likely act as a stressor to the more moderate and political approaches the MB has operated under for the past several decades. The need to maintain its power will cause tension between the ultra-conservative Salafists, the second largest winner in the People's Assembly, and the more moderate MB. This tension will potentially cause the MB to maintain a more moderate stance in contrast to the ultra-conservative Salifists in order to maintain power. Third, the revolution created high expectations that the new government will be able to deliver improved public services to more people. The ability to provide improved services will depend on the continuance of billions of dollars in aid from the West. These requirements will be another constraint on the MB's ability to impose radical Sharia reforms, at least in the short term.

The TRISA Threat Report, "Muslim Brotherhood: New Constraints," explores these constraints and the implications they will have on the Morsi government.

SIGNALS RECONNAISSANCE

by Jerry England, OPFPR Doctrine Team

Signals reconnaissance is an essential element to the successful collection of accurate and timely information. It includes both intercept and direction finding (DF) on electronic emissions to identify and locate targets and to prioritize operations as a part of the larger information warfare (INFOWAR) campaign. Signals reconnaissance requires intelligence resources to perform analysis, validate any intelligence gathered from the exploitation of enemy emitters, and to identify high-priority targets for possible destruction, degradation, disruption, denial, deception, or further exploitation.

All types of electronic communications are vulnerable to both deception and jamming. In politically sensitive situations or instances where detection is undesirable in general, the OPFOR will avoid jamming the emitter to reduce the possibility of escalating the conflict. OPFOR commanders determine the priorities for signals reconnaissance by determining which high value targets (HVTs) must be found in order to successfully execute combat operations. If the collected intelligence value is of higher significance than the benefit of destroying the target, the commander must determine the best tactical course of action. He may decide either to destroy the target, to jam it, or to continue to exploit

the collected information. The electronic warfare (EW) company In the INFOWAR battalion at the army corps or army group level can locate HVTs in support of the signals reconnaissance brigade and on order attack targets electronically.

Signals reconnaissance units may also be able to determine the general location or direction of UAV flight by intercepting the downlink (UAV transmission) and using DF equipment. Based on this intercepted data, they may also be able to determine the number of UAVs in flight. In this event, the signals reconnaissance unit may be able to tip off air defense or other units in the projected path of the UAV(s) for further action. The cyber electromagnetic intercept/DF company has the capability to intercept satellite signals.

Equipment

Signals reconnaissance targets must be detectable in some manner in the electromagnetic spectrum. The OPFOR must have some system(s) available that can perform this detection. HVTs that do not generate an electromagnetic signature of some sort must be detected by some means other than signals reconnaissance.

HVTs sought by signals reconnaissance efforts are specific to the battle, the OPFOR plan and capabilities, and the enemy's plan and capabilities. However, some common targets for signals reconnaissance efforts include—

- Command posts
- Forward air controllers
- Logistics hubs
- Fire support systems
- Reconnaissance and surveillance systems
- Target acquisition systems

Signals reconnaissance information gained from electronic means is fused with information obtained from other sources. For example, the OPFOR can use trained reconnaissance teams or elements to—

- Put "eyes on" targets and objectives
- Collect required information
- Provide early warning
- Monitor lines of communication and movement corridors in a target area

Such reconnaissance could possibly include a signals reconnaissance capability such as those provided by special purpose forces (SPF) teams.

SPF Signal Team

SPF signal teams support SPF missions with mission command functions. The SPF signal team provides state-of-the-art secure long- and short-range communications for the SPF company and its deployed teams. Additionally, a single, small SPF signal team can provide long-range communications support for guerrilla units up to battalion size. A full SPF signal team can do the same for a brigade-size unit. Teams can also support insurgent operations. These teams may also serve in a signals reconnaissance collection role. In the collection role, the signal equipment is exchanged one-for-one with communications intercept and DF equipment. Each team then becomes a communications intercept and DF unit.

Electronic Intercept and Direction Finding

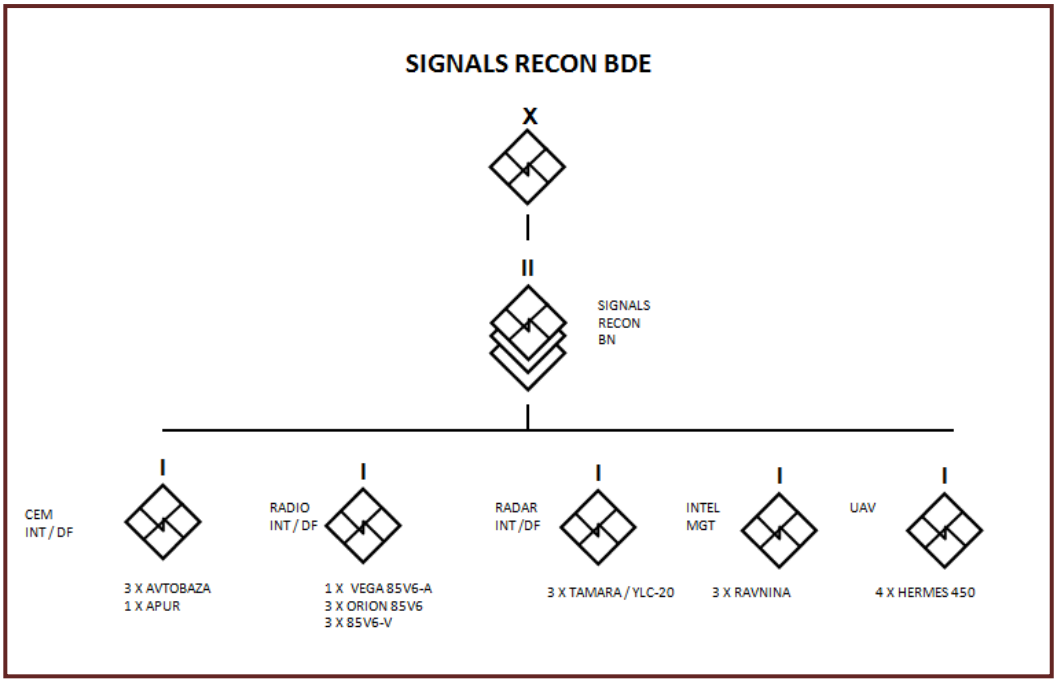
Electronic intercept and DF are the primary means of gathering enemy intelligence electronically. Electronic intercept involves receiving and processing message content, while DF locates enemy signal emissions.

The following distances are a rule of thumb for OPFOR intercept units to maintain reception of enemy transmissions within the area of responsibility—

- Artillery ground radar – about 25 km
- VHF – about 40 km
- HF ground waves about 80 km
- HF skywave – unlimited
- WiFi – about .2 km
- WiMax – about 25 km
- Radar – between 200 km and 400 km
- TACSAT – unlimited within the satellite beam footprint

These ranges can be diminished by several environmental factors such as complex terrain, dense vegetation, manmade structures and materials, combat conditions, weather effects, and solar effects. However, these ranges are greatly extended when airborne intercept is employed such as aviation assets or the UAV assets found in the signals reconnaissance battalion in the reconnaissance intelligence surveillance and target acquisition (RISTA) command.

Mass production of simple, rugged, easy-to-maintain ground-based and airborne intercept equipment contributes to the ubiquitous nature of OPFOR EW capabilities. These systems are generally less sophisticated than most Western equipment, however, and are limited in their effects.



The OPFOR DF capability is similar to that for intercept. Various types of mobile directional antenna systems can be used in a DF role. Units of the signals reconnaissance brigade of the RISTA command are positioned forward in order to intercept military and commercial communications, as well as radar systems. Tactical FM radios operating on low power can be picked up by DF units at a distance in excess of 10 km and high power signals detected at distances up to 40 km. DF operational accuracies are usually within ± 3.5 degrees.

DF is used to—

- Provide approximate locations of electronic emitters
- Provide locations which, when applied with SIGINT, terrain analysis, or other sources, can be refined to a target area of sufficient accuracy for artillery fires
- Develop a "picture" of the battlefield which reveals the disposition and possibly the intent of enemy units
- Provide adequate locations for firing on most radars and jammers

Signals Reconnaissance against Specific Systems

Because of the length of transmission, the peculiarity of their signal, and power output, jammers can be easily located and identified as targets for attack by suppressive fires. Ground radars, due to signal characteristics, also may be located with greater precision than normal radio emitters, often within 50 to 200 meters. Due to the proliferation of commercial mobile communications, the ability of signals reconnaissance assets to distinguish between friend or foe or military versus commercial becomes critical for analysis purposes. Information from DF resources is evaluated quickly, but usually requires further confirmation by other sources. Confirmed DF targets within conventional artillery range, which are extremely perishable and considered to be a serious threat, are given priority and engaged immediately.

About 25 seconds after communications begin, the targeting sequence can continue even if enemy communications cease. Accordingly, the danger point is reached when radio transmissions exceed 20 to 25 seconds.

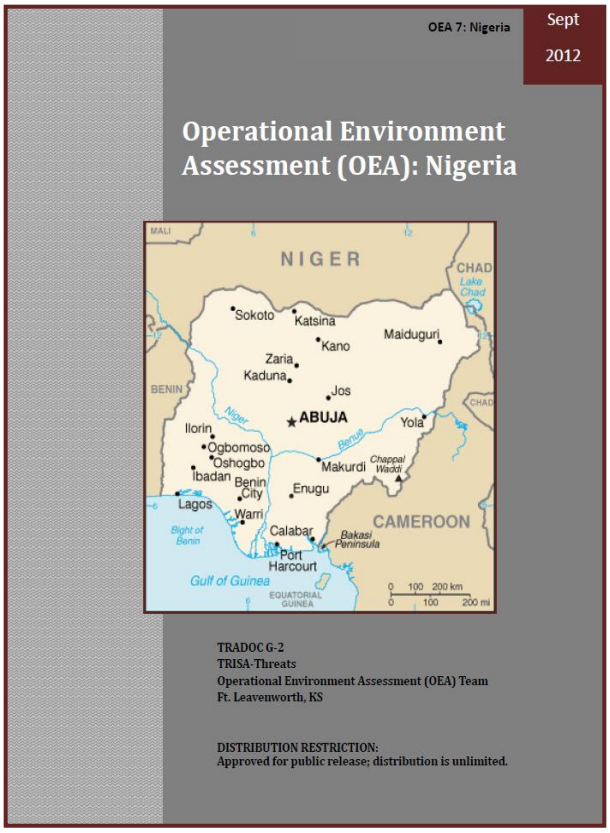
Besides the targets located by DF, it is expected that others will be developed due to the enemy's lax signal security and poor electronic counter-countermeasures.

(See WEG Sheet on page 19 of this issue of Red Diamond.)

OEA 7: NIGERIA PUBLISHED

by Angela Wilkins, OEA Team

The OEA Team recently published OEA: Nigeria. The purpose of an Operational Environment Assessment (OEA) is twofold. First, an assessment provides a detailed description and analysis of an operational environment (OE); second, it presents a methodology for the application of the OE framework to any real-world OE. The OEA framework is an analytical construct developed to explore the complex and ever-changing combination of conditions, circumstances, and influences that affect real-world military operations within a given OE. The framework provides a method to describe the conditions of military operations and capabilities, and is applicable across leader development, education, and training environments as well as real-world contingency planning or predeployment exercises.



OEAs are intended to support the Army training community in the development and execution of mission rehearsal exercises (MRXs), training exercises/events, and general cultural awareness training. This OEA, focused on Nigeria, presents a discussion of the **political**, **military**, **economic**, **social**, **information, infrastructure**, **physical environment** and **time** (PMESII-PT) variables, a trends analysis across variables, and a list of potential and realistic events in Nigeria.

Every OE is different. Each one is dynamic and multi-dimensional with its own degree of complexity. To better understand each OE's uniqueness, one needs to study and understand the variables, their synergy, and their overall influences on military operations. An OEA helps define the OE's nature and characteristics and seeks to present an understanding of the variables and their impact across the OE.

An OEA contains three key sections. Each section provides a comprehensive and complimentary look at the variables as they apply to Nigeria. The three sections are: 1) **Variables of the OE**, 2) **Trends Analysis**, and 3) **Events List**.

Key Themes for Nigeria

Several issues in the country of Nigeria dominate across all variables of the OE. Most prevalent is the divide between the Muslim North and the Christian South (50% of the country is Muslim and 40% is Christian). The different ideologies are exacerbated by the activities of extremist terrorist groups operating in the area, particularly Boko Haram and MEND [Movement for the Emancipation of the Niger Delta]. Boko Haram's activities, in particular, cannot be overlooked when studying Nigeria. The group is responsible for many attacks over the past five years, causing President Goodluck Jonathan to increase spending for police and to authorize searches and roadblocks to try and hamper its activities. Thousands of people have migrated to various parts of the country in an attempt to escape violence.

The North/South contrast comes to the forefront during elections every four years. There were rampant protests and riots that caused over 800 deaths when President Jonathan was elected in 2011. Although the People's Democratic Party (PDP) devised a plan that every eight years the president would alternate between a Muslim and a Christian, when Muslim President Yar'Adua died before completing his first four-year term, Vice President Jonathan, a Christian, stepped in. From this

point many Muslims assumed that the 2011 election would produce another Muslim president, and that Jonathan's tenure was only temporary. Then when Jonathan was elected to serve the next term (in 2011), Muslims cried foul.

Corruption and poverty together produce a multitude of problems for Nigeria. Extreme poverty pervades the country, affecting seven out of ten people. Corruption contributes to poverty by keeping any money to be had within a ring of certain people with no concern as to how it affects the majority of citizens. Politicians and ethnic leaders along with foreign corporations are the beneficiaries of the profits of the lucrative oil industry. Because Nigeria is home to 170,123,740 people, the actual number living in poverty is tremendous, and the effects range from illness due to lack of basic amenities and health care to more willingness to engage in violence because of disenfranchisement.

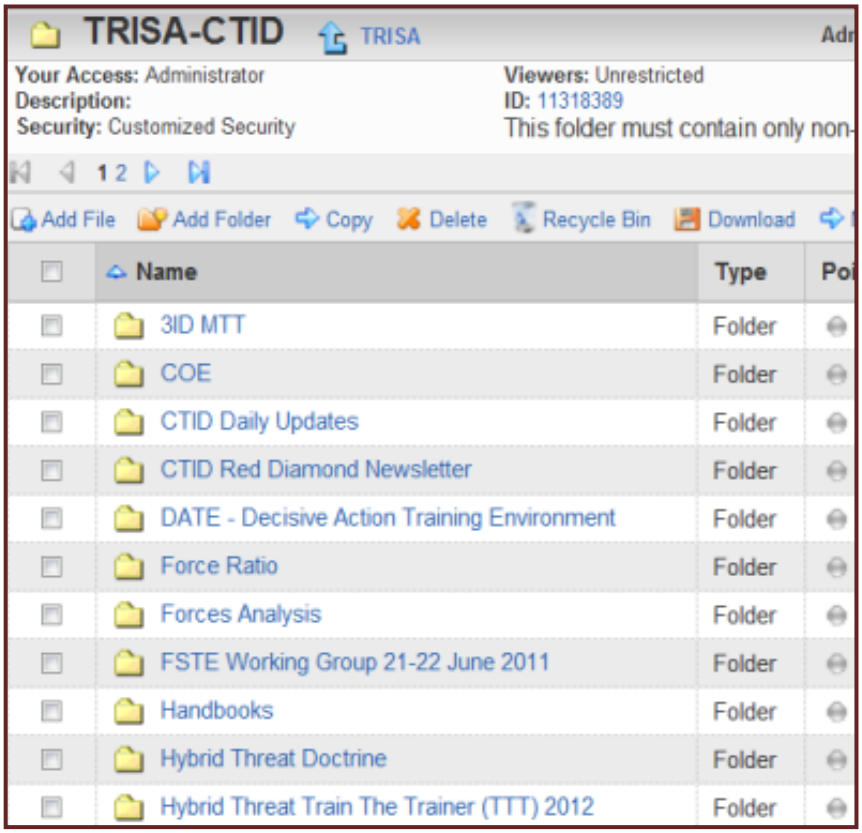
The oil industry is also the source of discontent and fighting because of its potential for increased revenue. Furthermore, oil expansion causes desertification, greatly reducing arable land. The crux of the problem is the mismanagement of resources. For instance, Nigeria has a hydrocarbon pipeline, but it is constantly subjected to vandalism because of inadequate security. In the agricultural sector, there is a lack of people who work in that business, despite the fact that the land in Nigeria is suitable for growing a wide variety of crops. Nigerians also choose to purchase imported items over items manufactured in their own country, believing them to be of better quality.

The bottom line for Nigeria is that a weak democracy and corruption have allowed violence and suffering by its people. The divide between the North and the South and all that it represents will at best keep the country in its current state of malfunction, and at worst plunge it into a civil war.

ACCESS TO THE DATE AND DATE-RELATED PRODUCTS ON AKO

In response to numerous calls and emails, here is a list of links for the Decisive Action Training Environment (DATE) and related products. Start with the TRISA CTID homepage on AKO. The top two pages have numerous folders full of the most recent CTID products, to include DATE 2.0.

- Decisive Action Training Environment (DATE)
- National Training Center OPORD files for 52ID OPORD 12-05-CEF-ATR-N
- 7th Corps OPLAN 12-01 (Atropian – Sovereignty)
- ATS-II SharePoint Site (DATE, JMRC, and NTC Orders)



WEG HIGHLIGHT: RUSSIAN AVTOBAZA GROUND BASED ELINT SYSTEM

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

Russian Avtobaza Ground Based ELINT System

SYSTEM:
Alternative Designations: 1L222
Date of Introduction: 1980-1999
Proliferation: at least 4 Countries*
Crew: 4
Description: Passive ELINT signals intercept system designed to intercept and locate pulsed airborne radars including fire control radars, terrain following radars and ground mapping radars as well as weapon (missile) data links.

SPECIFICATIONS:
Power Supply: 6V or 15 V DC
Weight: 13.3 t.
Frequency Range: 8 GHz to 17.5 GHz
Power (kW): 12 consumption

RECEIVER:
Range: 150 km
Sensitivity of receiver: -88dB
Receive modes: side-looking airborne radars (SLAR) used in combat aircraft, targeting radars of air-to-surface weapons, and radars used to guide aircraft flying at extremely low altitudes, early warning and control radars and jammers
Operational Range: X and Ku –Band
Target Data: Target quantity according to frequency, assignment of jamming systems, type of emitting radars and their angular coordinates
Frequency identification accuracy: ± 30MHz
Accuracy of DF, degrees:
Azimuth: 0.5
Elevation: 3
Target throughput: Up to 60 targets
Reaction Time: 50 µs

ANTENNA:
Description: Rotating parabolic antenna
Azimuth: 360°
Elevation:
18°- 8.5 to 10.2 GHz
30°– 13.4 to 17.5 GHz
Rotation: 6 -12 orbits per minute

OPERATION:
- Frequency Range: 8,000 MHz-17,455 MHz
- Adjustable prioritization of target sets
- Up to 100 meters distance from automated command post (ACP)
- Monitors 15 targets per second up to 60 targets
- Less than 25 min set up time
- Real time self reporting status updates
- Provides location data, and target processing for Ground-Based Aircraft Radar Jamming System

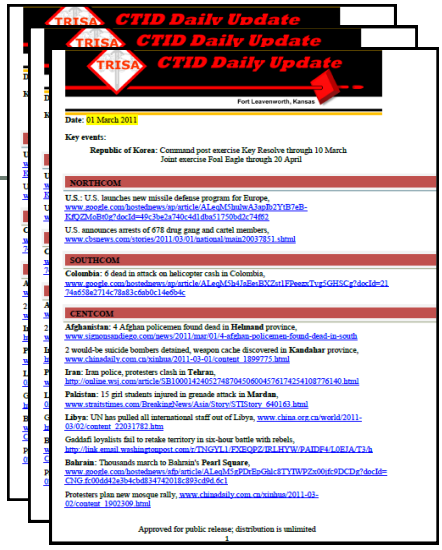
Environmental conditions:
Operation:
Ambient temperature, ° C from -45 to +40
Humidity 98% at temp ≥25 ° C

VARIANTS:
Avtobaza-M Target detection range of up to 400 km (est.)

Frequency range: .2 to 18 GHz

NOTES: It was reported by at least one source to have been modified to receive and locate emissions associated with satellite telephones.
It was reportedly proliferated to Iran and Syria in 2011 -2012.

MONTHLY WRAP-UP OF CTID DAILY UPDATES



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

02Oct—**Nigeria**: Boko Haram kills 11 in **Maiduguri**, **Zamfara**, and **Anambra**; threatens traditional rulers

02Oct—**Turkey**: 12 PKK members killed in **Şemdinli**

03Oct—**Syria**: Jihadist group claims execution of 20 Syrian soldiers

05Oct—**Cyber Security**: Evidence emerges that Iran is building its own hidden Internet

09Oct—**Mexico**: Mexican Navy believes it killed head of Los Zetas

10Oct—**U.S.**: Found in suitcase at LAX: Smoke grenade, billy clubs, hatchet, body bags, leg irons

10Oct—**Lebanon**: FSA threatens to take fight to Hezbollah stronghold in **Beirut**

11Oct—**Nigeria**: 14 killed in reprisals in **Plateau State**; gunmen kill two FRSC officers in **Kano**

12Oct—**Taiwan**: **Taiwan** blames Apple Maps for revealing its $1.2 billion top-secret radar base

16Oct—**Ecuador**: Belgian 8-ton cocaine seizure highlights Ecuador's role in transatlantic market

17Oct—**India**: Powerful bomb recovered from train track in **Assam**

18Oct—**Mali**: North Mali lawmakers call for 'urgent' military intervention

19Oct—**al-Qaeda**: U.S. blacklists Saudi national allegedly linked to al-Qaida network in Iran

22Oct—**Cyber Warfare**: Iran's global cyber war-room is secretly hosted by Hizballah in **Beirut**

23Oct—**Colombia**: Three military die in combat with FARC in **Arauquita, Arauca**

24Oct—**Israel**: 70 Grad and Kassam rockets, and mortar shells fired into Israel in 24 hours

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

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

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

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

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

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

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

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

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

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

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

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

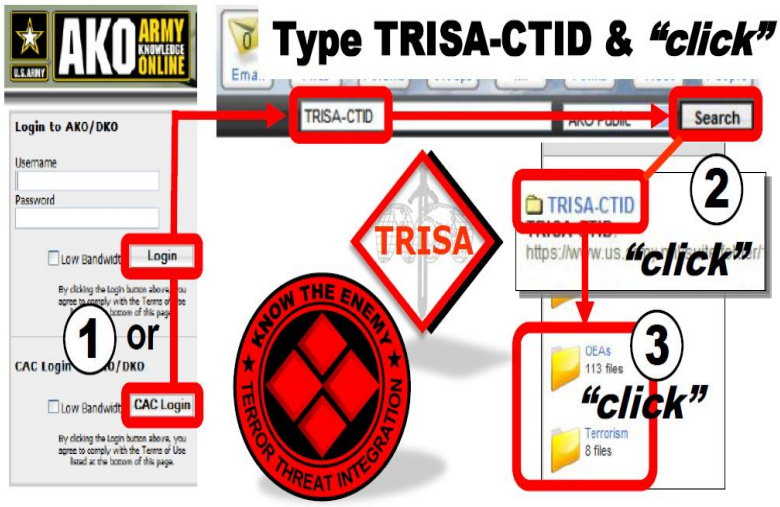
Joint Maneuver Readiness Ctr - OPFOR
SME: Mr Mike Spight BAE 684.7974
michael.g.spight.ctr@mail.mil

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

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

YOUR Easy e-Access Resource

AKO *Three "Click"* Drill-Down



Find Your Topic – Do Your Research

What We Do for YOU

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

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