U.S. TRADOC G2 Intelligence Support Activity

TRISA

Red Diamond

Complex Operational Environment and Threat Integration Directorate

Fort Leavenworth, KS | Volume 5, Issue 1 | JAN 2014

INSIDE THIS ISSUE

TRISA *Red Diamond* is published monthly by TRISA at CTID. Send suggestions to CTID
ATTN: *Red Diamond*
Dr. Jon H. Moilanen
CTID Operations, BMA
and
Mrs. Angela Wilkins
Chief Editor, BMA

IRREGULAR OPPOSING FORCES TC 7-100.3 JAN 2014

by Jon H. Moilanen, CTID Operations (BMA Ctr)

Army Training Circular 7-100.3, *Irregular Opposing Forces*, dated January 2014, addresses irregular opposing forces (OPFOR) for Army training, education, and various leader development venues. The irregular threats represent a composite of adversaries and enemies that comprise irregular forces. Three primary categories of irregular forces portrayed by the OPFOR are insurgents, guerrillas, and criminals. Other irregular OPFOR actors in a complex operational environment (OE) can include affiliates and adherents and/or mercenaries, corrupt governing authority officials, compromised commercial and public entities, active or covert supporters, and willing or coerced members of a populace. Some irregular OPFOR can be independent, non-aligned individuals. Any of these actors may operate with regular military forces as part of a hybrid threat (HT). All of these actors are capable of employing acts of terrorism.

Irregular Forces
Armed individuals or groups who are not members of the regular armed forces, police, or other internal security forces.
***DOD Dictionary of Military and Associated Terms* (2013)**

TC 7-100.3 will be available soon on the Army Publishing Directorate (APD) website at http://www.apd.army.mil/. (*Note.* The US Marines (pictured above) are part of an OE with threats during a noncombatant evacuation from Juba, South Sudan in January 2014.)

RED DIAMOND TOPICS OF INTEREST

by Dr. Jon H. Moilanen, CTID Operations and Chief, *Red Diamond* Newsletter (BMA Ctr)

This issue of TRISA ***Red Diamond*** spotlights several examples of IED tactics, techniques, and procedures (TTP) in US combatant commands. Open source information was a baseline for the related study.

Threats training by TRISA-CTID continues in conjunction with the Combat Training Centers (CTCs) and expanded to a training exchange with a NATO-hosted course as US and allies prepare for missions in Afghanistan. Another training opportunity occurs 10-14 March 2014 in the Hybrid Threat Train the Trainer course. Other training resources exist in the TRADOC G2 Training Brain Operations Center and Training Brain Repository (TBR).

Assessments include pending capabilities of Russian satellite developments in operational environments. Other assessments discuss a military variable in US AFRICOM. Another topic addresses hybrid threat for rigorous and realistic training with functional aspects of OPFOR tactics and terms (TC 7-100.2/100.3). The *Red Diamond* presents perspectives that address the many challenging threats and issues in complex, uncertain, and dynamic OEs and *CONDITIONS*.

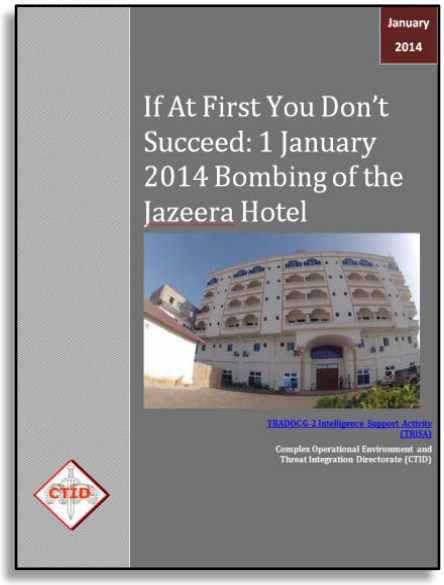
Email your topic recommendations to:

Dr. Jon H. Moilanen, CTID Operations, BMA CTR
jon.h.moilanen.ctr@mail.mil
and
Mrs. Angela M. Wilkins, Chief Editor, BMA CTR
angela.m.wilkins7.ctr@mail.mil

IF AT FIRST YOU DON'T SUCCEED: 1 JANUARY 2014 BOMBING OF THE JAZEERA HOTEL

An example of IED Tactics, Techniques, and Procedures

by Laura Deatrick, OEA Team (CGI Federal Ctr)



During the evening of 1 January 2014, the Jazeera Hotel in Mogadishu, Somalia, sustained its second complex attack involving improvised explosive devices (IEDs) in as many years. Initiating with a suicide vehicle-borne IED (SVBIED), the attackers then stormed the hotel compound in an unsuccessful attempt to gain entrance to the main building. The attack concluded with the detonation of a nearby vehicle-borne IED (VBIED) aimed at first responders. The new OEA Team Threat Report, *If at First You Don't Succeed: 1 January 2014 Bombing of the Jazeera Hotel*, examines the details of the attack and possible training implications.

On the evening of 1 January 2014, a number of Somali Federal Government senior officials were at the Jazeera Hotel. Popular with both foreigners and members of government, the facility possessed two restaurants, an equal number of conference rooms, and excellent security. The group was likely either holding a meeting at the hotel or enjoying dinner.

Around 7:30 p.m. local time an attacker rammed an SVBIED into a police car located next to the main gate, detonating his explosives and killing four security force personnel. Using the explosion as a diversion, two attackers wearing person-borne IEDs (PBIEDs) attempted to penetrate the compound; they were shot and killed by security forces before reaching the hotel entrance. Emergency personnel and additional security forces responded within minutes, and were assisting the wounded when a second VBIED, possibly an SVBIED, detonated only yards from the first explosion, killing at least four. The number of people wounded during the complex attack was at least 37.

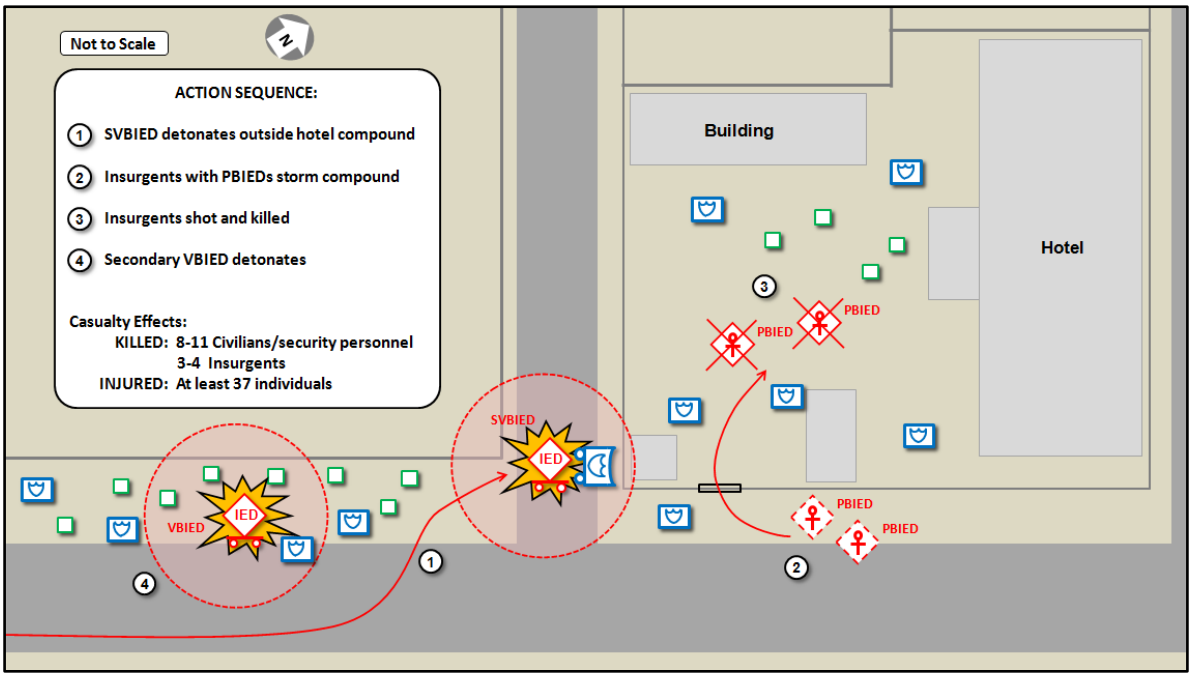


Figure 1. January 2014 Attack on the Jazeera Hotel

Several aspects of this event will make it of interest to trainers and scenario writers. First, it would be easy to mimic in the home-training environment, and the small number of attackers allows for efficient use of role players. Conflicting reporting regarding the second IED and the sequence of events makes the scenario particularly challenging for MI units. Finally, complexity is added due to the two-pronged attack and use of multiple types of IEDs.

The *If at First You Don't Succeed: 1 January 2014 Bombing of the Jazeera Hotel* Threat Report provides information to the Army training community on the January attack. It contains an event review and accompanying diagram, discusses recent threats and security, and considers the likely actors and their motives. In addition, the report provides an analyst assessment and examines training implications.

KNOW THE HYBRID THREAT FOR INSTITUTIONAL TRAINING DOMAIN – SPRING 2014

Complex Operational Environment and Threat Integration Directorate
by CTID Operations

CTID hosts the TRADOC G2 *Hybrid Threat Train the Trainer* course at Fort Leavenworth, Kansas, **10-14 March 2014**. The Hybrid Threat (HT) Train the Trainer course covers associated OPFOR applications depicted in the Army Training Circular (TC) 7-100 series that describes the hybrid threat and associated threats for training. The five-day seminar consists of instruction and practical exercises designed to train the trainer on HT concepts, actors, actions, and operations.

The training and education emphasizes practical exercises to plan and conduct small group experiences in threat functional tactics. Topics include the strategic environment, threat concepts and systems warfare, threat force structure, regular OPFOR units, insurgent cells, guerrilla units, criminal organizations, noncombatants, and the pervasive use of OPFOR information warfare (INFOWAR).

The intent of this event is to train attendees who return to their Center of Excellence, school or academy, installation and/or command activity to teach the hybrid threat as it applies to their operational environment. Attendees should have a minimum of one year remaining longevity in their duty assignment.

The course for March is FULL but we are in the planning stage for the course that will be offered in August (exact dates TBD). A waitlist to backfill the March course is available in case of attendee cancelations. For more information on this training, contact Jennifer Dunn at Jennifer.v.dunn.civ@mail.mil or 913-684-7962.

What is the *Hybrid Threat* (HT) for training? (TC 7-100.2)
In training exercises, the Opposing Force (OPFOR) HT is the diverse and dynamic combination of regular forces, irregular forces, and/or criminal elements all unified to achieve mutually benefitting effects—realistic and representative of actual threats.

NATO EXPEDITIONARY INTELLIGENCE TRAINING PROGRAM (EITP) AND CTID THREATS

Collaboration of TRADOC G2-TRISA-CTID and the EITP to NATO Full Spectrum Operations (FSO) Course

by Kristin Lechowicz, Threat Assessment Team (DAC)

In early December 2013, two members of the TRISA Complex Operational Environment Threat Integration Directorate (CTID) provided a mobile training team in support of NATO's EITP FSO course in Tallinn Estonia at NATO's Cooperative Cyber Defense Centre of Excellence (NATO CCD CoE). CTID's mobile training team provided 2.5 days of classroom instruction for the EITP's FSO course. The class material presented was modified and tailored from blocks of instruction based on CTID's Hybrid Threat Train the Trainer course. This was EITP's initial FSO course and was presented as a proof of concept for training NATO's forces.

EITP and FSO Course

NATO's support to operations in Afghanistan created numerous programs and support packages for training deploying coalition troops. One such program was NATO's Expeditionary Intelligence Training Program (EITP). EITP is embedded with the NATO School in Oberammergau and is a part of the Intelligence Surveillance and Target Acquisition (ISTAR) Department. EITP consists of intelligence professionals with diverse backgrounds that sometimes request subject matter experts to enrich course materials, or to provide a different viewpoint on the subject military intelligence.

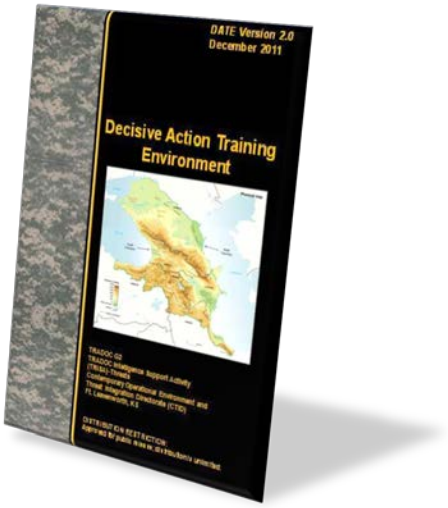
EITP was originally created to address any shortfalls with regards to intelligence personnel that were supporting International Security Assistance Force's (ISAF) mission. EITP has foreseen the potential downsizing of troops in Afghanistan and the need for future training that is not only focused on counterinsurgency (COIN) operations, but also on other elements of decisive action. The FSO course prepares the NATO's training community for future conflict beyond COIN. Much like the US Training community's decisive action concept, NATO's FSO course is preparing NATO forces with a similar construct and apparatus to be able to shift from a COIN centric fight to that of decisive action.

CTID's Mission

CTID is charged with the responsibility of creating complex operational environments (OEs) and dynamic hybrid threats that stress the capabilities of the US Army's training community. In this capacity, in 2010, CTID was charged with the creation of the *Decisive Action Training Environment (DATE)* which allowed the training community to shift from a counterinsurgency (COIN) centric focus preparing future forces for decisive action; however, at the same time not forgetting the pivotal lessons learned from the last 12 years of conflict. CTID's hybrid threat and *DATE* concepts integrate and complemented EITP's FSO course material.

Topics of Instruction

- Introduction to the Hybrid Threat
- Weapons and Technology of the Hybrid Threat
- Regular Forces
- Irregular Forces
- Criminal Organizations
- Terrorism
- Non-Combatants
- Information Warfare
- Functional Tactics [Offense and Defense]
- Operational Tactics



Mutual Benefits of Collaboration

CTID's participation in NATO Intelligence Support to Full Spectrum Operations Course accomplished several profound objectives for the TRISA team.

- Instructors built rapport and networked with NATO allies and EUCOM counterparts.
- Instructors developed subject matter expertise from group discussion that can be translated into complex operational environments and challenging threat composite products for the training community.
- Course and instructors supported NATO allies and EUCOM counterparts.
- FSO course builds and shares ideological training constructs such as the hybrid threat and *DATE*.

The following diagram uses one example of a potential advisory to illustrate the cycle which CTID products take real world threats and create real world composites for the training community. Using the US Army's *Decisive Action Training Environment (DATE)* and *Exercise Design* training circular, in addition to hybrid threat training doctrine, allows the training community to create an adaptive hybrid threat in a complex OE that will meet training objectives. Many of these products were highlight during the two and one-half day block of instruction.

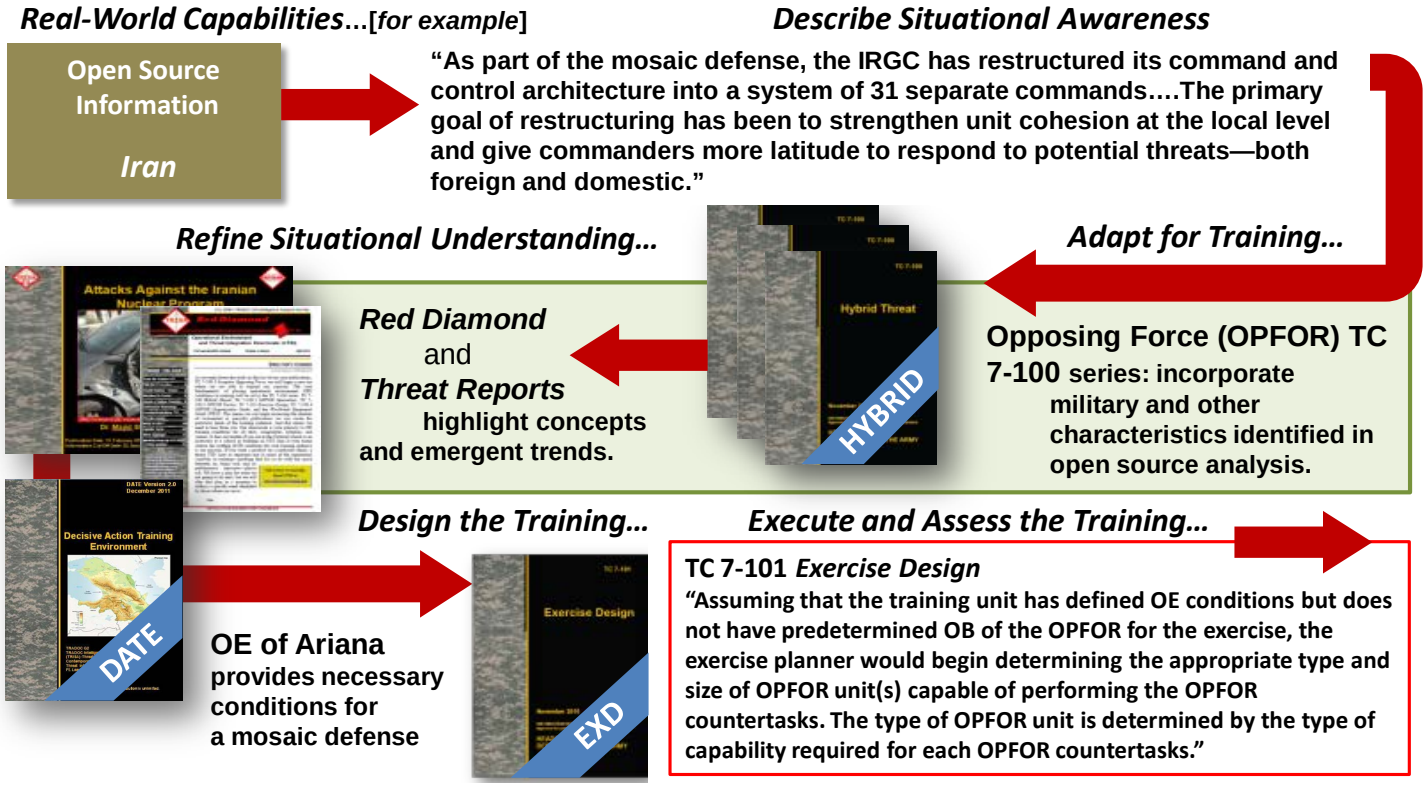


Figure 1. Application of a hybrid threat for training in complex operational environments (example)
(*Note.* Figure 1 diagram adapted from TRISA *DATE*/Hybrid Threat Integration Support for the Training Community. Iran information quote: *Source.* Michael Connell, *Iran's Military Doctrine* (2010).

The US training community as well as NATO partners should look to the future to prepare for the next potential threat. The changes in a number of OEs including the potential downsizing of troops from Afghanistan create an enigma for the training community.

NATO faces the same challenges with the potential shift from a COIN centric fight to decisive action. The ability to share lessons learned from organizations like CTID and EIPT will increase the likelihood that training will be able to meet the future warfighting demands. The relationship between these two organizations and the exchange of course material greatly benefits the training community and impacts US forces as well as allied forces.

KENYA'S MILITARY

by H. David Pendleton, OE Assessment Team (CGI Ctr)

Kenya is a large, mainly rural country in northeastern Africa known for its big game preserves. Tourism is a major industry as foreign visitors flock to the various wildlife centers operated by the Kenya National Park Service. Visitors can access the most modern comforts found in any large city in the capital, Nairobi, and then go to the outback areas where life differs little from hundreds, if not thousands, of years ago.

Since Kenya is a former British colony, the United Kingdom (UK) is responsible for Kenya's security from external threats through a series of agreements that began when Kenya became an independent country. With no need to deter an external enemy threat, the Kenya Defense Force (KDF) can concentrate on counter-insurgency (COIN) operations. The Kenyan-British defense relationship also allows Kenya to field a much smaller army than normally expected of a country of its size. The KDF is primarily a ground-based military with limited aviation and naval assets. Over 80% of the 24,490 personnel in the KDF serve in the army.

The KDF is an all-volunteer force without any conscription. Due to the prestige of the military and the lack of other potential occupations in the country, the Kenyan people find a military career highly desirable. Due to the numbers of prospective recruits who wish to join the KDF each year, the KDF maintains high standards that weed out those with physical, mental, or moral problems. While there is no organized reserve in Kenya, anyone that leaves the KDF in good standing before age 55 is considered part of the military reserve.

The KDF's national command structure originates with the president, who also serves as commander-in-chief of the military. The Minister of Defense reports to the president and supervises the Chief of the General Staff, similar to the British model. The army and navy commanders report to the Chief of the General Staff. The Eastern and Western Area commanders as well as the air force commander report to the army commander.

Without any need to worry about external threats, the KDF can concentrate on COIN, participate in the African Union Mission in Somalia against Islamist terrorists, and cooperate with other countries and organizations in various other peacekeeping operations. The continued exposure to Western militaries through the various peacekeeping missions, and COIN training conducted by US Soldiers, not only hones the KDF's technical and tactical skills, but improves its professionalism as well.

About 80% or 20,000 of the 24,490 KDF personnel serve in the army. The force fields one armored brigade with three battalions, one infantry brigade with three battalions, one independent infantry battalion, one infantry brigade with two infantry battalions, one airborne infantry battalion, one artillery brigade, one air defense artillery battalion; one engineer brigade with two battalions, and one independent air cavalry battalion.

Due to its historical ties to the British military and recent relationship with the American army, the KDF operates with a Western military mindset. The KDF runs a military education system similar to the US, with some schools for the various branches and others that concentrate on leadership, both for Kenyan officers as well as students from neighboring countries in the HOA region. The KDF conducts joint exercises with both the British and American militaries on a regular basis.

Kenya takes an eclectic approach to procuring its weapons. No one country's weapons dominate the KDF's equipment inventory: The KDF tanks come from both the UK and Russia; its other armored vehicles originate in Germany, China, France, and the UK; artillery was produced in Italy, Russia, France, and the UK; and anti-tank or anti-aircraft missiles were made in Sweden, Israel, Switzerland, Germany, France, Russia, and the UK. Like most of the other HOA countries that operate navies, the Kenya maritime element is primarily a coast guard with little blue-water capability. Kenya's navy protects not only the 536 km of Indian Ocean coastline, but Lake Victoria as well. The Kenya naval missions include the defense of its maritime territorial interests, protection of vital areas and installations, the safeguarding of its own and friendly shipping in its territorial waters, police enforcement of its territorial waters, surveillance of the exclusive economic zone, general coast guard duties, continuous sea patrols, and search and rescue missions. While small with only 1,490 personnel, the Kenyan navy is well-trained and possesses some fairly modern boats donated by the US. The Kenyan navy conducts joint exercises with the US and other countries, and helped to successfully conduct "Operation Linda Nchi" where it deployed two battalions of army troops into Somalia to hunt down kidnappers supposedly affiliated with al Shabaab.

The air force of 3,000 personnel is now under army control after an unsuccessful coup attempt in 1982. The air force flies Western aircraft from a variety of countries and uses tactics based on the training received from the manufacturers. Maintenance is an issue. Although Kenya purchased 15 F-5 fighters from Jordan in 2007 to create a fleet of 24 of the same type of aircraft, many of these are still not operational.

Kenya possesses several other organizations equipped with small arms that could be used in a paramilitary role. These units include the Police General Service Unit (PGSU) that monitors the country's borders, the National Security Intelligence Services (NSIS) responsible for intelligence collection, the Kenyan Customs Department of the Kenya Revenue Authority (KRA) - in which 34% of its agents are assigned to entry and exit points throughout the country, and the Kenyan Wildlife Service that normally uses its weapons to stop poachers.

While Kenya has a history of insurgent activity, many threat groups are no longer as strong as they once were because of successful KDF campaigns against them. The Sabaot Land Defense Force (SLDF) in the Rift Valley and Western provinces began as a self-defense force against other political parties. The Moorland Defense Force (MDF) sprang up in response to the SLDF actions against its people. The Political Revenge Movement (PRM) also began in response to the SLDF. In 2008, the KDF went into Kenya's western provinces and eliminated the SLDF, MDF, and PRM either by forcing their surrender or killing off their leaders. Some remnants of these groups may still be in hiding. The Somali Islamist group al Shabaab has also been known to operate in Kenya, mainly through the affiliated Muslim Youth Center.

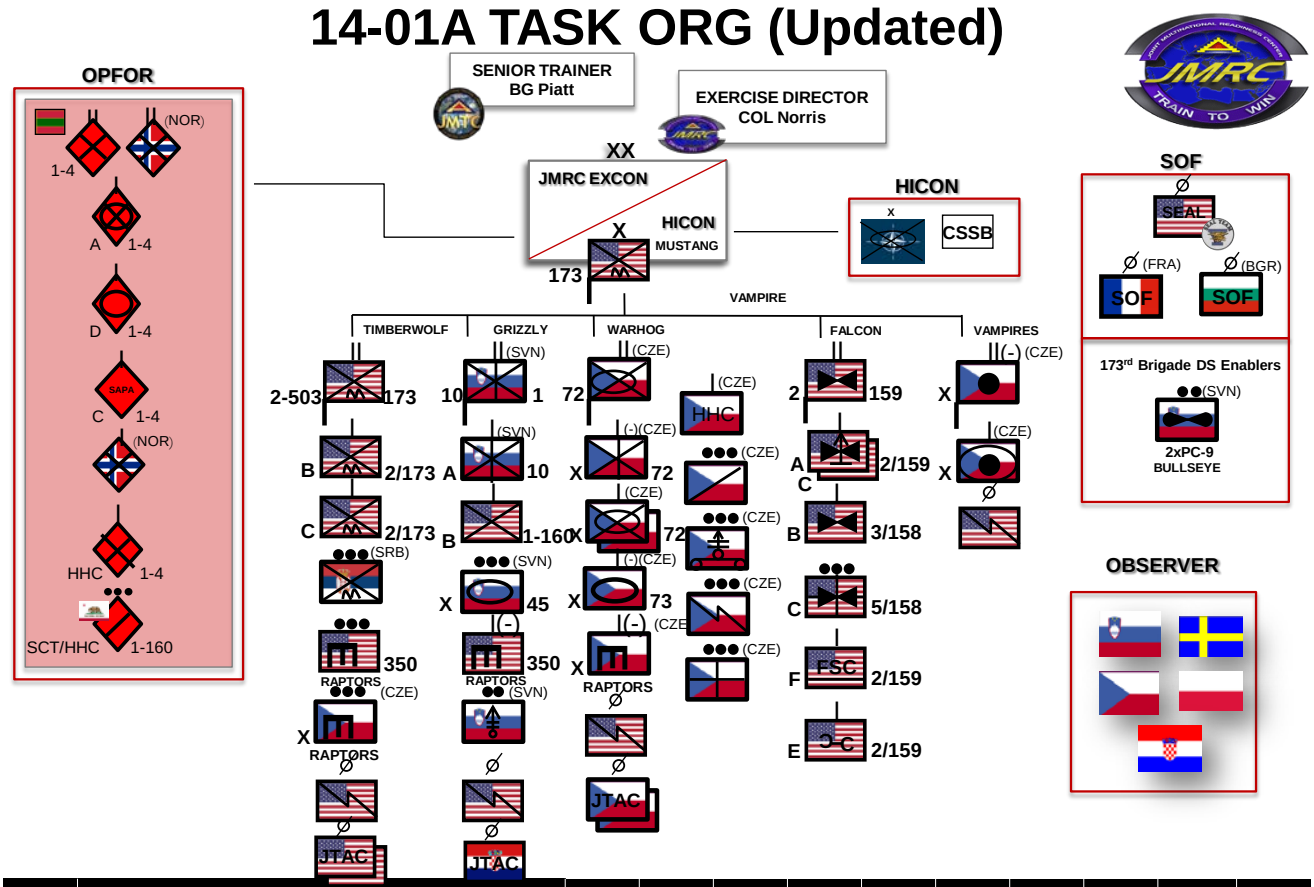
Kenya is a strong ally of the US in the war on terrorism. The KDF continues to improve its COIN operations, not only through training by the US and other Western militaries, but also by experience gained in successful campaigns that eradicated the various insurgent groups in the Rift Valley and Western provinces. The KDF also continues to participate in various peacekeeping operations that improve its professionalism by contact with Western militaries. While small, the KDF is a highly-skilled force when compared to its regional neighbors. For more information on Kenya or other Horn of Africa countries, please see the *Horn of Africa Operational Environment Assessment* on ATN (ATN > DA Training Environment > CTID Operational Environment Page > Operational Environment Assessments).

JMRC DECISIVE ACTION EXERCISE (DAX): COMBINED OPERATIONS AND HYBRID THREAT

by Mike Spight, Training, Education and Leader Development Team (CGI Ctr)

DAX 14-01A was conducted at the Joint Multinational Readiness Center (JMRC), Hohenfels, Germany 7-27 November 2013. It was designed to serve as a "proof of principle for the European Response Force (ERF) that facilitates multinational partnership at all echelons" and "improve NATO interoperability by integrating Warfighting Functions, personnel, and doctrine across a multinational spectrum through execution of a Brigade Decisive Action training environment."[1]

Although previous DAXs planned and conducted at JMRC included North Atlantic Treaty Organization (NATO) partner unit participation (both with the Rotational Training Unit [RTU] and as part of the Opposing Force [OPFOR]), this rotation featured significantly more NATO troop involvement than US troops who were predominately from the 173rd Airborne Brigade Combat Team. For this specific rotation, an element from the 173rd's HQ acted as the Higher HQ Control (HICON), working out of the JMRC Operations Center. One of the Brigade's subordinate units, 2nd Bn/503rd PIR (-), did operate in the "box," but at a reduced strength of two Rifle Companies, a Combat Engineer Platoon, an additional Signals Team, a Serbian Army Airborne Infantry Platoon, and two USAF Joint Tactical Air Control Teams. However, that Bn (-) would not be the only force available to the BLUFOR. A Slovenian Infantry Bn including a Platoon of T-72 MBTs, a Rifle Company from the 160th Inf Bn (California National Guard), and a Czechoslovakian Infantry Bn also included a Company (-) of T-72 MBTs. The entire BLUFOR Task Organization was very robust, with both attack and lift aviation assets and a Battery (-) of Czech self propelled 152mm howitzers.



JMRC	OCT AUGMENTS & OBSERVERS			OPFOR												
OCT	U'R	CONUS	MULTI-NATIONAL	160 SCT	Norway	1-4 IN BN	COBS	SRB	1-160IN	173d ABN	350 EN	SVN	CZE	MN SOF	2-159 ARB	14-01A TOTAL
170	0	0	54	30	200	600	90	30	125	350	95	200	590	30	300	**2894**

Figure 1. Task organization for DAX 14-01A with total troop count

Special Operations Forces (SOF) were not left out of this exercise. Elements from a US Navy SEAL Team, French and Bulgarian Special Forces (a total of approximately 30 SOF personnel) supported the BLUFOR as well, with missions focused on Direct Action and Personnel Recovery.

Also, as you look at the OPFOR's task organization (Figure 1), you'll note that B Company is not listed. A sizable portion of the company had been tasked to provide support to the Royal Military Academy-Sandhurst (RMA-S) during this time period, and was not available to participate in the DAX. RMA-S was training in the extreme north west portion of JMRC's maneuver area, which was "OFF LIMITS" for both BLUFOR and OPFOR during the conduct of DAX 14-01A.

Note that the Norwegian Inf Bn (-) that comprised part of the OPFOR also included a company of ten (10) Leopard MBTs. Combined with the tanks of 1/4th Inf Bn's Delta Company, the OPFOR was set to provide the BLUFOR with a formidable opponent. As a whole, the OPFOR replicated both regular and irregular forces, with C Co portraying an insurgent force, the South Atropian People's Army (SAPA).

The RTU commander's (173rd Airborne Brigade Combat Team) training objectives for this rotation were:

1. **Conduct Mission Command**
2. **Conduct Offensive Tasks**
3. **Conduct Defensive Tasks**
4. **Conduct Stability Operations**
5. **Employ Fires**[2]

All of these training objectives had undergone counter task analysis by the OPFOR Bn commander and staff, and they subsequently developed a plan to fully test the RTU with a rigorous concept of operations developed and rehearsed to focus on each of the their training objectives.

Replicating the 2nd Bn, 112th Brigade Tactical Group (BTG) of the Arianian Army, the OPFOR's combined arms rehearsal (CAR) was held in their Bn classroom on 18 November, the day before the force-on-force phase of the training rotation began (19-24 Nov). The OPFOR Battalion S3, the Norwegian Bn S3, all primary staff officers, reconnaissance unit leaders, and company commanders briefed their missions in support of the plan to the OPFOR and Norwegian Bn commanders. Three possible courses of action (COA) were briefed, and the decision was made to go with COA 2, which consisted of four phases:

- Phase 1-**Build Combat Power/Establish Tactical Assembly Areas**
- Phase 2-**Reconnaissance in Depth/Deception Operations/Aerial Reconnaissance**
- Phase 3-**Attack (Dispersed Attack) to Seize Objective XERXES**
- Phase 4-**Hasty Defense**

Note that in TC 7-101, *Exercise Design,* Appendix B, there is no such task as "Hasty Defense;" OPFOR doctrinal defenses are the maneuver or area defense. However, during the counter task analysis process, if it is determined that there is no OPFOR doctrinal task that will adequately counter a BLUFOR training objective, then the OPFOR can choose a task from the Army Universal Task List (AUTL). In this case, as one of the BLUFOR training objectives was to quickly conduct a Counter Attack in response to the OPFOR Dispersed Attack, the OPFOR commander and Staff selected Hasty Defense from the AUTL. The OPFOR's Hasty Defense would eventually evolve into an Area Defense once the BLUFOR was ready to conduct its Deliberate Attack against the OPFOR during the last 24 hours of force-on-force.

The OPFOR Bn commander made the decision to execute COA 2. Note that in Figure 2, the Norwegian Bn (-) is identified as TF North. But once the CAR began, it was clear that the OPFOR Bn commander and already directed that the Norwegian Bn (-) would assume TF South's mission, and the OPFOR Bn would execute the missions of TF North and the Deception Force. It would appear that this decision was driven by the fact that the Czech Bn, with its platoon of T-72 MBTs, would be positioned on the southern most Avenue of Approach, and the OPFOR Bn commander had determined that the Norwegian Bn (-), with its company of ten (10) Leopard MBTs was a better choice to perform TF South's mission against the heavier Czech Bn.

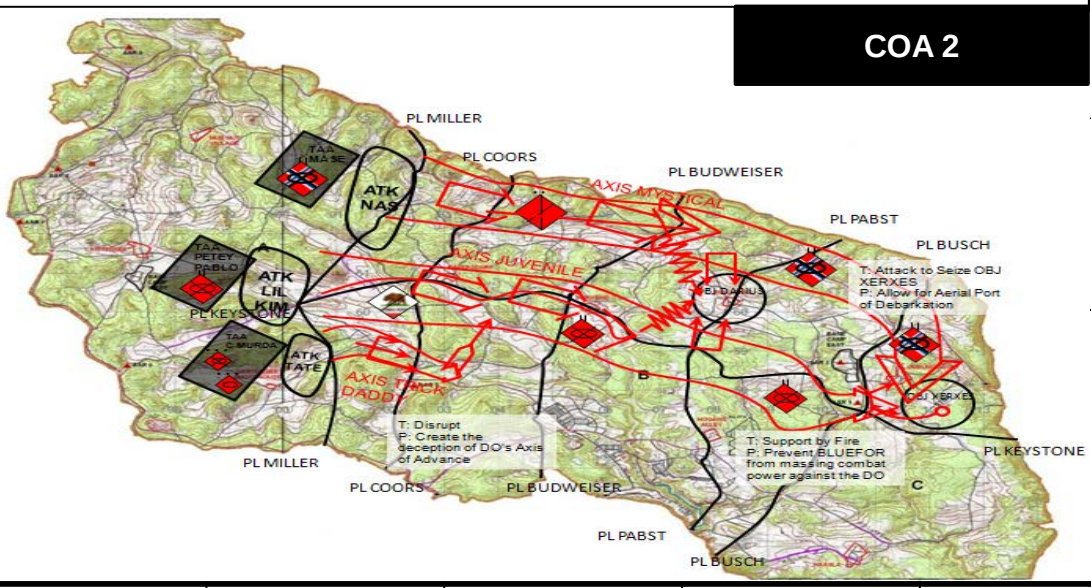
Once STARTEX was called, SAPA was already present in the BLUFOR's rear areas, and rotary wing insertions of OPFOR recon teams were achieved during hours of darkness. Those OPFOR recon and SAPA teams soon had "eyes on" BLUFOR units, critical assets and both Objectives Xerxes and Darius.

Concept of the Operation: 2/112th BTG attacks to seize OBJ XERXES. 2/112th BTG accomplishes this by conducting an envelopment. BTG receives AWT attachment from Falcon Team consisting of 4 LH-72s. TF North the DO conducts an attack to seize OBJ XERXES along Axis MYSTICAL. Decisive to this operation is the seizure of the STOL strip. This is decisive because it allows for follow on forces to reinforce the BTG by means of an aerial port of debarkation. 2/112th assumes tactical risk by attacking along two axis of advance through known enemy obstacles and armor formations. We mitigate this risk through the use of aerial reconnaissance, scout positions over watching enemy positions, fires, as well as deception operations. TF South attacks to seize OBJ DARIUS along AXIS Juvenile IOT divert enemy combat power away from the DO. BTG Scouts conduct reconnaissance IOT identify enemy positions. At End State 2/112th BTG has seized OBJ XERXES and DARIUS and is prepared to execute a hasty defense to PL COORS.

Commander's Intent
Purpose of this operation is to establish an aerial port of debarkation. Identify enemy recon elements and defensive positions within AO. Destroy enemy forces and establish axes of advance. Critical is the identification of enemy disposition and composition , and securing OBJ XERXES.

Key Tasks
- Conduct FPOL with 2/114th
- Conduct Screen IVO Mekhrably
- Seize OBJ DARIUS
- Seize OBJ XERXES
- Travel along AXIS MYSTICAL and JUVENILE
- O/O conduct hasty defense vic PL COORS

Timeline
- 19000NOV13-Occupy TAAs
- 19NOV13-Scout insertion
- 19NOV13- Aerial recon
- 20NOV13- IDF destruction of obstacles/defensive positions
- 200600NOV13- Attack to seize OBJs
- NET201500NOV13- OBJ XERXES seized
- NLT 201700NOV13- BTG prepared to conduct mobile def



4 Phase Operation	TF SOUTH	TF NORTH	FIRES	SCOUTS	SUPPORT
Phase I- Build combat power/occupy TAAs Phase II- Reconnaissance Phase III- Attack to Seize Phase IV- Hasty Def	T: Attack to seize OBJ DARIUS P: Divert BLUEFOR combat power away from the DO	T: Attack to seize OBJ XERXES P: Allow for the establishment of an aerial port IOT mass combat power with follow on forces	T: Fix T: Destroy P: Allow BTG FOM P: Deny enemy FOM and the ability to mass combat power	T: Route reconnaissance T: Area reconnaissance P: Deny BLUEFOR the ability to mass combat power P: Enable BTG FOM	T: Control sustainment operations at the BTG level P: Support BTG through sustainment operations with all classes of supply

Figure 2. OPFOR concept of the operation for COA 2

The OPFOR Deception Force (Team BUGABOO) was to advance along Axis TRICK DADDY but only succeeded in drawing off minimal BLUFOR (Czech) from their defensive positions along Axis JUVENILE. Team BUGABOO was subsequently destroyed by the BLUFOR. OPFOR also initiated their main attack along Axis MYSTICAL (TF North) and along Axis JUVENILE (fixing attack executed by TF South). It was hoped that Axis JUVENILE would exploit the unit boundary between the Slovenian and Czech units and any failure on their part to adequately coordinate their defense along that seam.

The OPFOR's Recon assets and SAPA played essential roles during the attack, and TF North was able to reach Obj Xerxes, defeat BLUFOR units defending it, and seize the STOL strip. Unfortunately, TF South was not able to reach, much less seize or fix and bypass, Obj Darius, and their attack culminated west of the Obj. If they had not been halted by a stiff BLUFOR defense, part of TF South would have been able to continue on to Obj Xerxes, and support TF North, which was subsequently defeated by BLUFOR units conducting a counter attack to regain the STOL strip.

Throughout this DAX, close air support and UAV simulations were the norm as inclement weather (actual) limited the amount of rotary wing or UAV sorties that could be conducted over the entire six days. Indirect fires simulations were heavily utilized by OPFOR SAPA and recon teams as they engaged BLUFOR assets, in particular critical assets/systems.

This entire exercise was more scripted than it normally would have been due to the large quantity of NATO partner involvement and their unfamiliarity with the hybrid threat concept. The amount of free play was, as a result, limited in order to control the ebb and flow of the exercise, and to ensure that the RTU commander's training objectives were met to the maximum extent possible, and that the focus remained on building solid interoperability practices throughout all exercise participants.

The main points taken away from DAX 14-01A is that the hybrid threat and decisive action are no longer limited as doctrinal concepts only in vogue with the US Department of Defense. NATO partner units are now participating in these exercises, and the TRADOC Intelligence Support Activity has provided support to NATO personnel via a Mobile Training Team. (*Note.* That training effort is described in a separate article by Kris Lechowicz in this issue of the *Red Diamond*.)

Notes

[1] JMRC, "14-01A Exercise Objective," Rotation 14-01A Final Planning Conference Out-Brief, 12 September 2013, slide 7.
[2] JMRC, "14-01A Exercise Objective," Rotation 14-01A Final Planning Conference Out-Brief, 12 September 2013, slide 9.

THE TRAINING BRAIN REPOSITORY *"AS-IS"—"TO BE"*

Training Brain Repository

TRADOC G2 Training Brain Operations Center

by Training Brain Operations Center

> *I have spent a month creating a training event with the same amount of detail. If there is an existing event or even part of events in the database, it can be DONE in less than a day. It is easy to use with good design principles implemented*.

This comment (above) came from a Fort Campbell, KY, Senior Opposing Force (OPFOR) analyst during the initial unit testing in late August 2013 of the Training Brain Repository or TBR. The TBR achieved initial operating capability (IOC) in November 2013. The TBR capability began as a simple concept outlined at the Army Training Summit II to automate the exercise design process. The concept became reality in 2012 and grew to its current presence on NIPRNET and SIPRNET.

After over 10 years of continuous combat operations, unit commanders will begin to transition from Counterinsurgency Operations to a Decisive Action trained and Regionally Aligned Army requiring a focus on the systems/capabilities necessary to fight and win Unified Land Operations. According to the FORSCOM Commander's FY14 Training Guidance, two of the critical missions are a return to core competencies and training management, which the TBR is there to assist.

The TBR is a pre-JCIDS developmental software application that automates the Army exercise design process as described in the Headquarters, Department off the Army TC 7-101, *Exercise Design.* This guide provides a user the capability to create, store, access, modify and reuse exercise Warfighter Training Support Packages. The TBR currently provides a TRISA-defined Operational Environment (OE), currently the *Decisive Action Training Environment (DATE),* in support of live field training exercises. During FY14, command post exercises and exercises conducted within a constructive simulations environment become the focus. Leveraging the TBR, users (unit trainers, exercise designers, intelligence staff, experimenters and curriculum developers) will dramatically reduce the time required to design an exercise while increasing the accuracy and realism of an OE. These leaders and support staff will be able to define and request their own specific set of training data.

Dave Paschal, Training Brain Operations Center (TBOC) Deputy Director of Operations, describes the TBR as a capability built similar to TurboTax® and AutoTrader.com® capabilities. The TBR guides the user through the exercise design process, including blue force and opposing forces units and tasks. Once fully implemented, it should provide a user an 80% solution, reusing tasks, Master Scenario Event Lists (MSEL), events, storylines, and higher headquarters' operational orders. In this manner, users do not have to consistently create their own, saving them weeks or even months of time developing the training exercise. The TBR supports the development of unit tasks based upon a unit's specific Mission Essential Task List (METL), Joint universal tasks, and Army tactical tasks. The TBR will recommend corresponding OPFOR tasks, provide searchable storylines, events and role players, develop a timeline to reflect the MSEL, and develop the higher-unit Operations Order (OPORD) with annexes, as well as other training related documents. The end state will allow an Army commander and staff to collaboratively develop and plan an exercise based upon realistic and evolving data from the *DATE*, the Army Common Framework of Scenarios or a future OE.

FY14 brings considerable growth for the TBR. Phase 4 began in SEP 2013 and continues for a year with subsequent phases planned. The TBR will be the Army's "start" point within the Integrated Training Environment (ITE) for exercise design and composition. The TBR will provide modeling and simulation formatted blue, red, and green STARTEX data in support of constructive simulations no later than 09 SEP 2014, with the initial output being the Order of Battle Service (OBS) specification. Target simulations include Joint Conflict and Tactical Simulation, Warfighter's Simulation, and One Semi-Automated Force. Additionally, the TBR will allow users to develop and modify unit task organizations and to digitally depict operational graphics and Department of Defense Military Standard MIL-STD-2525C compliant military symbology.

TBOC is working with Joint Staff J7 to ensure that there is a connection with the Army ITE and J7's Joint Live Virtual Constructive 2020 (JLVC 2020) federation. The TBR establishes the weld point between the Army and Joint architectures. The goal is for an Army ITE enterprise-user to compose his joint exercise using the TBR.

_____

RUSSIAN SATELLITE DEVELOPMENTS

by Steffany A. Trofino, Threat Assessment Team (DAC)

There are multiple uses and benefits satellites provide; however, from a military perspective satellites are becoming vital in the role of global security and directly impact military operations in remote locations. Satellites enhance protection of security interests at home and abroad. The use of space and the inherent need to protect the use of space is increasingly important for the US Government during the past decade. In an era where military operations are dependent on information derived from satellite systems, the need to understand adversarial nation's satellite systems and how these systems may be used against US interests is vital in maintaining superiority in the military domain.

Since its inception, Russia's space program has continued to adapt new technologies, providing the Russian space program the status of being a frontrunner in global satellite research and development programs. During the Cold War, the Soviet Union was the first country to place a man into orbit. With Russia's recent advancements in military communication, imagery, and navigation satellite systems, Russia remains a top contender in the space research and development sector. Russia has indicated that advancements and further development of space assets will become a key priority for its security.

Understanding military communication, imagery, and navigation satellite systems will increase a soldier's awareness of Russia's enhanced satellite capabilities. Ultimately, this may leave a soldier with an understanding of how such systems may be countered while operating in the field. While there are several types of Russian satellite systems, the most common in use today focus on communications, imagery, and navigation.

Strela 3M (Rodnik) Military Communication Satellites

The first Russian space launch of 2013 took place on Tuesday, 15 January from Plesetsk Cosmodrome and carried three military communication satellites into orbit. Specifications of the systems are not known at this time; however, the Rokot launch vehicle that carried the payload into orbit was a modified version of the Russian RS-18 (SS-19 Stiletto) ICBM, which was originally designed to carry nuclear warheads to long-range targets.[1] This highlights an example of dual-use technology that is also exhibited by both North Korea and Iran which may have been assisted by Russia, as both countries have used ICBMs as SLV. The trajectory orbit for the launch indicates the missile may have carried Strela 3M military communication satellites into orbit.[2]

Strela 3M satellites are referred to as store and dump communication satellite system. The satellite is designed to collect various types of communications (fax, email, telephone data) while traveling over a specific area and storing this information in onboard databanks. Once the system reaches a destination where it is able to communicate with receiving antennas (bandwidth unknown), the system then downloads the stored information to ground receivers. Strela 3M satellite systems operate in low earth orbits (99 miles to 1,200 miles above earth) and revolve around the earth every 116 minutes.[3] With an average revolution time of nearly two hours, the satellite travels around the earth twelve times per day collecting data and transmitting this information to ground stations. The life span of each system is reported to be five years.[4]

Communication satellites are just one of the systems that Russia continues to enhance. A growing trend toward Arctic Sea interests has also affected Russia's development in imagery satellite systems. The ability to collect images during prolonged periods of darkness, such as those experienced in the Arctic region, has been a priority of the space program for several years. As a result, Russia has developed the Kondor satellite, which is the country's first remote-sensing system capable of operating in inclement weather conditions.

Kondor Military Imagery Satellites

After several years of lengthy delays, on 27 June 2013 Russia launched the Kondor satellite system into orbit. It is claimed to be Russia's first remote-sensing satellite operable in all weather conditions.[5] The Kondor is a synthetic aperture radar satellite capable of receiving, storing, and transmitting high precision data to ground stations in the microwave band in real time.

Kondor Satellite Specifications

Spacecraft mass	Originally 800 kilograms (by 2007 reported to be 1,150 kilograms)
Payload mass	350 kilograms (as of 2007)
Orbital altitude	500 kilometers (450-900 kilometers)
Orbital inclination	Up to 98 degrees toward the Equator
Image resolution (radar)	1-3 meters
Observable swath	1,200 kilometers (600 kilometers to each side of the flight path)
Radar antenna diameter	6 meters
Radar antenna frequency range	S-band (9.5 centimeters)
Spectral range of the imaging system	Optical and/or infrared
Operational life span	5 years
Launch vehicle	Strela Orbital Rocket (different from the Strela 3M satellite system)
Launch site	Baikonur, Site 175, Silo No. 59

Figure 1. Kondor satellite (*Note.* Data provided by Kondor developer NPO Mash circa 2011[10])

The system is designed to film the earth constantly in all weather conditions using high resolution, 1 millimeter images. The optical-electronic equipment can receive, store, and transmit to ground stations data from both the visible and infrared bands.[6] Kondor satellite modifications provide up to one-meter resolution of photographic and topographic images.[7] The satellites weigh up to 1,150 kg and have a life expectancy of five years.

Deputy of the Russian space agency Roscosmos Anatoly Shilov indicated that "the Kondor is an 800 kg Earth remote-sensing spacecraft designed to provide high-resolution radar imagery and terrain mapping in real-time."[8] It will be launched as part of the so-called Arktika Earth observation satellite grouping for observation of the Arctic region. Shilov stated further, "As a rule, 90% of the time the Arctic region is covered with clouds or remains in darkness due to long polar night season. In such conditions these satellites are indispensible."[9] During a recent IDEX 2013 show, Kondor developer NPO Mash disclosed that it had been preparing not one, but two launches of satellites in the Kondor series scheduled for 2013, one for the Russian Ministry of Defense and one for an undisclosed foreign customer.

GLONASS Military Navigation Satellites

Development of Russia's global navigation systems (GLONASS) began in 1976 by the Soviet military. Between 1982 and 1995, a series of satellite launches supported the navigation system's network capabilities until the network was complete. In October 2011, GLONASS achieved full global coverage, employing a total of 24 navigation satellites into the GLONASS network. In 2007, Russia signed a contract to provide GLONASS services to India.[11]

Within the past two years, the GLONASS satellite designs have undergone several upgrades resulting in the latest systems: GLONASS K and GLONASS K2. The most advanced system, GLONASS K2, will feature capabilities to transmit signals in the L1 and L2 frequencies in addition to the current L3 signal transmission capability in the 1205 MHz band. Additionally, the latest systems will have a 10-year service life, which is three years longer than its predecessor, GLONASS M.[12] The first planned GLONASS K2 launch is scheduled for 2014.[13] At the L1 frequency (1575 MHz) used by civil service providers, GLONASS K systems will offer a Binary Offset Carrier (BOC) 1,1. This will replace the BOC 2,2 option which were capable of jamming US military signals.[14]

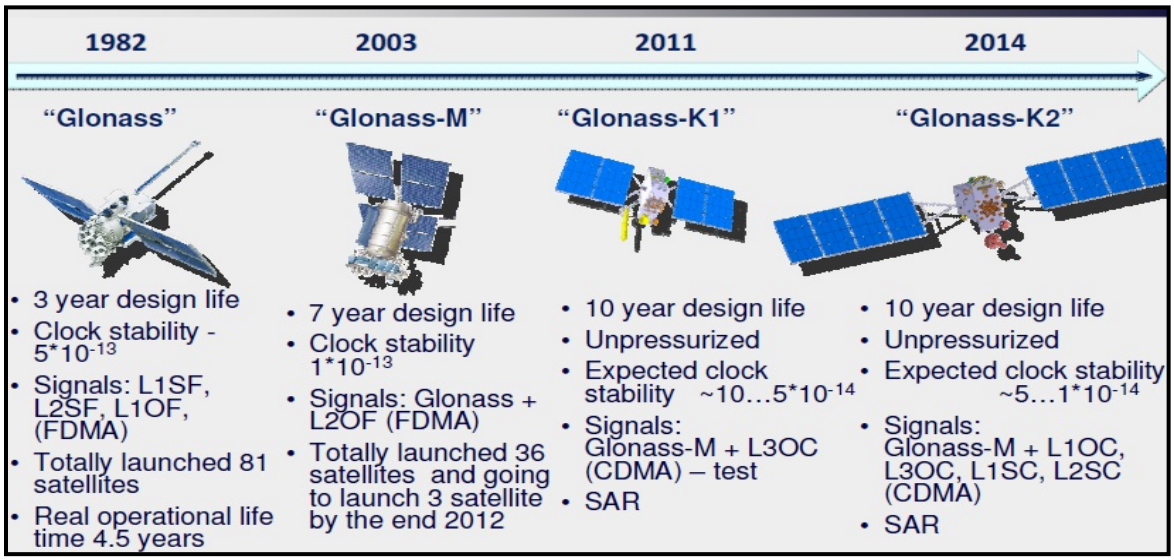


Figure 2. GLONASS future and evolutions (European Space Agency, 1 August 2012[15])

With GLONASS's enhanced capabilities such as longer orbital time and advanced signal capabilities, the network of the GLONASS constellation may require, over time, fewer resources to maintain it. Further, there will be a greater ability for less advanced nations to utilize the GLONASS commercial services, as subsidiary users provide greater capabilities for third party nations, such as India.

Understanding the approach Russia is taking with research and development programs pertaining to military satellite systems may provide analysts with a glimpse of what current vulnerabilities are present and the effective course of action Russia is taking to correct known issues. Additionally, as in the case of the Kondor satellite system, understanding the capabilities of the various systems will further provide analysts with information on what Russia believes may be of

significant importance to its military, in the future. As in the Kondor satellite system, the need to capture images through prolonged periods of darkness (such as the Arctic region) suggests Russia has a key interest in the region.

Notes

[1] "Russia set to launch three military satellites," RIA NOVOSTI, 15 January 2013.
[2] Stephen Clark, "Russia Launches 3 New Military Satellites," Spaceflight Now, 17 January 2013,
[3] Gunter Dirk Krebs, "Strela-3M (Rodnik-S, 14F132)," Gunter's Space Page, 23 May 2013.
[4] "Launch of Communications Satellites for Russian Defence Minister Failed - Daily." BBC Monitoring Former Soviet Union, 16 May 2013.
[5] "Russia may launch its first Earth remote sensing satellite in 2012," RIA NOVOSTI, 22 September 2011.
[6] "NPO Mashinostroyenia to launch two Kondor earth observation satellites," Interfax.com, 18 February 2013.
[7] "NPO Mashinostroyenia to launch two Kondor earth observation satellites," Interfax.com, 18 February 2013.
[8] Russia may launch its first Earth remote sensing satellite in 2012," RIA NOVOSTI, 22 September 2011.
[9] Russia may launch its first Earth remote sensing satellite in 2012," RIA NOVOSTI, 22 September 2011.
[10] Anatoly Zak, "Russia prepares to fly its first radar satellite," Russia Space Web, 22 February 2013.
[11] "Glonass System Satellites, Russian Federation," Aerospace-technology.com, 2012.
[12] "Russia to launch new generation satellite in 2013," RIA NOVOSTI, 16 November 2010.
[13] Yuri Urlichich, et al, "GLONASS Modernization," GPS World, 1 November 2011.
[14] "Russia's First GLONASS-K In Orbit, CDMA Signals Coming," Inside GNSS, 26 February 2011.
[15] GLONASS Future and Evolutions, European Space Agency, 1 August 2012.

OPPOSING FORCES' "BEST PRACTICES"

by Marc Williams, Training, Education, & Leader Development Team (CGI Ctr)

Accurately manned and portrayed opposing forces (OPFOR) are critical for challenging training. The standard for this is set at the combat training centers and their example is a good place to start for training at schools, centers, and home station. TRISA personnel' have been observing *Decisive Action Training Environment (DATE)* rotations at the Joint Readiness Training Center (JRTC) and have compiled a listing of "best practices" for others to follow.

At the Operations Group Level

Following TC 7-101, *Exercise Design Guide*. TC 7-101 is the place to start when planning an exercise. JRTC follows this TC, especially in the following areas:

- Getting the RTU commander's training objectives up front in the planning process.
- Using the OPFOR task organizations (TO) to build an effective scenario and task organize a realistic OPFOR.
- Conducting a countertask analysis and using Appendix B, the OPFOR Tactical Task List, to prepare for a rotation.

Using *DATE* version 2.0 as a basis to develop training scenarios. JRTC follows the *DATE* closely and adapts it to the needs of the rotational training unit (RTU). This allows them the flexibility to shift TOs and weight specific types of forces to counter the RTU commander's training objectives.

Outlining systems by Warfighting Function (WFF) to analyze realism and identify gaps. This includes liberal use of the Worldwide Equipment Guides (WEG) for weapons systems specifications. It also allows JRTC to see where capability gaps exist due to the OPFOR battalion being undermanned.

Reaching out for assistance once gaps are noted. RTUs at JRTC are Brigades, but the 1st Battalion, 509th Parachute Infantry Regiment (1-509 PIR) is an understrength unit with no assigned armor, aviation, fast attack aircraft, information warfare (INFOWAR), military police, or NBC capability. So, JRTC must reach out for assistance. In the past, this has included 11th Armored Cavalry Regiment (11 ACR) for armor and mechanized capability; 1st Information Operations (IO) Command for INFOWAR; 20th Support Command for chemical, biological, radiological, nuclear, and high-yield explosive (CBRNE) support; and 1st Maneuver Enhancement Brigade (1 MEB) for MP support. The US Navy has provided an

Aerostar team for UAS capability, US Air Force for an advanced gunnery training system (AGTS) team, and the US Marines for attack helicopters.

Detailing exercise rules of engagement (EXROE). A major objective of JRTC is to provide RTUs a tactical setting in which they can train as they will fight. The EXROE is designed to provide control while allowing maximum free play in a tactical setting. It also allows Observer-Controller/Trainers (OC/T) to objectively monitor a unit's performance. The EXROE establishes policies for the conduct of all training at JRTC. It portrays the lethality of all weapons systems (casualty and damage effects) as accurately as possible.

Replicating Realistic OPFOR in Training

- Conventional near-peer force. US forces must train to face near-peer forces in the future. JRTC replicates that capability with assigned paratroopers, highly trained with their weapons and drilled in decentralized combat. They are augmented with other capabilities as needed.
- Special Purpose Forces (SPF). SPF units are a real challenge for the RTU. Seldom operating in the open or on direct action missions, SPF teams operate behind the scenes, training, resourcing, and sometimes leading insurgent, guerrilla, or criminal elements.
- Irregular forces, especially insurgents and criminals. JRTC uses both the *DATE* and TC 7-100.3 dated 19 July 2013 for tailoring an OPFOR.
- JRTC noncombatants are portrayed by civilians on the battlefield (COB). These are role-players as US and host nation government officials, US expats working in the country, and villagers. Each are trained in their specific role and follow a role-players handbook while in the tactical box. As budgets shrink, this is becoming harder to portray.

Figure 1. Urban tactics Photo: *Fort Polk Guardian*

OPFOR Information Warfare (INFOWAR)

- JRTC OPFOR uses GPS jammers to great effect, and offensive computer actions to see the RTU plans, monitor their traffic, and insert decoy/false information into mission command systems. This includes the introduction of malware into RTU computers to take control of RTU systems and shut them down.
- Aggressively seizing RTU radios following a contact. These are used to monitor command orders and insert false/misleading orders.
- Consistent use of print and video media to present the OPFOR side of missions. This comes in the form of propaganda videos, newspaper articles, night messages, posters, handbills, and flyers.
- Intercepting unencrypted unmanned aerial systems (UAS) feeds to monitor RTU reconnaissance efforts and anticipate their intent.

At the OPFOR Unit Level

Scripted actions at JRTC usually include IED incidents, key leader engagements, media events, and chemical, biological, radiological and nuclear (CBRN) events. However, the biggest impact is in the free play action.

Use of a system to increase or lower OPFOR actions. JRTC uses a simple system of three levels with corresponding OPFOR actions and rules of action to control free play. This is designated daily by the COG and briefed to the OPFOR units at each battle update briefing. By simply stating "Today is Level ___," the COG can increase or decrease the intensity of action directed against the RTU. Changes can be requested by the OPFOR unit commander.

Conduct constant reconnaissance efforts at every level to identify unit locations, where RTU security is lax, and when units are moving. This becomes the targeting effort. The OPFOR will also observe known crossing points for water obstacles to monitor RTU vehicular activity and call for indirect fire missions.

1-509 PIR exploits every opportunity for intelligence, whether it is talkative Soldiers, open Internet sources (including unit and individual Facebook pages), or compromised radio networks. Examples include—

- Changing tactics, techniques, and procedures (TTP) if RTU elements are being successful, or battle damage assessments are undesirable.
- Shoot down RTU aircraft (including UAS) with small arms fire and MANPADS. No air threat is allowed to go unchallenged.
- Conduct counterreconnaissance efforts at every level to blind the RTU.
- State concise, clear orders followed by detailed rehearsals.

Figure 2. 1-509 PIR Commander delivering mission and intent in scenario rehearsal

- All weapons in the 1-509 PIR are zeroed every day of the exercise. The unit ensures all fires have BDA effects, and there is no use of unobserved fire.
- While in the defense, the OPFOR will liberally use obstacles which are then covered by indirect fire and small arms fire.
- Multiple layers of communications, not just tactical FM radios. There are also drills for reacting to compromised radio and computer networks.

The JRTC OPFOR fights to win every battle. Their mission in life is making the RTU have its toughest fight in Louisiana, not on a battlefield, and they excel at this mission. The best practices listed above will assist schools, centers, and home station training officers and NCOs in replicating a complex hybrid threat to challenge Soldiers at every level. Following the JRTC model will raise training standards at every level.

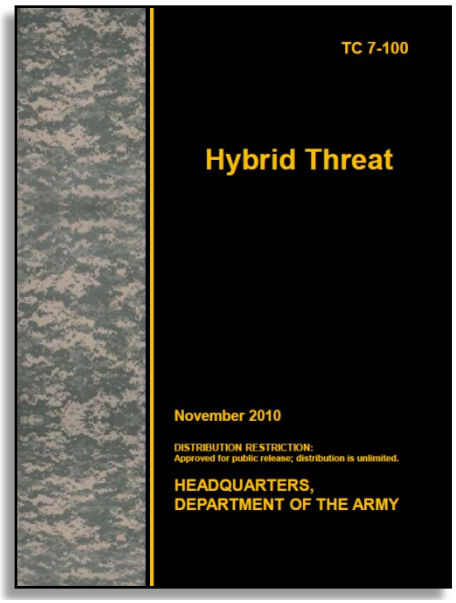
REVISITING THE HYBRID THREAT FOR TRAINING

by CPT Ari Fisher, Training, Education, and Leader Development Team

Recently, professional discussions and reading indicate that there are common misinterpretations in the Army's definition of the hybrid threat (HT). This article seeks to add clarity by revisiting some fundamental concepts found in TC 7-100, *Hybrid Threat*. Threat doctrine defines the HT for the Army as "the diverse and dynamic combination of regular forces, irregular forces, and/or criminal elements all unified to achieve mutually benefitting effects."[1] Often, interpretations present either monolithic hydras or the wolf in sheep's clothing type fallacies. The pitfall of these categorizations is that in and of themselves they form templates. Models by way of historical examples serve well as concrete experience and can be "*a"* but not "*the"* paradigm. Therefore, understanding the Army's definition of the HT lies within its adaptive composition and functional specificity rather than analogous comparisons against ill-conceived templates.

Concepts

Consistently we see categorization of the HT into monolithic hydras or wolves in sheeps' clothing. Monolithic hydras tend to be the manifestation of allied units or actors of varying types performing in collusion, sharing a common strategic vision, and possessing the capability of switching between conventional and irregular warfare at whim. On the other hand, wolves in sheep's clothing tend to be the expression of one actor who tactically fights opposite their designation of regular or irregular while sustaining themselves upon criminal proceeds. While both can be factual examples of a HT, trying to derive categories or a standard template for the hybrid threat is problematic. Therefore, there are some foundational concepts to keep in mind when considering the HT.



Conceptual consistencies carry throughout when evaluating hybrid threats. Fundamentally, "hybrid threats will use an ever-changing variety of conventional and unconventional organizations, equipment, and tactics to create multiple dilemmas."[2] Furthermore, "hybrid threats are networks of people, capabilities, and devices that merge, split, and coalesce in action across all of the operational variables."[3] Emphasis upon the term "ever-changing variety" serves to highlight the adaptive character of the HT and is innately contrary to a standard template. Furthermore, it is this attribute that should stand as substitute for the term asymmetry. An adaptive threat seeks effective countermeasures in disregard to its classification as traditional and conventional or asymmetric and irregular.

Hybrid threats will likely exploit synergy, employ a range of technologies, employ information warfare (INFOWAR) as a weapon system, and utilize complex battle positions (CBPs) and cultural standoff. Flawed is the idea that a HT will switch between conventional and irregular warfare at whim. Instead, an HT seeks to optimize the use of conventional and irregular warfare in concert. Often portrayed as a wolf in sheep's clothing, the conflict in Lebanon in 2006 serves more appropriately as an example of how an HT exploits synergy. It may be worth considering for comparison that the execution of conventional and irregular warfare simultaneously is the HT side of the decisive action coin. Also, an HT may seek to employ a range of technologies in effort to mitigate the US military's ability to achieve overmatch. Additionally, these specialized technologies may be more advanced than those held by friendly forces. Although these resources may come at varying costs, constantly reforming networks are habitually the source especially when there is a specific need and mutual benefit. Additionally, as a means, an HT will attempt to leverage as many components of INFOWAR as possible. This varies from perception management efforts within a local populace to inflicting damage on US military cyber infrastructure. Grandiose articulations portraying an HT leveraging niche technologies, all aspects of INFOWAR, and the ability to rapidly switch between conventional and irregular warfare describe the monolithic hydra. Finally, an HT will likely use complex battle positions (CBPs) and cultural standoff to protect against fires and surveillance. Fortifications, urban terrain, and subterranean facilities are some examples of CBPs. Cultural standoff uses more human aspects of the environment such as medical, religious, or other culturally sensitive facilities. Both CBPs and positions facilitating cultural standoff serve primarily to project the opposing force's power. These simple concepts identify essential and common HT traits, however, without having a standard guide, difficulty remains in articulating how these traits materialize. For this purpose, functional analysis may be most useful.

Functional Analysis

Accurately and effectively depicting the HT present without falling into a template fallacy is best achieved through functional analysis. Functional analysis is a method to help determine threat courses of action by developing how the threat may apply its capabilities against its objectives or intent; simply stated, the threat is equivalent to capabilities plus intent. Employing capabilities comes by way of tactical action which we group by function. These functions "do not change, regardless of where the force or element might happen to be located on the battlefield. However, the function of a particular force or element may change during the course of battle. While the various functions required to accomplish any given mission can be quite diverse, they can be broken down into two very broad categories: action and

enabling."[4] Consequently, functional analysis consists of resolving adversary intent and determining the capabilities available to perform the functions required to accomplish that objective.

Discovering adversary intent can be rather intangible. Often the answer lies within mission statements, stated goals, or historical activity. One thing is certain: the enemy seeks to win every battle. This determination should not be confused with the larger intent for that endeavor. Familiarly, describing opposing force objectives can be done in terms of purpose and end state.

Figure 1: Threat equation diagram

Functional tactics divides into two categories: action and enabling. Action functions are often, but not always, titled by their associative objective (i.e. assault element or exploitation force).[5] These elements are "normally responsible for performing the primary function or task that accomplishes the goal or objective."[6] Enabling functions, on the other hand, comprise "a set of capabilities that acts to assist those capabilities performing the action function."[7] Similarly titled to action functions, examples include fixing forces or breaching elements.

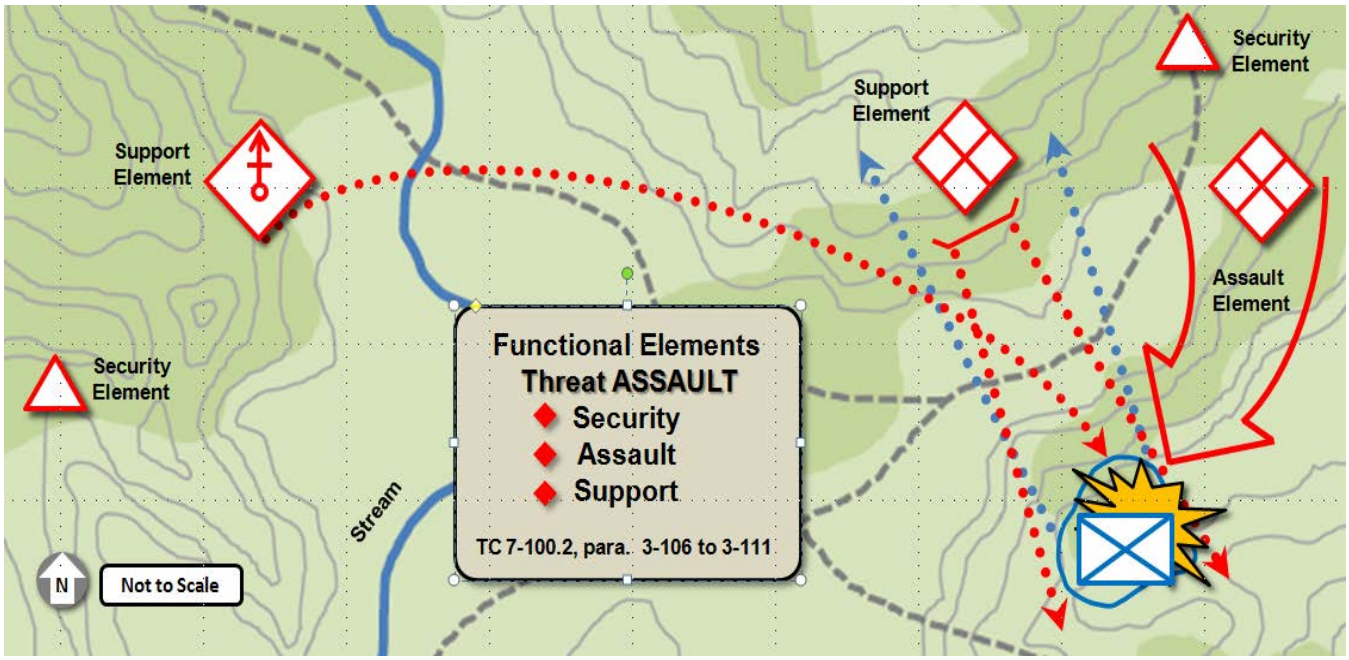


Figure 2: OPFOR tactical functions and terms (example)

There are some enabling functions so frequent they require special note. These include disruption, security, and fixing forces or elements. Disruption forces primarily exist to disrupt preparation or actions, destroy or deceive reconnaissance, and reduce the effectiveness of mission essential components of combat systems.[8] The security function seeks to "protect other capabilities from observation, destruction, or becoming fixed," facilitating isolation of the battlefield.[9] The fixing function attempts to "prevent opposing capabilities from interfering with mission accomplishment."[10]

Examples on how this can occur include, but are not limited to, suppression with fires, deception, counter mobility, or deprivation of logistics. Lending to their prevalence, these specific enabling functions share a commonality in that they have the ability to alter the combat power equation to be favorable to the adversary.

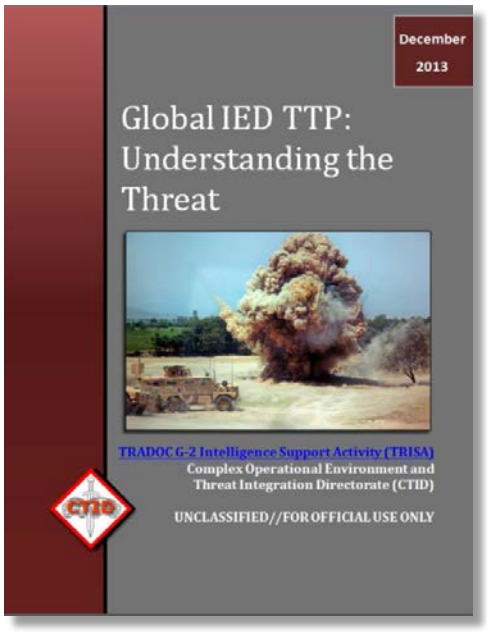
The HT places a premium upon adaptability. Looking beyond the Army's definition of the HT, TC 7-100 outlines fundamental concepts typifying that trait. Although manifestations or projections may actually be (or are believed to be) monolithic hydras or wolves in sheeps' clothing, the HT in an adaptive approach will attempt to exploit synergy, employ a range of technologies, employ INFOWAR as a weapon system, and use CBPs and cultural standoff. The challenge is to apply bedrock concepts to each problem with fresh eyes. Doing this by focusing on functional specificity will yield the most accurate representation. Consider HT adaptations in structure and action with a shade of irony as "paradoxically no matter what [the US Military] emphasizes, the military threats the United States is – or will be – most capable of defeating are the ones it is least likely to face, since potential adversaries will be deterred and seek other ways of confrontation."[11] Therefore, in order to see the enemy, we must first see ourselves.

Notes

[1] Department of the Army, TC 7-100 Hybrid Threat. Headquarters, November 2010.
[2] Ibid.
[3] Ibid.
[4] Ibid.
[5] Ibid.
[6] Ibid.
[7] Ibid.
[8] Ibid.
[9] Ibid.
[10] Ibid.
[11] Michael C. Horowitz and Dan A. Shalmon, The Future of War and American Military Strategy, Orbis, 23 February 2009.

IMPROVISED EXPLOSIVE DEVICES ACROSS AFRICA: SELECTED EVENTS

by Rick Burns (BMA Ctr) and Laura Deatrick, OEA Team (CGI Ctr) , and Jerry England, Threat Assessment Team (DAC)



Improvised explosive devices (IEDs) are not limited to the operational environments (OEs) of Afghanistan and Iraq. Despite the fact that the vast majority of Department of Defense (DoD) reporting is focused on these two OEs, IEDs are a global phenomenon. IED use will most likely persist well into the future and continue to pose a serious threat to both deployed US forces and US national interests across numerous OEs to include the United States.

A review of global IED incidents confirms that IEDs are a "weapon of choice for threat networks globally."[1] The North Atlantic Treaty Organization (NATO) and the Institute for Defense Analysis concluded that between "January 2011 and October 2012 there were 12,461 IED incidents globally, resulting in 27,169 casualties in 121 countries. Sixty-seven per cent of these attacks were conducted by 51 regional and transnational threat networks, while the other 33% were carried out by unknown perpetrators."[2] A recent JIEDDO report reveals that from August 2012 to August 2013 over 14,500 IED incidents occurred globally. The most active OEs outside of Afghanistan and Iraq in August 2013 were: Pakistan, Somalia, Colombia, and India.[3] IEDs are common across Africa. In December 2013, IED events revealed that the majority of IEDs occurred "within the Sahel Region of Nigeria, Niger, Libya, Mali, Somalia, Kenya, and Ethiopia."[4]

Most IED attacks in Africa are very simple in nature, with one perpetrator and no weapon other than the IED (or multiple "grenades"). Fewer than 20% of attacks were complex and encompassed situations such as multiple perpetrators; multiple IEDs; small arms fire (SAF) combined with IEDs; simultaneous attacks on multiple targets; and first-responder

attacks. The majority of African IEDs are stationary and placed at a specific location, such as in a shop, by a road, or next to a building.

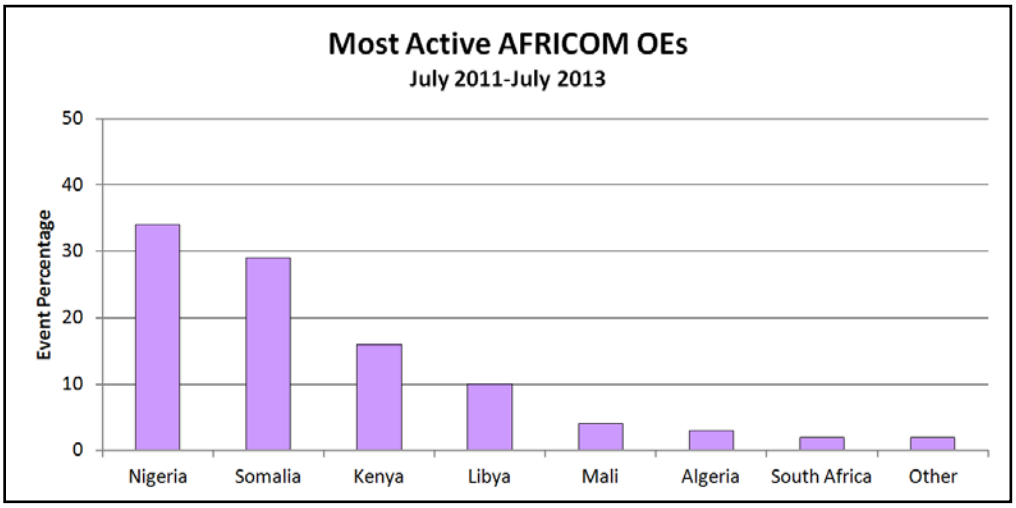


Figure 1. Understand the most active IED operational environments in AFRICOM

Across Africa, security forces were the most common known target of IEDs, followed by civilian non-combatants. Non-security government personnel accounted for about 10% of attack targets over the past two years. Other targets include foreign, media, education, infrastructure, and non-governmental organizations (NGOs). Of note, almost all IED activity of known or suspected origin was performed by Islamic individuals/groups. Of interest, al Shabaab is continuing to conduct more high-profile attacks and is expanding "its footprint to parts of northern Somalia."[5]

Groups known or suspected are—

- **al Shabaab** (Somalia, Kenya, Mali)
- **Boko Haram** (Nigeria)
- **Movement for Unity and Jihad in West Africa (MUJAO)** (Algeria, Mali, Niger)
- **AQIM** (Algeria)
- **Saccawu**—a labor union (South Africa)

The following five events represent the IED tactics currently being exploited across Africa. As with most threat actors, those operating in Africa will continue to refine, enhance, and adapt IED tactics, techniques, and procedures (TTP) as necessary and as supported by the OE. IED attacks will continue across the continent and will continue to be informed by lessons learned in the Middle East and Asia.

IED ATTACK ON CIVILIANS

The following tactic is an excellent example of a threat actor throwing an IED from a vehicle. This IED was thrown from a minibus against a civilian target in Kenya. Similar attacks have been conducted across Africa, specifically in Nigeria and Somalia.

While there is no definitive proof, al Shabaab is the threat actor linked to this event. Al Shabaab is a violent extremist organization that has led an insurgency using guerrilla warfare and terrorist tactics against the government of Somalia since 2006. The group regularly uses intimidation and violence to recruit new members. They are responsible for many assassinations of government officials, civil society figures, and journalists. Al Shabaab's IED use has increased since 2012 due to its capability to wage conventional attacks being greatly diminished. Typical tactics used are IEDs emplaced along roads, person-borne IEDs, and suicide vehicle-borne IEDs.

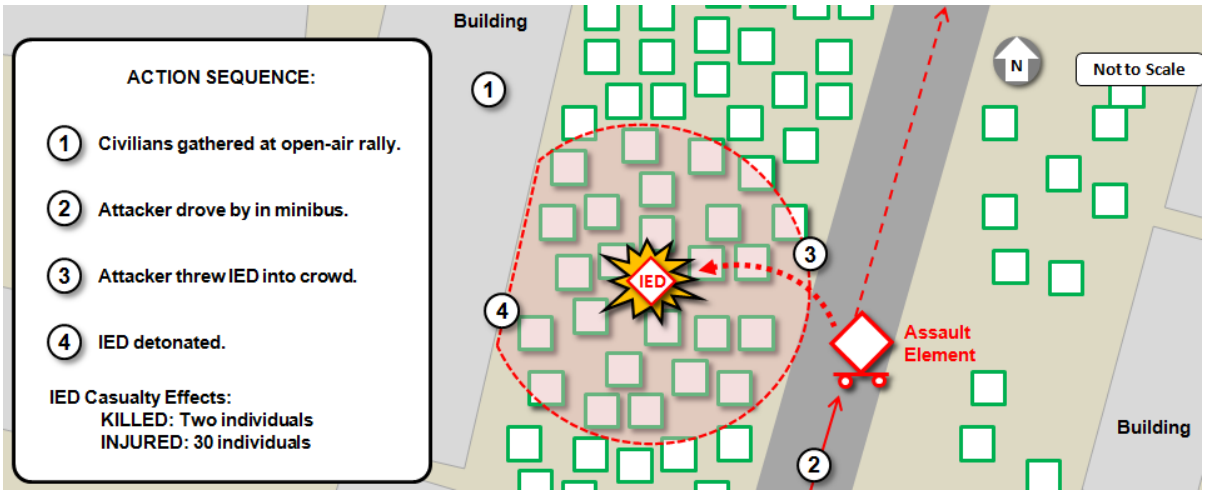


Figure 2. IED attack on civilians (example)

Prior to day of attack

- The al Shabaab assault element likely conducted area reconnaissance where the meeting was to occur. The rally had probably been publicized in advance.

31 March 2013

- The al Shabaab assault element drove the minibus on the main road close to the gathered civilians.
- An assault element member threw the IED out of the open window of the minibus.
- The IED, possibly a homemade grenade, detonated in the middle of the crowd.
- The assault element departed the scene.

Result

- Casualties were one civilian killed and 31 wounded. One of the wounded individuals subsequently died of his injuries.
- Roadblocks were set up after the attack and three suspects were eventually arrested.
- Al Shabaab released a statement regarding the attack, but stopped short of claiming credit.
- Attacks using both similar IEDs and TTP have occurred in Nairobi and Mombasa, and were generally credited to al Shabaab.

PERSON-BORNE IMPROVISED EXPLOSIVE DEVISE (PBIED) ATTACKS FOREIGN FIGHTERS IN MALI

The incident was selected as an example of typical PBIED attack used across Africa.

Prior to day of attack

- Militant reconnoitered the marketplace and investigated transportation options.
- The militant noticed that Chadian soldiers were frequent customers of the marketplace shops.
- The militant planned the attack and acquired a PBIED.

12 April 2013

- The militant took a car (most likely a taxi) to the target site.
- The militant arrived mid-morning, when the Chadian soldiers were most likely to be shopping in the marketplace.
- The militant approached a group of soldiers on foot and then detonated the PBIED.

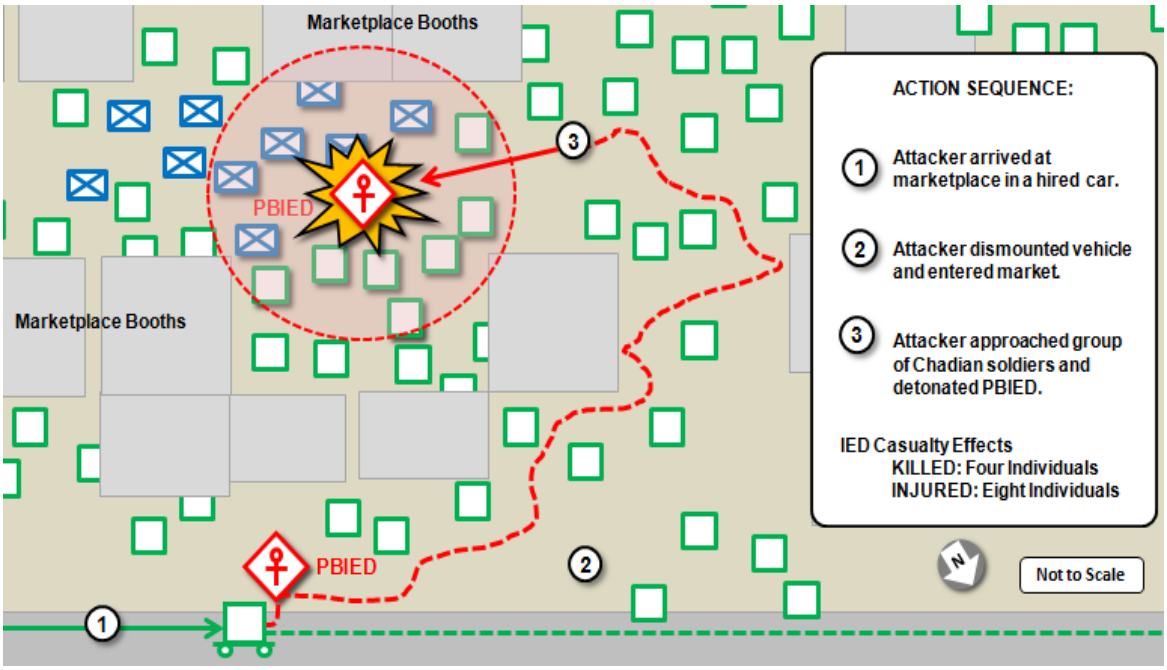


Figure 3. PBIED attack on soldiers and civilians (example)

Result

- Casualties were the bomber and three soldiers killed, four soldiers wounded, and five civilians wounded. One of the wounded soldiers subsequently died of his injuries.
- The city center was closed off and all vehicles searched after the attack.

IED ON CONVOY IN SOMALIA

This event is an example of IEDs emplaced along roads to directly attack military forces. These types of roadside IED TTP are common in Africa. In this case, the unit attacked was part of a multinational force. The convoy, carrying mostly African Union Mission in Somalia (AMISOM) troops, was attacked while en route to a base in Mogadishu's northern Shibis neighborhoods. The attackers successfully exfiltrated after detonating the IED.

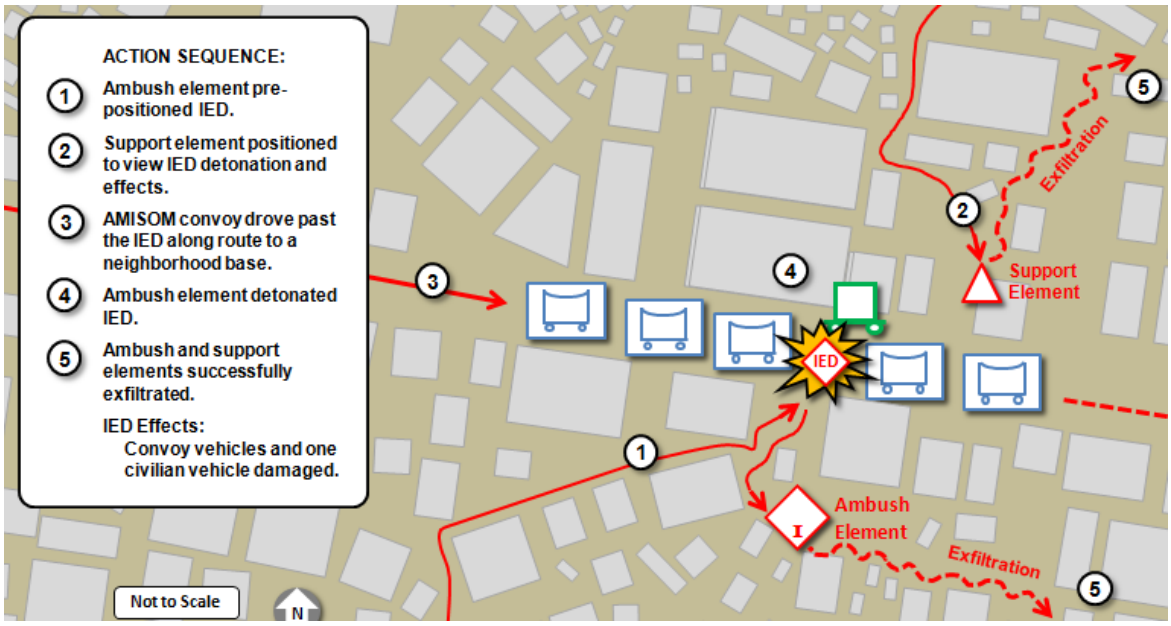


Figure 4. IED attack on convoy (example)

17 March 2012

- An al Shabaab ambush element prepositioned an IED on a main route known to be used by multinational forces.
- The support element positioned itself in order to view IED detonation and aftermath of the attack.
- An AMISOM convoy drove past the IED en route to a local base.
- The IED detonated.
- The ambush element most likely triggered the IED.
- Both ambush and support elements exfiltrated the area of attack.

Result

- The bomb damaged convoy vehicles and one civilian car.

SUICIDE VEHICLE-BORNE IMPROVISED EXPLOSIVE DEVISE (SVBIED) ATTACK ON INFRASTRUCTURE IN NIGERIA

This event is an example of a typical SVBIED attack common to Africa. Boko Haram conducted this attack against a telecommunications facility in Nigeria. Boko Haram is a militant Islamist group operating in Nigeria. Its main objective is to establish an Islamic state in Nigeria and institute sharia law throughout the country.

The group primarily targets security force personnel, local officials, and civilians. Typical IEDs used by Boko Haram are suicide IEDs (usually SVBIEDs) and vehicle-borne improvised explosive devises (VBIEDs).

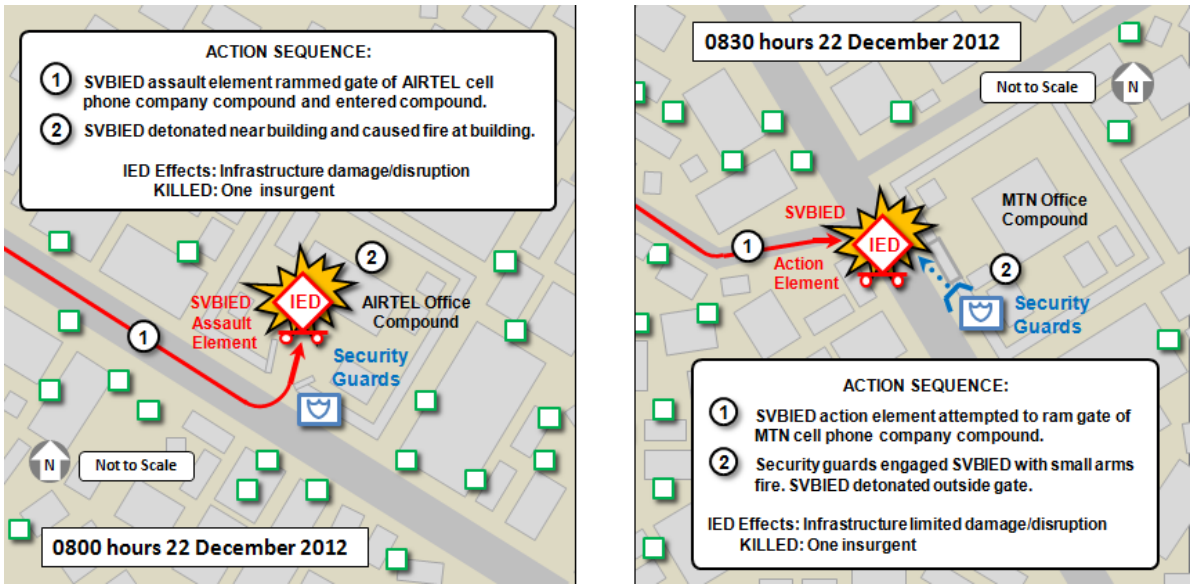


Figure 5. SVBIED attack on infrastructure (example)

22 December 2012

- At 0800 hours, an SVBIED driver approached and rammed a gate leading to the AIRTEL office building.
- The attack occurred on a Saturday when only one security guard was on duty at the gate.
- The SVBIED driver breached the gate and detonated his explosives close enough to the building to cause it to catch fire.
- At 0830, a second SVBIED attempt was made at the offices of MTN, the largest cell phone company in Nigeria.
- Security guards engaged the SVBIED driver with SAF.
- The driver was unable to breach the gate and exploded his vehicle at the gate.

Result

- There were reports of a limited interruption of cell phone service following the explosions.

IED AND VEHICLE-BORNE (VBIED) ATTACK ON GOVERNMENT BUILDINGS IN LIBYA

This attack represented the common tactic of VBIEDs and smaller IEDs used across Africa. It also had the characteristics of IED attacks perpetrated by international Islamist terrorist organizations across various OEs. This example highlights the focused targeting of political and governmental infrastructure.

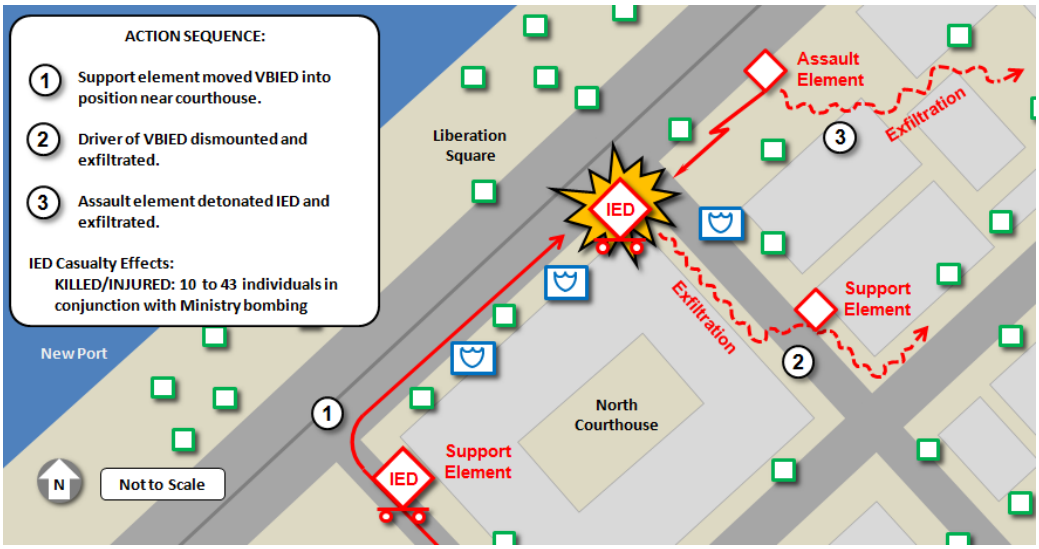


Figure 6A. Initial VBIED actions on political-governmental infrastructure

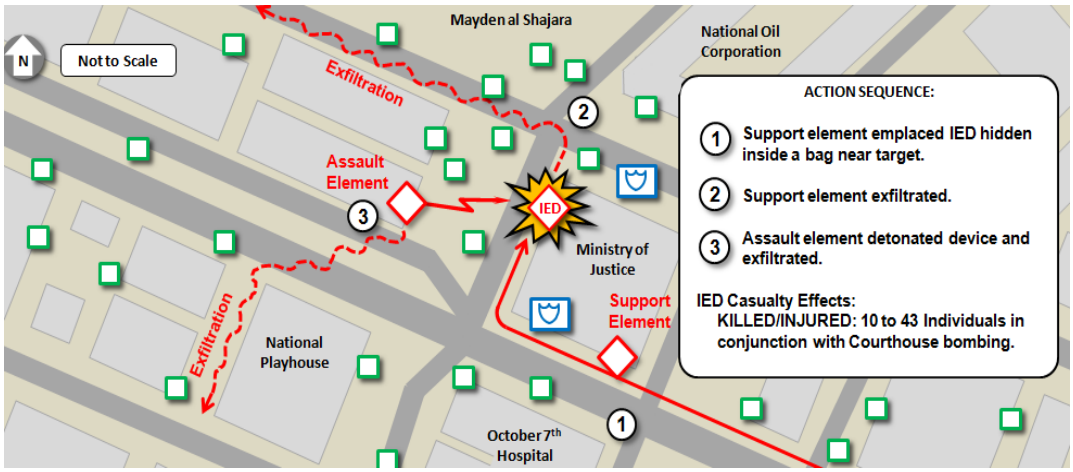


Figure 6B. IED and VBIED nearly simultaneous attacks on political-governmental infrastructure (example)

Prior to day of attack

- The action and support elements reconnoitered the area of attack.

28 July 2013

- The support elements moved the VBIED and smaller IED into position.
- The support elements exfiltrated the area.
- The action elements conducted simultaneous high-profile attacks at multiple locations.
- The targets were the locations of the 2011 initial protests of the Arab Spring. They were possibly targeted to undo support for the new government.
- Bombings occurred at 1900 hrs, after evening prayers and before a planned rally commemorating the death of a regime official that was martyred after defecting to the rebellion.
- The initial attack was a VBIED that was remotely detonated in front of the North Courthouse in Liberation Square.
- The second attack was against the Ministry of Justice building. This IED was a simple bag filled with explosives.

Result

- The explosion also damaged a hospital and the offices of the National Oil Corporation.
- Initial reports from security personnel included 10 casualties, revised by the Ministry of Health to 43.

IEDs are relativity easy to construct, depending on the type of device, and are generally effective on multiple levels. IEDs can be used at a tactical level with the target(s) being maimed or killed, or at a strategic level with the IED instilling terror in the population that influences political policy. Threat actors across Africa will continue to hone their IED skills and target US forces. For more information on African IEDs and global IED events see TRADOC G2's *Global IED TTP: Understanding the Threat*.

Notes

[1] JIEDDO, "Counter-Improvised Explosive Device Overview," 15 September – 15 October 2013.
[2] Jeffery T. Wickett, "IEDs: A Global Threat Requiring a Global Response," Counteriedreport.com, Spring/Summer 2013.
[3] JIEDDO, "Daily News Summary," 11 October 2013. Top OE analysis is based on open-source data and does not include Afghanistan.
[4] RAPID, "Global IED TTP Report," 8 January 2014.
[5] JIEDDO, "COIC Global IED Monthly Summary Report," March 2013.

WHERE ARE THE THREAT OPFOR PRODUCTS ON ARMY TRAINING NETWORK?

by CTID Operations

1. Go to ATN front-page.
https://atn.army.mil/

2. See "Training for Operations"
click "CTID Operational Environment Page"
or
3. See "DA Training Environment"
click "OPFOR & Threat Doctrine"

FIND DATA.

***ATN CTID front-page postings current as of 30 January 2014.**

by Jon H. Moilanen, CTID Operations (BMA Ctr)

Threat opposing forces (OPFOR) fight as a norm in a very practical manner. Threat OPFOR doctrine demonstrates a keen understanding and conduct of basic action fundamentals—*functional* tactics. The concept of *functional* tactics remains constant regardless of the size echelon executing a mission. The core principle is to clearly understand the threat objective. Then, organizing by functional requirement and capability, the threat synchronizes the functional execution of combat power capabilities at a specific place and time in order to achieve its objective against an enemy. Whether conducting a small dismounted unit raid on an observation post (OP) or attacking across a broad front with large mechanized and supporting aviation formations—*function* is the underpinning of understanding and effectively applying *"tactics is tactics is tactics."*

Functional Tactics and Adaptive Application

The US Army's Training Circular (TC) 7-100 series describes OPFOR that exist for the purpose of training US forces for potential or known missions. OPFOR reflect a composite of the characteristics of military and/or paramilitary forces present in actual operational environments (OEs). OPFOR may replicate an enemy that US forces are currently in conflict with or might confront during near-term and midterm missions. Similar to actual or potential adversaries, threats, or enemies, opposing forces in training present robust challenges that often reflect the composition and capabilities of a hybrid threat.

Hybrid Threat – The diverse and dynamic combination of regular forces, irregular forces, terrorist forces, and/or criminal elements unified to achieve mutually benefitting effects. (ADRP 3-0)

Functional Analysis

A threat OPFOR commander understands the mission and identifies the specific functions he intends subordinate forces or elements to perform. He applies a baseline tactical doctrine of a flexible, innovative, adaptive OPFOR with flexibility, agility, and initiative. The expectation of such complexity is applicable to the entire training and professional education communities, as well as individual Soldier, Department of the Army Civilian (DAC), and Army leader self-develpment. Environments to demonstrate and experience functional tactics range the Combat Training Centers (CTCs), the TRADOC Centers of Excellence (CoEs), schools and academies, and home station training by units and activities for operational missions.

The performance of tactical actions by OPFOR is similar to actions of US forces but focuses on the required function to determine what specified resources must be allocated to accomplish an expected outcome. Whether offensive or defensive in nature, the OPFOR commander analyzes the assigned or implied objective. Understanding available capabilities and/or the limitations and

constraints that exist for a task or mission, the commander allocates forces or elements to accomplish specified functions. The task organization is a structural representation of how the commander envisons the OPFOR to functionally perform its tactical actions and/or enabling support in mission accomplishment. The execution of functional tactics, based on functional analysis, is an integrated way to optimize capability effects with movement and manuever in a designated space and specified time period.

Functional Tactics (Concept)

The integrated conduct of primary and/or enabling actions by threat opposing forces (OPFOR) in order to achieve a task or mission objective.

TC 7-100.2, *Opposing Force Tactics*, is a basic reference on how an OPFOR commander specifies the initial organization or task organization of forces or elements within his level of command. At brigade or brigade tactical group (BTG) echelon and above in task organization, subordinate threat OPFOR units and organizations performing tactical functions are referred to as *forces*, while at battalion or battalion detachment (BDET) echelon and below, the units and/or organizations are called *elements*.

Threat OPFOR *Forces* and *Elements*

At the brigade or brigade tactical group (BTG) echelon and above, the subordinate threat OPFOR units and organizations performing functions are referred to as *forces*, while at battalion or battalion detachment (BDET) echelon and below, the units and/or organizations are called *elements*.

TC 7-100.2, *Opposing Force Tactics*

Functions do not change dependent on the size of a unit or formation. However, a function of a particular threat OPFOR *force* or *element* may change during the course of an operation. While the various direct and support functions required to accomplish a given mission can be quite diverse in their combinations as capabilities are applied in sequence, series, or parallel actions, two general categories of function are *action* and *enabling* functions.

With a common threat OPFOR language and terms, each individual and leader—particularly in a hybrid threat—acknowledges a clear understanding of how the commander or organizational leader intends to functionally operate and/or fight each of his subordinate's capabilities. Subordinates that perform common tactical tasks such as disruption, fixing, assault, exploitation, security, deception, or main defense receive a clear designation as disruption, fixing, assault, exploitation, security, deception, or main defense forces or elements. The use of precise functional designations for every force or element in a task organization minimizes any misunderstanding by subordinate units of the distinctive functions that the commander orders them to perform. These mission tasks are further confirmed during rehearsals, brief-backs, and backbriefs. This knowledge facilitates the threat OPFOR's ability to make quick adjustments and to adapt rapidly to unexpected conditions in a tactical situation.

Primary Functions: Action Forces and Elements

One part of the unit or organization conducting a particular offensive or defensive action is normally responsible for performing the primary function or task that accomplishes the overall mission goal or objective of that *action*. In general terms, that part can be called the *action force* or *action element*. In most cases, the higher unit commander identifies the action force or element with a more specific designation of its assigned mission or task.

For example, if the objective of the action at detachment level is to conduct a raid, the element designated to complete that primary action may be called the *raiding element*. In offensive actions at brigade or BTG and higher echelon, a force that completes the primary offensive mission by exploiting a window of opportunity created by another threat OPFOR is called the *exploitation force*. In defensive actions, the unit or organizations that perform the main defensive mission in the threat battle zone is called the *main defense force* or *main defense element*. However, in a maneuver defense, the main defensive action is executed by a combination of two functional forces of *contact force* and *shielding force*.

Supporting Functions: Enabling Forces and Elements

In relation to the action force or element, all other parts of a unit or organization conducting an offensive or defensive action provide *enabling* functions of various capacities to an action force or element. Each of these units or organization can be called an *enabling force* or *enabling element*. A specific functional title is assigned specific to the function or task to be performed. For example, a brigade-size force that enables by *fixing* enemy forces so they cannot interfere with the primary action is a *fixing force*. Similarly, an element that *clears* obstacles to permit an action element to accomplish a company detachment's tactical task is a *clearing element*.

Types of enabling forces or elements designated by their specific function may include—

- *Disruption force or element*. Operates in the disruption zone; disrupts enemy preparations or actions; destroys or deceives enemy reconnaissance; begins reducing the effectiveness of key components of the enemy's combat system.
- *Fixing force or element*. Fixes the enemy by preventing a part of his force from moving from a specific location for a specific period of time, so it cannot interfere with the primary threat OPFOR action.
- *Security force or element*. Provides security for other parts of a larger organization, protecting them from observation, destruction, or becoming fixed.
- *Deception force or element*. Conducts a deceptive action (such as a demonstration or feint) that leads the enemy to act in ways prejudicial to enemy interests or favoring the success of an OPFOR action force or element.
- *Support force or element*. Provides support by fire; other combat or combat service support; or command and control (C2) [the threat OPFOR uses the term "command and control"] functions for other parts of a larger unit or organization.

Tactics is Tactics

Large unit formations in offensive operations compared with a small unit assault illustrate the *functional* basis for actions and support as described in threat OPFOR doctrine. The historical vignette and assessment of major operations in an attack during *August Storm: The 1945 Strategic Offensive in Manchuria* by Glantz, presents a narrative of tactical actions and functions.

Large Scale Unit Tactics (Example WW II)

During the final phases of Russia's 1945 WW II combat actions in Manchuria, the 2d Red Banner Army conducted a supporting attack as part of the 2d Far Eastern Front in its strategic offensive operations. Three major subordinate organizations of the 2d Red Banner Army were an operational group comprised of two rifle divisions and two tank brigades; an operational group of one rifle division, one mountain rifle regiment, and one tank brigade; and a task-organized "fortified region" unit. The enemy in defensive positions along a major river line consisted of one infantry division and an independent mixed brigade of five battalions.

Artillery fires initiated the army attack that established multiple crossing sites across the river, but limited crossing equipment and bad weather conditions slowed Russian reinforcement of lead forces on the river's far banks. Gradually Russian momentum increased while supporting attacks focused on fixing and reducing enemy formations in their assigned zones. Other Russian units attacked and forced major penetrations on more than one axis in the army zone.

As enemy forces were defeated, contained in defensive positions in depth or were bypassed, Russian combined arms detachments task-organized from the operational groups exploited penetrations and continued to attack deep into the enemy rear areas. The enemy conducted strong resistance and conducted frequent localized sorties against Russian forces. Nonetheless, significant Russian artillery and aviation bombardment of enemy defenses and continued Russian ground maneuver attacks achieved enemy defeat and surrender.

The 2d Red Banner Army conducted successful offensive operations from 9-15 August 1945 over an area ranging 200 to 300 kilometers in width by 150 to 250 kilometers in depth. The army achieved its mission of fixing or defeating enemy forces in zone, and prevented their use against other major offensive actions of the 2d Far Eastern Front.

Summary from
August Storm: The 1945 Strategic Offensive in Manchuria **Glantz, D.M. (1983)**

This example of large-scale offensive actions and functions could be used in terms of how threat OPFOR brigade and task-organized higher echelon units could operate in training. The battle maps (see figure 1 and 2 below) of a corps-size area of operations in an attack have overlays with simplified symbols, control measures and terms. The small-scale unit sketches of an assault (see figure 1 and 2 below) focus also on function and tactical execution. The terms relate terms used as either threat *forces* or *elements*.

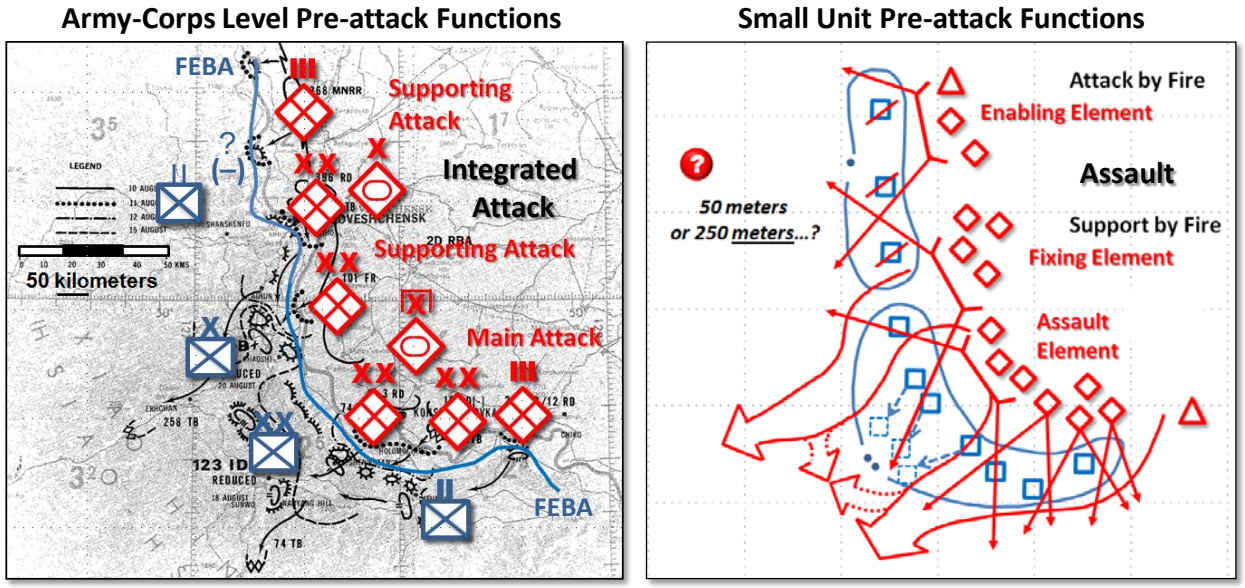


Figure 1. Echelon comparison of threat functions and terms (1 of 2) (example)

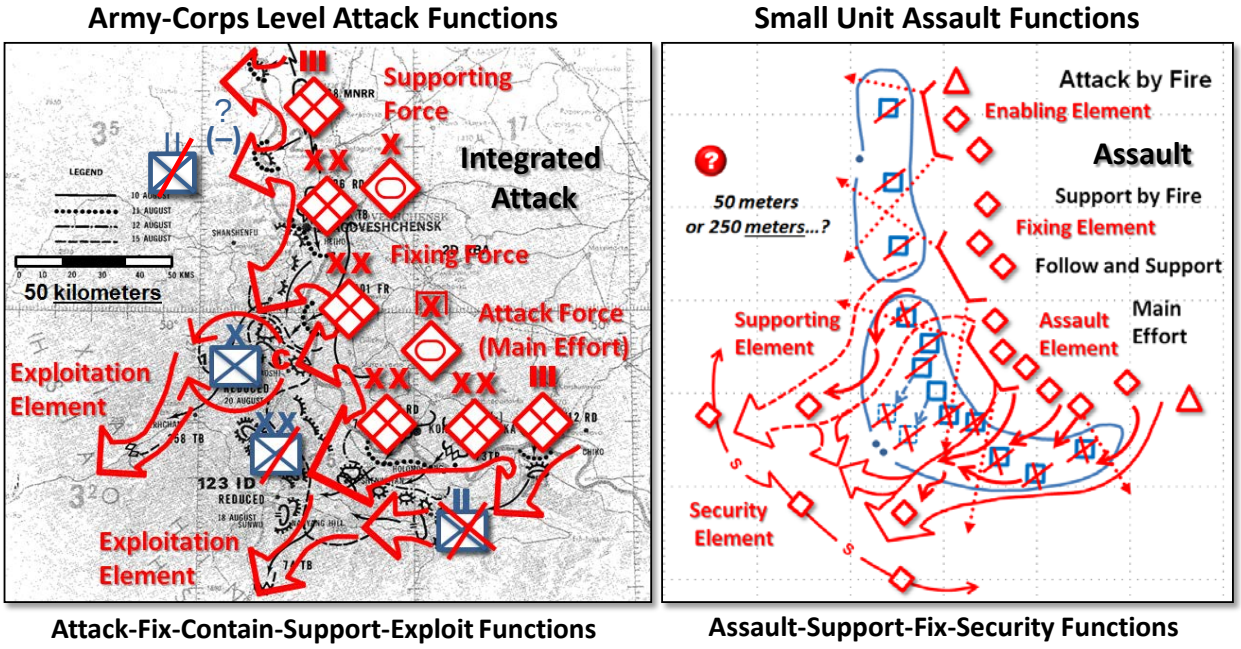


Figure 2. Echelon comparison of threat functions and terms (2 of 2) (example)

Other Threat Forces or Elements

In initial orders, some threat subordinates and capabilities are held in a status pending determination of their specific function. At the commander's or organizational leader's decision, some forces or elements may be withheld from initial actions, in *reserve*, so that this capability can influence unforeseen events or take advantage of developing opportunities. The designation of reserves is either a *reserve force* or *reserve element*. If and when such units are

subsequently assigned a mission to perform a specific function, they receive the appropriate functional force or element designation. For example, a reserve force in a defensive operation might become a *counterattack* force. In another defensive action example, a particular unit or organization may require protection from enemy observation or fire. To ensure that it will be available after the current action, the threat OPFOR commander designates that unit or organization as the *protected* force or element.

A unit or organization designated initially as a particular functional force or element may also be ordered to perform other or more specific functions during the course of an operation. In that case, the function of that force or element is more accurately described by that specific functional designation. For example, a disruption force generally disrupts enemy actions but also may need to conduct a "fix" function during a period of a tactical operation. In that case, the entire *disruption* force could become the *fixing* force, or parts of that force could become *fixing* elements.

Implications for US Army Training and Education

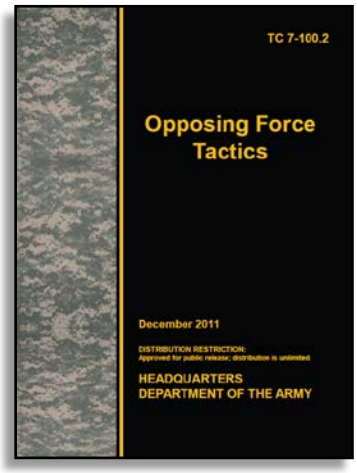
The Army provides several sources to describe opposing forces (OPFOR) for training. The training circular (TC) TC 7-100 series describes OPFOR within the conditions that exist for the purpose of training U.S. forces and achieving training objectives. A training objective consists of task, conditions, and standard. Readiness standards are identified by a unit commander and unit's mission essential task list and/or specified tasks for known or contingency operations. The *conditions* for Army training events must include a complex operational environment (OE) that is realistic, relevant, and challenging to the training unit, leaders, and Soldiers.

Condition. Those variables of an operational environment or situation in which a unit, system, or individual is expected to operate and may affect performance.

Department of Defense Dictionary of Military Terms

The threat in TC 7-100.2, ***Opposing Force Tactics***, reflects a composite of the characteristics of military and/or paramilitary forces that may be present in actual operational environments (OEs) in which US forces might become involved in the near-term and midterm. Like those actual threats or enemies, the OPFOR will continue to present new and different challenges for US forces. The overall nature of an OE is constantly changing and is an integral to situational awareness and understanding requirement for Army training.

TC 7-101, ***Hybrid Threat***, addresses an expanding category of threats and activities that do not fit into the traditional understanding of conventional and unconventional war. The focus is hybrid threats as simultaneous combinations of various types of activities by enemies and adversaries that will change and adapt over time. This TC summarizes the manner in which future threats operationally organize to fight us. Description includes the strategy, operations, tactics, and organizations of the Hybrid Threat (HT) in training exercises.



Another training circular in the series is TC 7-100.3, ***Irregular Opposing Forces***, [soon to be released on the Army Publishing Directorate website] addresses irregular opposing forces (OPFOR) which represent individual and/or composite threats and enemies. The three primary categories of irregular forces portrayed by the OPFOR are insurgents, guerrillas, and criminals. Actors may operate separately or in conjunction with one another and/or combined with regular military forces as a Hybrid Threat (HT). Other actors may be independent or may be affiliated or associated with irregular OPFOR through willing support or coercion, and/or be passive or unknowing supporters of the irregular OPFOR.

TRADOC G2 provides the threat conditions to live, virtual, constructive, and gaming (LVCG) training environments to replicate conditions representative of an actual OE. The CTID researches and sustains robust and realistic threat opposing forces for training. Requests for information and related training and education support can refer to subject matter experts and their contact information at the end of this newsletter.

WHERE ARE THE *THREATS* FOR DAILY SITUATIONAL AWARENESS-UNDERSTANDING?

by CTID Operations and TRISA Threats Terrorism Team (T3) – Terror Threat Integration

INSIDER THREAT

In addition to threats by foreign intelligence entities, insider threats will also pose a persistent challenge. Trusted insiders with the intent to do harm can exploit their access to compromise vast amounts of sensitive and classified information as part of a personal ideology or at the direction of a foreign government. The unauthorized disclosure of this information to state adversaries, nonstate activists, or other entities will continue to pose a critical threat.

Worldwide Threat Assessment of the US Intelligence Community
29 January 2014

It starts with...a Person...and ends with...Effects!

PRODUCTS SAMPLER FOR COMPLEX OPERATIONAL ENVIRONMENTS

by CTID Operations

Sampler of Products:

TC 7-100 *Hybrid Threat*
TC 7-101 *Exercise Design*
TC 7-100.2 *Opposing Force Tactics*

DATE v. 2.0
Decisive Action Training Environment

RAFTE-Africa
Regionally Aligned Forces Training Environment

***Horn of Africa OEA* 2013**
(Revised with seven states in HOA OE 2013)

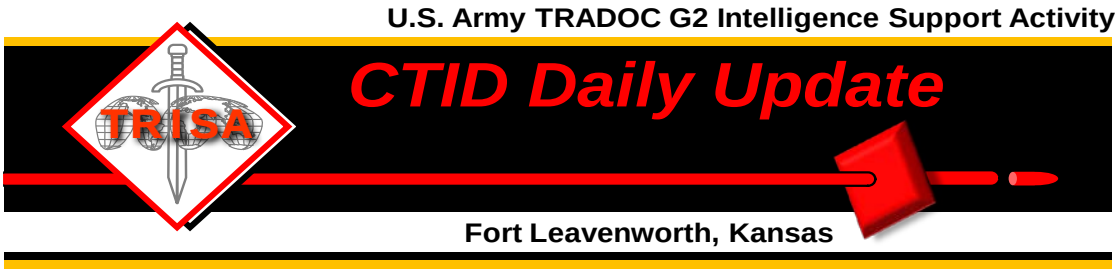
***Worldwide Equipment Guide* (WEG) (2013)**

TC 7-100.3 *Irregular Opposing Forces* (2014)

THREATS TO KNOW—*CTID DAILY UPDATE* REVIEW

by Marc Williams, Training, Education, and Leader Development Team (TELD)/JRTC LNO (CGI Ctr)

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 across the Combatant Commands (COCOMs). This list highlights key updates during the month.



03 January: **Al-Qaeda:** Abdullah Azzam Brigades chief captured in **Beirut**

Lebanon: Car bomb kills at least five in Hezbollah's **Beirut** stronghold

06 January: **Canada:** Blackout hit 30K in **Newfoundland** as 'polar vortex' sends **Prairies** into deep freeze

Yemen: Clashes kill at least 23 in north Yemen

08 January: **Syria:** Nearly 400 dead in five days of fighting between ISIS and other rebel groups

Venezuela: Outrage over beauty queen's slaying a call to action in crime-wracked Venezuela

10 January: **Al-Qaeda:** Syria militants said to recruit visiting Americans to attack US

Pakistan: Teen dies stopping suicide bomber at school

13 January: **SOUTHCOM:** Iran maintains terrorist cells in Latin America

Syria: 16 suicide attacks target Syria rebels in one week

15 January: **Missile defense:** China has successfully tested its first hypersonic missile

Afghanistan: 16 Taliban militants killed, 30 IEDs seized in Afghan operations

17 January: **US:** USDOT continues targeting Sinaloa Cartel leadership

Cameroon: Nigerian military chases terror suspects to Cameroon, kills 60

24 January: **Israel:** Israel busts 'global jihad' terror cell planning attacks, including against US Embassy

Pakistan: Six Pakistani police officers are shot dead protecting Spanish cyclist

27 January: **Al-Qaeda:** Al-Qaeda groups vow to continue attacks against Hezbollah

Egypt: Ansar Jerusalem claims SAM attack as three Soldiers killed in Sinai bus ambush

29 January: **Syria:** Turkish jets strike ISIL convoy in Syria

US: South snowstorm: State of emergency in Alabama and Georgia, five dead in Alabama, 940 confirmed accidents in Atlanta

CTID Points of Contact

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

Deputy Director, CTID Ms Penny Mellies
penny.l.mellies.civ@mail.mil **684.7920**

Liaison Officer (UK)
[pending arrival]

Operations -CTID Dr Jon Moilanen
jon.h.moilanen.ctr@mail.mil BMA **684.7928**

Threat Assessment Team Lead DAC 684.7960
Mr Jerry England jerry.j.england.civ@mail.mil

Threat Assessment Team Ms Steffany Trofino
steffany.a.trofino.civ@mail.mil **684.7960**

Threat Assessment Team Mrs Jennifer Dunn
jennifer.v.dunn.civ@mail.mil **684.7962**

Threat Assessment Team Mr Kris Lechowicz
kristin.d.lechowicz.civ@mail.mil **684.7922**

Worldwide Equipment Guide Mr John Cantin
john.m.cantin.ctr@mail.mil BMA **684.7952**

Train-Edu-Ldr Dev Team Lead DAC 684.7923
Mr Walt Williams walter.l.williams112.civ@mail.mil

TELD Team/NTC LNO LTC Shane Lee
shane.e.lee.mil@mail.mil **684.7907**

TELD Team/RAF LNO CPT Ari Fisher
ari.d.fisher.mil@mail.mil **684.7939**

TELD Team/JRTC LNO Mr Marc Williams CGI
james.m.williams257.ctr@mail.mil **684.7943**

TELD Team/JMRC LNO Mr Mike Spight
michael.g.spight.ctr@mail.mil CGI **684.7974**

TELD/MCTP LNO Mr Pat Madden BMA
patrick.m.madden16.ctr@mail.mil **684.7997**

OE Assessment Tm Lead BMA **684.7929**
Mrs Angela Wilkins angela.m.wilkins7.ctr@mail.mil

OE Assessment Team Mrs Laura Deatrick
laura.m.deatrick.ctr@mail.mil CGI **684.7925**

OE Assessment Team Mr H. David Pendleton
henry.d.pendleton.ctr@mail.mil CGI **684.7946**

OE Assessment Team Mr Rick Burns
richard.b.burns4.ctr@mail.mil BMA **684.7897**

OE Assessment Team Dr Jim Bird
james.r.bird.ctr@mail.mil Overwatch **684.7919**

CTID Mission

CTID is the TRADOC G2 lead to study, design, document, validate, and apply hybrid threat in complex operational environment CONDITIONS that support all US Army and joint training and leader development programs.

What We Do for YOU

- **Determine threat and OE conditions.**
- **Develop and publish threat methods.**
- **Develop and maintain threat doctrine.**
- **Assess hybrid threat tactics, techniques, and procedures (TTP).**
- **Develop and maintain the *Decisive Action Training Environment (DATE)*.**
- **Develop and maintain the *Regionally Aligned Forces Training Environment (RAFTE)*.**
- **Support terrorism-antiterrorism awareness.**
- **Publish OE Assessments (OEAs).**
- **Support threat exercise design.**
- **Support Combat Training Center (CTC) threat accreditation.**
- **Conduct "Advanced Hybrid Threat Tactics" Train the Trainer course.**
- **Conduct hybrid threat resident and MTT COE train the trainer course.**
- **Provide distance learning (DL) COE Train the Trainer course.**
- **Respond to requests for information (RFIs) on threats and threat issues.**

YOUR Easy e-Access Resource

With AKO access--CTID products at:
www.us.army.mil/suite/files/11318389