U.S. ARMY TRADOC G2 Intelligence Support Activity

TRISA

Red Diamond

Contemporary Operational Environment and Threat Integration Directorate (CTID)

Fort Leavenworth, Kansas | Volume 2, Issue 11 | November 2011

INSIDE THIS ISSUE

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

OEA TEAM: INCREASING IED USE OUTSIDE CENTCOM

These cheap homemade devices are becoming an increasingly popular weapon choice for terrorists, criminal organizations, and others.

By H. David Pendleton, OEA Team

A recent *USA Today* article highlighted the increased number of improvised explosive device (IED) attacks outside of Afghanistan and Iraq over the first nine months of 2011 compared to the previous year. While the number of attacks has drastically increased, IED attacks outside the United States Military's Central Command (CENTCOM) area of responsibility (AOR) are not an entirely new phenomenon. The same author wrote a similar May 2008 *USA Today* article. What has changed is that IED use as a tactic has expanded beyond terrorist groups to criminals and other groups around the world. The CTID Threat Report, IED Proliferation Outside CENTCOM, provides background on the expanded use of IEDs outside of CENTCOM and examples from other AORs.

THE COST OF IEDS HAS DROPPED DRAMATICALLY — AVERAGING $265 IN 2009, COMPARED WITH A PRODUCTION COST OF $1,125 IN 2006.

Many groups including terrorists and criminals have used IEDs as a preferred tactic for several years for multiple reasons. First, the materials to make IEDS are abundant, regardless of whether the bomb-maker uses military material or civilian products. Second, an IED reduces the user's exposure to a superior military or police force. Third, bomb-makers can produce IEDs cheaply. In 2006, materials to produce an IED cost about $1,125, but by 2009 the cost had dropped to $265. Remote-detonated IEDs cost bomb-makers only another $80 in materials. Fourth, IEDs cause a government's police and military to expend significant amounts of resources in terms of both time and money to prevent the explosion, mitigate the blast's effects, and/or track down the culprits involved. Lastly, many criminal organizations have adopted IEDs due to the apparent success of homemade explosive devices in the Middle East.

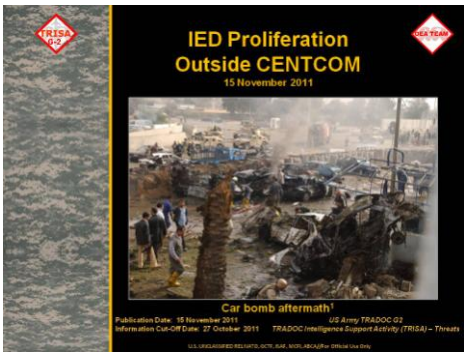
In an October 2011 article, the Joint Improvised Explosive Device Defeat Organization (JIEDDO) reported a to-date 2011 average of 608 attacks per month in 99 different >

OEA TEAM: INCREASING IED USE OUTSIDE CENTCOM *(continued)*

countries, more than double the average over the last three years. During the first nine months of 2011, government officials discovered 367 homemade bombs in the United States alone, according to JIEDDO. Action on Armed Violence, a British-based organization that maintains a database of worldwide explosive attacks since October 2010, supports JIEDDO's figures.

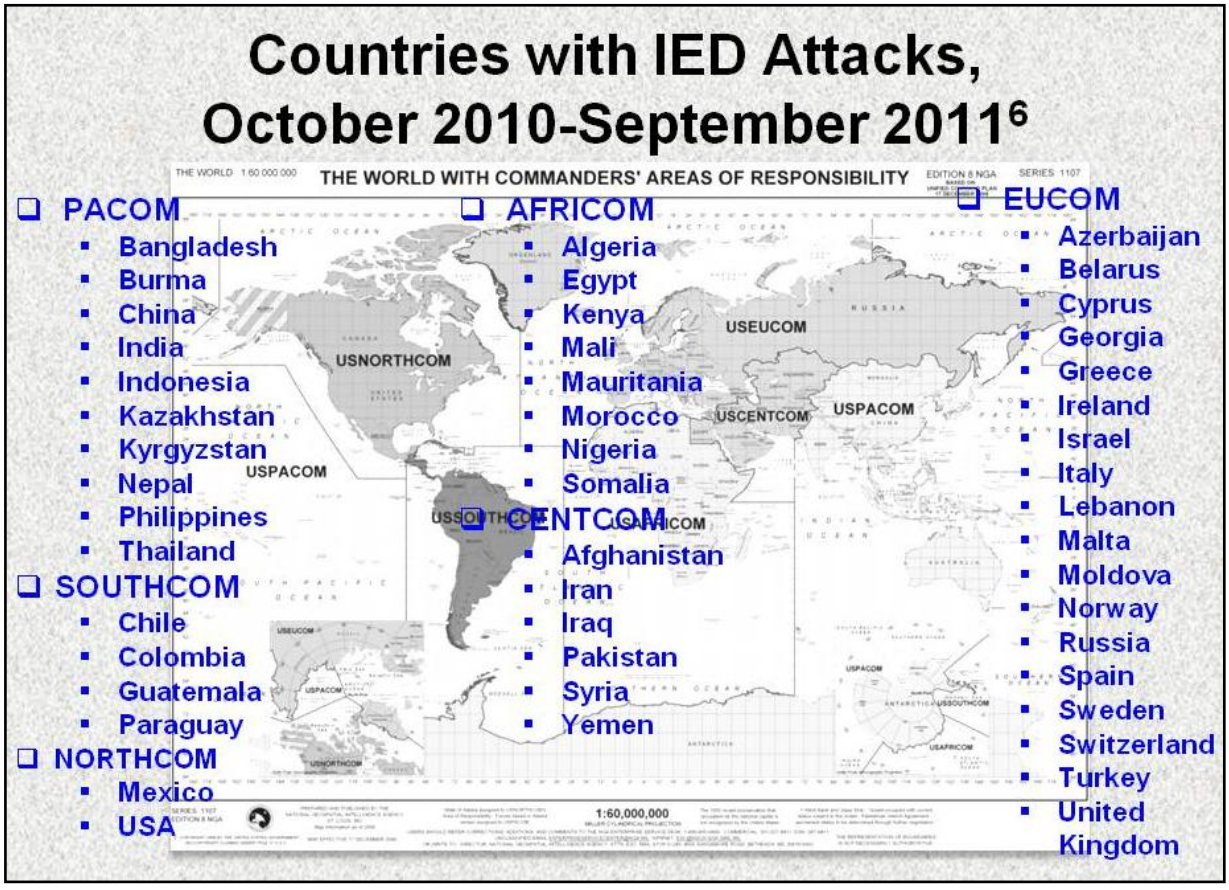
IEDs can range from very small devices—such as a letter bomb intended to injure the individual who opens it—to the very large—such as a truck bomb intended to blow up an entire building and kill hundreds of people. Bomb-makers also use whatever vehicles are available to hide IEDs, including animals, bicycles, motorcycles, cars, and trucks. The IED user's intent is to advance his agenda through a high-profile event at the expense of his victims, most of whom are chosen at random.

Over the past year, all Combatant Commands saw increased IED use in their AORs. In Asia in March 2011, an individual sent parcel bombs to three moderate Islamic leaders because of their willingness to work with members of other religions. In Europe in April 2011, two individuals—for reasons that are still unclear—placed an IED in a Minsk subway. The explosion killed 12 people, injured another 126 individuals, and paralyzed the entire Minsk public transportation system. In Colombia in July 2011, FARC guerillas injured two government soldiers by placing an IED on a horse and exploding it when the military got close to the animal. In Algeria, an Al-Qaida group took credit for an August 2011 pickup truck bomb that drove into a police station and injured approximately 30 people, half of them police officers. In Mexico in October 2011, a drug cartel lured an army patrol into a high-speed chase and then detonated an IED in a parked car as the military vehicle slowed to turn a corner.



It is likely that the trend for increased IED use outside of CENTCOM will continue for the foreseeable future. Terrorists, criminal organizations, and other disgruntled individuals see homemade bombs as a cheap and effective method to achieve their goals.

While it is impossible to prevent all IED attacks, situational awareness and vigilance by military and law enforcement will likely reduce the number of successful IED attacks and/or mitigate their effects.



6. Action on Armed Violence, Explosive Violence Reports, 1-31, 1 October 2010-29 September 2011, http://www.aoav.org.uk/archive/archive2/explosive-violence-monitoring-project-publications (accessed 24 October 2011); Map from Oak Ridge National Laboratory website, ORNL, accessed 8 August 2011 and modified by TRISA Threats, 15 August 2011, modified by TRISA, 25 October 2011

OEA TEAM: A CLOSER LOOK AT THE LORD'S RESISTANCE ARMY

The OEA Team's newest threat report shares information for Soldiers, scenario developers and trainers on this brutal Ugandan rebel group, it TTP, and LRA's long-running conflict with local government officials.

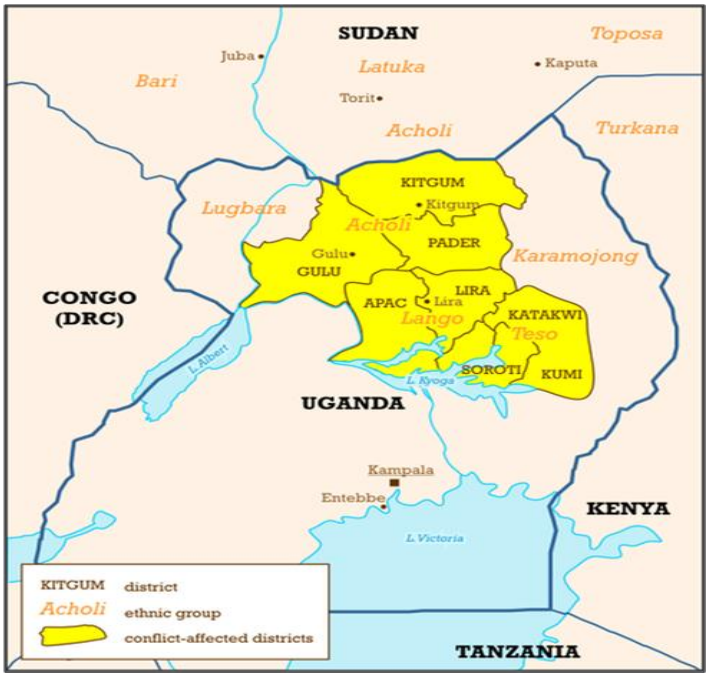
By Raines Warford, OEA Team

The Lord's Resistance Army, or LRA, is a violent rebel group led by a self-proclaimed prophet, Joseph Kony. The group arose out of the defeated Holy Spirit Movement that was created in 1986 by Kony's aunt Alice Auma. Formed in 1987, the LRA was first called the Uganda People's Democratic Christian Army. The name was later changed to Uganda Christian Democratic Army, and finally to the Lord's Resistance Army in 1991. The fighting between the Ugandan government and the LRA, now nearly a quarter century in length, is the longest running conflict in Africa.

The LRA's members initially were predominately Acholi people, an ethnolinguistic group in northern Uganda. The LRA claims to defend the Acholi. However, the group's extreme brutality is practiced against all, including the Acholi. The LRA is one of the most brutal forces in the world, routinely targeting civilians. The rebel group is notorious for murder, torture, mutilation (cutting off noses, ears, and lips is a common LRA TTP), rape, abductions of children and adults, and pillaging. Since 1987, the LRA has abducted tens of thousands of children, forcing them to serve as soldiers, laborers, and sex slaves.

Kony portrays the LRA as a Christian group whose goal is to establish a government in Uganda based on the biblical Ten Commandments. In reality, religion is used to ensure adherence to Kony's will and to sustain an environment where Kony and his commanders are feared and obeyed. Kony justifies extreme violence as a necessary "purification" of the Acholi.

Though the LRA originated in northern Uganda, it has since spread to South Sudan, Congo, and the Central African Republic. In 1994, the LRA gained the military, financial, and logistical support of the Sudanese government under President Omar al-Bashir. This was in response to Ugandan President Yoweri Museveni's support of the Sudan People's Liberation Movement/Army, which was fighting the Sudanese government. Today, the SPLM/A is the main governing party in the newly independent Republic of South Sudan. The result was the expansion of an internal Ugandan insurgency into a regional conflict. Functioning as mercenaries operating from bases in South Sudan, the LRA fought the SPLM/A.



Uganda districts affected by Lord's Resistance Army

In 2002, Uganda launched Operation Iron Fist, a cross-border offensive into southern Sudan to destroy the LRA. The operation failed and the LRA moved into northern Uganda's Lango and Teso regions, attacking civilians and causing massive displacement of the population. By 2004, 1.7 million people had been displaced. In 2005 reports revealed that nearly 1,000 people per week were dying in the IDP camps established to "protect" against the LRA.

In 2005, the International Criminal Court (ICC) issued arrest warrants for Joseph Kony and four of his commanders (two of those commanders are now deceased). The ICC charged Kony with 12 counts of crimes against humanity and 21 counts of war crimes. That same year, the Sudanese government and the SPLM/A signed the Comprehensive Peace Agreement, and the LRA was abandoned by its patron. More than a decade of Sudanese support is >

THE UGANDAN ARMY LAUNCHED UNSUCCESSFUL OFFENSIVES IN 2002 AND 2008 TO DESTROY THE LRA.

OEA TEAM: A CLOSER LOOK AT THE LORD'S RESISTANCE ARMY *(continued)*

perhaps the major reason why the LRA has survived so long.

Peace talks between the Ugandan government and the LRA started in 2006. They were eventually halted at the end of 2008 as Kony repeatedly refused to sign the final accord. During the negotiations, Kony sent raiding groups to southern Sudan, Congo, and CAR, abducting civilians to fill his ranks and stealing supplies. Facing 33 criminal counts in the ICC, Kony has no intention of making peace and giving up his power.

On 14 December 2008, the Ugandan army conducted Operation Lightning Thunder, a joint offensive with the Congolese and southern Sudanese militaries against the LRA in northeastern Congo. The operation succeeded in destroying the LRA bases around Garamba National Park in eastern Congo; however, the LRA commanders escaped. The poorly planned offensive resulted in the LRA dispersing across the region. In retaliation for the operation, the LRA carried out a series of attacks in northeastern Congo, killing more than 865 civilians and beginning a renewed campaign of violence against civilians in northeastern Congo, South Sudan, and the Central African Republic.

Over a four-day period beginning on14 December 2009 (the anniversary of the start of Operation Lightning Thunder), the LRA conducted a series of attacks on civilians in the Makombo region of northeastern Congo. The "Makombo Massacres" resulted in more than 321 civilian deaths and 250 abductions, with many of the abductees being children.

In May 2010, the U.S. LRA Disarmament and Northern Uganda Recovery Act was signed, mandating "…a strategy to guide future United States support across the region for viable multilateral efforts to mitigate and eliminate the threat to civilians and regional stability posed by the Lord's Resistance Army." The Act authorized the President "…to provide additional assistance to the Democratic Republic of Congo, southern Sudan, and Central African Republic to respond to the humanitarian needs of populations directly affected by the activity of the Lord's Resistance Army." It also encouraged U.S. funding of relief and reconstruction efforts.

LORD'S RESISTANCE ARMY LEADER JOSEPH KONY COMBINES RELIGION AND SUPERSTITION WITH BRUTALITY TO ENSURE OBEDIENCE.

In an October 2011 letter to House Speaker John Boehner, President Obama announced the deployment to Uganda of approximately 100 U.S. military personnel to help regional forces "remove from the battlefield" Joseph Kony and senior LRA leaders. The letter further states "although the U.S. forces are combat-equipped, they will only be providing information, advice, and assistance to partner nation forces, and they will not themselves engage LRA forces unless necessary for self-defense."

This new threat report, developed from unclassified sources, can be used for training and scenarios

Having kept his insurgent movement viable for nearly a quarter century, Joseph Kony has proven himself a clever leader. He exploits religion and superstition, along with brutality, to ensure obedience. Kony also exploits regional politics and borders. The Sudanese government's support helped the LRA survive for years, and dispersing his forces into several countries' territory complicates efforts to combat Kony. Defeating the LRA will prove no simple task.

The Lord's Resistance Army Threat Report provides information to Soldiers, scenario developers, and trainers regarding Joseph Kony's enduring insurgency. The information within the report can be utilized as a basis for information briefings, developing realistic training scenarios, and many other applications.

OEA TEAM: GROWING USE OF SUICIDE ATTACKS, ASSASSINATIONS IN AFGHANISTAN

Learning about suicide bombers' increased targeting of Afghan government, military, and political leaders as well as pro-governmental tribal leaders can help reduce the success of such attacks.

By Raines Warford, OEA Team

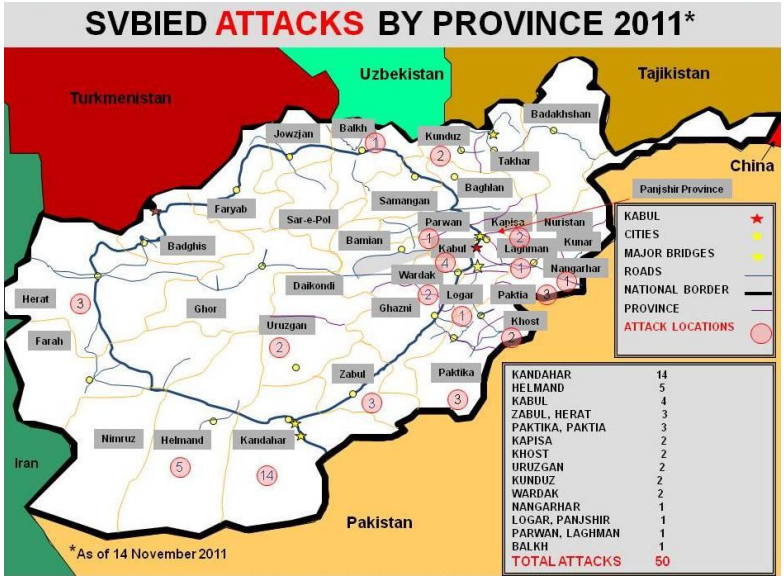
Over 700 suicide bombings occurred in Afghanistan between June 2003 and 14 November 2011. Though the attack incidents were initially infrequent, they have remained at over 100 bombings per year for the last five years. Recognizing the probability of an increase in suicide bombings, in October 2005 I began collecting open-source information regarding suicide bombings in Afghanistan in an effort to identify TTP and trends. This developed into the Suicide Attacks: Afghanistan Threat Report.

Examination of the suicide attacks reviewed in the Suicide Attacks: Afghanistan Threat Report revealed a significant increase in the use of suicide bombers as instruments of assassination in 2011, though the total number of suicide attacks remains consistent with previous years' rates. The change in the targets of suicide bombing targets, identified in the accumulated data, warranted a separate analysis that is presented in the Suicide Assassinations: Afghanistan Threat Report.

Methodology

Both Threat Reports are based on information derived from unclassified sources such as news reports, studies, and papers produced by government and nongovernmental organizations. While it is not possible for this analysis of open source information to determine the intended target of every suicide attack, it does assess the likely target of many attacks.

In the Suicide Attacks: Afghanistan and Suicide Assassinations: Afghanistan Threat Reports, the suicide attacks covered are placed in one of two categories, either body-borne attacks or suicide vehicle-borne improvised explosive device (SVBIED) attacks. Body-borne attacks are characterized by the bombers carrying the explosives on their person (most often wearing a suicide vest) while approaching their target(s) on foot. In SVBIED attacks, the explosives are transported in a vehicle of some type and/or the attacker approaches the target(s) using some form of transportation other than by foot. SVBIED attacks include suicide-vest bombers on motorcycles or bicycles.



Initially concentrated in Kabul, suicide attacks have spread to nearly every Afghan province—with the majority in provinces bordering Pakistan.

In the Threat Reports, multiple suicide attackers at the same location have been counted as one suicide attack—unless the suicide bombers utilized different delivery methods or the bombings were separated by a significant amount of time or distance. For example, if an SVBIED was detonated and two suicide bombers wearing explosive vests then attacked at the same location, it would be counted as two suicide attacks (one SVBIED and one body-borne attack).

For purposes of the Suicide Assassinations: Afghanistan Threat Report, attacks are differentiated as successful assassinations or unsuccessful suicide assassination attempts. Suicide attacks that killed an Afghan politician or law enforcement, military, or intelligence service official in a leadership role or a pro-government tribal leader are considered successful suicide assassinations. Suicide attacks which wounded such individuals or occurred in close proximity to them or their office or vehicle are considered unsuccessful suicide assassination attempts. It is certainly possible that other suicide assassination attempts have occurred that were not noted as having targeted a particular leader either associated with the Afghan Government or >

OEA TEAM: GROWING USE OF SUICIDE ATTACKS, ASSASSINATIONS *(continued)*

recognized as adhering to a pro-Afghan Government stance. However, in this Threat Report, only those suicide attacks which met the criteria above were considered in the statistical analysis.

Results

An examination of the data reveals some intriguing information. Suicide attacks were originally concentrated in Kabul, with all attacks in 2003 and 2004 occurring in that province. In 2005, suicide bombings were carried out in Kabul, Kandahar, Herat, and Balkh provinces. Since 2005, suicide attacks have occurred in almost every Afghanistan province, with the majority happening in provinces bordering Pakistan. Kandahar Province, the birthplace of the Taliban, has experienced more suicide bombings each year than any other province. It comes as no surprise that suicide assassinations and suicide assassination attempts are also highest in Kandahar.

Initially, suicide bombings predominately targeted foreign soldiers and then progressed to targeting Afghan security forces. Currently, insurgents appear to be emphasizing the use of suicide bombers for the purpose of assassinating specific Afghans who are identified as government or government agency leaders, or civilian leaders who are pro-government. Afghan government officials such as politicians, law enforcement and/or military leaders, intelligence officials, and pro-government tribal leaders are prominent targets for suicide assassins.

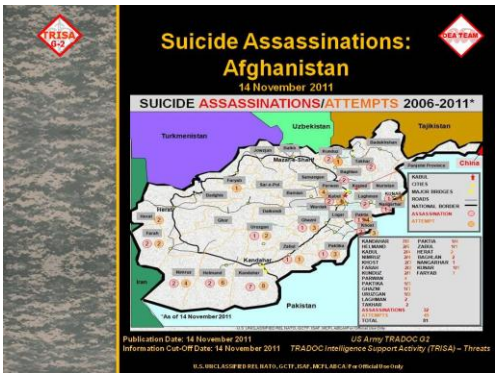
Interestingly, the incident generally accepted as Afghanistan's first suicide bombing, the 09 September 2001 killing of Northern Alliance Commander Ahmad Shah Masood by two al-Qaeda operatives posing as journalists, with a bomb hidden in a video camera, was a suicide assassination. Despite this initial success, suicide bombing apparently was not utilized again as an assassination method in Afghanistan until March of 2006.

The absence of suicide assassinations/attempts for a period of four and a half years is puzzling. Once the TTP reemerged, the number of suicide assassinations and attempts remained consistent, averaging 10.6 attacks per year from 2006 through 2010. In 2011, though, 28 attacks have occurred—14 of which were successful suicide assassinations (as of 14 November).

A possible explanation for the sudden increase in the utilization of suicide bombings to assassinate Afghan leadership may be that insurgents are responding in kind to the targeting of their own leadership. Data collected by Bill Roggio and Alexander Mayer and published on The *Long War Journal* website reveals that U.S. aircraft strikes against Taliban leaders in Pakistan more than doubled in 2010 compared to 2009. Perhaps correspondingly, suicide assassination attacks in Afghanistan have already more than doubled in 2011 compared to 2010. While not definitive proof, this presents a possible cause-and-effect relationship.

Increased suicide assassination attacks in Afghanistan may be an insurgent response to assassinations of their leaders.

The effectiveness of suicide assassination attacks in Afghanistan notably increased in 2010, though the total number of incidents remained consistent. The average success rate of suicide assassinations over the four-year period from 01 January 2006 to 31 January 2009 was only 28.5%, with a single-year high of 36% in 2008. Six of the 11 suicide assassination attacks in 2010 were successful—a 55% success rate.



As of 14 November, 14 out of 28 suicide assassination attacks during 2011 have been successful—a 50% success rate. Though the total number of suicide assassination attempts more than doubled so far in 2011 compared to 2010, the success rate decreased by 5%. It is unclear why suicide assassinations are less effective this year than last. Rather than speculate on possible reasons, the Suicide Assassinations: Afghanistan Threat Report presents the data and allows readers to draw their own conclusions.

The Suicide Attacks: Afghanistan and Suicide Assassinations: Afghanistan Threat Reports, while not finished intelligence products, provide information to deploying units, scenario developers, and trainers regarding the threat from suicide attacks and assassinations in Afghanistan. The reports provide information including data, trends, details of attacks, and maps with attack locations. These Threat Reports are frequently updated—usually whenever a new attack occurs. The information in the reports can be utilized as a basis for force protection briefings, developing realistic training scenarios, and many other applications.

OPFOR DOCTRINE: MANPADS AMBUSH BY INSURGENTS WITH SPF SUPPORT

By Jon Moilanen, OPFOR Team

Functional Organization of Elements to Conduct an MANPADS Ambush

An *ambush* is a surprise attack from a concealed position, used against moving or temporarily halted targets. In an ambush, enemy action determines the time of attack, and Opposing Force (OPFOR) insurgents choose the place of attack. This example uses a man-portable air defense system (MANPADS) to ambush an enemy helicopter.

The OPFOR considers every insurgent with a MANPADS to be an air defense firing unit. Although the desired effect of the ambush is to destroy an enemy aircraft, success can also be preventing an enemy aircraft from conducting its intended air activity. The sudden, unexpected destruction of an aircraft can significantly degrade an enemy operation. Just one air defense ambush can temporarily disrupt enemy ground and air operations in the conduct of a mission. *(See Chapter 11, TC 7-100.2,* Opposing Force Tactics*, for information on air defense ambushes that can be used by OPFOR insurgents.)*

Background Situation

A multi-functional insurgent direct action cell is operating in restrictive mountainous terrain. Ambushes have been successful against motor convoys along a single roadway through the mountain chain. The OPFOR insurgents have observed an increase in enemy helicopter surveillance along the valley route at low to medium altitudes. The local insurgent organization requests clandestine

Enemy helicopter moments before air defense ambush

support from a regional governing authority adjacent to the geographic territory of the insurgency. The capability provided is a task-organized special-purpose forces (SPF) air defense team comprised of four SPF soldiers and three Starstreak MANPADS missiles. The SPF team infiltrates into the insurgent area. *(See FM 7-100.4,* OPFOR Organization Guide*, for SPF team organizational options and principle weapons and equipment.)*

Air Defense Ambush

The OPFOR insurgent air defense ambush is conducted in three phases: deployment, preparation, and execution. After infiltrating into the area, the SPF team trains the insurgent cell on missile system maintenance, operations, and air defense ambush tactics.

Deployment. The SPF team remains with the insurgents to observe and advise on insurgent tactical operations. A related SPF task is to report on insurgent air defense ambush successes for use in the insurgency's information warfare (INFOWAR) campaign. *(See Chapter 15, TC 7-100.2,* Opposing Force Tactics*, for more information on SPF and their support of OPFOR insurgent actions.* The Worldwide Equipment Guide, Volume 2*, presents details on the Starstreak missile in an air defense role.)*

Preparation. This example of an OPFOR insurgent ambush using a MANPADS has three types of elements:

- **Ambush elements.** A primary OPFOR insurgent element with two missiles and an alternate element with one missile, in separate locations, comprise the ambush elements. The insurgent cell leader commands both elements. The SPF team leader and SPF communications specialist accompany the insurgent cell leader to observe ambush actions. The SPF assistant air defense team leader and machinegunner locate with the alternate ambush element to observe from that vantage point.
- **Security elements.** Insurgent security elements locate some distance from the ambush site kill zone, each armed with automatic weapons and hand-held radios, in order to provide early warning of any approaching enemy helicopter and/or any ground maneuver forces along the route. Other insurgents

>

OPFOR DOCTRINE: MANPADS AMBUSH BY INSURGENTS *(continued)*

provide local security for each of the two ambush elements.

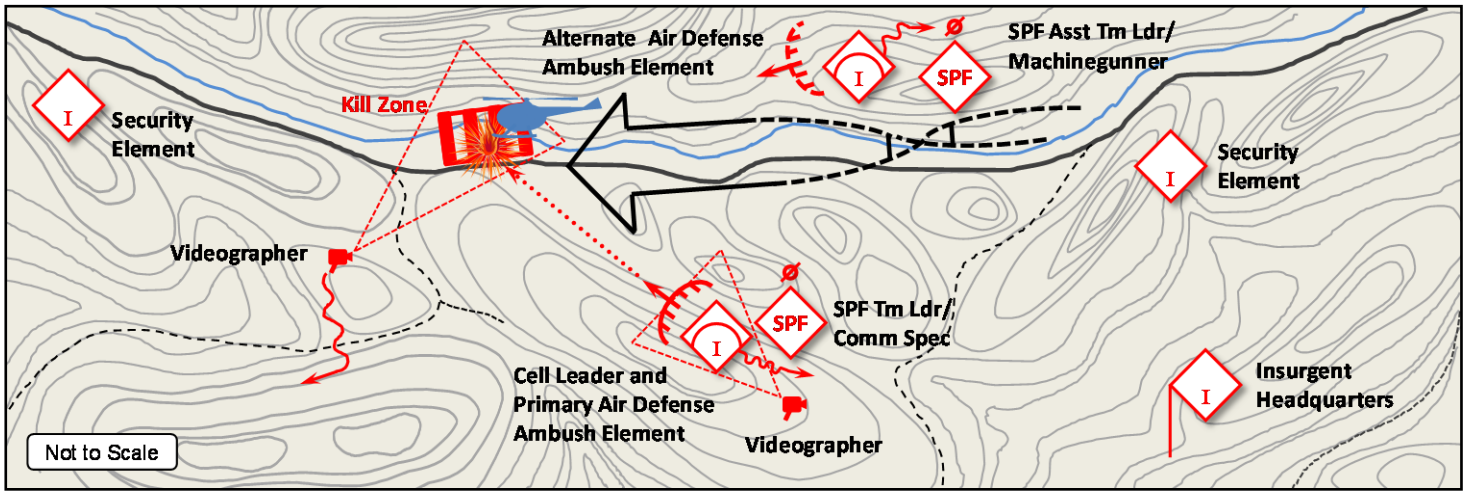
- **Support element.** A videographer pre-positions near the primary ambush element to record preparations for the attack and the missile launch against a helicopter. A second videographer locates high on the mountainside above the kill zone and prepares to record the missile hit and subsequent helicopter crash. After the attack, the audio-video coverage will be transferred to a courier for hand-delivery to a regional media outlet in support of the insurgent INFOWAR campaign.

Execution. Security elements report the approach of a single light observation helicopter flying down the valley. No ground maneuver or logistics vehicles are on the road. Both ambush elements, accompanied by SPF, move from hide positions to their camouflaged firing positions, masked by terrain, and prepare to attack. The order to attack is on command of the insurgent cell leader. The attack plan is for only the primary element to launch their Starstreak missile. If the ambush is successful, the alternate element will not fire. If the primary missile misses the helicopter, the insurgent cell leader will give permission for the alternate ambush element to engage the helicopter.

The insurgent cell uses two camouflaged fire teams for the attack—a primary element to launch the initial missile and a second to complete the mission if the first missile misses its helicopter target.

The helicopter flies into the kill zone. The primary ambush element confirms acquisition of the helicopter and receives permission to fire the Starstreak missile. The high-velocity missile hits and causes an immediate flight failure. The helicopter attempts to auto-rotate to a semi-level clearing on the mountain slope, but crashes into the mountainside, and explodes moments later. The air defense ambush destroys the helicopter, and no crew members survive the explosion.

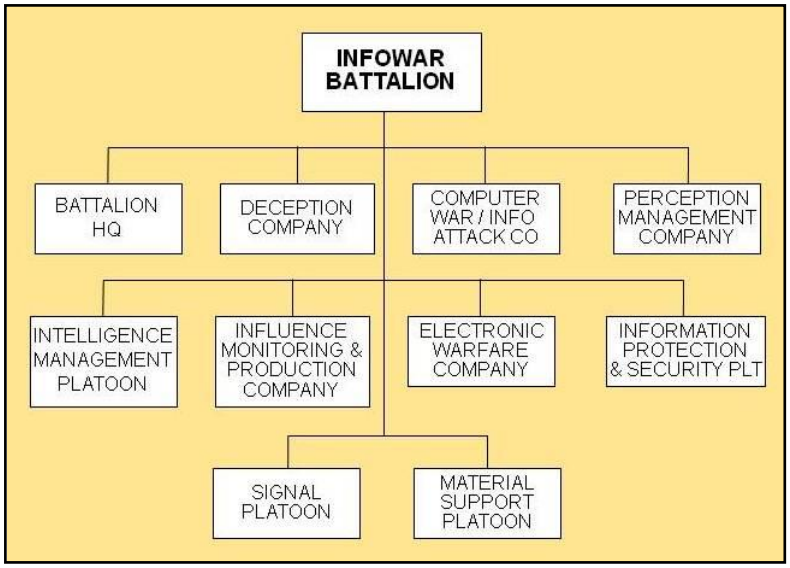
Both ambush elements move to a common rendezvous and conduct a review of the mission. The SPF team remains with the local insurgent organization for another week to conduct tactics training and missile equipment preventive maintenance with other insurgent cells. As the SPF team exfiltrates from the mountain valley, Starstreak missiles are now part of the insurgent arsenal—with trained insurgent missile gunners for air defense ambush and other tactics along an enemy logistics route in a mountain corridor.



Insurgent MANPADS ambush with special purpose forces support

OPFOR DOCTRINE: HOW-TO'S FOR AN EFFECTIVE OPFOR INFOWAR BATTALION

By Jerry England, OPFOR Doctrine



The OPFOR is constantly increasing the levels of technology used in its communications, automation, reconnaissance, and target acquisition systems. In order to ensure the successful use of information technologies and deny its enemy the advantage afforded by such systems, the OPFOR has continued to refine its doctrine and capabilities for information warfare (INFOWAR). The OPFOR knows it cannot maintain continuous information dominance, particularly against peer or more powerful opponents. Therefore, it selects for disruption only those targets most critical to ensuring the successful achievement of its objectives. It attempts to gain an information advantage only at critical times and places on the battlefield. *(See TC 7-100.2* OPFOR Tactics, *Chapter 7 Information Warfare.)*

INFOWAR Battalion

The tactical and operational organization used to perform the OPFOR INFOWAR mission at both the operational and tactical level is the INFOWAR battalion. Comprised of five specialized companies and four support platoons, the INFOWAR battalion is a multifunctional organization conducting the following tasks against the enemy:

- Destroy and degrade information systems, sensors, and the means to communicate.
- Disrupt/control the flow of information.
- Deny enemy forces the ability to collect information on the OPFOR.
- Deceive decisionmakers.
- Exploit weaknesses in electronic and information assurance countermeasures.
- Influence key leaders, and the population within the area of operations.

Tank decoy

Each company applies its unique skills and resources both individually and with other OPFOR units to achieve information dominance at critical points in the course of operations. The INFOWAR battalion can help create the necessary windows of opportunity for many types of offensive or defensive action by executing effective deception techniques, perception management, electronic warfare (EW), computer warfare, and physical destruction operations.

Deception Company

The deception company produces products and talking points designed to mislead enemy decision-makers, cause confusion in the decision-making process, and persuade the local population and/or international community to support OPFOR objectives. The OPFOR operational level deception plan is implemented by the deception company. Specialized equipment includes decoys and transmitters designed to mimic actual units in the field. An Internet production platoon is tasked with creating disinformation products and digital profiles for fabricated organizations and individuals. The deception company works closely with the perception management company when necessary to achieve effects with the local population and/or the international community.

Computer Warfare/ Information Attack Company

The computer warfare / information attack (CW/IA) company is the heart of the OPFOR's computer warfare operations, charged with attacking enemy computer systems or command nodes through unauthorized access (hacking) and insertion of malicious software. The CW/IA company will develop software packages designed to perform the necessary functions on target systems. The functions can range from simple denial of service attacks to manipulation of utility >

OPFOR DOCTRINE: HOW-TO'S FOR OPFOR INFOWAR BATTALION *(continued)*

control systems. However, they usually include five main steps.

1. Use zero day attacks or social engineering to infiltrate the target system.
2. Establish command and control through remote access tool.
3. Elevate access and authorization privileges.
4. Acquire data and prepare for electronic exfiltration.
5. Electronically exfiltrate from the target system.

The CW/IA company may employ elements of the perception management company to assist in using social engineering techniques to gain access to the targeted systems. In step four, data may be harvested for intelligence purposes or manipulated in order to sabotage the enemy's decisionmaking process. In step five, the exfiltration plan may include steps to erase evidence of the breach and to include an electronic back door as an access point for future operations. The steps above describe a technique typically used to harvest information for intelligence purposes. However, the OPFOR can use the same technique to access its enemies' systems in order to degrade, deny, or destroy their operations.

Perception Management Company

The perception management company assists the OPFOR commander in creating a perception of the truth that best suits the OPFOR. The perception management company uses its psychological warfare and direct action platoons to engage in subversion, sabotage, coercion, or extortion to influence key leaders among the population and its enemies' forces. The purpose of these operations is to project a message favorable to the OPFOR. The dissemination platoon will create and distribute products and conduct local level key leader engagements with themes designed to influence the local population. The research and planning platoon will conduct opinion polls and other surveys to gauge effectiveness and plan for future operations.

Influence, Monitoring, and Production Company

The influence monitoring and production company will conduct media manipulation operations and public affairs operations for the purpose of building public and international support for the OPFOR's military actions. Reinforcement of its message (preferably by different sources) is also a powerful tool the OPFOR uses to convince the target audience of the OPFOR position. The OPFOR exploits the international media's willingness to report information without independent and timely confirmation. Operations targeting the media are aimed at influencing domestic and international public opinion. OPFOR techniques seek to define events in terms the OPFOR chooses. While most aspects of media manipulation are applicable at the operational level and above, operations at the local level can have major effects on the tactical fight.

Jamming system

Soldiers attending a hacker class

Electronic Warfare Company

The EW company provides support to the OPFOR with jamming and target location capabilities. The EW company has the mission of protecting OPFOR forces from attack, denying information to the enemy, and disrupting and intercepting the enemy's voice and data communications. The EW company also possesses a unmanned aerial vehicle platoon to provide aerial jamming capability against specified targets. Equipped with a network of electronic attack and signals reconnaissance elements, the EW company monitors the electromagnetic spectrum and disrupts hostile transmissions by jamming enemy communications nodes. The EW company has the capacity to disrupt, deny, and degrade enemy communications across a wide area of the electromagnetic spectrum. Some of the targets include global navigation satellite systems, tactical voice communications, cell phones, personnel communications devices, tactical data networks, and enemy radar systems.

TRAINING & EDUCATION TEAM: UPDATED TRAINING ENVIRONMENT TO SUPPORT KEY TRAINING AT HOME STATION

Scheduled to be released in December on AKO, the Decisive Action Training Environment (formerly the Full Spectrum Training Environment) will provide tools to help battalions and smaller develop customized training.

By LTC Terry Howard, Training & Education Team

After 9/11, most U.S. Army pre-deployment preparation shifted away from using local Home Station Training (HST). Training was done by the Combat Training Centers (CTC)—the National Training Center at Fort Irwin, CA; the Joint Readiness Training Center at Fort Polk, LA; the Joint Multinational Readiness Center at Hohenfels, Germany; and the Mission Command Training Program (formerly the Battle Command Training Program). Taking advantage of modern technology, the Army sent lessons learned in major Afghanistan and Iraq theaters of operation to the CTCs so they could be taught in near-real time—using Mission Readiness Exercises (MRXs) to train Rotational Training Units (RTU) preparing for deployment.

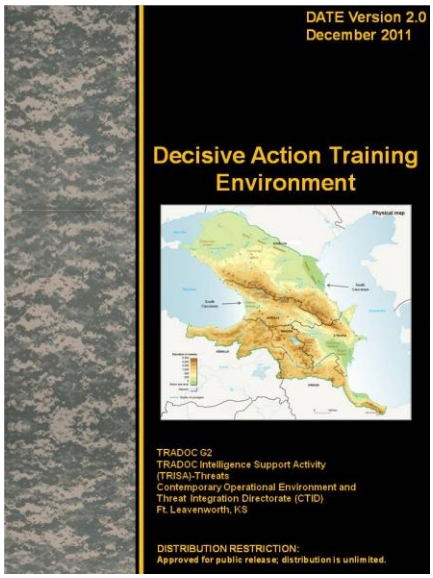
With the conflicts in Afghanistan and Iraq coming to a close, the military will need to adjust its training strategy for the next conflict. "Where" the next conflict will be and "who" we will face is anybody's guess. However, no matter where U.S. Soldiers are sent, they will need to be properly trained to fight in any region of the world.

As the conflicts in Iraq and Afghanistan draw to a close, the U.S. Army likely will return to home station training to prepare Soldiers for future conflict.

In an era of worldwide financial crisis and with U.S. Defense cuts being tossed around in Washington, the U.S. military faces some tough challenges ahead. Perhaps the toughest will be keeping Soldiers fully prepared to fight anywhere in the world, while on a limited budget. Because of the enormous cost of sending a unit to train at a CTC (often in excess of $30 million for a Heavy Brigade Combat Team), future use of the CTCs will most likely become less frequent.

To reduce training costs, HST will be "how" the Army trains its force the majority of the time. Battalion-size units and smaller will likely train at their respective military posts, and their training will use a scenario or scenarios based on the new Decisive Action Training Environment (DATE), previously known as the Full Spectrum Training Environment. This TRADOC G2-approved document defines operational environment (OE) conditions for building decisive action training scenarios. The DATE OE consists of five fictional countries (Ariana, Minaria, Atropia, Donovia, and Gorgas) located in the North and South Caucasus. The DATE views these five actors through the lens of the eight PMESII-PT variables and includes a detailed presentation of TC 7-100 compliant orders of battle.

It is important to note that DATE is not a scenario. It is a tool to support development of a scenario. Each training venue will produce its own unique scenario based on conditions represented in the DATE and described in the TC 7-100 series. Current anticipation is that all CTCs,

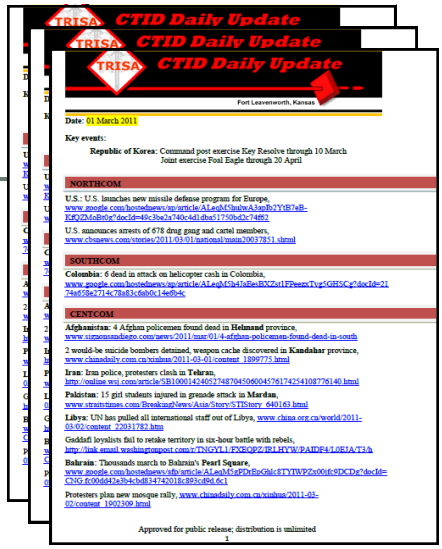


power projection platforms, and exercise divisions—as well as National Guard and Reserve units—will use DATE-based scenarios to support decisive action training.

DATE 2.0, which is scheduled to be released on AKO in December, may be used throughout the Army—supporting realistic training on "what" Soldiers will likely experience in a future operational environment on the battlefield. For example, armored vehicles and Unmanned Aerial Vehicles (UAV) were not used frequently by enemy forces in Iraq or Afghanistan but likely will be in future conflicts. Thus, scenarios based on the DATE will provide Soldiers with many new challenges they didn't experience in the current theater of operations.

Shrinking Department of Defense budgets will force the Army to face new training challenges. However, even with a limited budget, America's Soldiers must remain prepared for the next conflict—wherever and whatever it will be.

MONTHLY WRAP-UP OF CTID DAILY UPDATES



CTID analysts produce a daily *CTID Daily Update* to help our readers focus on key current events and developments applicable across the Army training community. Available on AKO, each *Daily Update* is organized topically across the Combatant Commands (COCOMs). This list highlights key updates during November 2011. The *Daily Update* is a research tool, and an article's inclusion in the *Update* does not reflect an official U.S. Government position on the topic. Also, CTID does not assume responsibility for the accuracy of each article.

Nov 1—**U.S.**: DHS drones to monitor nearly entire northern border

Nov 1—**Romania**: 73 kilograms of radioactive uranium stolen

Nov 2—**Cyber**: "Anonymous" backs off as Mexican Zetas drug cartel threatens violence

Nov 2—**Mexico**: Mexico's army finds catapults used to fire drugs into U.S.

Nov 3—**Colombia**: Shifting security patterns on Colombia's borders

Nov 3—**Russia**: Russia successfully test fires Topol RS-12M ICBM

Nov 4—**U.S.**: Muslim "homegrown" terrorism in the United States: How serious is the threat? (Belfer Center PDF)

Nov 4—**North Korea**: The collapse of North Korea: Military missions and requirements (Belfer Center PDF)

Nov 7—**Nigeria**: Boko Haram stage bloody attacks in Damaturu and Maiduguri

Nov 8—**China**: Plans for a 33-ton helicopter

Nov 9—**Iran**: Iran sought miniaturized nuclear weapon design to fit missiles

Nov 10—**Somalia**: Somalia's al-Shaba says "obtained radar equipment to detect enemy aircraft"

Nov 10—**China**: China's elite are privately talking about a revolution

Nov 14—**Zimbabwe**: Zimbabwe Defense Force takes delivery of 20K AK-47 rifles from China

Nov 15—**Philippines**: Philippines troops capture 3 Abu Sayyaf terrorists

Nov 15—**Russia**: Russia's T90M main battle tank

Nov 16—**Colombia**: FARC appoints Timochenko as new supreme leader

Nov 17—**U.S.**: Large drug tunnel found on California border

Nov 17—**Pakistan**: Haqqani releases training camp video

Nov 18—**Egypt**: Tens of thousands protest in Cairo

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

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

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

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

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

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

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

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

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

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

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

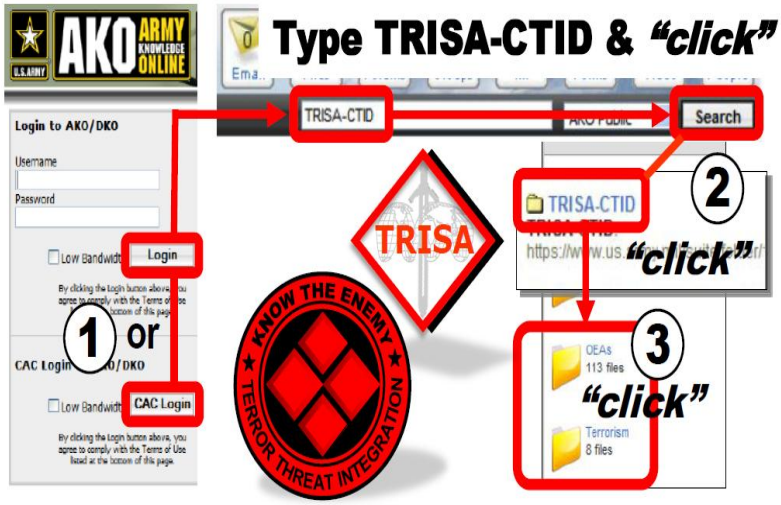
Joint Maneuver Readiness Ctr - OPFOR
SME: Mr Mike Spight BAE 684.7974
michael.g.spight.ctr@mail.mil

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

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

YOUR Easy e-Access Resource

AKO *Three "Click"* Drill-Down



Find Your Topic – Do Your Research

What We Do for YOU

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

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