U.S. ARMY TRADOC G2 Intelligence Support Activity

TRISA

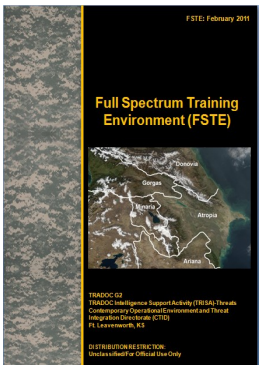
Red Diamond

Contemporary Operational Environment and Threat Integration Directorate (CTID)

Fort Leavenworth, Kansas Volume 1, Issue 2 DEC 2010

Full Spectrum Training Environment (FSTE) Q & A

INSIDE THIS ISSUE:



Question 1: What is the FSTE?

The FSTE is a document that defines the conditions of the operational environment (OE) used to build full spectrum operations (FSO) training scenarios. In this case, the OE consists of four fictional countries (Ariana, Minaria, Atropia, and Gorgas) located in the South Caucasus. The FSTE is comprised of four sections: 1) Strategic Overview; 2) OE variables for all four countries; 3) Events List; and 4) Detailed order of battle for all four countries. The FSTE provides the user with a discussion of the conditions and characteristics of the all four OEs for use in scenario building and exercise design.

Question 2: What is an event list?

The event list (Section 3) presents a red event linked to selected variable conditions within the OE. The event is then linked to specific FSO METL tasks. The list can be used to help generate events for each exercise and to help highlight the relationship between variable conditions and possible blue actions.

Question 3: Why a new document?

Based upon the guidance from the CSA and feedback from all the Combat Training Center (CTC) Commanders, TRADOC G2 was tasked to develop an "OEA-like" product to support the develop of a FSO common training environment across all CTCs. The document will provide a fictional look at four OEs (through the lens of the eight PMESII-PT variables) and a detailed presentation of a FM/TC 7-100-compliant order of battle.

Question 4: Is it a complete scenario?

No. The FSTE is not a scenario. It is a tool to support the development of a scenario. Each CTC is still responsible for the production of each scenario.

Question 5: Who are the primary users of the FSTE?

The primary users of the product are the CTCs, power projection platforms, and exercise divisions.

Question 6: When will the FSTE be published?

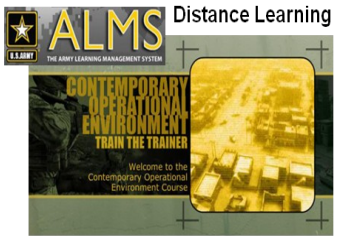
The FSTE will be published in February 2011.

Question 7: How can I get a copy?

The FSTE will be posted to either AKO or a SharePoint site in February 2011. Specific site location will be announced in an upcoming RED DIAMOND.

NEWSLETTER DISTRIBUTION UNLIMITED

Training and Education



TRISA Resident Course-Leavenworth

Operational Environment Distance Learning Course Released

by Walter Williams

The COE distance learning (dL) course was released and uploaded to the Army Learning Management System (ALMS) server on September 29, 2010. This course is a version of the resident course taught by TRADOC G2, TRISA-Threats annually at Fort Leavenworth, Kansas. TRISA-Threats is currently pursuing a maintenance contract with the Army Training Support Center (ATSC) to update this version to include topics like hybrid threats and exercise design. The dL version replaces the hard copy training support package (TSP) that was provided to the CTCs and TRADOC Centers of Excellence (CoE)/Schools for the training of their respective Observer Controllers and Staff and Faculty.

The principal audience for the course is Staff and Faculty, Observer Controllers at the CTCs, students, and civilian personnel. TRADOC CoE/Schools can use the COE dL course to supplement the Army Basic Instructor Course (ABIC) instruction as well as to certify personnel to be the lead COE trainer at Reserve Component (RC) training locations. The COE dL course may also be used by the TRADOC CoE/Schools and CTCs to provide foundational knowledge of the OE as well as to reinforce training and education of the OE to students and Soldiers. The bottom line is that TRISA-Threats is providing a long awaited tool to assist trainers and educators in their efforts to provide the best training and education of their Soldiers, leaders, staff and faculty, students and civilian personnel.

The directions to the course are: Log into **AKO**. Select **Self Service** and then select **My Education** or **My Training**. Select **ALMS** and then select the **catalog search tab**. Then type Contemporary Operational Environment or COE in the search block. You must register for the training before you begin. Once you have registered for the course, you will receive an "auto generated email confirming your registration.

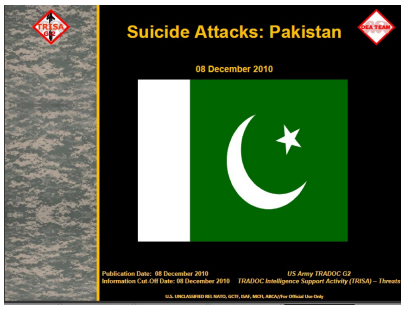
The COE dL course does not replace the resident OE Train the Trainer course. The resident course will continue to be conducted annually. ***Effective 1 October 2010, the resident course was renamed the Hybrid Threats Train the Trainer Course of Instruction (HTT3-COI)***. Additionally, TRISA-Threats will continue to conduct mobile training team (MTT) assistance visits as requested. Future versions of the HTT3-COI and MTTs will be based upon the assumption that the respective training and education audience has a foundational knowledge of the OE.

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

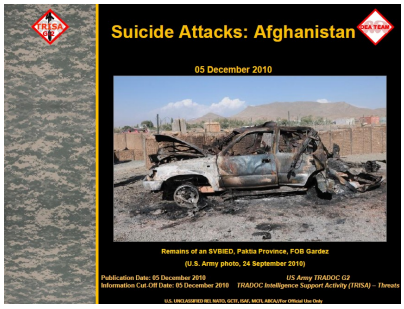
OEA Team

Recent OEA Team publications

The following OEA Team products were recently released to support the Army training community. The OEA Team produces Operational Environment Assessments (OEAs), and threat reports to help provide an understanding and awareness of various OEs and threat actors operating within them.

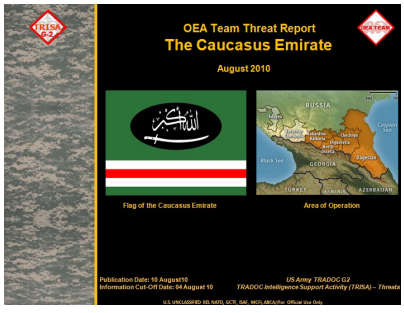


Our newest product, *Suicide Attacks: Pakistan* was developed to help inform deploying units, scenario developers, and trainers of the current threat from suicide attacks in Pakistan. The report provides a detailed timeline of attacks from January 2010 to the present. A short description of each attack is provided.



Suicide Attacks: Afghanistan is similar in structure and purpose to the Pakistan report. The report also provides a detailed look at suicide attacks across Afghanistan and discusses common TTPs. A map of all attacks is provided.

The newly update OEA Team handbook *Threat Actors: Afghanistan,* provides an overview of threat actors operating in and around Afghanistan. The handbook focuses on insurgent, criminal and terrorist organizations currently active in the OE. Each group's origins, structure, and common TTP are presented.



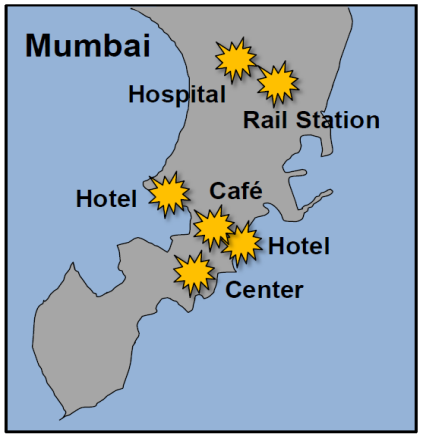
The Caucasus Emirate threat report presents a discussion of the emerging threat of a unified insurgent group, Caucasus Emirate operating in the North Caucasus area. Group origin, leadership structure, and common TTPs are addressed. On 25 June 2010, the leader of the group, Dokka Umarov, was designated a global terrorist by the U.S. Department of State.

Tactics, Techniques, and Procedures (TTP)

TTP 1: Mumbai Mass Murder and Hostage Crisis

by Jon Moilanen

Overview. On 26 November 2008, a heavily armed ten person terrorist cell attacked several prominent sites in Mumbai, India in nearly simultaneous assaults, that caused over 170 deaths and wounded over 300 additional people in site seizures and hostage crises lasting over 60 hours. The cell was linked to the ***Pakistan-based Lashkar-e-Taiba (LeT)*** terrorist group. The choice of targets as business and commercial hubs, famous entertainment sites, and cultural landmarks was combined purposely with indiscriminate killing in a populace as well as focused murder of people based on their nationality or religion. LeT's intent appeared to be exceptional psychological trauma on a major urban population and nation, undermine the confidence of India's ability to protect its people and foreigners, and expand a LeT regional agenda to global attention and international ideological extremism.

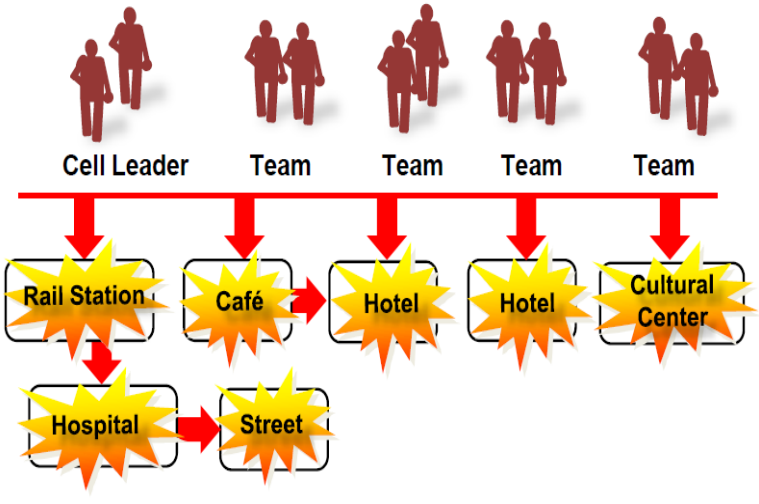


Attack Location

Terror Tactics. The terrorist cell was thoroughly trained and indoctrinated. More than one year in preparation, surveillance and reconnaissance refined intelligence. Methodical conduct of infiltrating to the objective area was followed by ruthless actions at each objective and corresponding exploitation of mass media during and after the crisis. The terrorists used a global positioning system (GPS) and an array of communications to transit over 500 kilometers of sea to a rendezvous point off the shoreline of Mumbai.

Having seized a small fishing trawler at sea, the terrorists murdered the crew and transferred their weapons and explosives to an inflatable boat to reach the shore. Four two-person teams went ashore and used taxis while one team walked to their target. A fifth two-person team continued in an inflatable boat along the shore to their target. With all teams at their urban objectives, attacks were initiated within minutes of each other at five dispersed locations. Mass murder occurred as terrorists used semiautomatic rifle fire and hand grenades against people in a rail station, hospital, urban streets, café, hotels, and Jewish cultural center.

Earlier, IEDs had been hidden in two taxis timed to explode well after the main attacks were underway. These explosions caused additional confusion and mayhem in the first hours of the incident. After attacking the café, one team quickly joined the team assaulting a hotel, killing people, starting fires in the hotel, and seizing hostages. Hostages were seized at a Jewish cultural center and eventually murdered. Another team entered a second hotel and immediately started killing people and seizing hostages. One team shot people randomly in a train station, a hospital, and departed to possibly link up with other team members but were killed in a city street confrontation with police. Several other IEDs were emplaced at some of the sites but were discovered prior to causing casualties.



Mumbai Attack Cell

The terrorist team members were well armed with AK-56 assault rifles, pistols, hand grenades, explosives for IEDs, and basic food and water. They communicated with each other and operational handlers remote from Mumbai with cellular telephones, Voice over Internet Protocol (VOIP), satellite telephone, personal digital assistant (PDA) devices, and referenced high-resolution satellite imagery. Handlers provided ideological encouragement and direction, and tactical advice observed from live media coverage at the attack sites. Local law enforcement was initially overwhelmed by terrorist firepower. Once Federal military forces arrived on site, police and military forces killed nine terrorists and captured one terrorist.

Assessment. A small well trained and resourced terrorist cell of 10 men attacked several public and relatively unprotected urban targets in nearly simultaneous assaults to mass murder, seize sites, and take hostages. The terrorists expected to be killed during the LeT inspired mission while obtaining several days of constant world media coverage of the terror and attention to the terrorist organization's agenda. Effective intelligence sharing among governmental agencies might have disrupted or defeated the attack. Law enforcement agencies must have sufficient and immediate capability to protect its citizenry and counter an active shooter crisis. ***Multiple site, nearly simultaneous terrorist attacks will require immediate responsive support from specialized forces*.**

TTP 2: Vehicle-borne IED (VBIED): Stop and Ram

Enemy Intent. Demoralize citizenry and coalition forces with indiscriminate suicide attacks. In this vignette, a "snap checkpoint" is the identified objective with soldiers as primary targets. Insurgent team with two civilian vehicles positions based on insurgent observer report of checkpoint at location used several times in past and planned for possible attacks.

Shape Condition. Vehicle #1 starts non-threatening low speed passage into checkpoint lane toward search area. Vehicle #2 positions in wait line one to several vehicles behind vehicle #1. Vehicle #1 creates an incident negotiation the temporary obstacles in the alert line.

In this case, the driver stalls the engine and indicates to coalition forces that the vehicle will not restart. Checkpoint soldiers cautiously approach the driver and vehicle. Driver of Vehicle #2 and dismounted observer track checkpoint soldier actions. With their attention focused on the stalled vehicle, the driver of vehicle #2 identifies a vulnerability and route for a high speed assault with his VBIED.

Attack Target. Vehicle #2 races out of wait line and rams vehicle #1 with a cluster of soldiers and nearby civilians. VBIED detonation causes several fatalities and casualties. Observer records immediate action of checkpoint for after action review and future attack improvisations.

Article of Interest

Non-State Actor INFOWAR Tactics

by Justin Lawlor

The evolving nature of INFOWAR (information warfare) has allowed non-state actors to establish capabilities and pursue their group objectives in ways previously denied them. Three particular events illustrate likely types of INFOWAR threats the U.S. Army will face in the coming decades. The U.S. Army and the Government in general, needs to be familiar with such attacks to generate the ability to counter and remediate these enemy actions.

Project Chanology

Background: As part of an ongoing mass protest against the Church of Scientology, an Internet-based mass movement known as "Anonymous" launched a coordinated, but widely disseminated, INFOWAR attack beginning in 2008 and continuing through the year. Coordinated through a series of online message boards, Internet relay chat rooms, and other anonymous means, Project Chanology was successful at disrupting the activities of the Church of Scientology through distributed denial of service attacks (DDOS), computer attacks, black faxes, and perception management operations.

Tactics: The Project Chanology campaign started in March 2008. These attacks were identifiable by their cooperative nature versus top-down command and control. Individuals who wanted to participate were directed to a website where targeting data, like fax numbers and websites, were available for download.

Implications: The U.S. Army and much of the U.S. Government are vulnerable to such a mass-movement. The dependence upon public facing websites for recruiting, administration and other important tasks for the U.S. equals vulnerability.

Distributed Denial of Service—A computer warfare attack in which the bandwidth or service of the targeted computer system is flooded with data, rendering it useless.

Black Fax—A fax designed to render a fax machine useless through excessive toner use. A black piece of construction paper is faxed, denying the recipient use of his fax machine.

Perception Management—Perception management involves measures aimed at creating a perception of truth that best suits OPFOR objectives. It integrates a number of widely differing activities that use a combination of true, false, misleading, or manipulated information. Targeted audiences range from enemy forces to the State's own citizens.

The Mavi Marmana Incident and the Power and Limits of Perception Management

Background: In an attempt to publically break the Israeli blockade of Gaza, the Turkish nongovernmental organization (NGO) The Foundation for Human Rights and Freedoms and Humanitarian Relief (IHH is the Turkish acronym) IHH attempted to precipitate a confrontation with the Israeli Defense Force (IDF). The goal was to create an incident where the appearance of an overwhelming Israeli overreaction to a charity flotilla would create a backlash in which international pressure would force Israel to lift or modify the current blockade of the Gaza Strip.

The NGO's endstate was not achieved, mostly due to aggressive control of the information environment by the IDF. In the aftermath of the incident, the Israelis went on the perception management counteroffensive, and released multiple videos on *YouTube,* both raw and interpretive, to present the Israeli version of events.

Tactics: The Turkish NGO insured that an international incident would be provoked by attacking an Israeli special operations forces (SOF) boarding party with lethal melee weapons, while filming the entire incident.

***Implications**:* The Israeli boarding was planned to be executed with the minimum force possible, likely in order to forestall an international incident. The Israeli SOF landed with only side arms and less-than-lethal weapons. Ironically, this lack of force created an even more violent situation. Excellent preparation in providing a narrative to immediately contradict the accounts of unreasonable force presented by the NGO protestors allowed the Israelis to achieve their endstate.

For more background on the Mavi Marmana incident, check out the TRISA Threat Report, "INFOWAR Analysis of the Gaza Flotilla Raid."

Al Manar TV and Public Relations

Background: Al Manar TV, a subsidiary of Lebanese Hezbollah, is an important INFOWAR tool used to both harden and shape Lebanese public opinion and provide an outlet for Lebanese Hezbollah leadership to make public pronouncements.

Al Manar continues to be an important outlet for Lebanese Hezbollah, despite al Manar's label by the U.S. Government as a Designated Terrorist Entity.

Tactics: Al Manar is not just a useful tool for perception management, but at least one individual has been indicted for using his al Manar credentials to further his intelligence collection requirements. Message content will also differ depending upon the language, with Arabic language messages often much more harsh in content and tone than English language ones.

Implications: Not all journalists are created equal. It is likely that INFOWAR-savvy adversaries will continue to use journalists for perception management and intelligence purposes. All troops should continue to assume that any footage or journalist attention can be exploited for INFOWAR purposes and act accordingly.

For more background on Iranian IW operations, check out the TRISA Operational Environment Assessment: Iran, and TRISA Threat Reports, "IW Considerations during the Iranian Election Protests, June 2009" and "Iranian Uniforms: Implication for U.S. Forces."

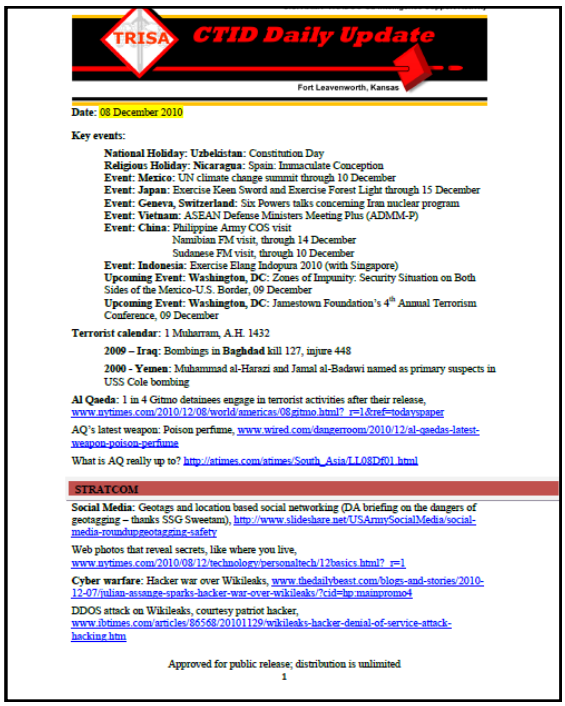
Conclusion

We must assume that INFOWAR adversaries are supple, creative, and committed. Even if denied their immediate objectives, like in the case of the Mavi Marmana, adversaries will continue an attritional strategy against U.S. interests. Knowledge and awareness of adversaries' increasingly pervasive nature in the battlefield should be a key element of all training and point of awareness for operational commanders.

Requests for Information

- ***Your source for information on all OPFOR and Threat issues***
- ***See SME list on page 9 for key POCs***

Other CTID Products



TRISA **CTID Daily Update**

Fort Leavenworth, Kansas

Date: 08 December 2010

Key events:

National Holiday: Uzbekistan: Constitution Day
Religious Holiday: Nicaragua: Spain: Immaculate Conception
Event: Mexico: UN climate change summit through 10 December
Event: Japan: Exercise Keen Sword and Exercise Forest Light through 15 December
Event: Geneva, Switzerland: Six Powers talks concerning Iran nuclear program
Event: Vietnam: ASEAN Defense Ministers Meeting Plus (ADMM-P)
Event: China: Philippine Army COS visit
Namibian FM visit, through 14 December
Sudanese FM visit, through 10 December
Event: Indonesia: Exercise Elang Indopura 2010 (with Singapore)
Upcoming Event: Washington, DC: Zones of Impunity: Security Situation on Both Sides of the Mexico-U.S. Border, 09 December
Upcoming Event: Washington, DC: Jamestown Foundation's 4th Annual Terrorism Conference, 09 December

Terrorist calendar: 1 Muharram, A.H. 1432

2009 – Iraq: Bombings in **Baghdad** kill 127, injure 448

2000 - Yemen: Muhammad al-Harazi and Jamal al-Badawi named as primary suspects in USS Cole bombing

Al Qaeda: 1 in 4 Gitmo detainees engage in terrorist activities after their release, www.nytimes.com/2010/12/08/world/americas/08gitmo.html?_r=1&ref=todayspaper

AQ's latest weapon: Poison perfume, www.wired.com/dangerroom/2010/12/al-qaedas-latest-weapon-poison-perfume

What is AQ really up to? http://atimes.com/atimes/South_Asia/LL08Df01.html

STRATCOM

Social Media: Geotags and location based social networking (DA briefing on the dangers of geotagging – thanks SSG Sweetnam), http://www.slideshare.net/USArmySocialMedia/social-media-roundupgeotagging-safety

Web photos that reveal secrets, like where you live, www.nytimes.com/2010/08/12/technology/personaltech/12basics.html?_r=1

Cyber warfare: Hacker war over Wikileaks, www.thedailybeast.com/blogs-and-stories/2010-12-07/julian-assange-sparks-hacker-war-over-wikileaks/?cid=hp:mainpromo4

DDOS attack on Wikileaks, courtesy patriot hacker, www.jbtimes.com/articles/86568/20101129/wikileaks-hacker-denial-of-service-attack-hacking.htm

Approved for public release; distribution is unlimited
1

Check out CTID's Daily Update. This document provides a daily round-up of news events across the global. The purpose of the document is simply to inform readers of current developments and to highlight significant publications. News events are listed by COCOM. The Daily Update can be mailed to you directly. If you are interested in receiving the update please notify Mr. Marc Williams.

YOUR Subject Matter Experts

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

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

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

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

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

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

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

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

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

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

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

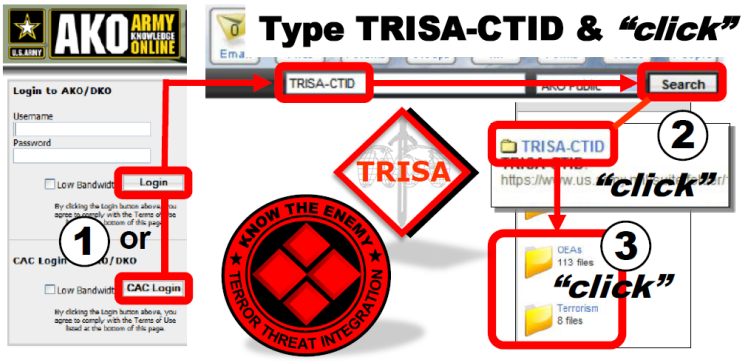
Joint Maneuver Readiness Ctr - OPFOR
SME: Mr Mike Spight BAE 684.7974
michael.spight@us.army.mil

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

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

YOUR Easy e-Access Resource

AKO *Three "Click"* Drill-Down



Find Your Topic – Do Your Research

What We Do for YOU

- Determine OE Conditions
- Publish OE Threats in FSO
- Publish Army OPFOR Doctrine
- Assess Threat-Enemy & TTP
- Support Terrorism Awareness
- Publish OE Assessments

Director's Corner: *Looking Ahead --*

Welcome to Issue No 2 of our Red Diamond Newsletter. I hope you find this product useful in your efforts to train the force. This newsletter is not our product, it's yours. If there is something in the area of operational environment or threat for training that you would like to see explained, developed or highlighted - please let us know. I choose subject areas for the newsletter based upon requests from the Soldiers we train (and as much as we can, the Marines, Sailors and Air-men with whom we train and fight). Tell us what you need to know more about and we will get it to you.

- Jon Cleaves