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 4 April 2011

New Threat Report: Thailand-Cambodia Border Dispute

INSIDE THIS ISSUE:

- *OEA Threat Report* 1
- *Cruise Missiles* 2
- *Rest of the Hybrid Threat* 4
- *TTP* 6
- *CTID Update* 8

The OEA Team has published a new threat report. *Thailand-Cambodia Border Dispute* presents an analysis of the long-term disputed territorial issues between Thailand and Cambodia. Specific attention is given to the historical boundary dispute over the Preah Vihear temple. The report concludes with a discussion of the political and military implications of the dispute and its potential to trigger a regional conflict.

Thailand-Cambodia border dispute basics:

- Both Thailand and Cambodia claim the Preah Vihear temple complex, a 1.8 square mile piece of ground located on their common border.
- The temple complex sits atop a cliff in the Dangrek Mountains that divides Thailand and Cambodia. (*See map*)
- The area contains no natural resources that either side can exploit.
- Cambodia, with Chinese assistance, continues to build an improved road to the temple through the disputed territory.
- Temple visitors from the Thai side need permission for Cambodian border security personnel to enter the territory.

The threat report is posted on AKO.

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

NEWSLETTER DISTRIBUTION UNLIMITED

Article of Interest

Introduction to Cruise Missiles

by Kristin Lechowicz

Many countries in the global arena, including potential threats to the US, are procuring cruise missiles (CMs) as an inexpensive alternative to ballistic missiles and aircraft. CMs are an economical and accurate delivery system that can be used for conventional, nuclear, chemical, and biological warheads. CM proliferation poses an increasing threat to US national security interests. As the technology matures, both state actors and non-state actors are becoming increasingly able to acquire CMs and effectively employ such capabilities.

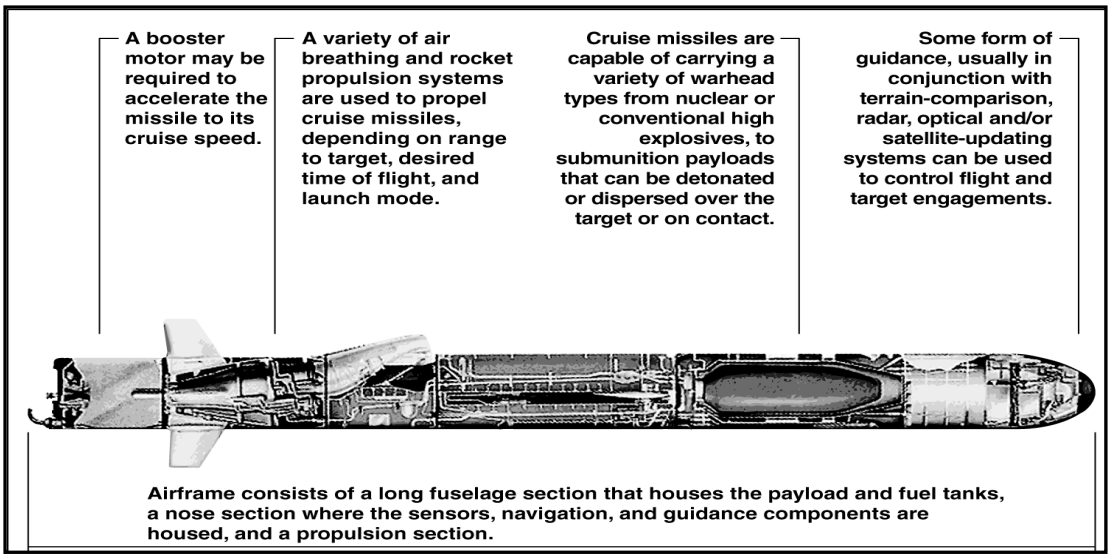
This article provides a basic introduction to CMs and addresses the following critical categories:

- What is a CM?
- What are the basic components?
- What are CM capabilities, ranges, and guidance system? This article is a follow-up to the Red Diamond article: Introduction to Theater Ballistic Missiles.

What is a CM?

Cruise missiles are basically unmanned, precision guided, subsonic weapons that are propelled by either rocket motors or jet engines. A CM assumes a non-ballistic flight path remaining within the atmosphere (air breathers), while ballistic missiles travel above the atmosphere. Modern CMs offer flexibility in payload and multiple launch configurations, including air, sea (surface and subsurface), and ground capabilities.

CM's small size (as opposed to most ballistic missiles), programmable delivery course, and low terrain-hugging capability make them an excellent delivery system and difficult to counter. The more modern CMs can take roundabout routes to engage their targets. CMs have the ability to circumvent known defenses and engage targets from suspected gaps in radar and surface-to-air missile coverage. The majority of CMs are anti-ship missiles, however, the new land attack missiles are becoming more sophisticated.



CM Basic Components

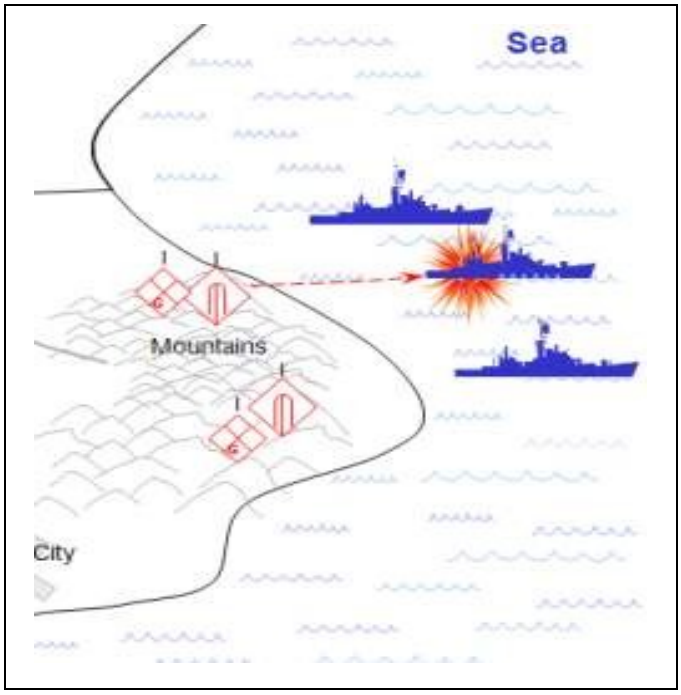
The four main components of CMs are a propulsion system, guidance and control system, airframe, and the payload. CMs are designed to have the booster rockets fall off after the fuel is depleted. After this action, the turbofan engine or jet engages and the tail fins, air inlet, and wings unfold. The diagram above breaks down and illustrates the main components of a typical turbo fan cruise missile. On target impact the missile explodes and it is destroyed.

Article of Interest

CM Capabilities

CMs are relatively mobile and easy to conceal. Even after launch, most missiles can avoid detection by traveling at low altitude, under many radar horizons and use terrain masking until the CM reaches the target. Newer CMs present even greater challenges to aircraft and air defense assets by integrating stealth features that make them even less visible to radars and infrared sensors.

The OPFOR, or a real world threat, could use CMs to target CONUS or OCONUS population centers, forward deployed military bases, naval assets, airfields and other fixed and mobile targets. The example on the right shows the OPFOR using mountainous terrain to launch cruise (anti-ship) missiles at vessels. This example is similar to the attack that Hezbollah perpetrated against an Israeli corvette, INS Hanit, during the 2006 Lebanon war. The Israeli ship was heavily damaged and was rendered combat ineffective. This was the first time that a non-state actor had shown such a capability. The OPFOR could use CMs and the natural terrain as choke-points to snare naval assets, logistics enablers, or targets of opportunity.



CM Ranges

The ranges of cruise missiles vary greatly from 50 miles (the French Exocet anti-ship missile) to 2,200 miles (the Russian AS-15 Kent). For naval assets, 50 miles would allow a naval ship to attack another vessel that would not be visible on the ocean horizon. In theory, a Russian AS-15 Kent has the range to be launched from Moscow and reach Tehran. Great disparity in missile ranges does not affect the weapon's lethality.

CM Guidance Systems

The overall sophistication of CMs have increased greatly with technological advancements. This is especially true with regard to guidance systems in the era of more capable Global Navigation Satellite Systems (GNSS) like GPS, Russian GLONASS, Chinese Beidou, and the European Galileo. These advanced guidance systems, in combination with autonomous onboard systems, have allowed CMs to become more accurate in acquiring targets. The basic CM guidance controls consist of one of four different systems that direct the missile to its target: Inertial Guidance System (IGS), Terrain Contour Matching (TERCOM), GNSS (GPS), and Digital Scene Matching Area Correlation (DSMAC). Most newer CMs use a combination of systems to provide redundancy and precision in a combat environment.

- IGS tracks detected acceleration via accelerometers from missile movement compared against a known first position, usually the launch position, to determine current location.
- TERCOM uses a radar that compares terrain features while in route to a pre-stored (loaded on the missile) 3-D mapped terrain database.
- GNSS, like GPS, uses satellites and an onboard GNSS receiver to verify the missile's position.
- DSMAC uses a camera and an image correlator to identify the target (good for use in moving targets).

Conclusion

As CMs become more sophisticated, their proliferation represents a clear and challenging threat to the US. The likelihood of these weapons falling into the hands of radical non-state actors was realized as witnessed by the 2006 Lebanon war. These weapons are viewed by many as reasonably economical, accurate delivery systems that can launch a number of different payloads, which provides a deep strike capability. The US will likely face the challenging threat put forth by CMs in the future.

Training and Education

Nation-State Paramilitaries, Terrorists, Criminal Organizations and Mercenaries—the Rest of the Hybrid Threat

by Michael Spight

What are hybrid threat (HT) organizations and their capabilities? My previous Red Diamond article addressed guerrilla and insurgent groups; their tactics, techniques, and procedures (TTP); and how they might be replicated as part of the CTC OPFOR during a full spectrum exercise (FSX). This article will define the remaining four elements (nation-state paramilitaries, terrorists, criminal organizations, and mercenaries) of the hybrid threat and discuss how CTCs might effectively replicate the capabilities of the hybrid threat against Rotational Training Unit (RTUs-BLUFOR) in a manner that supports conventional OPFOR formations and provides a real challenge for the RTU during an FSX. The definitions for these types of units/groups from TC 7-100 are as follows:

Nation-State Paramilitaries: [Member of]…forces or groups distinct from the regular armed forces of any country, but resembling them in organization, equipment, training or mission. (JP 3-24) ***(NOTE: Paramilitary forces may also incorporate guerrilla, terrorist, mercenary, or insurgent forces, if they resemble "them in organization, equipment, training or mission." Primarily, however, they are government forces consisting of internal security forces, border guards, or national police that are not extensions of or connected with national military forces.)*** Government paramilitary forces may conduct operations in conjunction with government, regular military formations.

Terrorist: An individual who commits an act or acts of violence or threatens violence in pursuit of political, religious, or ideological objectives. (JP 3-07.2***)(NOTE: A terrorist organization can also be classified as insurgents, guerrillas, or paramilitary, based upon how they are equipped, their level of training, and the acts they commit for their "cause.")*** They can also augment state military/paramilitary organizations, especially if the state is a terrorist state or has ties with domestic and/or foreign terrorist organizations.

Criminal Organizations: We need to look no further than our common border with Mexico to see the incredible influence which trained, organized, armed, politically savvy, and ruthless criminal organizations can have over a legally constituted and elected government. Their effects on that nation's economy; safety, and security of honest citizens; law enforcement; and military are absolutely astounding. And the influence they have over US policy regarding drug enforcement, border security, and immigration clearly show how well organized, motivated, and intelligent criminal leaders who have trained, loyal, and sangfroid "soldiers" in their employ can "degrade a social and political environment," and they are doing exactly that North of the Rio Grande. Other examples are FARC in Columbia; international drug trade as practiced in Afghanistan (Taliban, various Afghan warlords); and "The Golden Triangle" region of China, Burma, and Thailand and the influence of warlords like the late Kuhn Sa. Money, drugs, guns, and an incredible ability to influence governments and citizens to their own benefit, in many cases, are what make these organizations so dangerous within their own country and, too often, across international borders. Their considerable skill sets could be used by government, terrorist, or guerrilla forces in future conflict with the US in exchange for the ability to operate successfully and to discourage or eliminate certain other criminal organizations with whom they compete for business or influence. In any event, they present a potential threat that requires US forces to be aware of their presence and capabilities within an OE, and to be prepared to respond militarily if necessary.

Mercenaries: Generally, individuals with military training and experience who use sell their services to one side or another in armed conflicts for private financial gain. ***If they take part in hostilities, they can be considered unlawful enemy combatants.*** The Geneva Convention describes them as individuals or groups possessing the following characteristics:

Training and Education

- Recruited either locally or abroad
- Involved in direct combat operations
- Motivated by desire for private gain
- Are not nationals of either party to the conflict; not residents of the territory in which combat operations are being conducted
- Are not members of the armed forces of any party to the conflict
- Are not on official military orders/seconded/attached from another nation's military service that is not directly involved in the conflict (advisor, military exchange, or trainer)

For example, some you may be familiar with the fact that during our Revolutionary War, King George of England recruited a regiment of Hessian riflemen (Germans, from the state of Hesse) to serve against us. They were paid for their services, were not from a state that was a party to the conflict, and were not part of a foreign military service that was seconded to the British Army—they were mercenaries. More recently, in the 1960s, during frequent conflicts in sub-Saharan Africa, mercenary units were known for their brutality and effectiveness against various uprisings, such as the Simba rebellion. Former British Army Officer, Colonel Mike (aka Mad Mike) Hoare, organized, trained, and led both 4 and 5 Commando (aka "Wild Geese Commando") in the Congo. He was hired (and paid) by the Congolese Prime Minister, and his force was made up of primarily South Africans, a few Americans, Continental Europeans, and fellow Brits. Of note is the fact that in many cases, mercenary forces can be expected to be very well equipped and very experienced in military TTP.

Tactics

With the possible exception of a robust state paramilitary force, terrorists, criminal groups, or mercenaries would not (acting independently) provide a serious, realistic challenge to a well-trained and led, motivated BCT. That said, those organizations can plan, coordinate, and execute ICW state paramilitary or regular military units the following types of missions: gathering intelligence on BLUFOR OB, locations, strength, etc.; identify, exploit, or attack BLUFOR vulnerabilities and key nodes; engage in activities that draw the attention of BLUFOR away from OPFOR main force movement and intent. And remember this: the HT is a CAPABILITES based OPFOR, not a NATION STATE/NON-STATE ACTOR based OPFOR. We are preparing for possible engagement with real world capabilities, not a specific country or non-state actor. Realistically, their capabilities could perhaps be best used as an Enabling Element in support of OPFOR conducting operations as an action element during an FSX. Diversions, support by fires, covering withdrawal by regular OPFOR elements…all of these actions (and more) are certainly possible scenarios for an OPFOR paramilitary, terrorist, criminal organization, or mercenary element.

How can Nation-State Paramilitaries, Terrorists, Criminal Organizations, and Mercenaries be most effectively replicated on a CTC? Create battlefield "friction" that BLUFOR will be forced to plan for and/or react to: terrorists embedded with the local civilian population in cells, criminal organizations that are shaking down the locals and stealing supplies from the BLUFOR, mercenaries hired to engage or conduct recon against BLUFOR. And remember that there is always opportunity for these types of organizations to work together or even come over to the BLUFOR side if they see it to their long-term advantage. This will result in more friction and fog on the CTC battlefield that BLUFOR will be forced to deal with.

Locate/ID/Attack Key BLUFOR Systems (Logistics Nodes, MSRs, RSTA elements, C4I nodes)—all of these are important targets that can be very vulnerable to irregular force attack. The attack is not necessarily direct action by the element that locates and identifies the node; the irregular force element can pass information about the node back to OPFOR UAV and/or targeting assets for more detailed examination via UAV or a quick attack by OPFOR indirect fire or CAS assets.

Creative, aggressive use of OPFOR assets in the role(s) of paramilitaries, terrorist cells, criminal organizations or mercenary elements during FSX CTC rotations will provide rigor and a challenge to RTUs in an environment that is quite different than the COIN environment in which we have been operating over the past 10 years. All personnel, particularly those assigned to CTC OPFOR units and Ops Groups, are encouraged to refer to TC 7-100 (Hybrid Threat) and TRADOC G2 Handbook No. 1.08 (Irregular Forces).

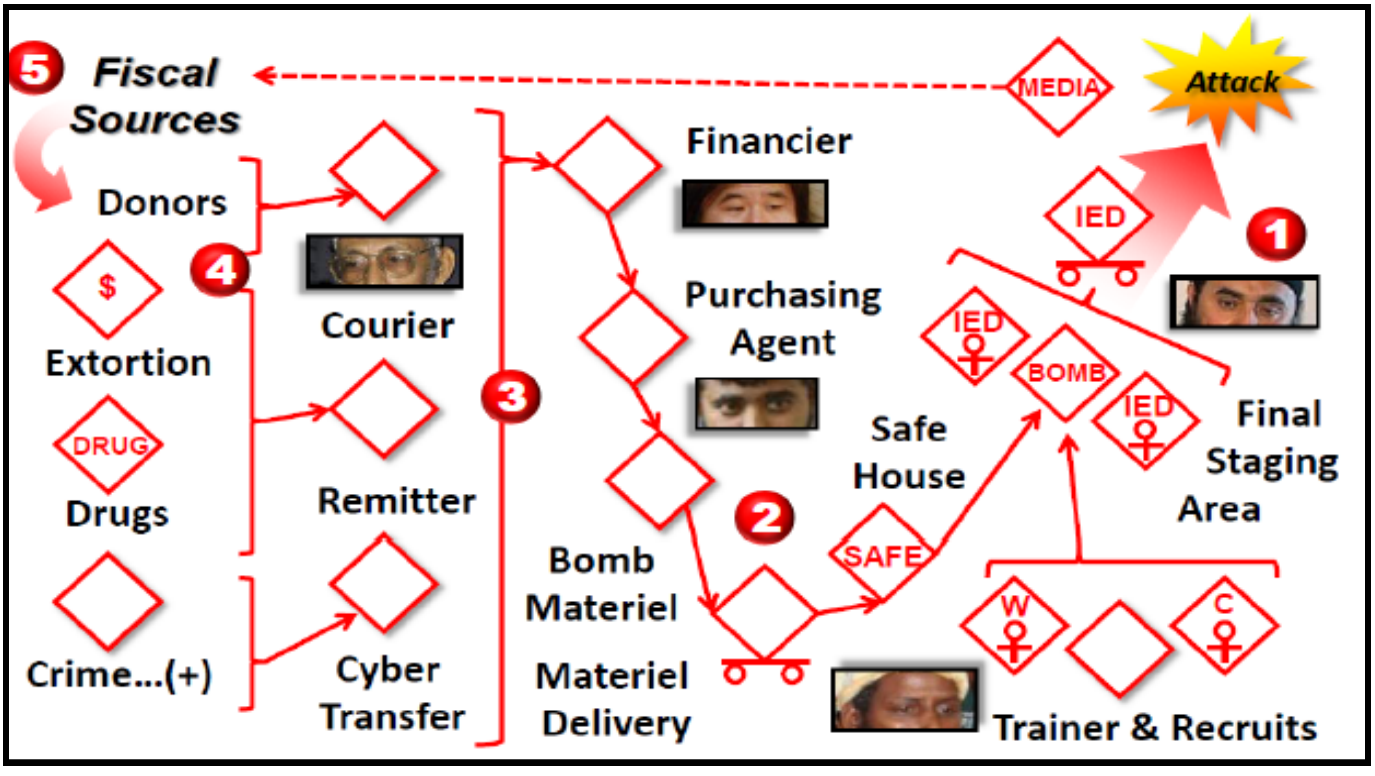
Tactics, Techniques, and Procedures (TTP)

Follow the Money: A Vignette of the "Innocent Dollar"

by Jon Moilanen

Backtrack -- the *"Bang" to the "Buck."* Forensic analyses of a series of bomb detonations indicate common bomb materials and explosives. Particular elements in the explosives are traced to a limited number of manufacturers. Traditional access routes for such material and additional intelligence narrow the probable source of the explosives in the region and area of operations. The manner of bomb construction indicates a particular terrorist cell and support operation in a regional locale.

Suspicious financial transactions in a selected period of time, combined with estimates of approximate costs of materials, are compared and further analyzed. A suspected financial hub is identified based on a noticeable number and type of finance actions occurring in a select time period prior to the bomb attacks.



Tactics, Techniques, and Procedures (TTP)

Number 4: Documenting the Banking Sources

Multiple money transfers arrive to a central financial institution. These finance centers reside in Europe, the Far East, and other sites such as the Caymans.

Number 3: Tracing the Money Flow

Electronic money transfers into a regional banking facility. That facility transfers several large sums of money into a regional banking facility suspected to be part of a terrorist safe haven support system. Materiel has been purchased.

Number 2: Connecting the Dots

Human intelligence confirms that a terrorist cell is in a developed phase of additional bomb attack preparation. Surveillance of safe houses and courier and remitter informant confirm that material and explosives are about to be moved along known trafficking routes to safe houses in the attack area.

Number 1: Enemy Disruption and Defeat

Four shipments are tracked and intercepted while in transit to the attack area. Three possible shipments may have eluded border controls and in-region check points. Focused intelligence operations continue.

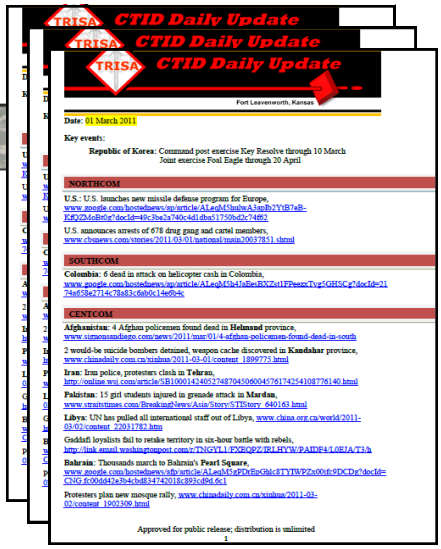
Number 5:But where did the money come from?

Funding comes from multiple sources and is often collected in small cash or electronic amounts to minimize the money signature and remain unnoticed. Possible funding sources include:

- "Unknowing" Donors who believe they are donating to a legitimate charity or nongovernmental organization.
- "Willing" Donors who actively support a political, social, or single-issue cause, and those for hire in criminal activities: extortion, kidnapping, theft, or robbery.

If you want to receive a monthly electronic copy of the Red Diamond please let us know and we will add you to the distribution list.

Monthly Wrap-Up of CTID Daily Update



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

1 April: What a cyberwar with China might look like.

1 April: Cameras and spy balloons increase in Afghanistan.

4 April: Swine flu in Venezuela.

4 April: 20 killed in clash between Lashkar-e-Islam factions.

8 April: According to the US Department of State, the FARC and Taliban are among the largest drug traffickers.

8 April: FARC detonates explosive device on gas pipeline.

8 April: "Iron Dome" system intercepts Gaza rocket.

8 April: Russia floats out new missile frigate for Caspian Sea.

11 April: New CFR publication: Fragile states, global threats, and international security.

11 April: As violent protests rage, Syrian officials seal off port city of Baniyas.

12 April: Mexican cartels migrating to the US.

12 April: Arab Risings, Israel, and HAMAS. (STRATFOR)

12 April: Arab spring knocks on Azerbaijan's door.

13 April: FBI Assistant Director's Congressional Testimony on cyber threats.

13 April: Rebels hijack Gadhafi's phone network.

14 April: Latin America increases military spending.

15 April: Violence rises as cartels splinter.

15 April: Libyan rebels claim cluster bombs used in Misrata.

25 April: Are drones a technological tipping point in warfare?

25 April: Central America: Drug gangs muscle into new territory.

26 April: Iraq, Iran, and the next move. (STRATFOR)

26 April: Syria escalates deadly crackdown.

27 April: Iraqi culture chief and top cop escape assassination.

27 April: Interpol warns of global security risk after Afghan jailbreak.

27 April: 183 bodies found in April in Mexican graves.

28 April: Pro-government forces take town in southern Somalia.

28 April: Six Islamists killed in Dagestan.

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

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

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

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

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

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

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

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

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

National Training Center - OPFOR
SME: 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

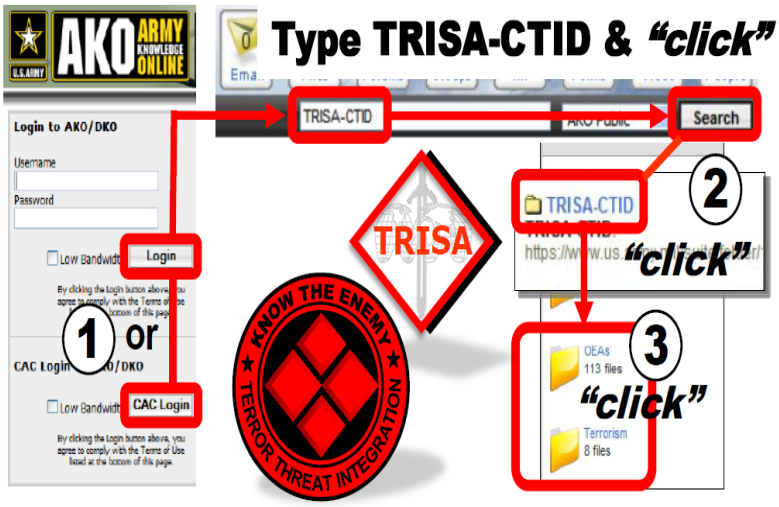
Joint Maneuver Readiness Ctr - OPFOR
SME: Mr Mike Spight BAE 684.7974
michael.spight@us.army.mil

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 Operational Environment Assessments (OEAs)**
- **Publish OE Threats in FSO**
- **Publish Army OPFOR Doctrine**
- **Assess Threat-Enemy & TTP**
- **Support Terrorism Awareness**

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