



# Red Diamond

## Complex Operational Environment and Threat Integration Directorate

Fort Leavenworth, KS    Volume 4, Issue 5    MAY 2013

### INSIDE THIS ISSUE

WETED Threats .....	4
SVIED Bombing .....	6
Russian Kondor .....	10
Hybrid Threats .....	14
Threat Boat Ops .....	15
Suicide Attack .....	21
CBP Defense .....	22
Update Summary .....	30

*Red Diamond* is a newsletter published each month by TRISA at CTID. Send your suggestions to CTID on article content.

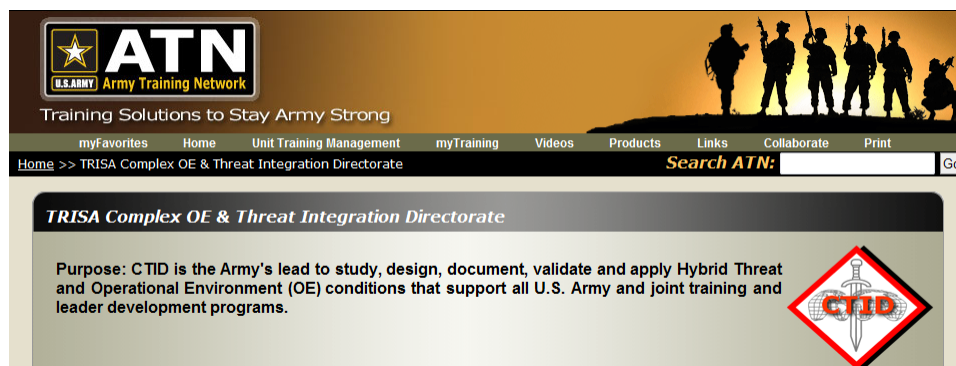
ATTN: Red Diamond

Dr. Jon H. Moilanen  
CTID Operations, BMA  
and  
Mrs. Angela Wilkins  
Chief Editor, BMA



## HYBRID THREAT AND OPPOSING FORCE: *NEW ON ATN!*

by Jerry England, Threat Integration Team (DAC)



The Complex Operational Environment and Threat Integration Directorate (CTID) has continued to improve its presence on the Army Training Network (ATN) Portal. The site is a joint effort between CTID and ATN to provide Soldiers and trainers access to Threat doctrine and Threat force structure. Included in the site are links to CTID's doctrinal publications such as TC 7-100.2, *Opposing Force Tactics* and TC 7-101, *Exercise Design Guide*. These documents are instrumental in helping trainers develop meaningful exercises both at the various Combined Training Center (CTCs) as well as at Home Station Training. Go to [https://atn.army.mil/dsp\\_template.aspx?dpiID=311](https://atn.army.mil/dsp_template.aspx?dpiID=311) to see the Threat doctrine material available on ATN.

Recently, a new page directing users to a variety of Operational Environment Assessments (OEAs) and other Threat products has come online. The new page, currently under development, houses many of the most requested products from CTID. See [https://atn.army.mil/dsp\\_template.aspx?dpiID=377](https://atn.army.mil/dsp_template.aspx?dpiID=377) to see all of the products available on the new page. (Continued on page 14)

Eventually the two pages will be linked together in order to better support exercise designers and improve the integration of detailed Threat data with current operational environment (OE) information. The combination of this material will be an essential tool for exercise design. From irregular Threat force structures to tank specifications, the site provides useful information for a variety of echelons and theaters.

## RED DIAMOND TOPICS OF INTEREST

by Dr. Jon H. Moilanen, CTID Operations and Chief, *Red Diamond* Newsletter

This issue of *Red Diamond* begins with the continuation of the series from the **TRISA Wargaming, Experimentation, Test, and Evaluation Directorate** (WETED).

Other articles feature the recent suicide vest attack on the embassy in Ankara, an operational environment assessment of Djibouti from the perspective of the military variable, and an orientation on **Jabhat al-Nusra** (JN) in contemporary operations.

Threat tactics, techniques, and procedures (TTP) is demonstrated by small boat operations in Nigeria by the **Movement for the Emancipation of the Niger Delta** (MEND) and pirates in Somalia. The article assesses recent tactics to include swarm-based maneuver, using speedboats in the swamps to quickly attack targets in succession, improved firepower and combat training, and tactical reach of small boat operations in the coastal regions.

Another article addresses Russian preparations to launch the **Kondor satellite system** into orbit by the end of 2013. Russia claims “remote sensing” capabilities designed to film the earth 24/7 in all weather conditions.

Defense of a Threat **complex battle position (CBP)** emphasizes TTP and functional organization from an opposing force (OPFOR) perspective. Whether in an urban or rural setting, understanding the security measures, fighting position purposes, and an integrated defense concept are fundamental to “**Know the Threat—Know the Enemy!**”

### Send Your RFI

Do you have a “threats” topic you would like discussed in the TRISA *Red Diamond*?

Submit your request for information and we may include a CTID response in a future issue of the *Red Diamond*.

Email your topic recommendations to:

**Dr. Jon H. Moilanen, CTID Operations, BMA CTR**  
[jon.h.moilanen.ctr@mail.mil](mailto:jon.h.moilanen.ctr@mail.mil)  
and

**Mrs. Angela M. Wilkins, Chief Editor, BMA CTR**  
[angela.m.wilkins7.ctr@mail.mil](mailto:angela.m.wilkins7.ctr@mail.mil)

**WE are at WAR!...on TERROR**

**Know the Threat - Know the Enemy**

**US ARMY TRADOC**  
**KNOW THE ENEMY**  
**TERROR THREAT INTEGRATION**

**TRISA**

*Trained  
Ready  
Adaptive  
Decisive*

**TRADOC G2 Handbook No. 1.07 C3**  
**A Soldier's Primer to Terrorism TTP**  
Tactics, Techniques, and Procedures  
in  
Complex Operational Environments  
TRADOC G2 Intelligence Request Activity (TRISA)  
Postcard with Title, Values  
August 2013

**TRADOC G2 Handbook 1.07 C3**

**Counter the Terrorism TTP**

Access AKO with password.  
<https://www.us.army.mil/suite/doc/14886365>  
See *A Soldier's Primer to Terrorism TTP*.  
TRISA WOT Poster No. 08-13  
Complex Operational Environment and Threat Integration Directorate (Photo: U.S. Army, SSG Shane Hamann)

## Director's Corner: Thoughts for Training Readiness



by Jon Cleaves, Director, Complex Operational Environment and Threat Integration Directorate

I had the extremely great pleasure this month of training some of our fine Soldiers directly. Always the best part of my job is when I have the opportunity to interact with the troops and help them gain understanding of our future adversaries. At one point during one of the blocks of instruction, I was asked a question about the threat in an example with which we were working. The question was about the distance between two threat elements. I answered that they would be disposed far enough apart that US forces could not decisively engage them both simultaneously.

"Yes, but how far?"

"That depends on the terrain and our weapon systems."

My answer was not initially satisfactory. The expectation in the room was that there was a stock answer for these two threat elements, a natural distance apart that could be codified and smart-booked. And therein lies one of our greatest challenges. Tactical intelligence analysis, if it ever was, is not about geographically disposing the threat pieces according to some schematic. It's the concepts these young Soldiers need, not a "red-only" wiring diagram. Once I took them through what decisive engagement meant, the weapons with which we could be expected to engage them, and the impact of the terrain on that engagement, the answer fell right out. But the larger lesson was that any significant change to either our capability or the terrain made the final answer quite different.

The Army needs to teach threat tactics, not threat control measures. We will continue to lead this effort, including a partnership with the great team at the ICoE to look at our tactical intelligence analysis doctrine. If you find yourself asking the '2' (or the OPFOR at a training center) for a template, I submit that you are asking the wrong question. The enemy can't be "templated" (mostly because that is not a verb...), but he can be predicted.

**Jon**

[jon.s.cleaves.civ@mail.mil](mailto:jon.s.cleaves.civ@mail.mil)

### What is the *Hybrid Threat* (HT) for training? (TC 7-100.2)

In training exercises, the Opposing Force (OPFOR) HT is the diverse and dynamic combination of regular forces, irregular forces, and/or criminal elements all unified to achieve mutually benefitting effects—realistic and representative of actual threats.

### CTID Red Diamond Disclaimer

The *Red Diamond* presents professional information but the views expressed herein are those of the authors, not the Department of Defense or its elements. The content does not necessarily reflect the official U.S. Army position and does not change or supersede any information in other official U.S. Army publications. Authors are responsible for the accuracy and source documentation of material that they reference. The *Red Diamond* staff reserves the right to edit material. Appearance of external hyperlinks does not constitute endorsement by the U.S. Army for information contained therein.

# THE WETED “PLAYING FIELDS”

*OE and Hybrid Threats in Wargaming, Experimentation, Testing, and Evaluation*

by Mike Sullivan, TRISA-WETED Red Team, (ThreatTec LLC Ctr)



Much of what WETED does is about the beginning. Simply stated, any exercise or experiment to which WETED applies resources and expertise is founded on a scenario which drives what forces are to be engaged, what equipment they will have, where the fight will take place, and often most importantly, how many of the PMESII-PT elements will be in play. This article discusses what the collective WETED experience has been in recent years regarding all of the above.



First and foremost is the scenario itself. By and large these are built and approved by ARCIC and evolve over time. Many are classified because of where they take place. Others are more general and speculative. All share a core intent—provide the director and senior command involved with the most stressful and realistic environment possible as a means of assessing the performance of U.S. Forces in engagements with capable and committed enemy forces with certain advantages because they are on their home “turf.”

The most typical physical features of recent scenarios involve availability of ports and airfields, road and highway networks, complex (built up, hills and mountains, lakes and dams) terrain, restricted frontages, and unrestrictive weather. As the Army examines its capability of getting to where it needs to go and dominating an enemy force on arrival or soon thereafter, “access” is critical. Because much of what WETED does is focused almost exclusively on the Army, many of the challenges of an attacking force getting across the shore and to the APOD are often assumed away.



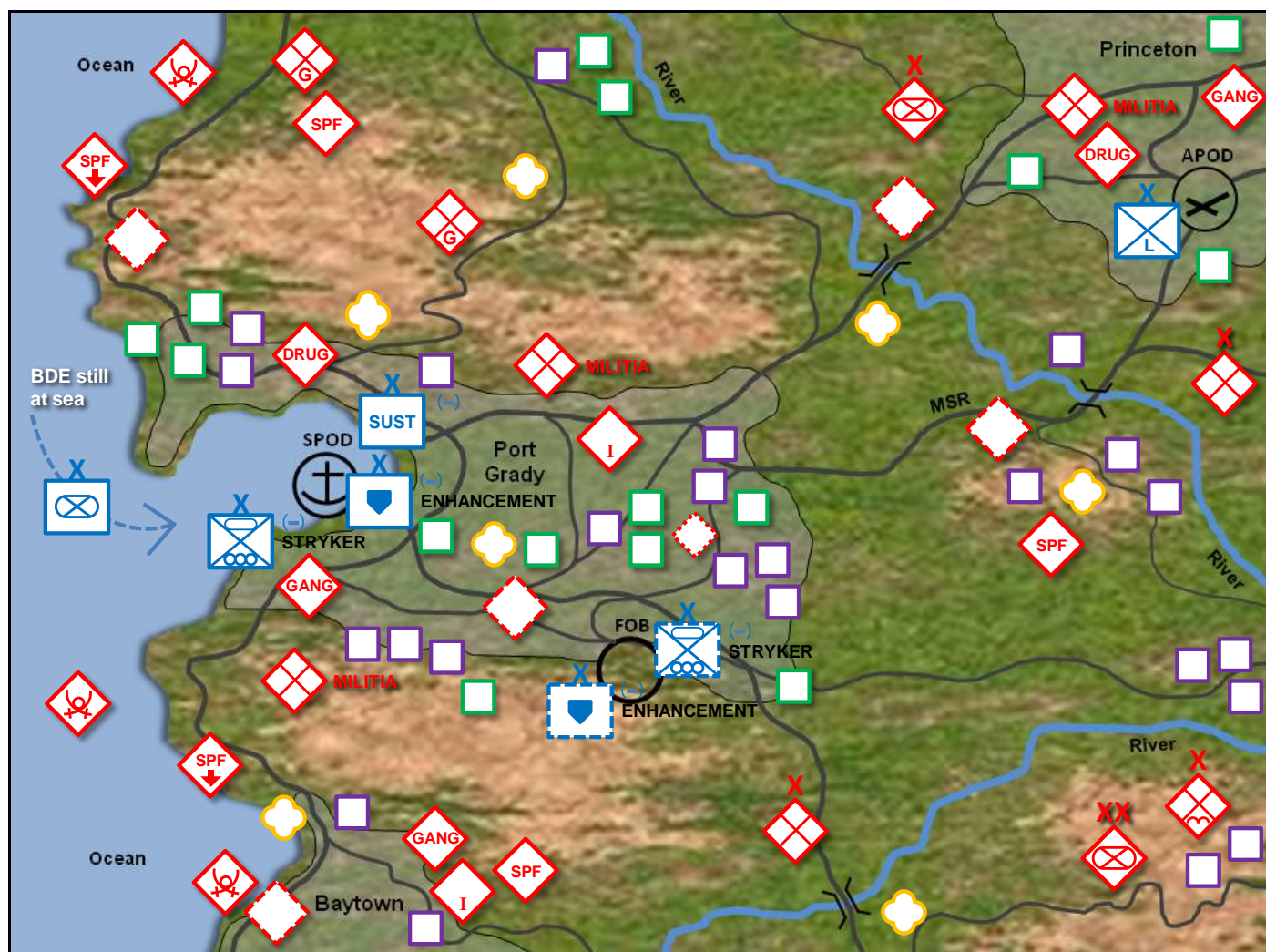
Most scenarios posit the multi-brigade size Blue Force as having arrived in theater and established a secure area for reception of follow-on forces and continuous logistics activities. The units are fully modernized infantry, heavy, Stryker brigades supported by equally modern artillery, aviation, air defense, and engineer units. Intelligence reads are provided by every level of capability, including what are regarded as “national” assets. Joint support is provided by USAF tactical air, UAVs, and C2/ISR enhancements. Naval gunfire and limited carrier-based attack air support is an occasional feature of the Blue picture. Logistics and most other forms of combat and combat service support come from FSBs and, in recent events, Maneuver Enhancement Brigades.



TRADOC G2 TRISA representatives participate in scenario development and usually “build” the forces that “fight” inside the experiments or exercises. This ensures both credibility and continuity of effort across the several Army and joint laboratories in which they take place.

Red forces are always sizable and capable, if somewhat less “modernized” than those on the Blue side. The scenario portrays them as being a threat regionally and, occasionally, internationally with credible WMD capability. The national leadership will be firmly in control and somewhat

predictable. C2 is often highly decentralized with forces empowered to operate freely within broad doctrinal concepts and national “intent”. Local popular support will be firm and responsive during the campaign. Regular forces will not be a major combat match for the Blue brigades but able to engage and defeat small blue units at selected times and places. Militia and local sympathetic paramilitary units will be entrenched and effectively hidden in built up and rural areas. Local police will also be part of the threat, but necessary allies in population control. An integrated and extensive Air Defense capability will be able to confound much of what the USAF could do in close air support. Artillery and mortars will have and use precision munitions to good effect. There will be a small and hard to find naval component and a huge commercial and fishing fleet capable of interfering with and reporting on Blue ship movements. (See figure 1 for an illustration (example) of how the Blue and Red forces are typically arrayed at the start of an exercise/experiment.)



**Figure 1. Array of actors in an exercise or experiment (example)**

All of this, the scenario, the Blue Force and the Red Forces and homeland, will be inserted into one of two exercise designs. The most common is a simulation supported experiment involving multiple labs and Centers of Excellence. A federation of simulations (ONESAF, JANUS, MTB, AWSIM, FIRESIM, etc.) will be connected digitally to produce effects and ultimately data for the responsible analysts to consider as findings and recommendations for the force developers.

The other design is the one used at the higher level exercises such as *Unified Quest*, the CSA’s annual strategic review wargame. It is often referred to as a “table top” game or MAPEX. In this design, groups of players on both sides develop moves that are presented to a panel of adjudicators and assessed for their effectiveness and impact on the other side. Ultimately, panels of senior leaders examine the emergent findings and recommendations for the CSA to consider as he competes for the resources needed to build and sustain the Nation’s Army for missions 8-10 years in the future.



Of these two designs, the one that is able to best examine forces in the full PMESII-PT context is the second. Simulations are very good and getting better at showing the effects of engagements between weapon systems, equipment, and structures. They are much less effective at showing what happens in minds, hearts, and amidst the clutter of towns, villages, cities and even the open spaces around them. The “table top” environment lends itself to at least discussion of the effects and impact of all aspects of PMESII-PT, particularly when the panels are populated with experienced players willing to realistically assess those effects and impacts. The TRISA WETED Red Team is particularly valuable in these discussions; the perspective embedded in the Team is deep (many members are from the Vietnam era and lived through several Army Transformations) and broad (the TRISA WETED leadership has consciously built a Team with full spectrum experience in Joint, Heavy, Light, SOF, Artillery, Aviation, Regular Army, Army National Guard, USMC, Intelligence, Public/Legislative Affairs, combat, non-combat, peace enforcement, humanitarian, counterterrorism, and senior leadership activities). Moreover, in that the Team is not on active duty or government employees, it is unconstrained in offering its perspective in what can be contentious discussions on those panels.

Next month in the *Red Diamond*, WETED describes how effective a typical set of Red TTP can be at forcing the Blue side to reconsider whether it has in fact gained full and secure access to the AOR. In the meantime, we can use your thoughts on the WETED “playing fields,” particularly on how the Models and Simulations community can improve the PMESII-PT “realism” of their tools. For example, a specific challenge is: why isn’t there a non-lethal munitions capability for forces to use for population control in an urban fight? Please share your comments and questions with us by emailing WETED point of contact at [sullivan0505@msn.com](mailto:sullivan0505@msn.com).

#### **Militia (Opposing Force)**

An organization which generally refers to citizens trained as soldiers (as opposed to professional soldiers), but applies more specifically to a state-sponsored militia that is part of the state’s armed forces but subject to activation only in an emergency. To avoid confusion, the TC 7-100 series uses *militia* typically in the latter sense. Irregular forces might be referred to or declare itself as a “militia;” however, the term *militia* is not typically used to describe guerrillas, insurgents, or criminals associated with opposing forces.

TC 7-100.2, *Opposing Force Tactics*

## **OLD GHOSTS FROM THE COLD WAR: THE ANKARA EMBASSY BOMBING**

### ***Irregular force with suicide vest assault against a fixed site***

by Jim Bird, OE Assessment Team (Overwatch Ctr)



**Figure 1. Sanli’s SVIED and DHKP/C banners**

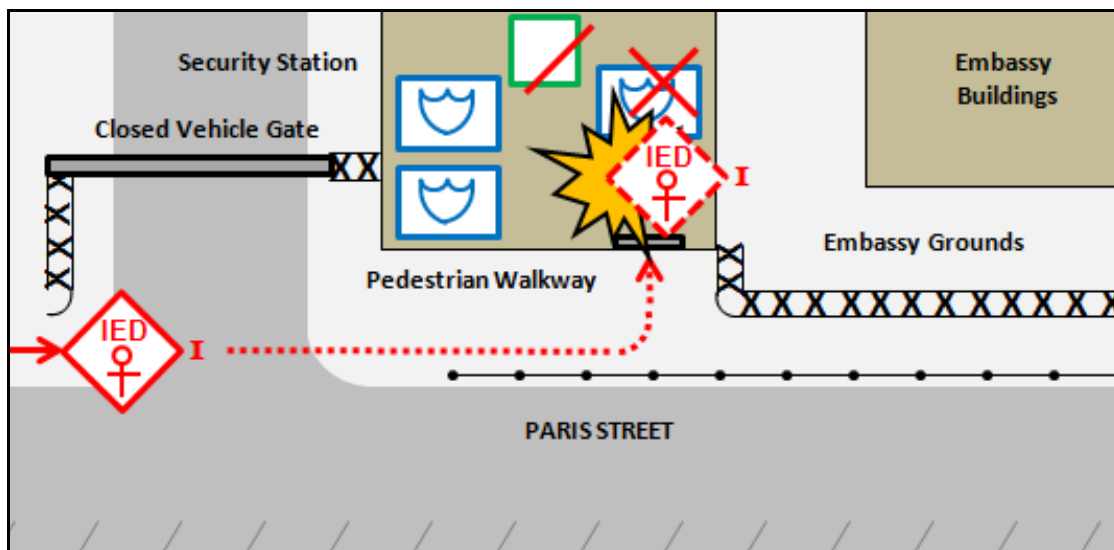
Newly-appointed Secretary of State John Kerry experienced a challenge his first day at the office on 1 February 2013. No sooner had he been sworn in that day when he learned that the American Embassy in Ankara, Turkey, had suffered an attack by a lone suicide bomber. Although two people (including the perpetrator) died at the scene, a measure of consolation still remained: no American lives had been lost, and what intelligence experts described as “the robust, layered security” of the U.S. Embassy compound prevented serious penetration of the exterior perimeter and minimized the number of casualties.<sup>1</sup> A newly-released OEA Team Threat Report, [\*Old Ghosts from the Cold War: The Ankara Embassy Bombing\*](#), examines the circumstances surrounding the attack, the background of the suicide bomber, and possible training implications for Troop Program Units.

Early in the afternoon (local time) of 1 February 2013, a Turkish national, Ecevit Sanli, walked toward an access control building located on the outer perimeter of the U.S. Embassy at Ankara, Turkey. Neither his dress nor his deportment suggested anything more ominous than performing routine courier duties. Because he carried an envelope in one hand, security personnel probably thought Sanli intended to drop off a document. Once Sanli reached Gate 2, Mustafa Akarsu, the guard posted there, opened the exterior door of the gatehouse, a standard procedure in the absence of a drop-slot for packages.



**Figure 2. Closed circuit surveillance-suicide bomber approaches gate**

Security cameras captured what happened after Sanli stepped into the checkpoint. Once inside, the bomber unsuccessfully attempted to pass through a metal detector. When its alarm sounded, Sanli panicked and reached for the detonator on his suicide vest improvised explosive device (SVIED). Closed-circuit television (CCTV) footage went black immediately after a voice yelled, "Run away, a bomb!" The ensuing explosion killed both the terrorist and the security guard, and seriously wounded Didem Tunkay, a well-known Turkish television journalist who also happened to be passing through the checkpoint when Sanli detonated his SVIED.



**Figure 3. Suicide vest bomber assault on the embassy security control point**

The investigation later revealed that Ecevit Sanli was a convicted terrorist with a mental condition contracted during a prison hunger strike. He had recently reentered Turkey illegally after violating parole, and was wanted for questioning by Turkish authorities. He was also a member of the outlawed Revolutionary People's Liberation Party-Front (DHKP/C), a radical, Marxist-Leninist organization with a past dating to the Cold War days of the early 1970s. Tensions rose to the surface in January 2013 when authorities learned of a recent DHKP/C decision to attack foreign targets. In the wake of leftist demonstrations in Adana, Gaziantap, and the port city of Iskenderum, Turkish security forces launched a preemptive strike against the group, rounding up more than one hundred of its members and sympathizers before the month ended. Although the DHKP/C's "People's Cry" website linked the embassy attack to the arrival of NATO Patriot missile batteries in Turkey, the real reason behind the bombing was probably a push-back against intense pressure recently applied by Turkish authorities.

Immediately following the bombing, embassy personnel as well as Turkish police sprang into action, the former by moving present-for-duty staff to a safe haven inside the compound, and the latter by swarming the exterior of the embassy perimeter in an impressive show of force. Shortly thereafter security personnel restored order, and Ambassador Francis Ricciardone emerged to publicly condemn the perpetrators, express solidarity with the Turkish government, and extend sympathies to the family of Mustafa Akarsu, the slain security guard. Ambassador Ricciardone characterized Akarsu as “a great hero,” and later attended his funeral.<sup>2</sup>

Several aspects of the Ankara Embassy bombing will attract the interest of trainers and scenario writers. First, it is an excellent example of an “SVIED Recon and Return” attack as explained on page 63 in TRADOC G2 Handbook No. 1.07 C3, [A Soldier’s Primer to Terrorism TTP](#). The real-world scenario described in this *Threat Report* can be easily replicated in home-station training environments, and would require very few personnel to act as role players. Finally, the report drives home the point that layered physical security and force protection measures, together with current and well-rehearsed evacuation plans, can combine to minimize or neutralize the effects of a terrorist attack.

The [Old Ghosts from the Cold War: the Ankara Embassy Bombing](#) *Threat Report* provides information to the Army training community on the 1 February 2013 attack. Besides an event review accompanied by a diagram and photographs, the report examines the threat actors and their motives, provides an analyst assessment of the attack, and suggests the feasibility of applying lessons learned to home station training environments.

## Endnotes

<sup>1</sup> Scott Stewart, [“Soft Targets Back in Focus,”](#) *Stratfor Security Weekly*, 14 February 2013.

<sup>2</sup> [“U.S. Ambassador Attends Security Guard’s Funeral,”](#) *Hurriyet Daily News*, 2 February 2013.

# HORN OF AFRICA OEA DJIBOUTI: MILITARY VARIABLE PREVIEW

## *Capabilities in an Operational Environment*

by H. David Pendleton, OE Assessment Team (ISC-CG Ctr)

In the fall of 2013, the TRISA-CTID OEA Team intends to release an updated version of its Horn of Africa (HOA) Operational Environment Assessment (OEA). The HOA OEA was last published in February 2009 and much has changed in the area since that time, including the division of one country, Sudan, into two separate states—South Sudan and Sudan. An OEA examines the political, military, economic, social, information, infrastructure, physical environment, and time (PMESII-PT) components of an operational environment (OE). This *Red Diamond* article specifically focuses on the military variable for Djibouti; articles highlighting the military variable for the other HOA countries may follow in subsequent issues.

Djibouti is a small but strategically important country for the US that is located on the Gulf of Aden just south of the Red Sea and across the gulf from Yemen. While a poor country, Djibouti is the lifeline for landlocked Ethiopia, as almost all of the latter’s exports and imports go through the port located in Djibouti City. The city, Djibouti, lies on the southern coast of the Gulf of Tadjoura, and is one of the busiest harbors in the region. Due to the increase in import/export activity since Ethiopia no longer uses the ports in Eritrea, Djibouti is in the midst of constructing a new port on the northern side of the gulf at the city of Tadjoura.

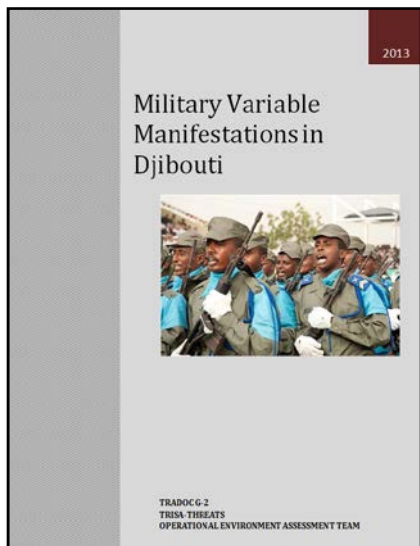


After the events of 11 September 2001, the US negotiated the rights to station military personnel in Djibouti. Since then, the US Combined Joint Task Force-Horn of Africa (CJTF-HOA) has called Camp Lemonier near Djibouti City home. Currently about 1,200 US military personnel serve in the CJTF-HOA contingent, including a squadron of F-15E Strike Eagles and a Civil Affairs unit. CJTF-HOA members help train members of the Djibouti military and other forces in the

HOA region. France, Japan, and Germany also have a military presence in Djibouti. In total, there are about 5,000 foreign troops stationed permanently in the country.

Due to the presence of the foreign troops, only about 11,000 personnel serve in the *Forces Armées Djiboutiennes* (FAD), or the Djibouti military, but that equates to about 3% of the entire population. The naval and air force portions comprise only about 1,000 members. The 11,000 total personnel also include 2,000 military personnel that belong to the *Gendarmerie Nationale* and 2,000 members of the *Force Nationale de Sécurité* (National Security Force). The National Security Force (NSF) is under the operational control of the Minister of Interior (MOI) and not the Minister of Defense (MOD).

Due to an active duty recall program enacted in 2008 and the adoption of the *Service Nationale Adapté* (national service requirement) five years earlier, most young Djibouti adult males have some military experience. The two-year national service requirement consists of three months of training followed by professional training in one of 21 trades that are supposed to help the soldiers when they return to civilian life.



The FAD contains all three military branches—army, navy, and air force—that operate under the auspices of the Chief of Staff of the Army, who reports to the MOD, who is subordinate to the commander-in-chief, the Djibouti president. The NSF reports through the MOI to the president. In addition to the three branches, three command headquarters—north, central, and south—also report to the Chief of Staff.

Not including the 4,000 members of the gendarmerie or the NSF, there are about 5,500 members in the FAD's army component. The major army units include one Republican Guard Regiment, four infantry regiments, one armored squadron, one mobile force infantry regiment, one artillery battery, one airborne company, one support/logistics group, and one headquarters regiment. FAD members often receive their training from Ethiopian defectors or Yemenis, as they have experience with much of the former Soviet/Russian equipment the FAD uses. Over the last decade, the FAD has received additional training from the US, French, and German forces stationed in the country.

The army elements use primarily French or former Soviet/Russian equipment, but the FAD operates a smattering of other countries' weaponry. The FAD army fields no main battle tanks and armor equipment is generally limited to reconnaissance vehicles, armored personnel carriers, and a very few number of infantry fighting vehicles. Many of the vehicles are non-operational for maintenance issues, usually a shortage of spare parts.

The navy is quite small and operates more as a coast guard than a blue water navy. There are only 380 personnel and they operate barely more than a dozen boats. The primary mission of the navy is to deter smugglers and deal with piracy more than to conduct combat operations against an armed enemy. Much of the naval fleet is Western in origin, including a number of US-built Zodiacs useful for the navy's primary missions.

The air force is a component of and subordinate to the FAD. Only about 600 personnel compose the *Force Aérienne du Djibouti* or the Djibouti air force. Most of the pilots learned to fly in France so their doctrine is Western in nature. Most of the aircraft are designed for transportation, including all fixed-wing airplanes. The combat exceptions include two Mi-24 Hind helicopters that can be used for both transportation and for ground attack missions. The air force is more to inspire FAD morale than actual combat effectiveness.

The *Gendarmerie Nationale* and the NSF are both paramilitary forces that could be used for combat. They carry small weapons and usually travel in wheeled vehicles. The NSF, however, must borrow vehicles from the army to move its forces.

There are several non-state paramilitary forces in Djibouti. The *Front pour la Restauration de l'Unité et la Démocratie* (FRUD) has been around since August 1991 when three Afar opposition groups joined forces. The FRUD broke apart in 1994 and the majority signed a peace treaty with the Djibouti government that year and became a political party by

1996. The FRUD-Combattant continued to fight against the Djibouti government, but then signed its own peace treaty in 2001. While FRUD-Combattant is now a government opposition political party, it still possesses weapons and a combat capacity.

The major private security organization in Djibouti is the group formerly known as Blackwater Worldwide. The government hired the company in 2008 to help combat piracy in the HOA area. Most private security organizations will only possess small arms and are usually supportive of the Western powers.

Djibouti is an ally of the US, and Western powers continue to improve the FAD's readiness through CJTF-HOA training teams and exercises. Djibouti's strategic position will likely cause American forces to remain in country for the foreseeable future. See the HOA OEA when it is published later this year for more details on the Djibouti military and the other seven PMESII-PT variables.

## RUSSIA'S AEROSPACE DEFENSE FORCES SATELLITE SYSTEM: KONDOR

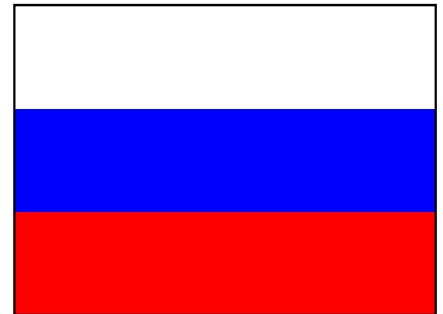
---

### *Near-term capabilities in Complex Operational Environments*

by Steffany A. Trofino, Threats Integration Team (DAC)

Since its inception from the Cold War era, Russia's space program has continued to adapt to evolving technologies, making the Russian military space program a front runner in global satellite research and development programs. During the Cold War, the Soviet Union was the first country to place a man in orbit. Since then, Russia has remained a top contender in the space research and development sector and has recently indicated that advancements and further development of space assets will become a key priority for Russia's security.

Significant transformations in the Russian military space program have taken place over the past twenty years. After the collapse of the Soviet Union on 7 May 1992, Russian President Boris Yeltsin signed a presidential decree reorganizing the Russian military space units into Russian Military Space Forces (VKS), merging existing space units into Russian Strategic Missile Forces (RVSN). Unfortunately, with the degradation of the Russian economy during the 1990s, existing Russian space assets deteriorated as improvements were difficult to facilitate during times of fiscal constraint. In an additional effort to financially consolidate, in 2001 Russian Space Forces were again split from RVSN and renamed Space Forces of Russia (KVR). However, with improvements in the Russian economy during the first decade of the 21<sup>st</sup> century, newer, more advanced systems began to replace old, outdated systems as Russian defense expenditures gradually increased.



One and a half years ago on 1 December 2011, another change to the Russian Military Space program took place as the program evolved into what is known today as Russian Aerospace Defense Forces. Russian Aerospace Defense Forces is commanded by Major General Alexander Golovko and is tasked with overseeing Russian missile defense programs as well as the creation, deployment, maintenance and control of in-orbit space vehicles. The Russian Aerospace Defense Forces are structured into two primary components: Space Command and Air and Space Defense.

#### **Russia's Space Command consists of the following components:**

- 153rd is the main trial center for testing and control of space systems and is named after G.S. Titov. It is located at Krasnoznamensk, Russia just outside of Moscow and was formally known as Golitsyno-2 (up until 1994). Comparatively, it is similar to the United States Joint Functional Component Command for Space and Global Strike (JFCC SGS) under US Strategic Command, Offutt AFB, Omaha, Nebraska.
- 820th is the main center for early warning surveillance. It is located in Solnechnogorsk, Russia 65 km outside of Moscow.

- 821st is Russia's primary space surveillance center located on the outskirts of Moscow in Noginsk-9, Moscow Oblast. This center primarily monitors various Russian surveillance programs to include Dunay-3U radar station, Krona space object recognition station, Zelenchukskaya, Karachay-Cherkessia, Krona-N, Nakhodka, Primorsky Krai, the Moment space surveillance complex, as well as Okno center located in Tajikistan, Okno-S, and finally Primorsky Krai. It is led by Oleg Maydanovich who was the former head of the Titov Centre.

#### **Russia's Air and Space Defense Command consists of the following missile defense divisions:**

- 9th Missile Defense Division (A-135 anti-ballistic missile system) in Pushkino, 30 km northeast of Moscow.
- 4th Missile Defense Brigade in Dolgoprudny, 20 km north of Moscow.
- 5th Missile Defense Brigade in Vidnoye, a suburb of Moscow.
- 6th Missile Defense Brigade in Rzhev, Russia which is located in Tver Oblast.
- Test facilities under the command include State Testing Plesetsk Cosmodrome which is located in Arkhangelsk Oblast (800 km north of Moscow) and the Kura Test Range located in northern Kamchatka Krai in the Russian Far East.

The Air and Space Command is led by Sergey Popov who was formerly in charge of air defense in the Air Force.

Multiple Russian Aerospace Defense Forces are located throughout Russia, yet several bases also remain in the Commonwealth of Independent States countries such as early warning radar stations in Kazakhstan, Belarus and the Okno facility in Tajikistan.

While transformation continues within Russia's Aerospace Defense Forces, a growing trend in Russia's research and development programs is placing an emphasis on advanced satellite systems such as the Kondor class satellite system, which is Russia's first remote sensing satellite system scheduled to be launched in late 2013.

#### **Kondor Satellite**

After several years and lengthy delays, Russia is preparing to launch the Kondor satellite system into orbit (by end of 2013). As it is claimed to be Russia's first "remote sensing" satellite system, the Kondor satellite system is a synthetic aperture radar system capable of receiving, storing, and transmitting to ground stations high precision data in the microwave band, in real time.<sup>1</sup>

The system is designed to film the earth constantly in all weather conditions. The optical-electronic equipment can receive, store, and transmit to ground stations data in both the visible and infrared bands.<sup>2</sup> Kondor satellite modifications provide up to one meter resolution.<sup>3</sup> The satellites weigh up to 1,150 kg and have a life expectancy of five years.

Deputy head of the Russian space agency Roscosmos Anatoly Shilov indicated that "the Kondor is an 800 kg Earth remote-sensing spacecraft designed to provide high-resolution radar imagery and terrain mapping in real-time." It will be launched as part of the so-called Arktika Earth observation satellite grouping for observation of the Arctic region. Shilov further stated, "As a rule, 90% of the time the Arctic region is covered with clouds or remains in darkness due to long polar night season. In such conditions these satellites are indispensable."<sup>4</sup>

During a recent IDEX 2013 show in February 2013, Kondor satellite developer NPO Mash disclosed that it had been preparing not one but two launches of satellites in the Kondor series scheduled for 2013 – one for the Russian Ministry of Defense and one for an undisclosed foreign customer.

#### **\*Kondor Satellite Specifications**

Spacecraft mass	Originally 800 kilograms (by 2007 reported to be 1,150 kilograms)
Payload mass	350 kilograms (as of 2007)
Orbital altitude	500 kilometers (450-900 kilometers)

Orbital inclination	up to 98 degrees toward the Equator
Image resolution (radar)	1-3 meters
Observable swath	1,200 kilometers (600 kilometers to each side of the flight path)
Radar antenna diameter	6 meters
Radar antenna frequency range	S-band (9.5 centimeters)
Spectral range of the imaging system	Optical and/or infrared
Operational life span	5 years (3-10 years)
Launch vehicle	Strela
Launch site	Baikonur, Site 175, Silo No. 59

#### **\*Known Participants in the Kondor Project**

Prime developer	NPO Mashinostroenia, Reutov, Moscow Region
Deployable radar antenna	OKB MEI, Moscow
Radar imaging system	NPO Vega (a.k.a. OAO Kontsern Vega)
Optical payload	LOMO (St. Petersburg)
R10 solar array driving mechanism	VNIEM
Onboard avionics	Aksion holding, Izhevsk
ARK-20 power distribution and management system	AVEKS (formerly OKB-12) Moscow

*\*Data provided by Kondor developer NPO Mash circa 2011<sup>5</sup>*

As Russia continuously adapts to maintain a competitive edge in space research and development, more advanced systems will become a predominant factor. In December 2012, Prime Minister Dmitry Medvedev approved a plan to increase expenditures allocating 68.71 billion dollars (2.1 trillion rubles) to Russia's space program in support of research and development supporting Russia's advancements in space between 2013 and 2020.<sup>6</sup> As known specifications of advances in Russian space systems become more transparent, interested parties will have the ability to conduct reverse assessments on various Russian systems and seek to capitalize on the systems' weaknesses and/or vulnerabilities.

## Endnotes

<sup>1</sup> RIA Novosti, "[Russia may launch its first Earth remote sensing satellite in 2012](#)," 22 September 2011.

<sup>2</sup> Interfax.com, "[NPO Mashinostroyeniya to launch two Kondor earth observation satellites](#)," 18 February 2013.

<sup>3</sup> Interfax.com, "[NPO Mashinostroyeniya to launch two Kondor earth observation satellites](#)," 18 February 2013.

<sup>4</sup> RIA Novosti, "[Russia may launch its first Earth remote sensing satellite in 2012](#)," 22 September 2011.

<sup>5</sup> Anatoly Zak, "[Russia prepares to fly its first radar satellite](#)," RussianSpaceWeb.com, 22 February 2013.

<sup>6</sup> The Voice of Russia, "[Russia to invest 2.1 trillion rubles in space industry until 2020](#)," 27 December 2012.

## AIR DEFENSE SYSTEMS: A FIGHT FOR AIRSPACE CONTROL

### *Complex Operational Environments*

by Lieutenant Colonel (P) Thomas Georges, Training, Education, & Leader Development Team/RAF LO

The concept of using aerial means against an adversary is found as early as 1783, but the military use of aerial systems was not documented by the US until mid-1800. Although primitive by today's standards, men carried by balloons and utilized for observation purposes was a

great accomplishment for the day. Although the balloon was advanced because it flew far above the range of weapons of the time, air defense means (primarily rifle and cannon fire) limited balloon use because the attempts made to shoot it down were enough to scare

personnel out of the sky. Eventually, the balloon was essentially eliminated for military use with the introduction of the airplane.

As aircraft and missile technology increases, so too do the air defense measures built to destroy the advanced flight technology, thus fueling the continual battle between air/missile and air defense artillery (ADA) systems to control air and space. Although surface-to-air missiles are classified by guidance, mobility, altitude and range, the missiles can be broken down into main surface-to-air missile categories which include: man portable air defense systems (MANPADS); long, medium and short range missiles; anti-ballistic missiles; and anti-satellite missiles.

MANPADS are easy to use, easily concealable and, relatively inexpensive surface-to-air missiles. With little training, a single individual can operate a MANPADS by simply pointing at a target, activating the target lock and pulling the trigger. Due to the ease of use, lethality, and low cost, MANPADS are an attractive commodity and reportedly older versions can be acquired on the black market for a few hundred dollars. Various countries produce MANPADS but the most common include the Russian Igla (SA-18) which has a two color infra-red homing system and a range of 5.2 km, the Chinese FN-6 which has an infrared homing system and a range of 6 km, and the US Stinger which has an infrared homing system and a range of 4.8 km.



**Figure 1.** [MANPADS](#)

Numerous types of long, medium and short range surface-to-air missiles are in production and exist with continual upgrades with technology. Depending on design, long, medium and short missile systems can deliver nuclear, biological, chemical (NBC) or conventional type warheads. Anti-ballistic surface-to-air missiles are missiles designed to destroy ballistic missiles in flight. While a number of anti-surface-to-air missile systems are produced and technically fall into

this category, few are capable of intercepting today's intercontinental ballistic missiles (ICBMs) in space due to speed and distance. Systems capable of destroying ICBMs include the Russian A-135 and US Midcourse defense system.



**Figure 2.** [Surface-to-air missiles](#)

Anti-satellite surface-to-air missiles are missiles designed to neutralize or destroy satellites. Although missile system capabilities to destroy satellites still exist, such as China's Xichang Satellite Launch Center, other means of satellite destruction have developed to include air-to-space missiles, ground-based lasers, and directed energy weapons.

With adjustments and upgrades, systems of the past are reemerging as a form of defense against stealth technology. Militaries are finding the older, very high frequency/ultra high frequency (VHF/UHF) band radar systems and their new variants resurface as a better ADA defense system against modern aviation than that of the more modern S-band radar-based ADA systems. Older radar systems detect the radar cross section (RCS) of an aircraft, which the design of stealth aircraft is unable to hide.

MANPADS are easily deployable, relatively inexpensive to produce in relation to an aircraft and a formidable deterrent for a pilot to not fly in an area. Due to technological development of today's MANPADS, a single untrained individual can effectively counter the well-educated pilot and has the means to defeat the most technically advanced aircraft. Has technology returned the advantage to the ADA operator and enabled the scare tactics which worked back in the mid-1800s? If scare tactics are not a factor, militaries must weigh the advantage of time and money expended in a pilot and aircraft against that of the time and money expended for that of a MANPADS and operator; thus, the introduction of the Unmanned Aerial Vehicle (UAV) to the airspace.

# HYBRID THREAT AND OPPOSING FORCE: *NEW ON ATN!* (CONTINUED FROM PAGE 1)

by Jerry England, Threat Integration Team (DAC)

Recently, a new page directing users to a variety of Operational Environment Assessments (OEAs) and other Threat products has come online. The new page, currently under development, houses many of the most requested products from CTID including—

- **OE Quick Guides**
- **Decisive Action Training Environment (DATE)**
- **Red Diamond Newsletters**
- **Threat Assessments**
- **OE Estimates**
- **Terrorism Handbooks**
- **Threat Reports**











The Regionally Aligned Force Training Environment (RAFTE)-Africa will be added at a future date.

Eventually the two pages will be linked together in order to better support exercise designers and improve the integration of detailed Threat data with current operational environment (OE) information. The combination of this material will be an essential tool for exercise design. From irregular Threat force structures to tank specifications, the site provides useful information for a variety of echelons and theaters.

See [https://atn.army.mil/dsp\\_template.aspx?dpID=311](https://atn.army.mil/dsp_template.aspx?dpID=311)

A sample of Threat force structure in process of upload and update on the ATN site is as follows:

**Doctrinal Resources & References:**  
[FM 7-100.1 Opposing Force Operations](#)  
[TC 7-100 Hybrid Threat](#)  
[TC 7-101 Exercise Design Guide](#)  
[Insurgent Functional Cell Symbols](#)  
[Worldwide Equipment guide 2012 - Volume 2 Air and Aid Defense 2012](#)  
[Decisive Action Training Environment \(DEC 2011\)](#)  
[FM 7-100.4 Organization Guide](#)  
[TC 7-100.2 Opposing Force Tactics](#)  
[OPFOR Unit Symbols](#)  
[Worldwide Equipment guide 2012 - Volume 1 Ground Systems 2012](#)  
[Worldwide Equipment guide 2012 - Volume 3 Naval and Littoral Systems](#)

Threat Force Structure			
	<a href="#">01 Mech Inf Div (IFV)</a>		<a href="#">02 Mech Inf Div (APC)</a>
	<a href="#">03 Tank Division</a>		<a href="#">04 Mtzd Inf Div</a>
	<a href="#">05 Separate Combat Brigades</a>		<a href="#">06 Combat Brigades</a>
	<a href="#">07 Combat Support Units</a>		<a href="#">08 Combat Service Support Units</a>
	<a href="#">09 Guerrilla Brigade</a>		<a href="#">10 Insurgent Orgs</a>

To Submit Feedback or Leave Comments, Please Contact [Jerry England](#)

[How To Use](#) | [Site Map](#) | [Contact](#) | [iSALUTE](#) | [Mail Products](#)Training Solutions to Stay Army Strong.

# BOAT OPERATIONS – NIGERIA AND SOMALIA

---

## *TTP in maritime and littoral areas of an Operational Environment*

by Marc Williams, Training, Education, & Leader Development Team (ISC Contractor)

It is easy for ground forces to forget the need for boats when they get fixated on maneuvering on land. But water features such as rivers, creeks, swamps, lakes, and littoral ocean areas are both obstacles to be breached and avenues of approach. For this, ground forces need boats, especially specialized ones for shallow draft, speed, and silent running. This article will address successful small boat operations by militants in Nigeria (Movement for the Emancipation of the Niger Delta, or MEND) and pirates in Somalia.

### **Boats in the United States**

In the US, boats are defined as watercraft less than 65 feet long. Boats enable the Navy and Coast Guard to perform missions such as rendering aid to people and property in distress at sea and protecting ports, waterways, and shores. Our sea Services also use boats to enforce Federal laws in waters under US jurisdiction.

Boats are so important to the Army that the Transportation Corps manages a large fleet of around 300 watercraft in two categories: lighterage and floating utility. This provides the critical link of moving combat power from strategic sealift ships to beachheads and ports.<sup>1</sup> Tactical units use small boats to contact littoral sea operations (infiltration and assault) and riverine missions.

The United States sells military small boats (USN and USCG) through the Foreign Military Sales (FMS) program (<http://www.nipo.navy.mil/ABOUT/security-assistance/Foreign-Military-Sales/small-boats/>)

According to the US Navy program executive office, these boats include:

- [26 Foot Patrol Boat](#)
- [9.2 Meter Rigid Inflatable Boat](#)
- [25 Meter Fast Patrol Craft](#)
- [26 Foot Patrol Boat](#)
- [28 Meter Coastal Patrol Craft](#)
- [30m - 35m Coastal Patrol Boats](#)
- [32 Foot Patrol Boat](#)
- [34 Foot Protection Boats](#)
- [36 Foot Mini Armored Troop Carrier](#)
- [39 Foot Interceptor Boat](#)
- [55 Foot Patrol Boat](#)
- [Defender Class Response Boats](#)
- [Diving Support Vessel](#)
- [Fast Missile Craft \(FMC\)](#)
- [Hydrographic Survey Vessel](#)
- [Hydrographic Survey Vessel2](#)
- [Inflatable Boats](#)
- [Interceptor Boat](#)
- [MK V Patrol Boat](#)

- [Passenger Logistics Support Vessel](#)
- [Patrol Craft Coastal & MK III PB](#)
- [Rigid Inflatable Boat \(RIB\)](#)
- [Search and Rescue Boats](#)
- [Special Forces Rigid Inflatable Boat](#)

From USCG, this includes:

- [Arch Angel Fast Response Boat](#)
- [Defender Class Response Boats](#)
- [Law Enforcement Response Boat](#)
- [Protector Coastal Patrol Boat](#)
- [Response Boat – Medium \(RB-M\)](#)

#### **Complex Conditions in an OE**

In training or on actual operations, Army units could encounter the boats listed above. Not only will State forces use these, but so will militants and criminals. The militants in Nigeria have been very effective with small boat operations, as have the criminals (pirates) of Somalia.

## Nigeria

There has been a series of violent uprisings in the Niger Delta since 1966 and that includes private militias, ethnic militias, and pan-ethnic militias. The table below gives a better of idea of the scope of the problem faced by the Nigerian government.<sup>2</sup> Of these groups, the “Pan-Ethnic Militia” MEND is the largest and most powerful, specifically targeting government troops and multinational oil companies.

Private Militia	Ethnic Militia	Pan-Ethnic Militia
1. Niger Delta People Volunteer Force (NDPVF)	1. The Meinbutus	1. Movement for the Emancipation of the Niger Delta (MEND)
2. Adaka Marines	2. Arugbo Freedom Fighters	2. The Coalition for Militant Action in the Niger Delta (COMA)
3. Martyrs Brigade	3. Iduwini Volunteer Force (IVF)	3. The Niger Delta People Salvation Front
4. Niger Delta Volunteers	4. Egbesu Boys of Africa	
5. Niger Delta Militant Force Squad (NDMFS)		
6. Niger Delta Coastal Guerrillas (NDCGS)		

### Movement for the Emancipation of the Niger Delta (MEND) Tactics

MEND's attacks involve substantially more sophisticated tactics than those of previous militant groups in the Niger Delta. MEND's recent tactics include:

**Swarm-based maneuvers:** guerrillas are using speedboats in the Niger Delta's swamps to quickly attack targets in succession. Multiple, highly maneuverable units have kept the government and Shell's defensive systems off-balance defending their sprawling networks.

**Radically improved firepower and combat training:** allowing guerrillas to overpower a combination of Shell's Western-trained private military guards and elite Nigerian units in several engagements. (One of Shell's private military operators was captured as a hostage.)

**Effective use of system disruption:** targets have been systematically and accurately selected to completely shut down production and delay and/or halt repairs, and the guerrillas are making effective use of Shell's hostages to coerce both the government and the multinational corporations.<sup>3</sup>

The militants have repeatedly bombed pipelines, triggering an international increase in the cost of oil. They have also kidnapped foreign oil workers for ransom.

Activities decreased since the Nigerian government's offer of amnesty in 2009. However, operations have resumed since its leader, Henry Okah, was convicted in a South African court of masterminding the 2010 Independence Day bombings in Abuja which killed 12 people.

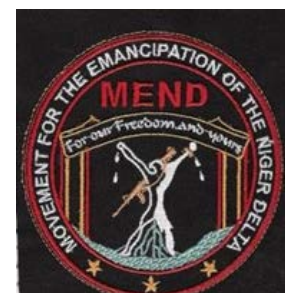


Figure 1. [MEND uniform patch](#)  
MEND Facebook© page, 23 April 2013

An example of one attack follows. The following narrative comes from *African Lions: The Colonial Geopolitics of Africa's Gas and Oil*, by Chris Stokel-Walker:<sup>4</sup>

### **MEND Attack on Ibeno Oil Facility (Stokel-Walker)**

The 74 ExxonMobil staff working at the Ibeno oil facility offshore the Akwa Ibom state in the Niger Delta would be forgiven for feeling slightly on edge as they went about their daily business on 14 November 2010. Offshore plants and rigs are by their nature isolated, often several miles offshore and sometimes hours away from contact with the mainland. That two days earlier the Movement for the Emancipation of the Niger Delta (MEND) had released the names of the seven workers they kidnapped earlier that week and explained in precise detail how they had encountered “stiff resistance from the Nigerian military” but overcome them in an “intense firefight” before attempting to set the High Island VII rig alight would be playing on the minds of those working at a separate rig. It was foreign-owned and therefore fair game to the eyes of MEND.

The sun was down at ten o'clock on a Sunday night and the Ibeno facility seemed calm on the surface. Undoubtedly some were worried, however, at recent attacks instigated by MEND – for good reason. The first sign of the attack was the crumpled booms of explosives detonating: they were rigged to the facility itself. Ibeno is one of eight platforms on the Oso field, sitting on a spoil that produces roughly 75,000 barrels of crude oil and 60,000 barrels of natural gas liquid (NGL) every day across all facilities.<sup>5</sup> The use of bullets, never mind heavy explosives, on an oil field is like holding a lit match to a powder keg.

Six speedboats raced alongside the facility and Ibeno was boarded by MEND fighters carrying guns. The boats flew white flags – but not to signify surrender in the western sense. MEND fly under the white flag of Egbesu, an Ijaw water spirit. They believe that they are defending the honour of Egbesu by keeping Delta waters in the control of the Ijaw people, and that by flying under his flag they will be protected from all bullets that come their way. There was a firefight to quell the military guard over the facility, and seven layworkers, all members of the Pengassan oil workers union were taken along with an eighth hostage, a member of management at ExxonMobil. They were whisked away to one of the many militant camps that MEND run on the Delta, some of which have come under protracted government rocket fire as an attempt to smoke out the fighters.

<sup>5</sup> [“Nigeria military frees oil hostages.”](#) *Al Jazeera English*, 18 November 2010.

The types of boats used by MEND vary, but one article by Sebastian Junger describes them as “light plastic speedboats with 75 horsepower engines. They take the top off the engine to get more cooling. They know exactly what they are doing.”<sup>6</sup>



**Figure 2.** [MEND speedboat with Egbesu flags](#)  
MEND Facebook© page, 23 April 2013

## Nigerian Government Response

The Nigerian government response to MEND's waterborne tactics has been to acquire more powerful patrol vessels. In 2009 they approved the purchase of two Israeli Shaldag MK-2 patrol boats for the army's use in the Niger Delta. The Nigerian navy is equipped with two 38-meter, Manta-class patrol boats built in Malaysia, and four 17-meter, Manta-class patrol boats built in Singapore. Additionally they have 20 troop carrying catamarans built in the Netherlands to be used by JTF in riverine operations.<sup>7</sup> The government troops supplement their surface force with air superiority employing both fixed- and rotary-wing aircraft.

## Somalia - Pirates

Somali pirates have adversely impacted international shipping in the Indian Ocean, the Arabian Sea, and the Gulf of Aden as a result of the Somali Civil War. Ranging out in small fast boats, the pirates developed tactics, techniques, and procedures (TTP) for quickly boarding and subduing ships.

## Somali Pirate Tactics

Somali pirates tend to operate a larger "mother ship" with two or more skiffs powered by twin 90 or 120 horsepower engines. Targets include tuna fishing fleets and long-range high-seas traffic. The pirates operate in three "generations" depending on experience and financial support:

The **first generation** consists of largely opportunistic pirating within 50 miles of Somali shores, especially in the Gulf of Aden, which has occurred for centuries. The **second generation** consists of more premeditated and longer distance raiding into the Somali Basin and around the Seychelles and involves mother ships that juggle dependence on bulky stores on board, with continued logistical support from home ports. The **third generation** Somali pirates will venture beyond the limits of even traditional Somali fishermen and threaten new sea lanes, including the vital East Asian energy lanes just off India's western shores.<sup>8</sup>

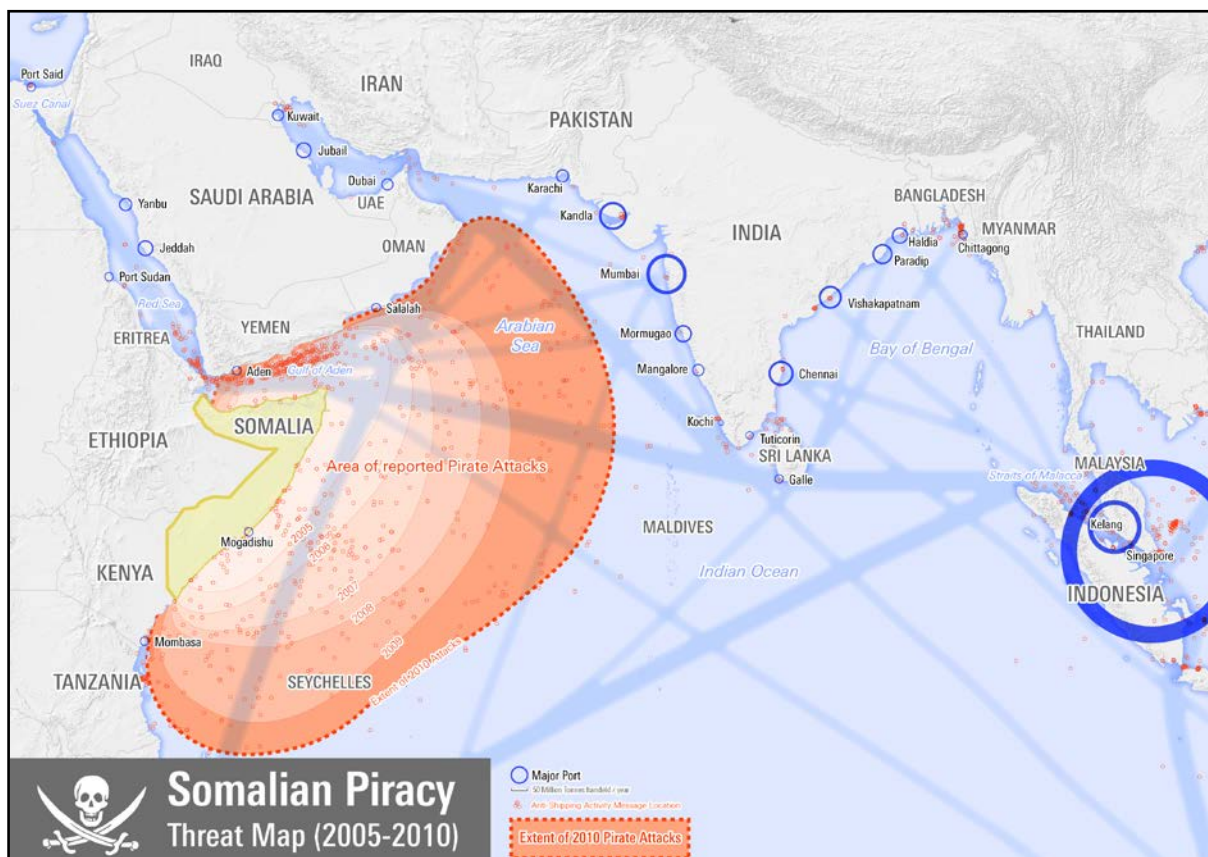


Figure 3. [Map of Somali pirate operations](#)

This “third generation” marks a seasoned pirate that can use forward support, “a technique first used in Gulf of Aden raiding, in which pirates relied on makeshift bases in Southern Yemen to resupply and refit, thanks to locals whose cooperation was likely bought with a promised share of the ransom. Evidence of forward support was discovered in the Seychelles early in 2009.”<sup>9</sup> Piracy pays. Ransoms paid out for kidnapped crews in 2010 were \$176 million, in 2011 it was \$159.62 million, and 2012 ransoms totaled \$31,750,000. And, piracy costs. Total cost of anti-piracy military operations in 2012 was \$1.09 billion.<sup>10</sup>

## Government Response



Figure 4. [EU NAVFOR logo](#)

In 2005 the losses to Somalia pirates became so great that the European Union (EU) instituted the Naval Force (EU NAVFOR) Operation *Atlanta* administered by Combined Task Force 150. In 2009 there were 86 attacks off the coast of Somalia. In 2010 there were 127 attacks of which 47 were successful. In 2011 there were 151 attacks but only 25 were successful. By February 2012, 1,000 pirates had been captured and were going through legal processes in 21 countries.<sup>11</sup> The success of the EU NAVFOR in 2008 prompted “the more professional pirates of the eastern Somali shoreline, some led by former Somali naval officers, to pivot back into the waters of East Africa and expand long-range operations even into the high seas of the western Indian Ocean. Those pirates are now extending operations to waters rich in prizes such as the Gulf of Aden.”<sup>12</sup>

By 2012, EU NAVFOR’s success had caused the pirates to change tactics again. Instead of using larger merchant vessels as mother ships, they had returned to using smaller dhows as mother ships, which makes them less suspicious. Countermeasures used on commercial ships now include private armed security guards, razor wire, and heightened monitoring watches when entering danger areas by crews on board.<sup>13</sup>

## Training Impacts

Few places where the US will operate will have no water approaches. Even in Iraq, a “desert” country, there were salt-water ports and two major rivers for operations. OPFOR doctrine recognizes this and equips its units for such contingencies. In [FM 7-100.4, \*Opposing Force Organization Guide\*](#), 11 assault boats with motors are part of the personnel and equipment list of the Brigade Tactical Group (Mtzd) (Antiarmor). Additionally in the same unit are six Zodiac inflatable boats with motors. OPFOR doctrine states, “In wartime, the State and its armed forces might nationalize, mobilize, confiscate, or commandeer civilian transportation assets that are suitable for supporting military operations. These assets can include trucks, boats, or aircraft.”<sup>14</sup> Throughout the equipment tables can be found amphibious tanks, amphibious self-propelled howitzers, amphibious trailers, underwater demolition sets and welding/cutting equipment, and underwater GPS systems for divers.



Figure 5. [EU NAVFOR units surveying Somali skiffs at sea](#)

The [Worldwide Equipment Guide \(WEG\)](#) has an entire volume dedicated to naval and littoral systems.<sup>15</sup> In the littoral section of the *WEG*, systems include fast attack craft, hydrofoils, catamarans, air-cushion landing craft, semisubmersibles, amphibious transporters, and very light craft. Other equipment can include unmanned underwater vessels (UUV) and wide use of inflatable boats (modular, rigid, and rigid-hulled).

“Coastal patrol, fast-attack, and landing craft can be used in inland waterways. Shallow-draft military riverine craft and commercial boats are widely used. Airboats can move quickly, even in the shallowest

waters. Barges can mount weapons and supplement carry capacity of vessels. Amphibious vehicles are widely used. Improvised swim assists such as bladders and barrels enable equipment and vehicles to cross water gaps. Hydro-propulsion water-craft and craft with snag protection are widely used. Jet skis (aka waverunners) can be adapted for military use, even mounting weapons and operating rapidly in shallow waters.”<sup>16</sup>

#### Littoral activities include the following:

- "Brown water" naval operations in coastal waters (out to as far as 200+ km from shore)
- Amphibious landing operations or port entry (opposed and unopposed)
- Coastal defense actions (including patrols, engaging enemy, and denying entry)
- Operations in inland waterways (rivers, lakes, etc)
- Actions in large marshy or swampy areas

#### OPFOR littoral activities can include (but are not limited to):

- Civilians conducting commercial and sport fishing, business transport, and shoreline maintenance, especially as a cover for monitoring BLUEFOR units
- Criminal activity; i.e. smuggling (weapons, explosives, drugs, humans, etc.) and illegal fishing
- Insurgent activity such as reconnaissance and surveillance, infiltration of forces, harassing attacks, demonstrations and hoax attacks
- Conventional attacks

Creative scenario developers can develop challenging training by using the real-world examples provided by MEND militants and Somali pirates, and by incorporating information from the [Organization Guide](#) and the [WEG](#).

#### Endnotes

<sup>1</sup> "Watercraft Categories, Watercraft Units, and Equipment," U.S. Army Transportation Regiment and Corps, 26 February 2013.

<sup>2</sup> Ibaba Samuel Ibaba, "Terrorism in Liberation Struggles: Interrogating the Engagement Tactics of the Movement for the Emancipation of the Niger Delta," *Perspectives on Terrorism*, Vol 5, Issues 3-4, September 2011, page 24.

<sup>3</sup> John Robb, "Nigerian Evolution," *Global Guerrillas*, 16 January 2006.

<sup>4</sup> Chris Stokel-Walker, "African Lions: The colonial geopolitics of Africa's gas and oil," Chapter 2, *lulu.com*, 5 February 2011

<sup>5</sup> "Nigeria military frees oil hostages," *Al Jazeera English*, 18 November 2010.

<sup>6</sup> Sebastian Junger, "Blood Oil," *Vanity Fair*, February 2007.

<sup>7</sup> Huhuonline.com, "Nigerian Army prepare for bloody showdown in Niger Delta!" *Modern Ghana*, 10 September 2009.

<sup>8</sup> Michael G. Frodl, "Somali Piracy Tactics Evolve; Threats Could Expand Globally," *National Defense*, April 2010

<sup>9</sup> Ibid.

<sup>10</sup> Jonathan Bellish, "The Economic Cost of Piracy 2012," *Oceans Beyond Piracy*, 15 April 2013.

<sup>11</sup> Frank Gardner, "Seeking Somali Pirates from the Air," *BBC News*, 21 February 2012 .

<sup>12</sup> Michael G. Frodl, "Somali Piracy Tactics Evolve; Threats Could Expand Globally," *National Defense*, April 2010.

<sup>13</sup> Jonathan Saul, "Somali Pirates Change Tactics To Evade Navy Heat," *Reuters*, 27 April 2012.

<sup>14</sup> FM 7-100.4, *Organization Guide*, 3 May 2007, page 3-20 .

<sup>15</sup> *Worldwide Equipment Guide*, Volume 3: Naval and Littoral Systems, August 2012.

<sup>16</sup> Ibid, page 3-2.



# JABHAT AL-NUSRA: ALEPPO SUICIDE ATTACK

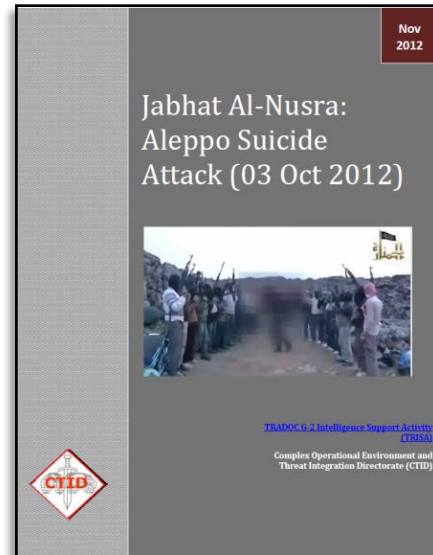
## *TTP in Complex Operational Environments*

by Rick Burns, OE Assessment Team (BMA Ctr)

*Jabhat al-Nusra li-Ahl al-Sham min Mujahedi al-Sham fi Sahat al-Jihad (JN)*, or "The Front for Aid to the People of the Levant by the Mujahideen of the Levant on the Battlefields of the Jihad," is a Syrian-based Salafist Islamist organization that officially announced its founding in January 2012. In the short span of a few months, JN has gained a reputation for bold and fearless fighting against Syrian security forces. Additionally, it has found great success in recruiting foreign fighters from Libya, Tunisia, Egypt, Saudi Arabia, Iraq, and the Balkans. Focusing on high-value military and government facility suicide bombings, JN has avoided angering the Syrian population with indiscriminate civilian collateral deaths.

JN is one of the diverse groups fighting for the overthrow of the Syrian government under the broad umbrella of the Free Syrian Army (FSA). It is active across all Sunni areas of the country, but most attacks have targeted Damascus. The organization has a significant presence in Syria's eastern border region, and to some extent in the rebel strongholds of Idleb, rural Aleppo, and northern Hama Province. This new organization will become increasingly problematic in a post-Assad government. Its growing fighting prowess, Salafist ideology, ability to attract foreign jihadists, and increasing acceptance among rural Syrians guarantees a post-Assad showdown between JN and those advocating for a more secular government.

On the morning of 3 October 2012, JN conducted attacks at three different locations in Aleppo, Syria. This operation included four VBIEDs, one RCIED, mortars, and the use of Syrian military uniforms to gain closer access to targets. The Aleppo operation showed a sophistication and intent reminiscent of al-Qaeda.



Having proven it is capable of sophisticated attacks against multiple and synchronized targets, the major limiting factor for the organization will be the availability of suicide bombers and explosive materials. With a growing army of foreign fighters and alliances with other Islamist groups such as al-Qaeda in Iraq, it should be able to overcome this limitation.

The November 2012 Threat Report, [\*Jabhat Al-Nusra: Aleppo Suicide Attack \(3 Oct 2012\)\*](#) provides information on the JN organization; relationships with other militant organizations; and current tactics, techniques, and procedures (TTP). It also provides details about a particular attack on 03 October 2012 that included multiple military and government targets.

***Do you know the Threat?  
He is watching YOU.  
PROTECT the Force.***



# IRREGULAR OPFOR DEFENSE OF A COMPLEX BATTLE POSITION (CBP)

---

## *Threat Defensive TTP in Urban or Rural Operational Environments*

by Jon H. Moilanen, CTID Operations and Threats Terrorism Team (BMA Ctr)

### Defense of a Complex Battle Position (CBP)

Irregular Opposing Forces (OPFOR) use camouflage, concealment, cover, and deception (C3D) measures as critical to the success of a CBP since the defenders generally want to avoid enemy contact. Additionally, cells in a CBP remain dispersed to negate the effects of precision ordnance strikes. Generally, once the defense is established, non-combat vehicles are positioned away from concentrations of personnel to reduce their signature in that operational environment (OE).

As stated in TC 7-100.2, *Opposing Force Tactics*:

#### Complex Battle Position

A *complex battle position* (CBP) is a **defensive** location designed to employ a combination of complex terrain, C3D, and engineer-like efforts to protect the units, cells, and/or elements within the CBP from detection and attack. Defensive measures deny seizure and occupation of a CBP by the enemy. CBPs typically have the following characteristics that distinguish them from simple battle positions (SBPs):

- ◆ Limited avenues of approach toward a CBP. (CBPs are not typically on or astride an enemy avenue of approach.)
- ◆ Observation of any existing avenues of approach.
- ◆ 360-degree fire coverage and protection from attack.
- ◆ Engineer-like efforts prioritizing to camouflage, cover, concealment, and deception (C3D) measures; and limited visible countermobility efforts that might reveal the CBP location.
- ◆ Large logistics caches.
- ◆ Sanctuary from which to launch local attacks.

Irregular Opposing Forces (OPFOR) defending in CBPs use restrictive terrain and countermobility efforts to deny the enemy the ability to easily approach the position. Construction of a CBP places special attention on the blending into the urban or rural terrain. The irregular OPFOR expects enemy reconnaissance, intelligence, surveillance, and target acquisition (RISTA) capabilities to normally be significant and recognizes that sophisticated RISTA capabilities may be supporting the enemy. An effective counter to such levels of sophisticated technology and systems may be to embed a CBP within a relevant population in an urban or rural environment. Examples include the use manmade underground shelters, tunnels, natural shelters such as caves, and village or city dwellings.

Cultural shielding is a tactical consideration to deny the enemy the ability to detect and attack a CBP. Examples of cultural shielding in order to create tactical standoff are using a religious location, school, community center, or medical facility as a base of fire or firing from within a crowd of noncombatants.

If a CBP is identified and attacked, the insurgent leader will engage as long as he perceives an ability to defeat the enemy. Prior to becoming decisively overmatched, he will withdraw in order to preserve his combat power. An insurgent leader can be directed by a higher insurgent organization to accept decisive engagement in order to support a larger mission of the insurgency.

## Functional Organization of a CBP Defense

The insurgent leader of the defending force organizes his subordinates as functional elements. Typical functional designations may include but do not necessarily require a—

- Disruption element.
- Main defense element.
- Reserve element.
- Support element.
- Deception element.

These functional elements conduct tactical actions very similar to those used in defending a simple battle position (SBP). Although these elements identify their basic functions, defense of a CBP may require subtle differences and may require more than one of each type of element.

### Disruption Element(s)

The disruption element of a CBP is primarily concerned detecting attackers and providing early warning to the defending force. The disruption elements may be directed to only observe and report enemy movements and maneuver but can also be directed to attack enemy forces once they pass the disruption elements. A combat security observation post (CSOP) can be used in this manner.

### Main Defense Element(s)

The main defense element of a CBP is responsible for defeating an attacking force. This element can be directed to delay an enemy while other cells or units withdraw from direct contact with the enemy. The kill zone and fighting position are basic building blocks in the defense of a CBP with a priority of effort to camouflage and concealment. A *kill zone* is a designated area on the battlefield where the opposing force (OPFOR) plans to destroy an enemy using obstacles and massed fires of direct and indirect weapon systems. Fighting positions are designated in one of four ways as follows:

- **Primary**—assigned and prepared as the principal location of employing a weapon and/or weapon system in the coordinated defense of a battle position.
- **Alternate**—identified and prepared to support the sector of responsibility of a primary fighting position and can be located to the front, flank, or rear of the associated primary fighting position.
- **Supplemental**—identified to defend with a sector of fire that is different from the primary position sector of fire and considers contingencies of the battle position defense. Preparations are conducted within the designated priority of effort.
- **Subsequent**—identified to defend a sector of responsibility in depth as assigned to a primary fighting position in the coordinated defense of a battle position. Preparations are conducted within the designated priority of effort.

**Note.** Preparation tasks for OPFOR defensive positions are listed and prioritized for action in TC 7-100.2, *Opposing Force Tactics*, chapter 4, Tables 4-1 to 4-3.

### Reserve Element(s)

The reserve element of a CBP exists to provide the insurgent leader with tactical flexibility. Tasks for a reserve element can include—

- Counterattack: A task to control the tempo of combat and regain the initiative.
- Block: A task that denies access to an area and prevents an advance in a designated direction or avenue.
- Delay: A task to trade space for time by slowing an enemy's momentum.
- Defend: A task to deny an enemy his objectives and/or weaken or culminate an enemy's capabilities.

### Support Element(s)

The support element of a CBP has tasks described in irregular OPFOR terminology that include command and control (C2) [similar to the U.S. Army concept of mission command]; combat support (CS), and combat service support (CSS) for the defending force. Other support functions can include direct and indirect fires; countermobility or mobility capabilities;

and/or information warfare (INFOWAR) activities. Support elements typically are located within the CBP but can be outside and in the vicinity of a CBP.

### Deception Element(s)

To deceive an enemy from discovering the nature of the CBP defenses and to draw fire away from actual CBP elements, the defending force may establish dummy or decoy firing positions and battle positions. In addition to enhancing force protection, the irregular OPFOR may use these deception elements as an economy-of-force measure to portray strength where none exists. (See figure 1 for fundamental tactical locations of fighting positions and security measures.)

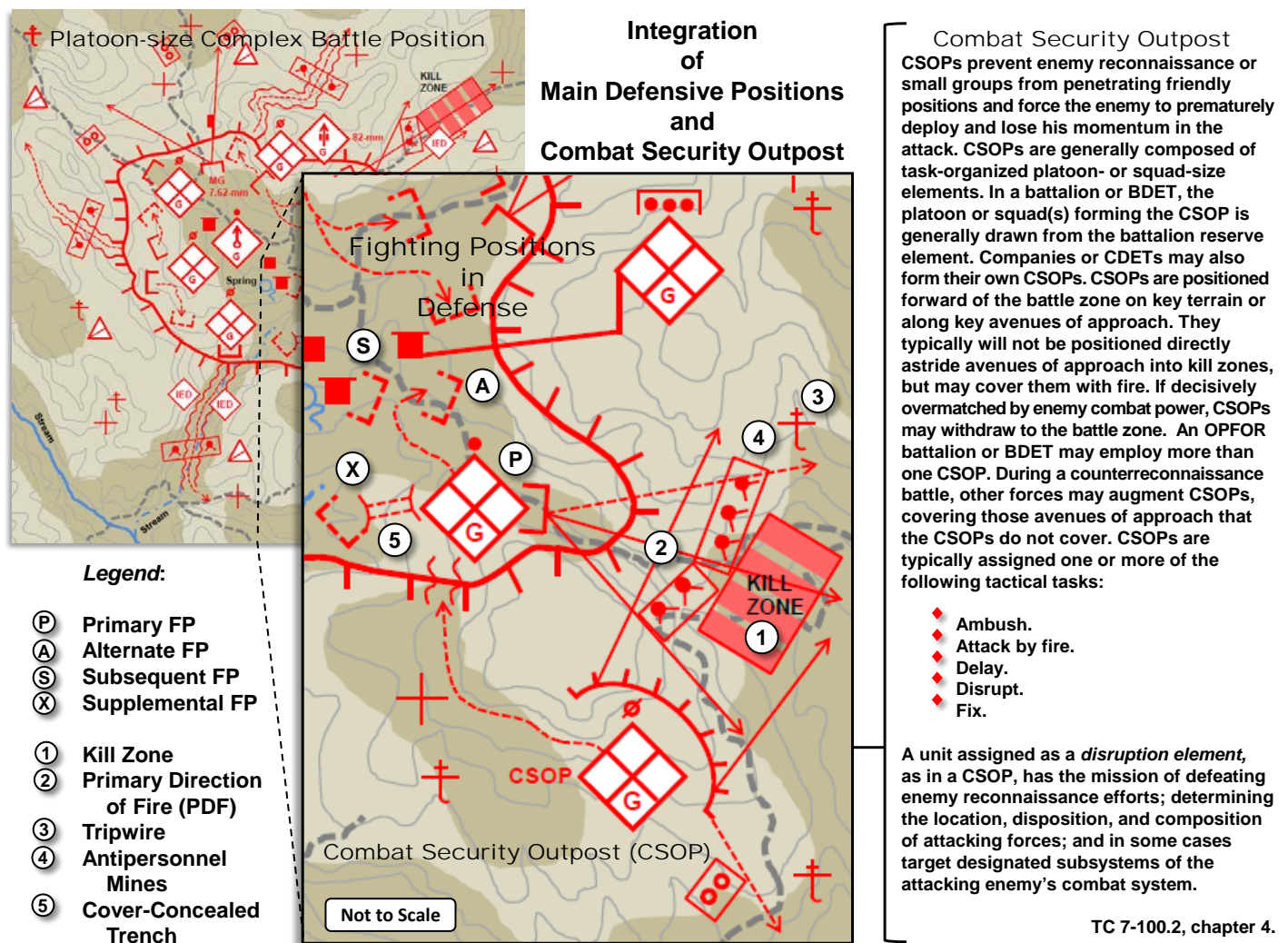


Figure 1. Fighting position considerations in a complex battle position (example)

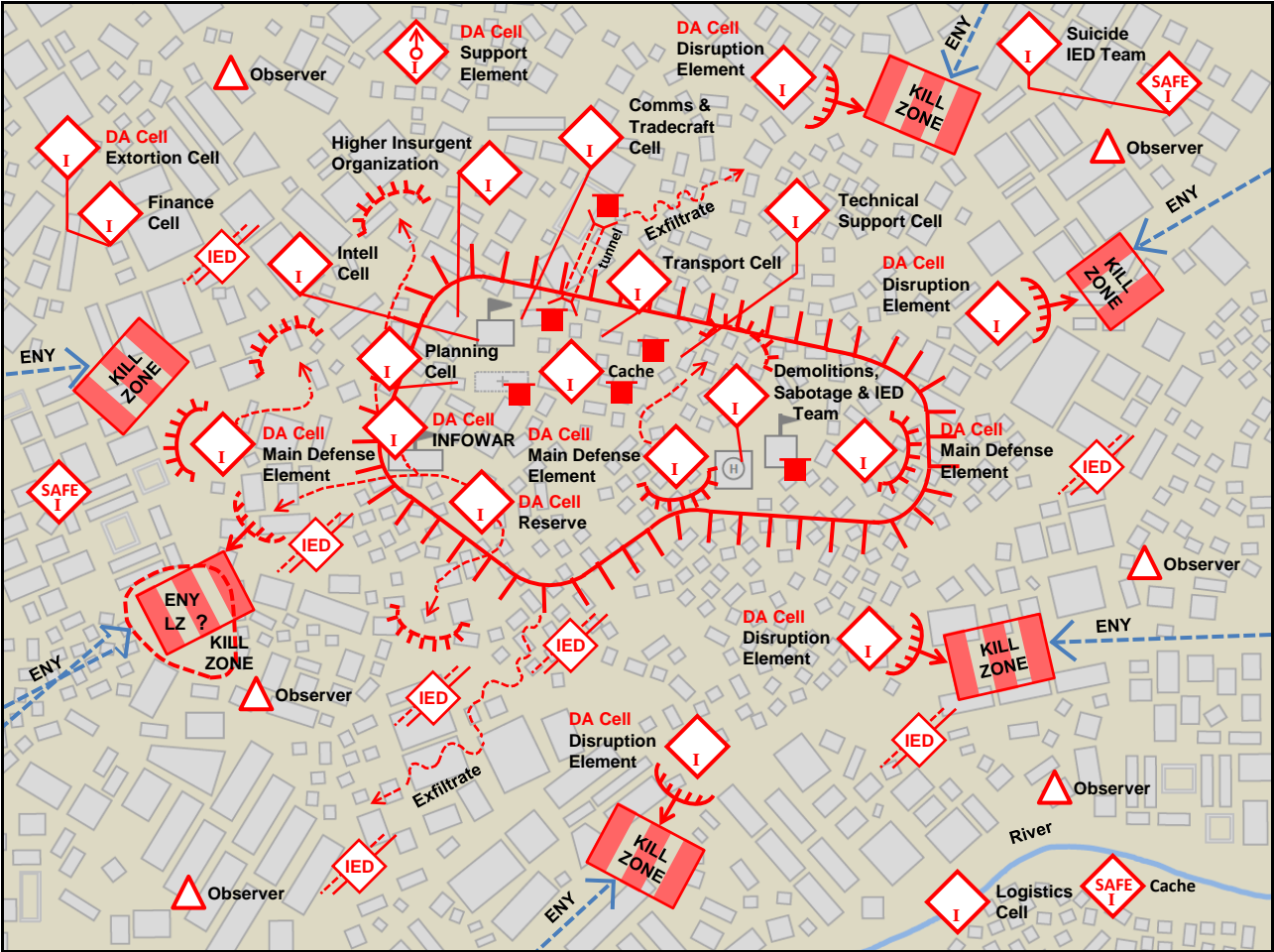
### Executing Defense of a CBP

The insurgent leader will determine whether or not to organize disruption elements in a disruption zone external to the CBP. He may determine that the manning and capabilities of his organization are more effectively used with security elements close to the defensive perimeter of the CBP. Whether near or distant from the CBP main defenses, security actions are disruption, active reconnaissance, and counterreconnaissance. However, contact with the enemy is on order of the insurgent leader.

## Protecting a Complex Battle Position

The normal intention is to prevent a CBP from being identified by enemy forces. However, if a CBP receives indications that the location has been compromised, the irregular force commander or leader activates multiple support capabilities, on order, to delay and/or disrupt attacking forces. For example, **disruption elements** in a **disruption zone** engage enemy forces in tactical depth as they approach a CBP or CBPs. Obstacles are armed and executed to slow or channel the enemy into kill zones, and direct and indirect fires coordinated by a disruption element delay or attrit enemy forces. **Main defense elements** and **support elements** engage the enemy as necessary to defeat an attack. The irregular commander or leader can also order a withdrawal under pressure with the intent to break contact and exfiltrate CBP elements from the area and preserve combat power.

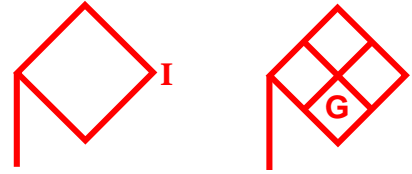
When necessary, main defense elements of the CBP mass direct and indirect fires to defeat an enemy attack. The insurgent leader of the CBP may retain a reserve element and commit it only when necessary to prevent defeat by enemy forces. Support elements in the support zone of a CBP provide support to defenders in the disruption zone and battle zone as required. In the event the leader orders a withdrawal from the CBP, some support elements will exfiltrate quickly while other elements such as indirect fires continue support to the main defense elements until directed to disengage by the leader. (See figure 2 for examples of a higher insurgent organization CBP defense in a complex urban area with its direct action (DA) cells and functional cells.)



**Figure 2. Insurgent complex battle position in an urban environment (example)**

## Command and Control of a CBP Defense

The irregular OPFOR leader [insurgent or guerrilla] will position himself where he can best command and control the defensive fight. Command and control of a CBP is generally more difficult than that of an SBP because the defenders are normally more dispersed. Insurgents operating in and from the CBP improve their security by using couriers and wired communication networks when practical.



## Support of a CBP Defense

Support of a CBP can be provided from within an insurgent organization and local resources in the **relevant population**. Some support may be allocated from higher-level irregular OPFOR organizations or from a state or non-state sponsor. Specialized support such as **special purpose forces** (SPF) can be temporarily associated with insurgents or guerrillas in a CBP in order to provide training, materiel, and/or tactical and technical advice.



## Reconnaissance



Reconnaissance assets observe avenues of approach to provide early warning and allow the insurgent leader time to defend or to exfiltrate personnel and resources from the CBP. Insurgents, guerrillas, and/or their active supporters embed themselves within local populations. Patrolling my clandestine cells, units, and/or elements maintain an active situational awareness of the area of responsibility in which they operate. The irregular OPFOR is less likely to engage in counterreconnaissance activities if these actions would reveal CBP location.

## Armored Fighting Vehicles

Armored vehicles are not the norm in a CBP. When possessed by the irregular OPFOR, armored fighting vehicles and ad hoc fighting vehicles mounting heavy weapons are normally concealed and covered in hide positions. An irregular OPFOR leader may retain armored vehicles as part of his reserve for quick response to contingencies in defense of his CBP.

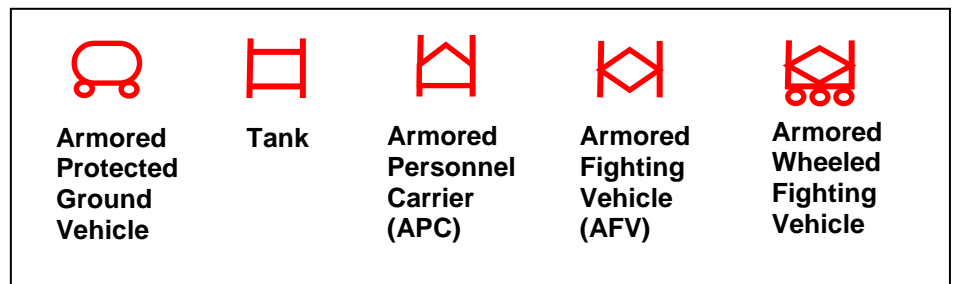


Figure 3. Opposing Force Armored Vehicle Symbols

## Fire Support

CBPs are typically self-supporting in their defense. Fire support assets normally locate within the CBP but may also locate outside of the CBP perimeter to best employ specific fires. Defenders employ these fires to—

- Defeat enemy forces in the battle zone.
- Attrit enemy forces along avenues of approach near a CBP.
- Disrupt enemy use of landing zones in the vicinity of a CBP.
- Delay enemy forces to support withdrawal of the irregular OPFOR from the CBP.



## Air Defense



Passive air defense is the norm for a CBP. Active air defense generally involves systems that do not emit an electromagnetic signature. Insurgents engage aerial targets on order of the insurgent leader. An **all-arms air defense** concept involves using weapons of all personnel of a CBP to protect against fixed- and rotary-wing aircraft threats. When available, shoulder-fired man-portable air defense systems (MANPADS) would likely be located in disruption or security element(s) that

occupy fighting positions near a CBP oriented on probable enemy air avenues of approach.

## Mobility and Countermobility

The irregular OPFOR conceals fighting and survivability positions using C3D techniques with locally available resources. Military-manufactured antipersonnel and/or antitank mines and/or IEDs are emplaced on or near likely enemy avenues of approach. Particular mines and/or IEDs are emplaced and secured with a cell designated to arm and/or detonate the munitions on order of the commander or leader. Insurgents and guerrillas use trained individuals, teams, and/or cells to conduct engineer-like activities for mobility and countermobility.


Although CBPs are not located astride enemy avenues of approach, the irregular OPFOR can channel enemy forces into kill zones. Obstacles are generally more protective in nature than obstacles used near an SBP. Irregular OPFOR may have varied specialized talents for engineer-like countermobility and mobility tasks. When supported overtly or covertly by a state sponsor, SPF or regular forces may be associated an insurgent or guerrilla organization in order to provide engineer training, materiel, and advice.

**Engineer-like Capabilities**

Irregular OPFOR insurgents and guerrillas do not have dedicated engineer cells, teams, or units for mobility and/or countermobility tasks. Insurgents and guerrillas are cross-trained in these skills and are task-organized as needed.

For example, insurgents sustain capabilities in a Direct Action Cell (Multifunction)

Guerrilla units may have elements of a sapper company; however, these guerrillas are *not* engineers in the manner of combat engineers of a regular OPFOR unit. Sappers are guerrilla infantryman focused on assault and breaching drills and related demolitions tasks.



DA Cell Multifunction      SAPPER      SPF

Special purpose forces (SPF) may operate with insurgents and/or guerrillas in order to train and advise on mobility and countermobility operations.

Voluntary or coerced support can be obtained from a relevant population.

## Logistics



Logistics operations of a CBP are generally self-sustaining and blend into the local commerce and daily operations of a relevant population in the vicinity of the CBP. Provisioning a CBP with regular resupply is facilitated by active supporters of the insurgent or guerrilla organization. The insurgent leader typically does not coerce local citizens to provide logistics support but can use extortion when critical commodities are required to sustain the CBP defense.

Supply caches and safe houses are distributed throughout the urban or rural area near the CBP. Other supply caches and safe houses are located within the CBP perimeter. [The OPFOR uses the term *combat service support* (CSS).]

## INFOWAR

Elements from the CBP may attempt to integrate within any local communities for the purpose of gathering information, collecting intelligence, and disseminating information warfare (INFOWAR) themes to the local relevant population. Active supporters of the irregular OPFOR assist the insurgent leader in keeping a low profile. INFOWAR activities may focus on downplaying the existence or significance of the CBP. Generally, the CBP will not conduct easily detectable INFOWAR activities that would call the enemy's attention to it.

If the presence of a CBP cannot be hidden, INFOWAR may attempt to convince enemy forces that the defenders are friendly to them. Activities may attempt to convince leaders of the governing authority that the insurgents are willing to affiliate or associate with them in levels of reconciliation.



Other INFOWAR techniques can portray the enemy force and governing authority as a corrupt regime to further isolate them from the relevant population. The insurgents can claim and demonstrate themselves to be the relevant population's protector. In some cases, senior irregular OPFOR leaders may conduct INFOWAR from a CBP to convince followers in other locations that they are still alive and leading their organizations in the struggle against the enemy.

INFOWAR can include support to provide basic social and civic services to the relevant population that is not being provided by the governing authority.

Other INFOWAR techniques can result in the gradual acceptance by the relevant population to the point that members of the insurgent organization become informal or legitimate representatives in civil governance. This recognition can lead to elected positions of authority through a state's formal voting processes and/or establishing self-proclaimed semi-autonomous enclaves within a state with which the irregular OPFOR is in conflict. In either case, the irregular OPFOR ensures a significant INFOWAR campaign to weaken enemy support and strengthen its own support from a relevant population.

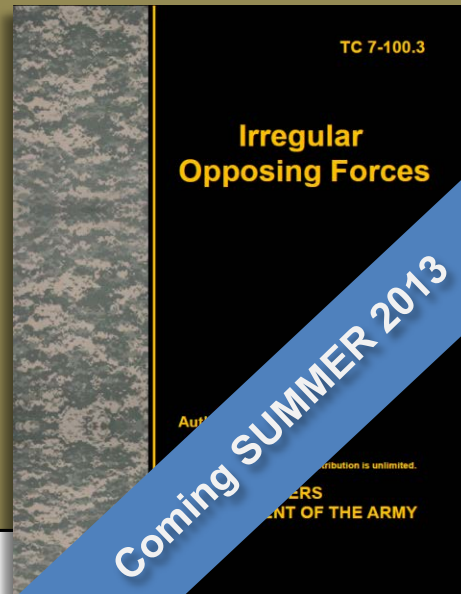
### Complex Battle Positions and TTP

These types of tactical descriptions and other tactics, techniques, and procedures (TTP) for irregular opposing forces will be in—

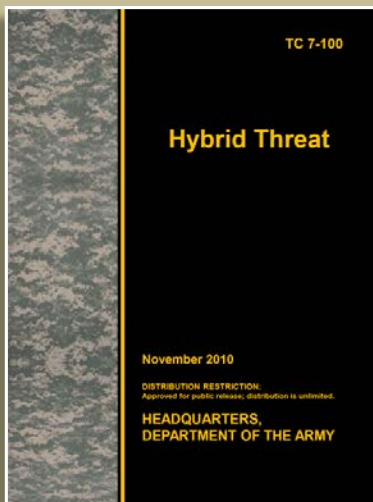
### U.S. Army Training Circular 7-100.3 *Irregular Opposing Forces*,

to be published in summer 2013.

Look for more information in the June 2013  
**TRISA Red Diamond**.



## *Do you understand adaptive operations-tactics of an OPFOR Hybrid Threat (HT)?*



### **Adaptive Tactics-Training Impacts-Opposing Force**

Success goes to those who master skills necessary to act, react, and adapt with speed and creativity. The OPFOR finds or creates critical vulnerabilities in its enemies. The OPFOR learns quickly.

OPFOR doctrine is **descriptive**—not prescriptive. **Functional Tactics** apply to regular and irregular forces, as well as to other force multipliers of a Hybrid Threat (HT) for training. Fundamental principles of OPFOR operations-tactics include:

- Reconnaissance-surveillance is continuous.
- Attack the will and resolve of a relevant population.
- Exploit information warfare (INFOWAR).
- Neutralize or avoid technological overmatch of an enemy.
- Expand the conflict to an enemy Homeland.
- Protect multiple sanctuaries, safe havens, and reserves.
- Employ any means to achieve OPFOR objectives and intent.

# THREAT PRODUCTS FOR COMPLEX ENVIRONMENTS

by CTID Operations



## Sampler of Products:

TC 7-100 *Hybrid Threat*

TC 7-101 *Exercise Design*

TC 7-100.2  
*Opposing Force Tactics*

DATE v. 2.0  
*Decisive Action  
Training Environment*

*Worldwide Equipment  
Guide (WEG)*

**COMING in 2013:**

RAFTE-Africa  
*Regionally Aligned Forces  
Training Environment*

TC 7-100.3  
*Irregular Opposing Forces*

For documents produced by TRISA's Complex Operational Environment and Threat Integration Directorate (CTID) of U.S. Army TRADOC G2, with Army Knowledge Online (AKO) access, see <https://www.us.army.mil/suite/files/11318389>

**Q:** Where do I go to e-retrieve TC 7-101, *Exercise Design*?

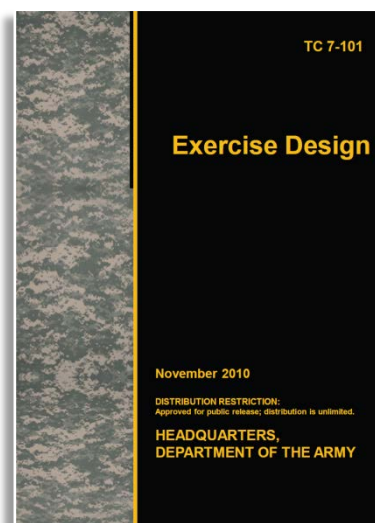
**A:** With AKO access, see  
<https://www.us.army.mil/suite/doc/26060848>

**Q:** Do you have a question on a Threat or Opposing Force (OPFOR) issue that CTID can assist you with in identifying a solution?

**A:** Send us a request for information (RFI).

**Q:** Do you have a question on using the Decisive Action Training Environment (v. 2.0) in your training, professional education, or leader development venues?

**A:** Send us an email with your issue.



# THREATS TO KNOW—*CTID DAILY UPDATE* REVIEW

---

by Marc Williams, Training and Leader Development Team/JRTC LNO (ISC-CG CTR)

CTID analysts produce a daily [CTID Daily Update](#) to help our readers focus on key current events and developments across the Army training community. Available on AKO, each *Daily Update* is organized across the Combatant Commands (COCOMs). This list highlights key updates during the month.



## Selected Topics:

**01 May. Tunisia:** [Tunisia forces clash with 50 armed militants in Mount Chaambi region](#)

**03 May. Cyber security:** [Military database of U.S. dams compromised by attackers](#)

**06 May. Colombia:** [Police seize major landmine stash in central Colombia](#)

**08 May. Indonesia:** [Indonesian police in shootout with Burma embassy bomb plot suspects](#)

**10 May. Somalia:** [Al Shabaab fighters loyal to Godane reportedly kill Al Amikri](#)

**13 May. Syria:** [Syria threatens to enter occupied Golan Heights after Israeli airstrike](#)

**Turkey:** [Twin car bomb attacks in Reyhanli, Hatay](#)

**15 May. U.S.:** [Seven chemical engineers from Pakistan, Saudi Arabia, and Singapore caught trespassing at Quabbin Reservoir, Massachusetts](#)

**Argentina:** [Drug trade "anarchy" in Tri-Border Area sparks controversy](#)

**17 May. Afghanistan:** [Hizb-i-Islami Gulbuddin suicide bomber kills 6 Americans, 9 Afghans](#)

**20 May. Syria:** [23 Hezbollah members killed in Syria](#)

**Russia:** [FSB prevents terror attack by militants trained in Pakistan, Afghanistan](#)

**22 May. U.S.:** [Man being questioned for Boston bombing connection shot and killed by FBI](#)

**Nigeria:** [Soldiers in heavy fighting with Boko Haram militants from Libya](#)

**24 May. Lebanon:** [Syria's war in Tripoli](#)

**Niger:** [Islamist suicide bombers kill 20 in Niger, seize hostages](#)

**29 May. Myanmar:** [Sectarian violence erupts in Lashio, Shan State](#)

**Pakistan:** [U.S. drone strike kills #2 of the Pakistani Taliban, six others in North Waziristan](#)

## CTID Points of Contact

<b>Director, CTID</b> Mr Jon Cleaves jon.s.cleaves.civ@mail.mil	DSN: 552 FAX: 2397 913.684.7975
<b>Deputy Director, CTID</b> Ms Penny Mellies penny.l.mellies.civ@mail.mil	DAC 684.7920
<b>Operations Officer, CTID</b> Dr Jon Moilanen jon.h.moilanen.ctr@mail.mil	BMA 684.7928
<b>Threat Integration Team Leader</b> Mr Jerry England jerry.j.england.civ@mail.mil	DAC 684.7960
<b>Threat Integration Team</b> Ms Steffany Trofino steffany.a.trofino.civ@mail.mil	DAC 684.7960
<b>Threat Integration Team</b> Mrs Jennifer Dunn jennifer.v.dunn.civ@mail.mil	DAC 684.7962
<b>Threat Integration Team</b> Mr Kris Lechowicz kristin.d.lechowicz.civ@mail.mil	DAC 684.7922
<b>Worldwide Equipment Guide (WEG)</b> Mr John Cantin john.m.cantin.ctr@mail.mil	BMA 684.7952
<b>Training &amp; Leader Development Team Leader</b> Mr Walt Williams walter.l.williams112.civ@mail.mil	DAC 684.7923
<b>Training &amp; Leader Development Team/RAF LNO</b> LTC Tom Georges thomas.c.georges.mil@mail.mil	USAR 684.7939
<b>Training &amp; Leader Development Team</b> LTC Terry Howard terry.d.howard.mil@mail.mil	USAR 684.7939
<b>Training &amp; Leader Development Team/JRTC LNO</b> Mr Marc Williams james.m.williams257.ctr@mail.mil	ISC-CG 684.7943
<b>Training &amp; Leader Dev Team/NTC &amp; JMRC LNO</b> Mr Mike Spight michael.g.spight.ctr@mail.mil	ISC-CG 684.7974
<b>Training &amp; Leader Development Team/MCTP LNO</b> Mr Pat Madden patrick.m.madden16.ctr@mail.mil	BMA 684.7997
<b>OE Assessment Team Leader</b> Mrs Angela Wilkins angela.m.wilkins7.ctr@mail.mil	BMA 684.7929
<b>OE Assessment Team</b> Mrs Laura Deatrick laura.m.deatrick.ctr@mail.mil	ISC-CG 684.7925
<b>OE Assessment Team</b> Mr H. David Pendleton henry.d.pendleton.ctr@mail.mil	ISC-CG 684.7946
<b>OE Assessment Team</b> Mr Rick Burns richard.b.burns4.ctr@mail.mil	BMA 684.7897
<b>OE Assessment Team</b> Mr Jim Bird james.r.bird.ctr@mail.mil	Overwatch 684.7919

## CTID Mission

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

## What We Do for YOU

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

## YOUR Easy e-Access Resource

With AKO access--CTID products at:  
[www.us.army.mil/suite/files/11318389](http://www.us.army.mil/suite/files/11318389)

**Note.** Copy-paste CTID POC email address for one-on-one CTID contact and coordination.

