U.S. TRADOC G2 Intelligence Support Activity

Red Diamond

Complex Operational Environment and Threat Integration Directorate

Fort Leavenworth, KS Volume 4, Issue 11 NOV2013

INSIDE THIS ISSUE

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

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

Training Circular 7-100.3, *Irregular Opposing Forces*, addresses irregular opposing forces (OPFOR) for Army training and represents a composite of actual threats and enemies that comprise irregular forces. Three primary categories of irregular forces portrayed by the OPFOR are insurgents, guerrillas, and criminals. Other irregular OPFOR actors in a complex operational environment (OE) can include affiliates and adherents, and/or other willing, coerced, passive, or unknowing supporters. Some irregular OPFOR can be independent, non-aligned individuals. Any of those forces can be associated with each other, mercenaries, corrupt governing authority officials, compromised commercial and public entities, active or covert supporters, and willing or coerced members of a populace.

These actors may operate with regular military forces as a hybrid threat (HT) for training. All of these actors may employ acts of terrorism. Training Circular (TC) 7-100.3, *Irregular Opposing Forces*, as part of the US Army TC 7-100 series, addresses irregular opposing forces (OPFOR). In Army training, professional education, and leader development experiences, irregular OPFOR represent a composite of threats that will be present in persistent conflict and engagement. Irregular OPFOR are armed individuals or groups who are not members of the regular armed forces, police, or other internal security forces. However, the distinction of being armed as an individual or group can include a wide range of people who can be categorized correctly as noncombatants or be mistaken as irregular forces.

CTID will e-announce when the approved TC 7-100.3, *Irregular Opposing Forces*, is available on Army Training Network (ATN). Publication estimate: DEC 2013.

RED DIAMOND TOPICS OF INTEREST

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

This issue of TRISA ***Red Diamond*** spotlights Army Training Circular 7-100.3, *Irregular Opposing Forces* (OPFOR) that is in final review at the Army Publishing Directorate (APD).

An understanding of tactics and techniques in a cyber attack life cycle offers useful insights to addressing this emerging element of hybrid threat (HT) capabilities for training, as well as application in operational readiness.

Recent proliferation in and near Libya creates threats such as a man-portable air defense system (MANPADS) that can be replicated in training with threat actors obtaining capabilities from state and nonstate actors.

The antitank grenade launcher (ATGL) RPG-29 used in an urban ambush can be modified as a training incident for home station training or a combat training center.

A hybrid threat that included Syrian militia units conducted two massacres in Syria of civilian minority enclaves. Motivations and tactics of such regional actors demonstrate the complexity of persistent conflict.

Boat operations with drug trafficking organizations (DTOs) in Central America demonstrate significant threats in technical capabilities. This expanding DTO threat continues to adapt and challenge counteraction by regional states and agencies.

Email your topic recommendations to:

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

Director's Corner:
Thoughts for Training Readiness

by Jon Cleaves, Director, Complex Operational Environment and Threat Integration Directorate (TRISA-CTID)

The *Decisive Action Training Environment* (DATE) is a catalog of capability that must be many things to many people. Often, even the most routine user of the DATE has not explored all of the information contained within the base document or its many supporting publications. This can have the effect of leaving a person with certain impressions of the DATE that are based on only contacting it in certain areas in certain ways.

The key thing to remember is that DATE is a collection of likely conditions, not a statement on how things will be. The second most important thing to remember is that what is contained in DATE is driven by what tasks units must be able to perform and what capabilities those units bring to the table.

For example, DATE contains some pretty enormous regular force armies, with lots of significant military capabilities. Is that because we think that is what our next fight will be? No, that is because one of the many training audiences for DATE is ASCCs and Corps. Decisive Action is the simultaneous combination of offensive, defensive, and stability operations. The DATE therefore must contain capabilities that realistically challenge an ASCC/Corps conducting offense and defense. And as the world will be characterized by hybrid threats, exercise designers must have available to them capable threat regular and irregular forces. It's up to the commander how much of a mix is right for him to achieve his training objectives. Our job is to make sure all the tools necessary are already in the tool bag.

As an associated thought, correct portrayal of hybrid threat is really not so much about providing the right amount of regular forces as it is about providing the right amount of regular force CAPABILITY. Could a corps or division warfighter be entirely done with paramilitary groups providing the right regular force capability? Absolutely.

The bottom line of all this? Let us help you. DATE is a big world with a lot of choices to be made. You know what you want to do to train your unit and what mission essential tasks are most important to you. Where we can help is to make you aware of all the options for threat conditions and how to implement them. While you *can* use a previously completed exercise as an 80+% model for how yours is designed, there is no requirement to. If you feel current trends in threat portrayal do not fit your vision of how you want to train, give us a call. All the different ways to reach us are located in the back of every issue of *Red Diamond*.

Jon

jon.s.cleaves.civ@mail.mil

Army Readiness and the Future

As the Army adapts for the future, it will retain its ability to dominate on land across the range of military operations to prevent and deter aggression and shape the security environment. This will include the use of combined arms, campaign-quality forces, power projection capabilities and regionally aligned, mission-tailored forces. The United States does not seek war, but others must never doubt our ability to wage it and win decisively when it occurs.

***Army Strategic Planning Guidance 2013*, p.1**

THE CYBER ATTACK LIFE CYCLE: ESTABLISHING COMMAND AND CONTROL

Complex Threats and Cyber Attack

by Jerry England, Threat Assessment Team (DAC)

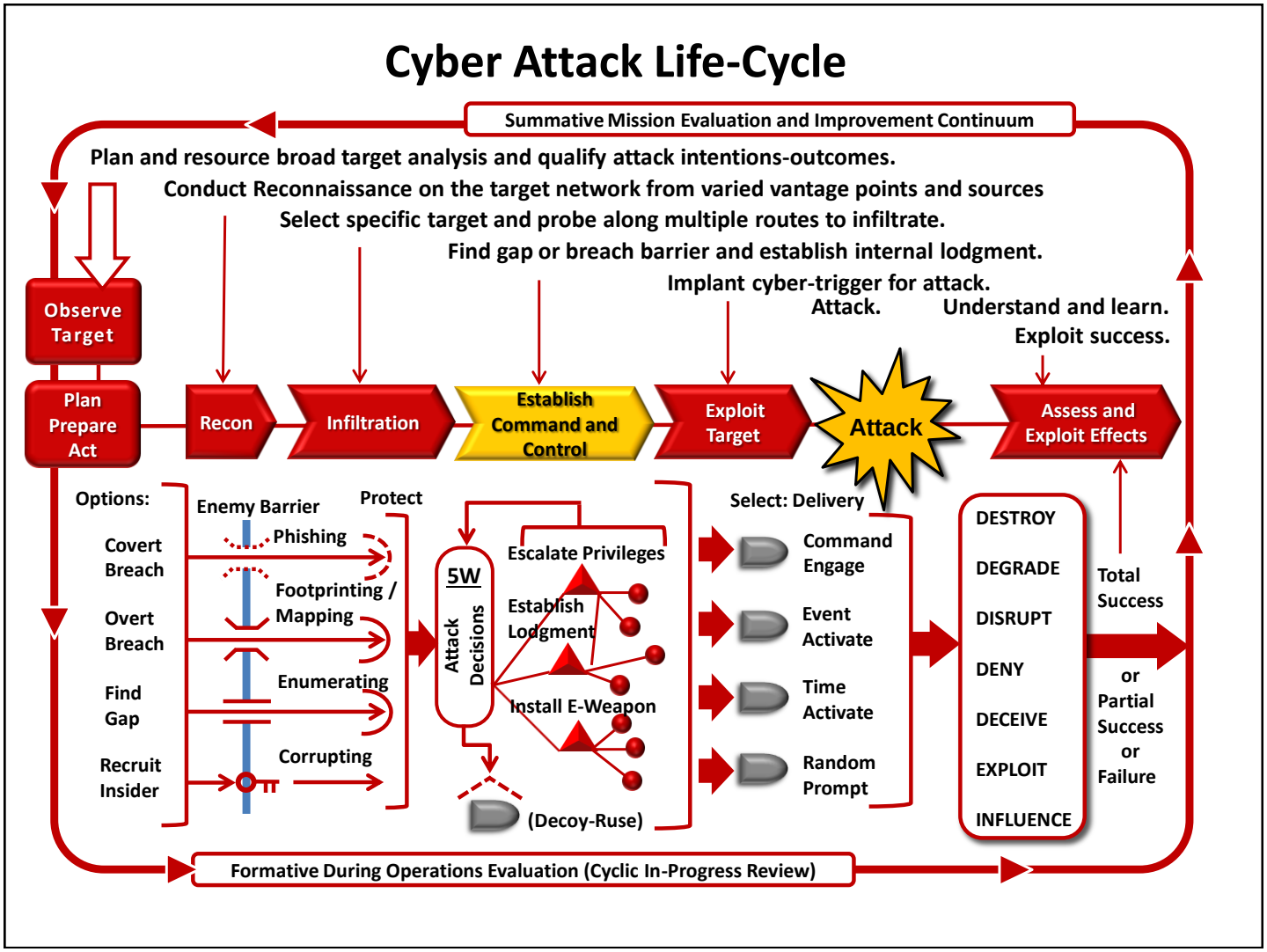


Figure 1. Cyber Attack Life Cycle (Source: TRISA-CTID, 2013)

Military operations rely on information and communications technology (ICT). The exposure of military systems and information resources to cyber attack is a reality as more warfighting functions become integrated with software and computer applications. As countries develop offensive cyber operations, the threat from computer warfare and information attack against friendly capabilities increases. For this reason, understanding the tactics and techniques of cyber attacks is a useful approach to addressing this emerging element of the hybrid threat. Devising a model for threat cyber operations based on current tactics and terminology will assist exercise designers to include threat cyber operations and meet future training objectives. The discussion below is the third part in a series that illustrates a model for describing the threat cyber attack lifecycle that focuses on the establishment of command and control (C2) architectures for threat offensive cyber operations.

Cyber Attack Life-Cycle

The threat conducts cyber attacks through a six step process designated the cyber attack life cycle (CALC). The six steps, however, do not occur sequentially and the threat can skip or repeat steps as it is appropriate. The steps in the cyber attack life cycle are—

- Reconnaissance.
- Infiltration.
- Establish C2 (formerly Establish Lodgment).
- Exploit Target.
- Deliver Attack.
- Assess and Exploit Effects.

Establish Command and Control

Establishing C2 is essential to cyber operations especially if the attackers intend to continue to exploit or attack the target system. The standard procedure for this step in the cyber attack lifecycle is to launch a portable executable (PE) that initiates a back door connection to the C2 infrastructure and runs the commands needed to allow live attackers to access the infected machine and escalate privileges.[1] Whether it is an open port, a poorly configured application or a systemic error in the application of security procedures, these vulnerabilities–once validated–provide repeated access to the targeted system and can be used to route data to and from the target system for the purpose of espionage, criminal activities, or to mount a Distributed Denial of Service (DDoS) attack.

In order to expand the range of the attack, the threat establishes backdoors-trapdoors via additional compromised machines. The attackers will then begin traversing the network infecting additional computers. The primary goal is to obtain domain administrator credentials and/or gain access to a system storing sensitive data. With acquisition of domain administrator credentials, the attacker can find servers hosting the desired data and gain access to the sensitive systems. Additionally, the attacker may download and install tools to penetrate even deeper into the network.[2]

The threat will typically exploit the vulnerability and establish a remote access tool (RAT) via a Trojan containing a number of PEs that facilitates drilling deeper into the network and for C2 purposes. To ensure sole access to the network and reduce the chance for discovery by the host system, the PE may include encryption, stealth programming, and patches for the initial network vulnerability.[3] The RAT software allows the threat to access the system by generating access requests from inside the compromised system in order to prevent tripping firewalls and other security systems. The other PE in the Trojan may include launchers that steal or manipulate data based on system configurations. In the case of targeted data attacks known as advanced persistent threat (APT), the C2 structure is designed to exfiltrate large quantities of data.[4]

Once the targeted system is compromised, the supporting C2 structure may include one or more servers and employ a number of system administrators. If the intent of the attack is a DDoS, the C2 server will provide access to the compromised "botnet" and allow system administrators known as "bot herders" to execute the cyber attack. The C2 infrastructure will include a number of capabilities depending on the sophistication of the builder; such capabilities may include encryption or a data compression module used to surreptitiously exfiltrate data as in the case of APTs. The threat's presence within the target network and its link to the C2 server, provide it with the cyber attack infrastructure necessary to repeatedly access the targeted information resources and/or continue offensive cyber attacks. One of the most developed underground ecosystems for cyber attacks is the bank Trojan known as Zeus. In 2011 there were over 90,000 variations used for a variety of target sets. The developers also provided updates and patches to customers wanting to upgrade the Trojan's capabilities.[5] This full-service malware is an example of next generation cyber threats that is both specialized and accessible to an expanding user base.

Establishing a reliable connection with a C2 server usually involves a RAT and will allow the threat to launch attacks and steal or manipulate information remotely. Many cyber attackers will use modified versions of tried and true cyber attack software suites such as Zeus, Dark Comet, or Gh0st RAT which have their source code on the Internet.[6] These malicious "builders" are developed by so-called electronic arms dealers that supply cyber weapons for customers with the intent and capability to attack sensitive networks.[7] RATs typically have these capabilities—

- Capture Keystrokes.
- Remotely Monitor Webcam and/or Microphone.
- File System Search.
- Use Local Command Prompt.
- Execute Arbitrary Programs.
- File Download and Upload.

The similarities in naming conventions, compilation dates, and C2 infrastructure indicate the possibility of shared development and logistics and specialization in the development of cyber weapons.[8]

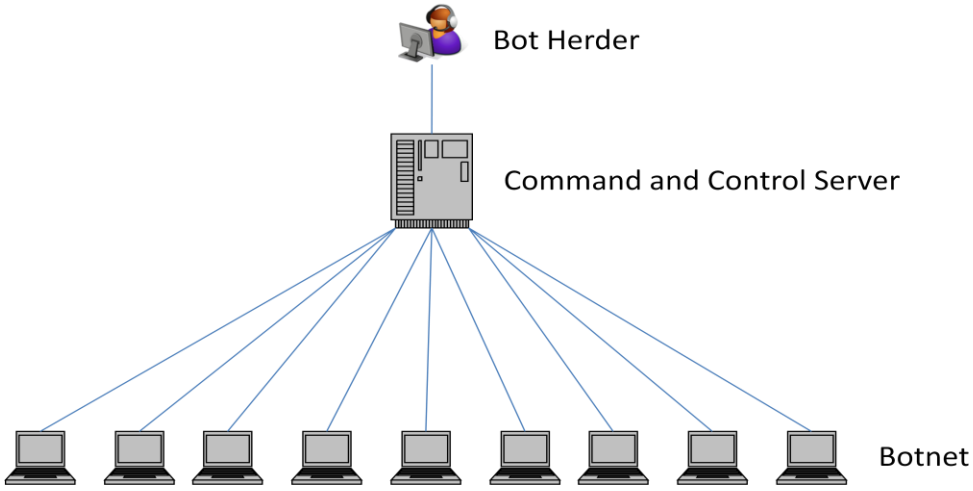


Figure 2. Botnet with a centralized C2 architecture Source: TRISA-CTID, 2013

Command and Control Architectures

Cyber attack techniques are constantly evolving and improving. Networks that provide support for malware are known throughout the hacker community. State-based actors have become familiar with these networks as they recognize the potential for cyber warfare and computer based attacks. C2 networks are evolving with the latest technology in enterprise resources. Cloud-based C2 networks are starting to replace simple structure with a single point of failure. As such it will be even more important to be able to identify the digital signature of malware as the likelihood of successfully finding the geographic location of the source of an attack will be resource intensive.

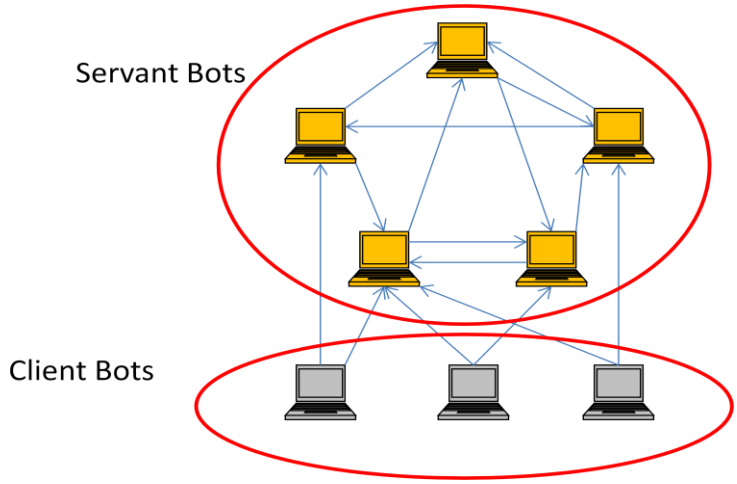


Figure 3. Botnet with a centralized C2 architecture Source: TRISA-CTID, 2013

Implications for Training

- Command and control resources can be located anywhere geographically, making attribution of attacks difficult for friendly forces, and enabling false flag attacks by the threat.
- Hybrid botnets operate in a peer-to-peer decentralized architecture, thus making it even more difficult to locate the main C2 node.
- Cyber operations will need to include traffic analysis of compromised systems to C2 servers as well as signature-based identification of attacking malware in order to classify and attribute source of the attack.
- Enumerating the entire network is required to stop a peer-to-peer botnet instead of just finding the C2 server.

Notes

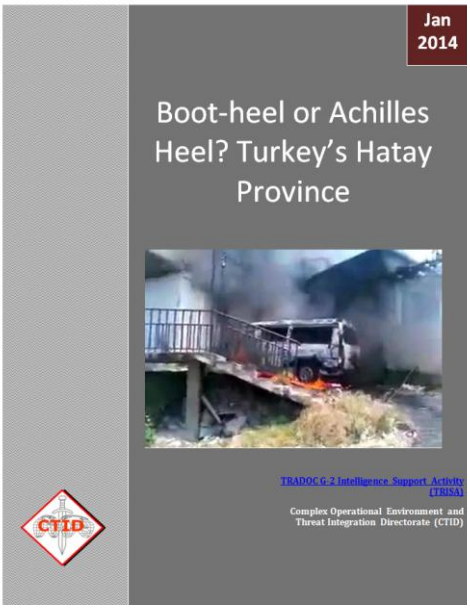
[1] Dmitri Alperovitch, Revealed: Operation Shady RAT, McAfee, 2011.
[2] Eric Chien and Gavin O'Gorman, The Nitro Attacks: Stealing Secrets from the Chemical Industry, Symantec Security Response, 2011.
[3] Kim Zetter, Google Hack Attack Was Ultra Sophisticated, New Details Show, Wired, January 2010.
[4] Symantec, 2013 Internet Security Threat Report Appendix, p 52, April 2013.
[5] Michael A Davis and Robert Lemos, Next-Generation Threats: The Inside Story, Dark Reading, p 3, Jan 2011.
[6] Alex Cox et al., The VOHO Campaign: An In Depth Analysis, RSA First Watch Intelligence Report, 2012.
[7] Fire Eye, Inc. Supply Chain Analysis: From Quartermaster to Sunshop, pp 9-13 , November 2013
[8] TRADOC G-2 Intelligence Support Activity, Complex Operational and Threat Integration Directorate, Red Diamond Issue 10 Volume 4, p 24.

BOOT-HEEL OR ACHILLES HEEL? TURKEY'S HATAY PROVINCE

by Jim Bird, Operational Environment Assessment Team (Overwtach Ctr)

Turkey, like the state of Missouri in North America, has a geographical "boot-heel." In contrast to its American counterpart, however, Turkey's southernmost province came into the national fold only after intense diplomatic wrangling that played out just before the outbreak of World War II. In the aftermath of a referendum boycotted by the local Alawite minority and plagued by allegations of voting irregularities, Hatay Province, formerly part of Syria, swung decisively into Turkey's political sphere of influence. Since that time, people residing in the province have been vexed with issues of national identity. The "Turkification" of Hatay Province is still very much a work-in-progress that remains problematic for the Turkish state.[1]

Figure 1. Map of Turkey with Hatay Province (highlighted)



An OEA Team Threat Report scheduled for publication early next year will examine the brief and troubled history of Hatay Province since its annexation by Turkey, with particular focus on events that have occurred since the Arab Spring of 2011. The Syrian civil war has opened old wounds and exacerbated the chronic problem of divided national loyalties. The Threat Report will examine the relationship between two events that occurred on either side of the Turkish-Syrian border in May 2013. The first was a twin vehicle-borne IED attack that destroyed a large portion of downtown Reyhanli, Turkey the day before Mother's Day, and caused over 50 deaths and dozens of injuries.[2]

The Reyhanli bombings were discussed in some detail in an article published in the September 2013 issue of the *Red Diamon*d, titled "War Comes to Reyhanli: Terrorist Attack of 11 May 2013." The other incident, equally important but under-reported in an American press still enthralled with the previous month's Boston Marathon bombing, was a massacre of Sunni villagers in Banias (spellings vary) Province, Tartus Governate, Syria by Alawite militias loyal to President Bashar Al-Assad.[3]

To examine the cause and effect between what Turkish authorities view as the overarching relationship between the Reyhanli IED attack and twin massacres in Banias only days earlier may hold insights useful to forces eligible for future deployments to the Mediterranean-North Africa (MENA) region.

Figure 2. Reyhanli, Turkey IED damage (See *right*)

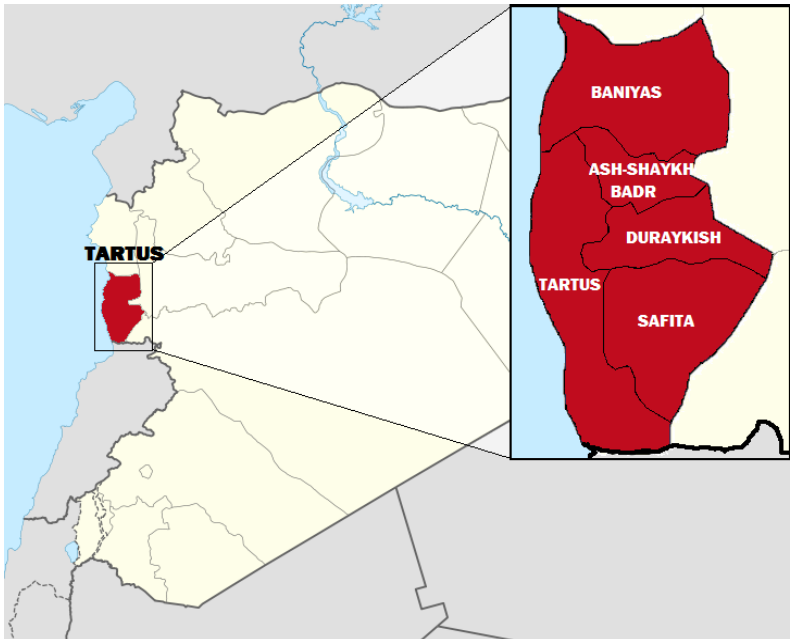


Figure 3. Map shows provinces within Tartus Governate, Syria

Two Atrocities, One Perpetrator

A significant aspect of the massacres in Banias and Reyhanli is that the same person, Mihrac Ural, may have perpetrated both. Ural, a native of Hatay Province, Turkey, embodies a combination of entrenched Cold War era left-wing extremism and a widespread sympathy among Turkey's minority Alawites for al-Assad's Syrian regime. Ural is believed to reside in Latakia, a Syrian governate that lies between Hatay Province, Turkey and Banias, a province in Syria's Tartus Governate pro-Assad militiaunits perpetrated two back-to-back massacres on 2 and 3 May 2013.[4]

A few days after the Banias episode, but before the car bombings in Reyhanli, a YouTube video surfaced on the Internet showing Ural, seated beside an Alawite cleric, advocating violence against Sunni enclaves in Syria. Referring to the Free Syrian Army and its supporters, Ural said, "Baniyas [Banias] is the only passage to the sea for these traitors . . . . We

must quickly besiege it, and I mean it, and start the cleansing."[5] The upcoming CTID Threat Report will provide details of what happened in Banias, based on a UN report of investigation released on 11 September 2013.[6]

Mihrac Ural's prior record of subversive activities throughout the Syrian-Turkish borderland convinced several government officials that he played a key role in planning and carrying out the atrocities in Banias as well as Reyhanli. Speaking less than a week after the Banias attacks, Turkish Foreign Minister Ahmet Davutoglu accused the Syrians of implementing a new strategy of "ethnic cleansing" in order to open "a space or corridor for a certain sect," meaning Alawites. A short time later, following the Reyhanli car bombings of 11 May, Davutoglu appeared live on Turkish television, saying that "those who committed the Banias massacre are responsible for these [Reyhanli] attacks."[8] It was probably no accident that in the days immediately following the Reyhanli bombings, Turkish authorities rounded up over a dozen leftists believed to have links to the Syrian intelligence community. Two groups in particular came under close scrutiny: the Revolutionary People's Liberation Party/Front (DHKP/C), and an offshoot organization called Acilciler, led by Mihrac Ural.

Figure 4. YouTube image of Mihrac Ural

Ural was once a member of the DHKP/C, a radical communist organization whose origins date to the early 1970s. His former colleagues allege that Ural had his own set of priorities that skewed the way he viewed the group's strategies and goals. While the DHKP/C sought to topple the Turkish government and replace it with the kind of "workers' paradise" once prevalent in Soviet bloc countries, the motivation behind Ural's priorities was a desire to see Hatay Province returned to Syria. Over time a DHKP/C schism developed when Ural organized Acilciler, or the "Urgent Ones," a name derived from a separatist manifesto titled "Urgent Problems of Turkey's Revolution."[9] Ural's former colleagues also allege that from the very beginning of his association with the DHKP/C, he exploited the organization according to plans formulated by the Syrian intelligence community. Some authorities inside Turkey have always accepted the notion that once the Cold War ended, the Mukhabarat (Syrian intelligence) retained terrorist sleeper cells inside Turkey that could be activated in future contingencies if Syria ever found itself in need of insurgent support. Ultimately, according to this view, the Syrian civil war acted as a catalyst that again allowed Ural and Acilciler to make a comeback as major threat actors in Turkey.[10]

Mihrac Ural as a Resurgent Threat Actor

After Ural fled to Syria in 1980, the al-Assad regime granted him Syrian citizenship. He then married into the al-Assad family, and eventually settled in Latakia governate. In addition to leading Acilciler, Ural also allegedly commands a number of Shabiha militia units, collectively called the Syrian Resistance, that are actively engaged in suppressing FSA rebels prosecuting the civil war against al-Assad. Ural's present purpose in life, according to one Turkish journalist, is to "stir up sectarian conflict in Hatay and other provinces with the hope that the Turkish government will abandon its anti-Assad Syrian policy."[11]

The National Counterterrorism Center indicates that between 2008 and 2010, the Kurdistan Workers Party (PKK) was behind 60% of the terrorist attacks carried out in Turkey, while only 5% were attributed to groups affiliated with the DHKP/C or militant Islamist factions. Since March 2013, however, a tenuous ceasefire arranged between Kurdish separatists and the Turkish government has held, significantly lowering the level of PKK violence. Meanwhile, the Syrian regime's motives for punishing the Turkish government for pursuing its anti-al-Assad policies remain strong as ever. Regional destabilization through the use of proxies is an effective tool available to Syrian intelligence. Now that PKK violence has waned, the DHKP/C and Acilciler still have much to offer Syria as potential resources for terrorism.[12]

Mihrac Ural as an Agent of State Failure

The longer the situation inside Syria remains in flux, the greater the potential that Syria as a nation-state may fracture, leaving sizeable geographic enclaves of minorities to fend for themselves. This is as true for the country's ruling Alawite faction as it is for any other group. Some people on the ground, naturally anxious about what the future holds, are sorting through possible contingencies and alternative courses of action. One plausible scenario would involve establishing a mini-state in the Alawite heartland, a mountainous region that parallels the Mediterranean coast and runs southward from Turkey's border with Syria and onward well into Lebanon. Such an "Alawite Fortress" would give Syria's anti-Sunni minority faction a natural perimeter from which to defend itself against Sunni reprisals in case the current regime collapses.[13]

The problem faced by Turkey (and personified by Mihrac Ural) is that fracturing of nation-states can become contagious. The topography of the border region that separates Turkey and Syria tends to render existing international boundaries irrelevant as a matter of practicality. The director of the Turkish Research Program at the Washington Institute for Near East Policy recently described the border as relatively flat, "with nearly no physical barriers. The more the political boundary dissipates, the more northern Syria and southern Turkey will merge into each other."[14] Such a merger, though perhaps a dream come true for Ural and his supporters, could have dire implications for Turkish sovereignty as well as regional stability.

What effect a fraying Syrian state could have on the US and its allies in the region is difficult to predict. The potential necessity for deploying forces can hardly be ruled out. Simply put, instability along the mountainous Mediterranean coastline – the geographical area that includes Turkey's Hatay Province and Syria's northwestern governates – acts as a magnet for non-state threat actors hostile to US interests. The main danger to the United States is the potential for Balkanization: that the entire area might dissolve into contending factions commanded by multiple warlords. Meanwhile any increased potential for lack of governance in a particular region increases the chances that the United States could be drawn into the conflict. Mihrac Ural's Acilciler and other separatist threat actors trying to destabilize the situation in the Turkish-Syrian border areas increase the centrifugal forces pulling against Turkey's central government. This, in turn, increases the potential for a contingency involving an American deployment in response to a request from a NATO ally.[15]

A Burgeoning Religious War

In May 2013 – the same month in which the Banias massacres and the Reyhanli car bombings occurred – Sunni cleric Yusuf Quaradawi of Qatar declared that destruction of the al-Assad regime was a Sunni "religious duty."[16] Such inflammatory statements prompted Gary Grappo, a retired senior Foreign Service officer and Ambassador to Oman, to predict that religious war was on the horizon in Syria, and that "other Muslim nations with large Sunni majorities, including . . . Turkey, would inevitably be sucked into the tempest."[17] Inherent in religious wars is the specter of a tit-for-tat cycle of reprisals and atrocities that could drag on indefinitely in the absence of authority strong enough to impose order.

An unforeseen emergency warranting NATO deployment to Alawite-inhabited portions of the Mediterranean coastline could have profound consequences for the US Army and its Brigade Combat Teams. Understanding the cultural and political complexities of Turkey's boot-heel could give US forces an advantage in a contest with future adversaries and provide a hedge against the law of unintended consequences. The coming OEA Team Threat Report addresses the connection between the Reyhanli and Banias incidents and the threat actors involved, and strives to deepen leaders' understanding of a volatile operational environment in the MENA region.[18]

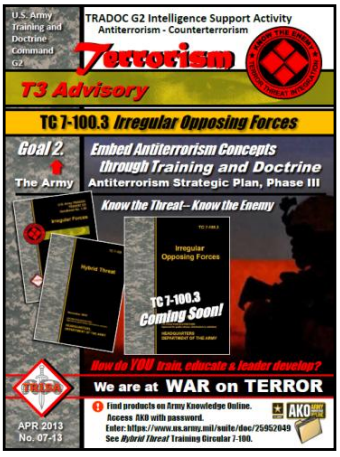
Notes

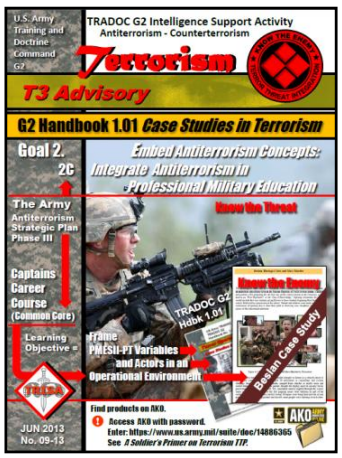
[1] HughEakin, "Will Syria's Revolt Disrupt the Turkish Borderlands?" *New York Review of Books,* 24 June 2011.
[2] "Turkey Detains Nine Over Deadly Bombings," *RAPID Weekly News Update* (FOUO, vol. 3 no.20), 17 May 2013.
[3] "Syrian Village Gives Up Secrets After Massacre," Muslim Village.com, 29 May 2013.
[4] Aydin Albayrak, "Mihrac Ural, A Man with a Long History of Terrorism," *Today's Zaman,* 14 May 2013

ARMY ANTITERRORISM THEMES: MONTHLY ANTITERRORISM CUES TO ARMY READINESS

by Jon H. Moilanen, TRISA-CTID Threats Terrorism Team (T3) (BMA Ctr)

The Complex Operational Environment and Threat Integration Directorate (TRISA-CTID) publishes a monthly *one-page* Threats Terrorism Team (T3) Advisory that complements the *Army's Antiterrorism Strategic Plan, Phase III*. See samples of FY 2013 monthly spotlights (below). To be on *T3 Advisory* e-distro, send email to jon.h.moilanen.ctr@mail.mil.





Are you Ready?—To Protect: Soldiers, Leaders, DA Civilians, and Families!

LIBYA: PROLIFERATION OF CAPABILITIES

by Steffany A. Trofino, Threat AssessmentTeam (DAC)

During the past two years, significant changes throughout North Africa have taken place. Long-standing authoritarian governments have been replaced with transitional governments responding to demands of societies seeking greater freedoms. Fundamental changes in political leadership and policy lead to unstable, uncertain times for newly-formed governments. Threat actors such as militant groups, insurgents, or criminal organizations will always seek to capitalize on opportunities during a country's transitional period, to their advantage.

Predominately, throughout Libya there has been a shift in the security environment which directly affects conflicts ongoing in neighboring states due to the spill-over effects and consequences of loosely governed borders. Libya's large arsenal of weapons collected over several decades from the Gadaffi régime have filtered into neighboring conflicts. Weapons currently arming threat actors in neighboring conflicts provide greater capabilities as they seek to destabilize transitional governments throughout the region. Threat actors in Syria, Mali, and Egypt are armed with weapons proliferated through the porous ungoverned borders of Libya and remain a concern to US national security interests in the region.

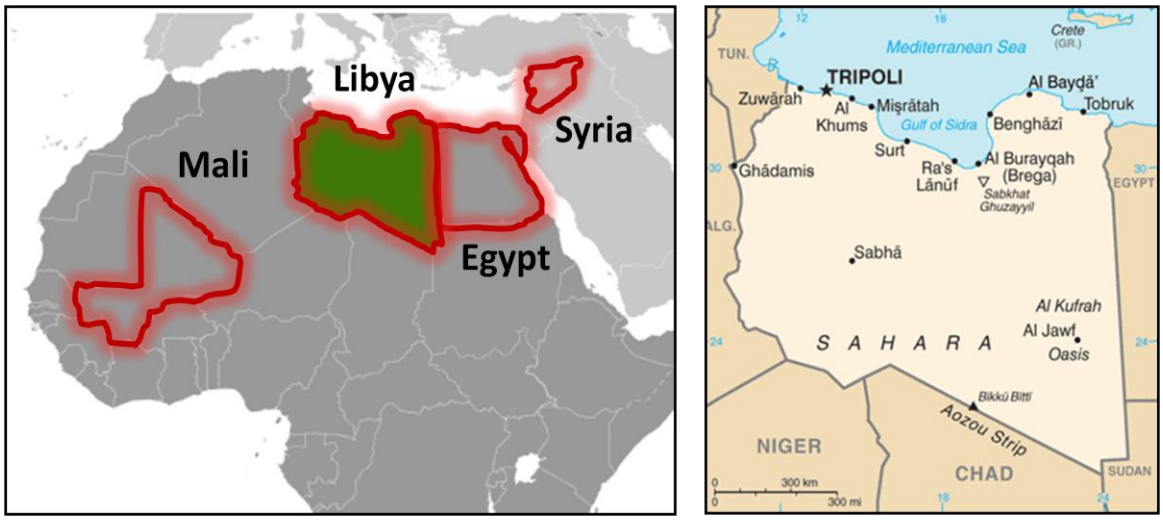


Figure1. Map of Libya and regional examples of weapons proliferation

During Libya's 2011 revolution, security forces became over-burdened as large protests continued throughout the country. Military garrisons inside Libya where large stockpiles of weapons were stored became loosely guarded. In several cases, military garrisons predominately located in east Libya were simply abandoned and unprotected from the general public.[1]

At a small armory complex near Sirte, locals reported that no security forces were available to guard the facility and weapons were removed daily by threat actors, paid contractors, and others. In one of the structures, the word "warhead" was stamped on dozens of sealed containers and at another depot, empty chemical agent munitions were found.[2] The US Department of State described the situation stating, "Since the February 2011 revolution, thousands of anti-aircraft missiles are still unaccounted for in Libya and extremist groups may use them against aircraft, including commercial flights."[3]

Figure 2. The Katiba's weapons. Wikimedia Commons,
(26 February 2011. Weapon crates broken open and found in Benghazi military garrison.)

Man-Portable Air Defense Systems (MANPADS)

While Libya collected several types of weapons over the years, surface-to-air missiles (SAMs), also referred to as man-portable air-defense systems (MANPADS), are of heightened concern to the US. It is estimated that Libya stockpiled 20,000 SA-7s and, of those systems, 10,000 are unaccounted for.[4] A multinational team of weapons experts has concluded most remaining MANPADS are likely under the control of regional military councils or threat actors.[5]

SA-7 SYSTEM

Alternative Designation: 9K32M Strela-2M

Date of Introduction: 1972

Proliferation: Worldwide

Target: FW, heli

Description:

Crew: 1, Normally 2 with a loader

ARMAMENT

Launcher

Name: 9P54M

Dimensions:

Length (m): 1.47

Diameter (mm): 70

Weight (kg): 4.71

Reaction Time (acquisition to fire) (sec): 5-10

Time Between Launches (sec): INA

Reload Time (sec): 6-10

Fire on Move: Yes, in short halt

Missile

Name: 9M32M

Range (m): 500-5,000

Altitude (m):

Max. Altitude: 4,500

Min. Altitude: 18, 0 with degraded Ph

Dimensions:

Length (m): 1.40

Diameter (mm): 70

Weight (kg): 9.97

Missile Speed (m/s): 580

Propulsion: Solid fuel booster and solid fuel sustainer rocket motor.

Guidance: Passive 1-color IR homing (operating in the medium IR range)

Seeker Field of View (^{o}): 1.9°

Tracking Rate (^{o}/sec): 6°

Warhead Type: HE

Warhead Weight (kg): 1.15

Fuze Type: Contact (flush or grazing)

Probability of Hit (Ph%): 30 FW/40 heli

Self-Destruct (sec): 15

Countermeasure resistance: The seeker is fitted with a filter to reduce effectiveness of decoy flares and to block IR emissions.

FIRE CONTROL

Sights w/Magnification:

Launcher has a sighting device and a target

acquisition indicator. The gunner visually identifies and acquires the target.

Gunner:

Field of View (^{o}): INA

Night Sight: None standard

Acquisition Range (m): INA

IFF: Yes (see NOTES)

VARIANTS

The main difference between the SA-7 and SA-7b is the improved propulsion of the SA-7b. This improvement increases the speed and range of the newer version.

SA-N-5: Naval version

HN-5A: Chinese version

Source: National War College Photo

Strela 2M/A: Yugoslavian upgrade

Sakr Eye: Egyptian upgrade

Strela-2M2: SA-7/7b and Strela-3 /SA-14 missiles converted with a Lomo upgrade 2-color IR seeker for detection/IRCM resistance similar to SA-18.

SA-7b can be mounted in various vehicles, boats, and vessels in four, six, and eight-tube launchers.

It can also mount on helicopters (including Mi-8/17, Mi-24/35 and S-342 Gazelle).

Figure 3. Basic specifications of the SA-7. [7]

The SA-7 can be used to target commercial, civilian, or military aircraft. During a press briefing on Libya, Andrew Shapiro, Assistant Secretary, Bureau of Political-Military Affairs at the US State Department stated, "One of our most serious concerns is the threat posed by MANPADS, and the potential threat loose MANPADS could pose to civil aviation."[6]

The threat to regional security imposed by MANPADS throughout Africa is not a new problem. Since 1975, 40 civilian aircraft have been hit by MANPADS, causing about 28 crashes and more than 800 deaths around the world.[8] Of those attacks, 28 have taken place in Africa. With recent conflicts escalating in Syria, Egypt, and Mali, the need to counter the proliferation of MANPADS out of Libya remains a priority for the West.

Syria

Since 2011, regional conflicts have continued throughout North Africa which challenge transitional governments as they seek to reform political policy as a result of the Arab Spring. For over a year the Free Syrian Army repeatedly sought the support of the US Government and requested arms to support military engagements against the Syrian régime. However, assistance from the US has been slow. Weapons looted from Libya may have the potential to fill this gap.

During an interview conducted by *Reuters*, British-Libyan arms dealer Abdul Basit Haroun openly boasted weapons from Libya are reaching Syrian opposition groups not only by charter aircraft but also by ships where weapons are hidden among humanitarian aid. Routinely, charter aircraft filled with Libyan weapons land in neighboring states where the weapons are then transferred to opposition groups in Syria.[9] *Russia Today* reported C-17 cargo planes (which are capable of carrying 70 tons of weapons) have landed at least three times in Libya during 2013. Each time, planes picked up a shipment of weapons which were then flown to the Turkish-Syrian border. From this point, the weapons were then transferred to Syrian rebels.[10]

Syria is but one of several examples in the region. Threat actors in Egypt as well as Mali are also finding ways to support their engagements against transitional governments, arming themselves with weapons smuggled out of Libya.

Egypt

As recent as 16 August 2013, a cargo vessel was seized by the Egyptian Coast Guard which contained a large cache of weapons smuggled out of Libya. According to the ship's registry, the last port of call listed prior to entering Egyptian waters was Misrata, Northern Libya.[11] As conflict in Egypt continues, weapons from Libya continue to make their way to threat actors throughout Egypt's Sinai Peninsula which is loosely guarded by security forces.

Mali

Mali is another highlighted example of destabilization exasperated due to illicit weapons trafficking out of Libya. Malian Tuareg mercenaries who fought for Gadaffi during the Libyan conflict routinely smuggle weapons across the border. As locals of the region, Tuareg's are familiar with the desert and know best opportunities (and trade routes) to transfer weapons across borders unobstructed. Malian army officials describe being over-run by heavily armed militant forces returning with heavy arms to Mali after fighting in Libya.[12] To date, the unguarded Libyan borders remain a heightened concern for Malian security forces.

Training Implications

The transitional political environments and loosely governed borders of Libya continue to contribute to the unstable security conditions throughout North Africa. Such conditions further destabilize neighboring state security in Mali, Egypt, and Syria. The training community may want to highlight the importance of border security. With a lack of governance or an effective rule of law, threat actors will continue to capitalize on opportunities to proliferate weapons from Libya to their advantage. The proliferation of weapons out of Libya enables threat actors throughout the region with strengthened capabilities to be used against US National Security interests in the region. These capabilities should be of primary concern to the US and our allies in the region.

Notes

[1] Jason Beaubien, "U.S. Fears Terrorists Could Acquire Looted Weapons," National Public Radio, 12 September 2011.
[2] Global Security Newswire, "Libyan Weapons Depot Unguarded, Open to Looters," 3 October 2011.

[3] United States Department of State, Travel Warning: Libya, no date.
[4] Scott Stewart, "The Continuing Threat of Libyan Missiles," STRATFOR, 3 May 2012.
[5] Andrew Chuter, "5,000 Libyan MANPADS Secured: Some may have been smuggled out," *Defense News*, 12 April 2012.
[6] Andrew J. Shapiro, "Comments on US Assistance To Help Dispose of Weapons in Libya," US Department of State, 11 December 2011.
[7] TRADOC G2, TRISA, World Wide Equipment Guide (WEG), Volume 2, Chapter 6, Air Defense, 2012.
[8] US Department of State, "MANPADS: Combating the Threat to Global Aviation from Man-Portable Air Defense Systems," Bureau of Political-Military Affairs, 27 July 2011.
[9] Jessica Donati, Ghaith Shennib, and Firas Bosalum, "The adventures of a Libyan weapons dealer in Syria," *Reuters*, UK, 18 June 2013.
[10] "Colonel Gaddafi's Legacy? Unregulated Libyan weapons 'flood' Syria," *Russia Today*, 22 June 2013.
[11] Illegal weapons shipment heading to Egypt "seized," *Libya Herald*, 16 August 2013.
[12] Ian Black, "West overlooked risk of Libya weapons reaching Mali, says expert," *The Guardian*, 21 January 2013.

BOATS PART 3. CRIMINALS: OPFOR TTP FOR MARITIME AND LITTORAL OPERATIONS

OPFOR TTP for Maritime and Littoral Operations in Training
by Marc Wlliams, Training, Education, & Leader Development Team (CGI CTR)

Why study boat operations when you are in an army? Because boats are another form of transport land forces use to overcome water obstacles and conduct littoral operations along coastlines. Successful land operations often depend on resupply over water, and naval operations depend on successful land operations to maintain unchallenged access.

Previous *Red Diamond* articles on boat operations focused on insurgents in Africa and guerrillas in Sri Lanka. This article covers criminals closer to home. Specifically, drug trafficking organizations (DTOs) from Colombia and Mexico use Central American countries (Ecuador, Costa Rica, and Panama) and Caribbean nations (Dominican Republic and Jamaica) as transit points.

Some DTOs operate on a scale often associated with nation-states. In the current war on drugs, DTOs are shifting drug smuggling routes from over land to sea lanes again. This is coupled with advances in boats and motors, to include the private development of drug- and human-smuggling submarines and semi-submersibles.

US History

> In 1870, Chinese immigrants became the first known drug smugglers when they began smuggling opium in merchant ship cargoes and baggage. Since then, drug smuggling by maritime routes has grown in size, scope, and sophistication as demand skyrocketed. For example, around the turn of the century, when cocaine use was first in vogue, a relatively limited amount of the population was directly affected by the problems of cocaine abuse. But in later years, as the drugs of choice shifted from cocaine to heroin and opium, then later to marijuana and back to cocaine, drug smugglers began utilizing maritime sea and air routes to transport larger shipments of drugs to the US. For nearly a century, the maritime drug smuggling business slowly evolved.[1]

Between 1994 and 2013, the number of annual Coast Guard drug intervention events has more than doubled (67 to 139) and the amount of cocaine seized has almost tripled (65K+ to 166K+ kilograms). However, the numbers for 2013 are only through May.[2]

Sea Smuggling Routes

The US coastline is large and difficult to secure. All sea smuggling routes pass through the Exclusive Economic Zone (EEZ) in Atlantic, Pacific, Caribbean, and Arctic waters.[3] Scoping this down to the Transit Zone, the size is still approximately six million square miles to be monitored and patrolled.[4] DTOs use the Transit Zone to move product and evade law enforcement efforts using a variety of craft. "The central Caribbean is once again becoming a preferred route for

transnational drug cartels. This is evidenced by increased cocaine seizures reported by authorities in countries such as Jamaica and the Dominican Republic.

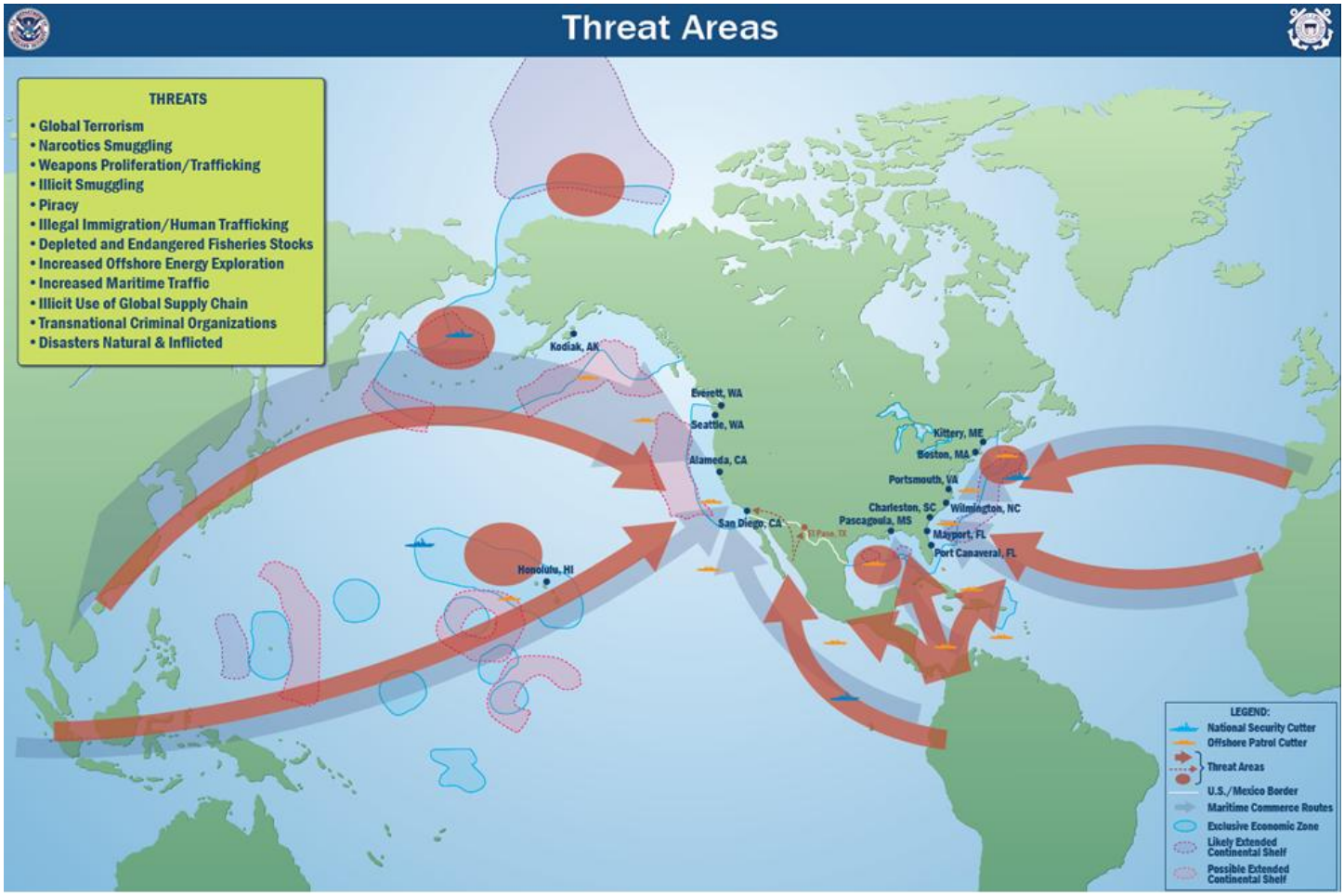


Figure 1. Threat Areas, from US Coast Guard Publication 3-0, *Operations*

In the late 80s and early 90s, the Caribbean was the preferred route of Colombian drug traffickers, but law enforcement efforts in the region during the last 25 years, especially off the Florida coast, shifted the route of shipments into Central America and Mexico."[5] Now with almost daily drug seizures on the US border, DTOs are shifting efforts back to the Caribbean. The poverty levels in that region make for a ready pool of workers for smugglers paying in cash. Jamaica and the Dominican Republic are the key transit points. Examples of illicit activities in the Caribdean region include:

- Jamaica: "Seizures of South American cocaine in Jamaica doubled during the first half of 2013 to 354 kilograms when compared to the same time period in 2012. The island is also used by transnational cartels to store shipments of heroin and marijuana. In fact, Jamaica is the Caribbean's leading exporter of marijuana."[6]
- Dominican Republic: "The Dominican Republic has been deemed as the Caribbean's largest transit point for drugs. In fact, US authorities are projecting that an estimated 6% of cocaine shipments that will eventually end up in the US will pass through the country in the next year. Geographically speaking, the Dominican Republic is the perfect receiving point for incoming Colombian drug shipments. Although hundreds of miles apart, Santo Domingo is a straight shot from La Guajira, Colombia. It is not coincidence then that 12 of the 13 individuals arrested in conjunction with cocaine seizures in 2013 were Colombian nationals." [7]

Boats

In the 1980s, the television show Miami Vice portrayed drug smuggling boats as the sleek, fast "cigarette" boats used in speed races. The truth in the 21st Century is less glamorous. DTO boats now tend to be lightweight fiberglass "panga"

boats that are commonly used in the American hemisphere for fishing. Pangas are 19-35 feet long and can carry one to five tons. They are powered with multiple engines to add speed and can travel up to 40 miles per hour. Two low-paid operators in a panga powered by multiple 200 horsepower outboard motors carrying five tons of cocaine represent a sizeable profit for DTOs. Common tactics, techniques, and procedures (TTP) for boats is to travel with minimum crew, travel at night, go as fast as possible through open water, depart from an inland cove or river, and arrive at the same with land transport personnel and vehicles waiting to reduce time on site.

Figure 2. **Go-fast boat seized by the USCGC *Valiant* (WMEC 621) on 31 May 2012 in the Caribbean Sea.**
***Note*.** Twin 200 horsepower engines and eight barrels of drugs. This boat carried 43 bales of cocaine with a wholesale value of $32.5 million. Source: USCG photo.

Figure 3. **A boarding team from the U.S. Coast Guard Cutter *Edisto* inspects a panga.**
Note. This panga had approximately 250 bales of marijuana aboard and keeps watch over three suspected smugglers after interdicting the vessel more than 100 miles southwest of San Diego, June 18, 2013. The panga, suspects and drugs were all turned over to the Mexican Navy. Source: U.S. Coast Guard photo by Seaman Ryan Taylor.

Submarines and Semi-Submersibles

In the news lately there has been a flurry of reporting and uproar over "drug submarines." The idea that anyone other than a nation-state could produce a submarine is treated as something like science fiction. However, given the resources of DTOs and the effectiveness of law enforcement efforts, submersible boats are now being built and utilized to transport illegal drugs into the US. Up to 100 feet long and capable of carrying 8 tons of product, these vessels are very difficult to detect. In Colombia, submarine construction sites are now classified as high value targets.[8]

Figure 4. This semi-submersible nicknamed "Bigfoot" (2008) was carrying four tons of pure cocaine.
Source: **US Coast Guard News .**

In 2008, the US assisted Mexico in finding its first drug submarine.[9] It was loaded with 5.8 tons of cocaine, was 30 feet long, had a crew of four Colombians, and was equipped with a GPS and a compass. In 2010, the US Drug Enforcement Agency (DEA) assisted the Ecuadorian government in locating and seizing a drug smuggling submarine. This vessel was a diesel-electric submarine capable of carrying tons of product, constructed and hidden in the Ecuadorian jungle.[10]

Most of the DTO effort appears to have moved to producing semi-submersibles instead of submarines.

Figure 5. (See *left*) A self-propelled semi-submersible is towed alongside the US Coast Guard Cutter off the coast of Central America (2009).
Note. A US Customs and Border Protection Maritime Patrol Aircraft detected the vessel, then the US Coast Guard Cutter *Jarvis* intercepted the vessel. Jarvis' crew found that vessel was loaded with narcotics, seized the SPSS, and detained the four crew members.

TTP for semi-submersibles include keeping the crew below decks, moving at night, launching from a river, offloading at sea with surface boats, and then sinking the vessel.

Impact on Training and Scenarios

DTOs are not bound by resources and neither are the transnational criminal organizations (TCO) portrayed in training. Real-world criminals are adaptable and determined to protect their illegal business. The use of submarines and submersibles presents a set of challenges not normally seen by an Army unit but one that must be addressed if the scenario includes a coastline. If smugglers can move large quantities of drugs at will, what is to stop them from moving personnel and weapons for the right price?

Notes

[1] US Department of Homeland Security, US Coast Guard, Office of Law Enforcement (CG-MLE), Drug Interdiction, last modified 6/25/2012.

[2] US Department of Homeland Security, US Coast Guard, Office of Law Enforcement (CG-MLE), Coast Guard Drug Removal Statistics, updated as of 3 September 2013.

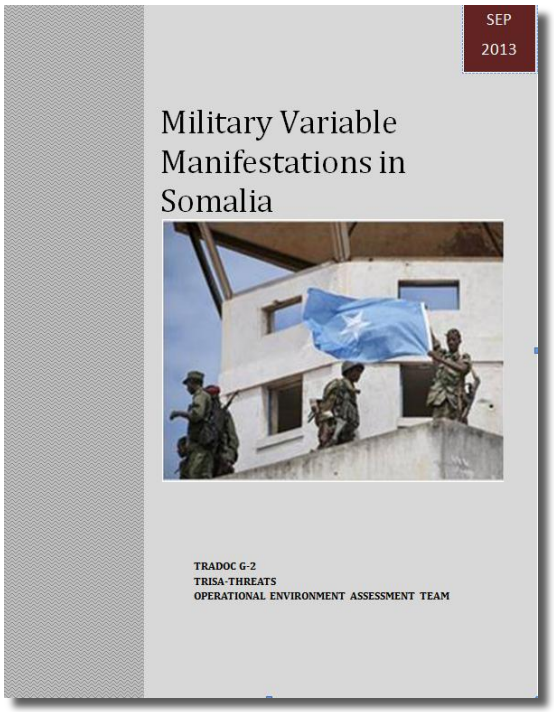
[3] Exclusive Economic Zone is the zone where the US has jurisdiction over natural resources. The US Exclusive Economic Zone (EEZ) extends no more than 200 nautical miles from the territorial sea baseline and is adjacent to the 12 nautical mile territorial sea of the US, including the Commonwealth of Puerto Rico, Guam, American Samoa, the US Virgin Islands, the Commonwealth of the Northern Mariana Islands, and any other territory or possession over which the United States exercises sovereignty. US Department of Commerce, National Oceanic and Atmospheric Administration, revised October 21, 2013.

[4] Transit Zone: a six million square mile area that includes the Caribbean and the Gulf of Mexico and the eastern Pacific Ocean; includes the principal routes used by drug smugglers.
[5] CNN Mexico,The Caribbean: A Preferred Route for Transnational Drug Cartels, 5 March 2013.
[6] CNN Mexico,Los narcotraficantes adoptan ruta del Caribe para traslado de droga a EU, 5 March 2013.
[7] CNN Mexico,Los narcotraficantes adoptan ruta del Caribe para traslado de droga a EU, 5 March 2013.
[8] National Geographic special: Inside cocaine submarines, 30 April 2012.
[9] Olga R. Rodriguez, US helps Mexico find drug submarine, 19 July 2008.
[10] Associated Press raw video: Seizure of a drug-smuggling submarine, uploaded 5 May 2010.

SOMALIA: MILITARY VARIABLE HIGHLIGHTS

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

In October 2013, the TRISA OEA Team published an updated version of its Horn of Africa (HOA) Operational Environment Assessment (OEA) that replaced the initial HOA OEA published in February 2009. In that short time, much has changed, 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) factors that affect a country or region. In advance of the OEA, which contains over 800 pages on the seven HOA countries, articles on the Djibouti, Eritrea, Ethiopia, and Kenya military variables received coverage in previous editions of the *Red Diamond*. This month's article will cover the Somalia military, while future Red Diamond issues will highlight the military variable for the remaining countries—Sudan and South Sudan.



Until very recently, Somalia was a failed state in northeast Africa on the Red Sea. Its semi-autonomous regions exhibited high levels of violence, served as a safe haven for pirates, and often allowed insurgent groups to operate with impunity. In the last couple of years Somalia, with the assistance of some of its neighboring countries, has driven the insurgents out of Mogadishu while the nascent Somali Federal Government (SFG) is attempting to become a functional national regime. The semi-autonomous regions of Puntland and Somaliland both field their own military forces in order to ensure a stable and peaceful environment for their regions.

Most of the soldiers that belong to the Somali military are former militia fighters for warlords supportive of the Transitional Federal Government (TFG), which became the SFG in late 2012. The SFG's army numbers between 10,000 and 12,000 personnel, with a planned ultimate end strength goal of 17,731 soldiers. Some Somali leaders feel that this number of soldiers is inadequate for patrolling the vast reaches of their country. Somalia also fields a small navy, but no air force. The Somali Police Force is potentially a paramilitary organization that aspires to reach a strength level of 10,000 officers. As of late 2011, the UN and the European Union (EU) had trained about 3,000 Somali police officers.

Because most of Somalia's soldiers formerly belonged to a variety of militia organizations, the quality of their training and readiness, as well as their discipline, leaves much to be desired. Without assistance, first from Ethiopia and lately by Kenya, the SFG/TFG would not have been successful in ousting the Union of Islamic Courts and the al Shabaab Islamist insurgent group, which once controlled much of Somalia's territory. Both African Union and other international

militaries have assisted in training Somali forces. These countries include Ethiopia, South Africa, Tanzania, Kenya, Uganda, France, Spain, and the EU.

There is no formal order of battle, units, or divisions within the SFG army. The disparate military groups still retain much of their militia flavor and are usually organized around clans supportive of a particular leader within the SFG government. The five largest SFG military groups, from largest to smallest, are the Majerteen sub-clan, from which former President Yusuf originated; the Marehan clan that comprised most of the former Jubba Valley Alliance; the Rahanwhein clan that traces its roots back to the Rahanwhein Resistance Army; the Hawiye clan's Abgal sub-clan, associated with former prime minister Ali Mohamed Gedi; and the Hawiye clan's Saad sub-clan, associated with Somali national police chief Abdi Hassan Awale Qeybdiid.

The numbers and types of weapons used by the SFG military are difficult to quantify. The years of warfare, the numerous militia groups, the illegal import of weapons, and more recent legal purchases skew the inventories of weapons available to the SFG. Based on weapons seen by outsiders, it appears that much of the equipment is of Russian/former Soviet Union origin, but there is a smattering of Western military equipment as well.

The SFG navy is more of a coast guard than a navy, with around only 500 personnel. The SFG navy operates a small number of patrol boats, but can only provide token opposition to the rampant piracy occurring off the Somali coast. Accordingly, the UN passed a resolution that allows the international community to enter Somali territorial waters to stop piracy and other criminal acts off the country's coastline. At any one time, there are about 20 international ships, a few foreign airplanes, and 1,800 non-Somali military personnel operating off the Somali shore in an attempt to keep the shipping lanes open.

The original Puntland army once numbered 3,200 members, but merged with other militia forces to form the TFG military in mid-2007. Due to minor conflicts between Somaliland and Puntland in late 2007 and ideological differences within the TFG, Puntland established a new separate military organization in 2008. The Puntland army fields 10,000 soldiers, and the coast guard contains about 300 sailors with eight bluewater capable vessels. The Puntland Police Force, the Puntland Intelligence Services, and the Puntland Maritime Police Force are also paramilitary organizations with combat potential.

Somaliland fields an army of approximately 15,000 soldiers apportioned among two armored brigades, one mechanized infantry brigade, fourteen infantry brigades, two artillery brigades, and one support battalion. These units, however, are much smaller than their designations suggest, even though they are organized around a more traditional military structure than that of the SFG. Somaliland also operates a coast guard, with 350 sailors and 26 small patrol boats, to deter piracy along its coast. The Somaliland Police Force is a paramilitary organization that has received both UN and United Kingdom training, while the 1,540 armed guards of the Custodial Corps operate the Somaliland prison system.

Insurgent Organizations (Example)

Many insurgent groups operate in Somalia. These groups include al Shabaab, Hizbul Islam, the Alliance for the Re-Liberation of Somalia-Asmara, the Muaskar Ras Kamoboni, the Jabhatul Islamiya Somalia, Muaskar Anole, and al-Qaeda (AQ) affiliates.

Due to the combined efforts of the SFG military and its neighboring countries, al Shabaab no longer controls Mogadishu and its remaining fighters have fled to more remote areas of Somalia for their own safety. A number of criminal organizations operate in Somalia, including several pirate groups that seize ships and hold vessels and crews for ransom. The major pirate factions include the Somali Marines, the National Volunteer Coast Guard, the Marka Group, the Puntland Group, and the Central Regional Coast Guard.

The Somalia military variable in the HOA provides additional details on the SFG's military forces, the insurgent groups, and the criminal organizations, to include their various arsenals. While Somalia was once the enemy of the West and its war on terrorism, the new SFG is a more positive force in the world's endeavors to stamp out Islamist insurgents.

Antitank Tactics and Techniques in a Complex Urban Environment
by Jon H. Moilanen, CTID Operations (BMA Ctr)

Using the antitank grenade launcher (ATGL) RPG-29 is a proven antitank ambush weapon-of-choice. The RPG-29 is especially successful in an urban environment when threat forces—or opposing forces (OPFOR) for training—coordinate observation and tracking of combined arms enemy forces in confined urban street networks, isolate armored vehicles from infantry forces, and ambush armored vehicles in a kill zone. Several recent engagements by insurgents and/or urban guerrillas against Syrian regular military forces demonstrate how a small antitank insurgent direct action cell or guerrilla unit hunter/killer team can effectively plan and execute an antitank ambush with the RPG-29.

Antitank Grenade Launcher (ATGL) RPG-29

The RPG-29 is a shoulder-launched 105-mm grenade weapon system. The warhead of the weapon is tandem high-explosive antitank (HEAT) shaped-charges that are capable of penetrating the more vulnerable areas of modern main battle tanks.[1] The two shaped-charges of the warhead can defeat even tanks with sophisticated vehicle armor and explosive reactive armor (ERA) appliqués. A high-explosive (HE) thermobaric warhead is also available and has multipurpose uses.

Figure 1. Antitank grenade launcher (ATGL) RPG-29 and 105-mm rocket grenade

At least two individuals—grenadier and assistant grenadier—normally comprise an RPG-29 team. During tactical movement and operations, one individual carries the launcher unit front section and the other individual carries the grenade-canister rear section. The two sections use couplings for quick assembly into a weapon system. A folding bipod can be used for improved stability when firing from a prone position. The grenadier has the option of optic-reticle or "iron-post" sights on the RPG-29 and can also mount a night sight. The number of grenades carried by the team or additional support members depends on the situation with a typical combat load per team of three or more grenade-canisters. Although platform variants include ground or vehicular pintle-mounted weapons, the focus of this article vignette is a shoulder-launch variant of the RPG-29.

Ambush Tactics and Techniques

An ambush is "a surprise attack from a concealed position, used against moving or temporarily halted targets.[2] In an ambush, enemy action determines the time, and the threat OPFOR set the place. Types of ambush can include purposes of *annihilation* to destroy the enemy, *containment* to prevent the enemy from using an avenue of approach or interdicting another action such as a raid or another ambush, and/or *harassment* to demoralize the enemy as a complement to other threat OPFOR information warfare (INFOWAR) and psychological warfare (PSYWAR) actions.[3]

Threat OPFOR ambush teams focus their plans and conduct on a primary kill zone and/or multiple alternate kill zones in a designated battle zone. Whether one ambush site or a series of recurring antitank ambushes, the primary purpose of the threat OPFOR is to degrade enemy capabilities while preserving or improving its own combat power. An ambush consists typically of three elements: ambush, security, and support.[4] The *ambush element* has the mission of attacking and destroying enemy elements in the kill zone(s). The *security element* provides early warning to threat OPFOR elements, prevents enemy elements from responding to the ambush before the main direct action is accomplished, and prevents the ambush elements from becoming decisively engaged. The *support element* provides direct and general assistance to the ambush elements to enhance the overall mission. This can include command and control, INFOWAR video or digital camera recording, and/or preparatory and post-operation mission support sites.

Ambush Vignette: RPG-29 versus Tank

The Situation. Regular military and internal security forces of the state are struggling to reestablish control of major geographic districts within the urban areas of the provincial capital. The local population expresses increasing dissatisfaction on the state's repressive actions and fighting in what many regional and global media outlets label as civil war. Public safety is not consistent, and law and order in many areas is relegated to militias of questionable purpose or neighborhoods watch groups.

The local insurgent organization leader directs its cells to coordinate directly with an affiliated guerrilla unit operating in the urban metropolitan area. Concurrently, an indigenous criminal organization brokers a partnership that mutually benefits the insurgency and the crime family's operations in the warehousing area of the city's deep-water port.

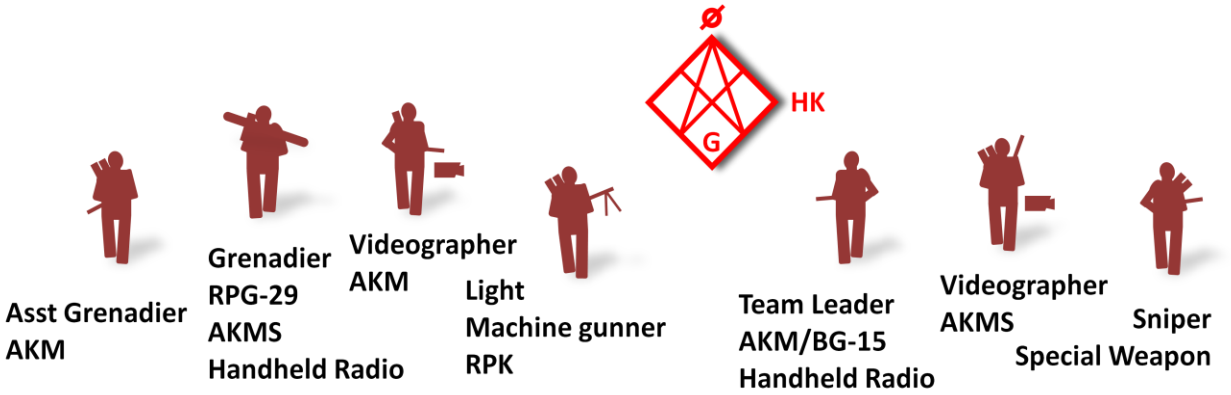


Figure 2. Guerrilla antitank hunter-killer team (example)

The guerrilla company task-organizes small "hunter-killer (HK) teams" to ambush enemy forces in the complex urban terrain. Platoon and team leaders, empowered with decentralized command and control, coordinate in their assigned urban neighborhoods with local criminal elements and other civilian active supporters of the insurgency to observe and report on the locations and movements of enemy forces. In this vignette, the HK team is comprised of five guerrillas: a team leader, grenadier, assistant grenadier, light machinegunner, and sniper.[5]

The insurgent organization allocates two insurgent-videographers from its information warfare (INFOWAR) cell to this HK team leader in order to record ambushes with the RPG-29 and the catastrophic effects on armored vehicles. (See Figure 2, *above*.) Depending on the size, nature, and focus of the insurgent organization, a direct action cell INFOWAR may be capable of several functions including selective sabotage actions, information management, media manipulation, psychological warfare (PSYWAR]), communications (cyber embeds via Internet sites, propaganda and

indoctrination videos, broadcast successes of the direct action teams), civic actions, and assist in the cyber-mining for intelligence. All of these functions integrate into mission task assisgnmenst and long-range goals.

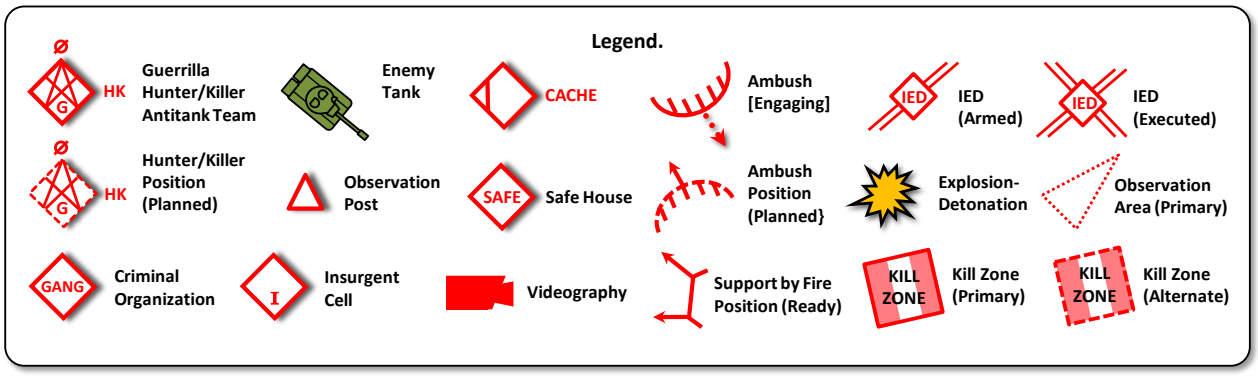


Figure 3. Legend for RPG-29 ambush of an enemy tank platoon (example figure 4)

Movement and Positioning for the Ambush

Local criminals report regularly on enemy force movements as tanks, armored vehicles, and dismounted soldiers patrol toward the urban area that is under nominal control of the insurgents. A succession of brief firefights separates dismounted enemy soldiers from a platoon of tanks as the tanks crash through a road block. ① An improvised explosive device (IED) in the obstacle damages the suspension of one tank as the three tanks continue down a boulevard.

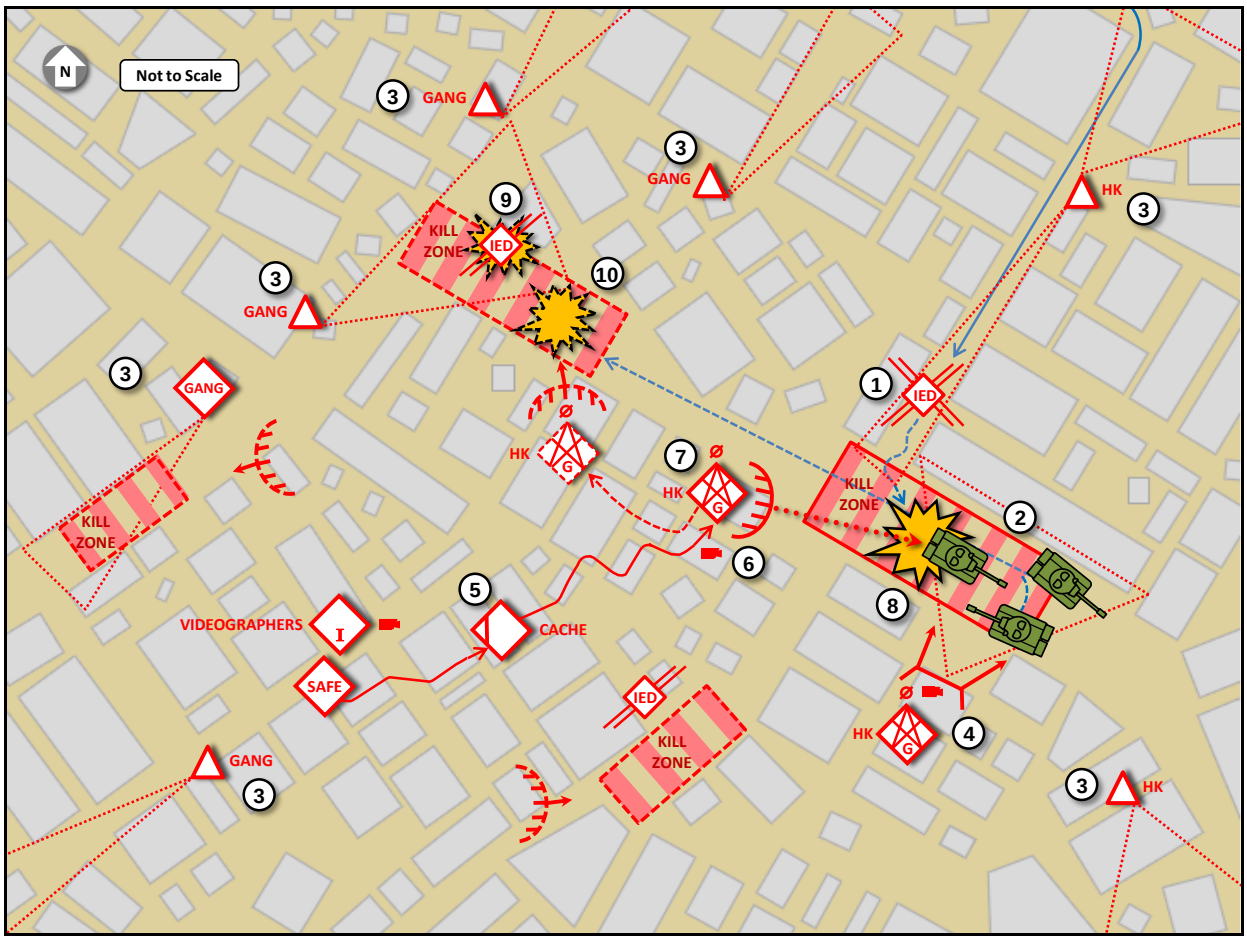


Figure 4. RPG-29 ambush of a tank platoon in urban terrain

A guerrilla security element observes the tank platoon's movement when they turn at a main intersection and halt. ② A guerrilla platoon leader alerts one of his HK teams prepositioned several blocks from the site to move and occupy

ambush positions. ③ As guerrilla security elements and local criminals monitor possible approaches into the area, the HK team leader establishes an overwatch support position and observes one crewman dismount who is apparently inspecting or working on a section of track or rear suspension. ④ Surprisingly, no other crewmen dismount for local security. Tank main guns remain stationary and orient down the main street over each tank's front glacis. Tank commanders are not traversing their cupolas to observe the immediate area for mutually supporting security.

Concurrently, other guerrillas of the HK team move from a safehouse to retrieve additional RPG-29 grenade canisters from a cache. ⑤ Previous rehearsals along multiple routes to primary and alternate firing positions allow the HK team to quickly occupy their primary position and prepare for the ambush. The HK team and videographer on the roof of a four-story building report their arrival to the team leader and perform final checks on the RPG-29. They remain concealed on the roof. The HK team leader updates the ambush element, security elements, and criminals acting as observers on enemy actions in the kill zone via handheld radio.

The HK team leader alerts the entire HK team and signals the RPG-29 team to conduct the ambush. The grenadier pauses for a moment crouched below a low wall on the roof, and focuses mentally while he thinks through his aim and fire sequence. He knows the stationary tanks are very vulnerable to his angle of fire. ⑥ After a deep breath, he partially exhales, stands up and calmly aims at the rear deck near the turret ring of the tank, and squeezes the ATGL trigger.

Note. This opposing force (OPFOR) insurgent ambush of a tank platoon with an RPG-29 is based loosely on a recent tactical engagement during the ongoing conflict in Syria. For videographer coverage of the incident, see Insurgent ambush element uses RPG-29 to destroy enemy tank.[6]

The Ambush

The backblast of the rocket-propelled grenade is momentarily deafening as the cloud of dust and debris rises from the roof. The grenadier, assistant grenadier, other guerrilla, and videographer are already racing down an interior stairwell in order to occupy an alternate firing position. ⑦ At a launcher-to-target distance of fewer than 300 meters to the tank, the grenadier knows he achieved a catastrophic hit on the tank.

The videographer with the HK team leader records the detonation of the grenade on the tank and the immediate large fireball and smoke from main gun ammunition propellant as it ignites inside the tank. ⑧ The HK team leader continues to observe from the overwatch support position as secondary explosions and small arms ammunition "cooks-off" inside the turret. As the support element observes and records the reactions of the two other tanks, one surprise is the survival of the crewman that had been checking the track or suspension on the now destroyed tank. He stumbles from the fire and smoke engulfing the tank and runs wildly down the street and out of sight.

No immediate reaction by the other two tanks is puzzling to the HK team leader, but eventually he observes one commander cupola traversing back and forth to scan the near-area of one flank. The tanks move slowly down the streetway and out of sight of the support element. However, criminals acting as observers report the location of the tanks as they attempt to find a way out of the maze of streets. ⑨ Near the original ambush, the lead tank detonates a large IED when it drives over a pile of rubble. The explosion breaks the left track and it slides slowly off the support rollers and onto the pavement. Only two crewmen jump from the burning tank and run to the one remaining tank. The trail tank stops and takes the two crewmen on board before starting to reverse down the street. By this time, the RPG-29 team repositions to intercept the tank and engage it from another roof-top firing position. ⑩ A detonation similar to the first ambush occurs. The RPG-29 HK team and the coordinated actions of a hybrid threat (HT) of insurgents, guerrillas, and criminals destroy an enemy tank platoon.

Ambush Assessment

The destruction of a three-tank platoon was a tactical success. A factor of more significance to the insurgency was the use of an INFOWAR cell to record the actions of the ambush, security, and support elements in the RPG-29 attack. With the rapid production of two videos spliced into a compelling visual story, the insurgent organization posted video-copies on the Internet within hours of the ambush and distributed them to regional media outlets. Indications of effective perception management within the insurgent INFOWAR campaign included:

- Enemy soldiers captured in subsequent weeks emphasize the negative psychological impact of seeing the effectiveness of the RPG-29 on their armored forces.
- Insurgent organization recruiters report an increase in the number of young males volunteering to join a direct action cell or urban guerrilla unit based on viewing this RPG-29 ambush video and other tactical actions promoted via the Internet.
- Insurgent organization and guerrilla unit trainers state that videos of actual tactical operations and techniques lessen the time required by recruits to acquire a satisfactory level of weapon skills in preventive maintenance, marksmanship, and tactical techniques.

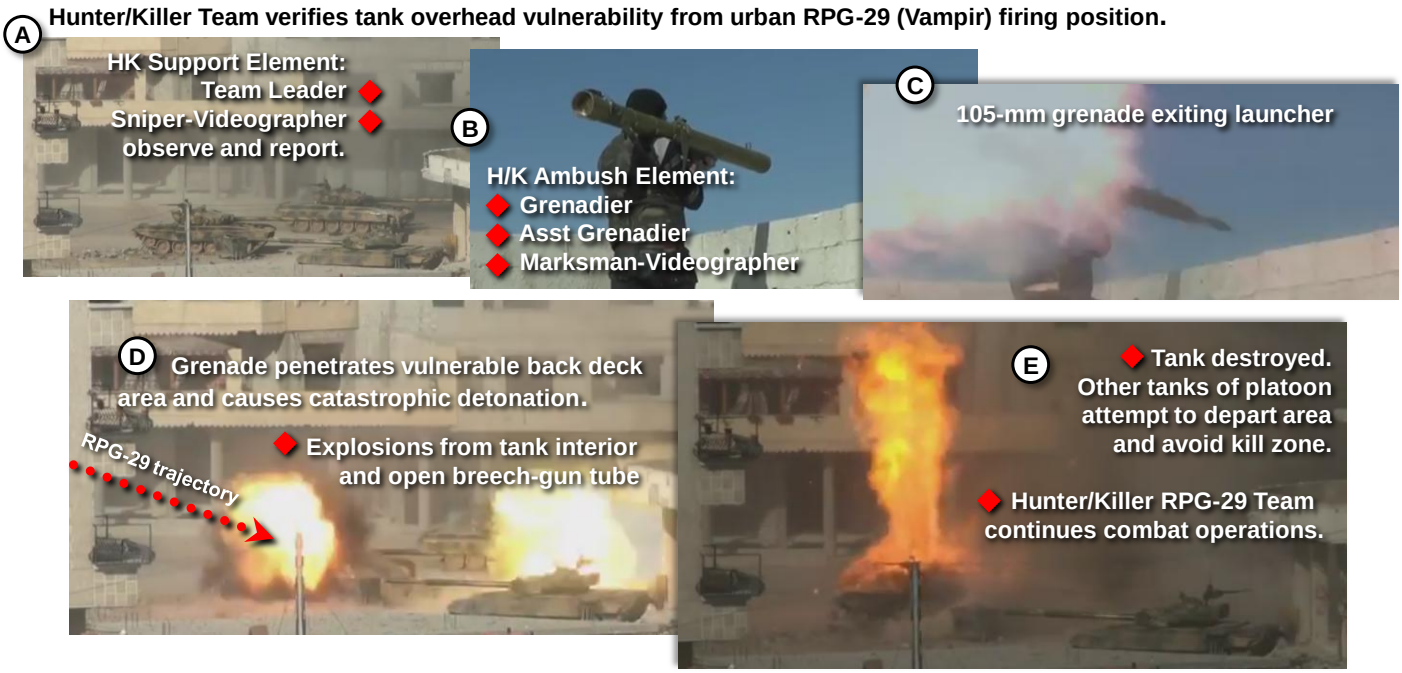


Figure 5. Insurgent ambush element uses RPG-29 to destroy enemy tank

Training Implications for Threat OPFOR

- Train and empower threat OPFOR small unit tactical leaders to act with initiative in support of a higher leader's mission and intent.
- Separate combined arms enemy forces such as armor and infantry from each other in urban terrain and fix-isolate a target.
- Maintain observation of obstacles and kill zones in order to improve effective conduct of direct actions that defeat or destroy a target.
- Ambush isolated enemy elements with sequential and/or nearly simultaneous attacks from multiple directions at ground level and/or raised urban infrastructure such as multi-story buildings.
- Defeat the individual enemy elements in detail and preserve threat OPFOR combat power.
- Distribute near real-time video-coverage of enemy combat losses to the Internet and media outlets as a threat OPFOR INFOWAR and PYSWAR combat multiplier.
- Conduct deliberate threat OPFOR after action reviews (AAR) of engagements soon after a combat action, and distribute tactical observations among other threat OPFOR cells or units.
- Reward successful threat OPFOR tactical leadership and cell-unit-team mission achievement.

Notes

[1] US Army Training and Doctrine Command G2, *Worldwide Equipment Guide.* vol. I (2012), "Russian 105-mm Antittank Grenade Launcher RPG-29 and RPG-32/Hashim," p 2-41.

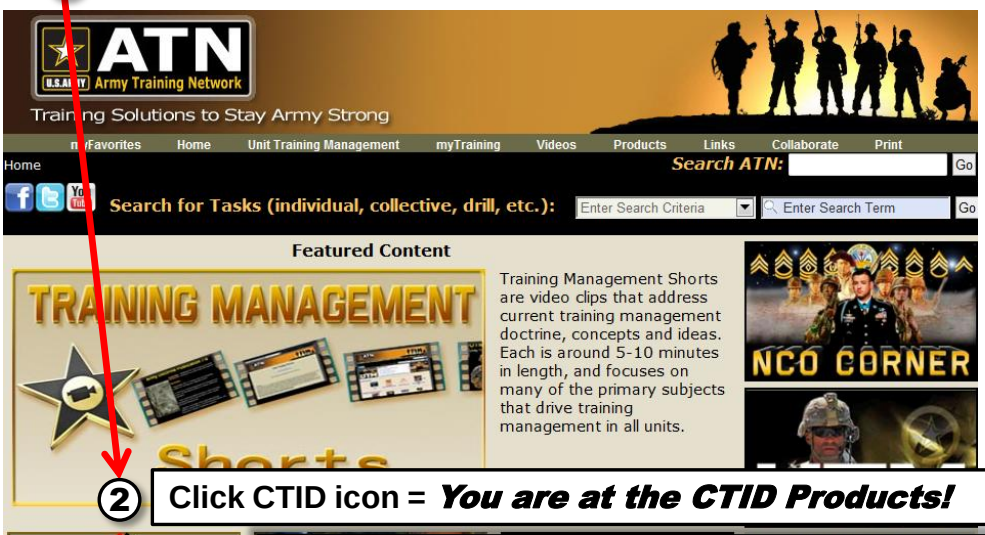
[2] Headquarters Department of the Army, Training Circular (TC) 7-100.2. *Opposing Force Tactics* (2011), "Ambush," para. 3-133.

[3] Headquarters Department of the Army, Training Circular (TC) 7-100.2. *Opposing Force Tactics* (2011), "Types of Ambush," para. 3-150.
[4] Headquarters Department of the Army, Training Circular (TC) 7-100.2. *Opposing Force Tactics* (2011), "Functional Organization for an Ambush," para. 3-137.
[5] Headquarters Department of the Army, Field Manual (FM) 7-100.4. *Opposing Force Organization Guide* (2007), Appendix E, "Guerrilla Hunter/Killer Company," with "HK Team, Team One," p. E-13.
[6] *Syrian rebels using RPG-29 to destroy SAA T-72,* Insurgent ambush element uses RPG-29 to destroy enemy tank (video).

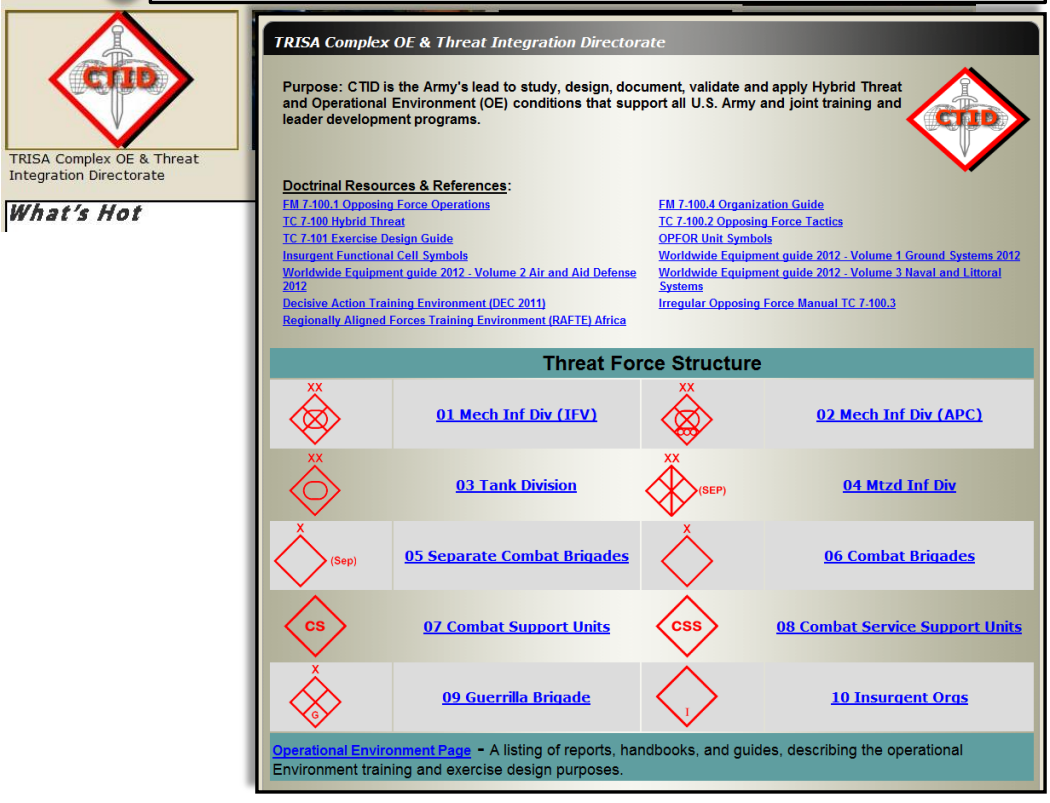
QUICK-EASY-EFFICIENT" = TWO "*CLICKS*" TO TRISA-CTID PRODUCTS

Go to Army Training Network

1 **Go to https://atn.army.mil/ with DOD-Approved Login = *Only 2 Clicks!***



2 **Click CTID icon = *You are at the CTID Products!***



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*

RAFTE-Africa *Regionally Aligned Forces Training Environment*

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

COMING in 2013:

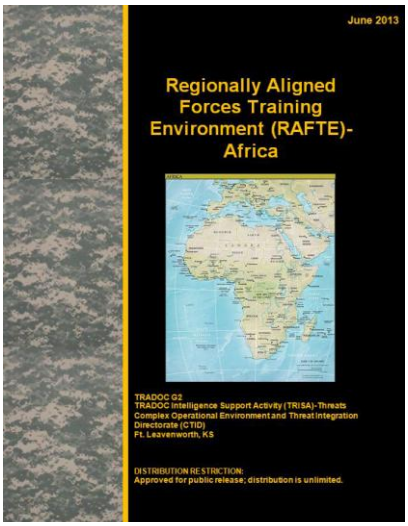
TC 7-100.3 *Irregular Opposing Forces*

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

For documents produced by TRISA's Complex Operational Environment and Threat Integration Directorate (CTID) of US Army TRADOC G2, with DOD-Approved Certificate Login access, see **https://atn.army.mil/**.

Q: *Do you need a copy of the Regionally Aligned Forces Training Environment-AFRICA?*

A: *With AKO access, see* **RAFTE-Africa**
https://www.us.army.mil/suite/doc/40395392



Q: *Where do I go to e-retrieve TC 7-100.2, Opposing Force Tactics?*

A: *With AKO access, see*
https://www.us.army.mil/suite/files/30894352

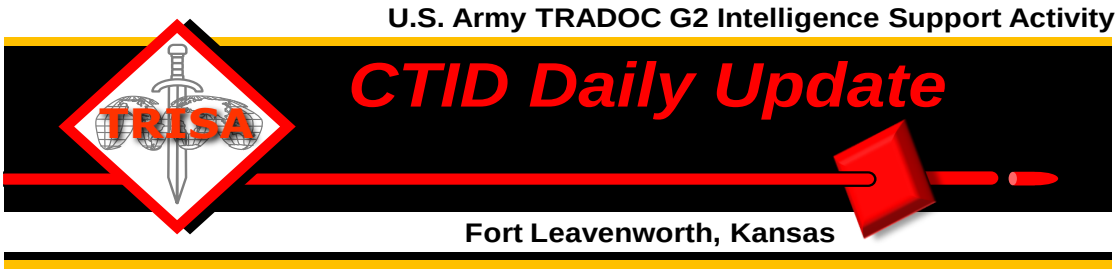
Q: *Do you have a question on a Threat or Opposing Force (OPFOR) issue that CTID can assist you with in identifying a solution?*

A: *Send TRISA-CTID a request for information (RFI).*

THREATS TO KNOW—*CTID DAILY UPDATE* REVIEW

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

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



November 2013 list for Red Diamond:

01 November: **Al-Qaeda:** Syria becomes largest home to al-Qaeda; jihadists find safe haven to plot attacks

Pakistan: Pakistan Taliban chief killed in US drone attack: Report

04 November: **Syria:** Iran Guards commander killed in Syria

Mediterranean Sea: Russia's 'aircraft carrier killer' Varyag and battle cruiser Pyotr Veliky arrive in Mediterranean

06 November: **Syria:** 16 killed, 90+ wounded in double bombing in Damascus

China: One killed, eight wounded after explosions rock Communist Party offices in Taiyun, Shanxi

13 November: **Afghanistan:** 37 Taliban militants killed, 17 injured in Afghan operations

Philippines: At least 2,275 people reportedly died in hurricane

15 November: **Syria:** Syrian army deploying forces along border near Lebanon's Beqaa Valley

Nigeria: 26 killed in Boko Haram night raids on Borno villages

18 November: **US:** Storms sweep across Midwest, six dead in Illinois

Colombia: FARC attack leaves 20 homes destroyed on Colombia - Ecuador border

20 November: **Al-Qaeda:** US drones kill three AQAP fighters in Yemen airstrike

Lebanon: Two blasts target Iranian Embassy in Beirut, killing Iranian cultural attaché and 22 others

22 November: **Brazil:** 1.4 million cases of dengue, 573 deaths

Middle East: The Saudis, Iran and the spreading Islamic Cold War in the Middle East

25 November: **Cyber security:** North Korea's "world class" cyber attacks coming from China

East China Sea: China bolsters East China Sea claim, warns of 'defensive measures'

CTID Points of Contact

Director, CTID	Mr Jon Cleaves jon.s.cleaves.civ@mail.mil	DSN: 552 913.684.7975
Deputy Director, CTID	Ms Penny Mellies penny.l.mellies.civ@mail.mil	684.7920
Liaison Officer (UK) [pending arrival]		
Operations -CTID	Dr Jon Moilanen jon.h.moilanen.ctr@mail.mil	BMA 684.7928
Threat Assessment Team Leader Mr Jerry England	684.7960 jerry.j.england.civ@mail.mil	
Threat Assessment Team	Ms Steffany Trofino steffany.a.trofino.civ@mail.mil	684.7960
Threat Assessment Team	Mrs Jennifer Dunn jennifer.v.dunn.civ@mail.mil	684.7962
Threat Assessment Team	Mr Kris Lechowicz kristin.d.lechowicz.civ@mail.mil	684.7922
Worldwide Equipment Guide	Mr John Cantin john.m.cantin.ctr@mail.mil	BMA 684.7952
Train-Educ-Ldr Dev Team Leader Mr Walt Williams	684.7923 walter.l.williams112.civ@mail.mil	
TELD Team/RAF LNO	CPT Ari Fisher ari.d.fisher.mil@mail.mil	684.7939
TELD Team/JRTC LNO	Mr Marc Williams ISC james.m.williams257.ctr@mail.mil	684.7943
TELD Team/NTC-JMRC LNO	Mr Mike Spight michael.g.spight.ctr@mail.mil	ISC 684.7974
TELD/MCTP LNO	Mr Pat Madden BMA patrick.m.madden16.ctr@mail.mil	684.7997
OE Assessment Tm Leader Mrs Angela Wilkins	BMA 684.7929 angela.m.wilkins7.ctr@mail.mil	
OE Assessment Team	Mrs Laura Deatrick laura.m.deatrick.ctr@mail.mil	ISC 684.7925
OE Assessment Team	Mr H. David Pendleton henry.d.pendleton.ctr@mail.mil	ISC 684.7946
OE Assessment Team	Mr Rick Burns richard.b.burns4.ctr@mail.mil	BMA 684.7897
OE Assessment Team	Dr Jim Bird james.r.bird.ctr@mail.mil	Overwatch 684.7919

CTID Mission

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

What We Do for YOU

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

YOUR Easy e-Access Resource

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