



Red Diamond

Complex Operational Environment and Threat Integration Directorate

Fort Leavenworth, KS Volume 4, Issue 4 APR 2013

INSIDE THIS ISSUE

Wargaming	4
Ambush TTP	6
Fiber Optic Cables...	8
OE Yemen.....	12
Gas Plant Attack	13
ATN Resource	15
PK Machine Guns ..	19
Raid TTP	22

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



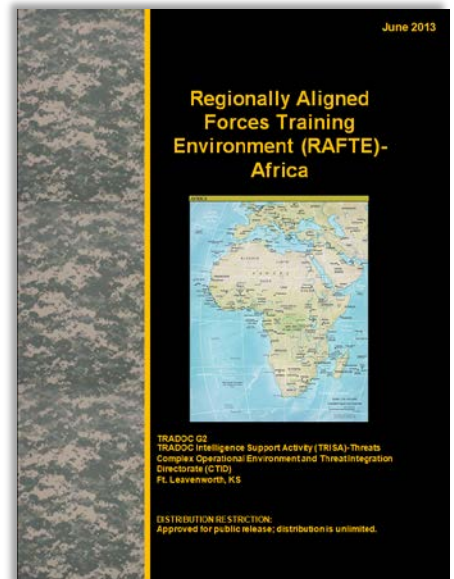
REGIONALLY ALIGNED FORCES TRAINING ENVIRONMENT (RAFTE)–COMING IN JUNE 2013!

by Angela Wilkins, OE Assessment Team Leader (BMA Ctr)

TRISA CTID will release the first supplement to the [Decisive Action Training Environment \(DATE\)](#) intended to train Regionally Aligned Forces (RAF) in June 2013. The supplement, designed to be used with *DATE*, is titled *Regionally Aligned Forces Training Environment (RAFTE)-Africa*. While this RAFTE's focus is Africa, RAFTEs may be developed for other regions pending future guidance.

RAFTE-Africa has two sections to serve the RAF training community. Section 1 identifies conditions that exist unique to an African operational environment (OE) that were not captured as part of the composite of real-world conditions in *DATE*. Section 2 names conditions already present in *DATE* that would not be encountered in an African OE. Trainers can save time by not developing training scenarios for RAF Africa training based on the conditions in Section 2.

CTID analysts designed Section 1 of *RAFTE-Africa* to be user friendly. Each African-OE unique condition is identified and defined. A brief explanation follows describing how or where the real-world condition is present in Africa. Then, a possible course of action for inserting the condition into the existing *DATE* is explained in detail. It's important to understand that the condition can be implemented more than one way, but we provided an option as an example. If the method provided doesn't work for specific training objectives, it can be changed. Finally, in some cases, related Events (See [DATE, Section 3: Events](#)) follow to further exemplify the effects of the presence of the condition for training, and each Event is tied to the Mission Essential Task List (METL).



RED DIAMOND TOPICS OF INTEREST

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

This issue of the **TRISA Red Diamond** introduces a series of articles on the training support of the TRISA Wargaming, Experimentation, Test, and Evaluation Directorate (WETED). Highly trained experts in threat emulation, current doctrine, and threat TTP are being used to stress Army leaders as they consider equipment, force design, and training options for the near and long term.

Other articles include potential threats to undersea fiber optic cables, operational environment assessments on Yemen, recent developments in a series of general purpose machine guns, and a modern armored infantry fighting vehicle.

Threat tactics, techniques, and procedures (TTP) employed in recent insurgent ambushes or raids include insurgents in Myanmar (Burma) disrupting enemy land transportation routes in their insurgent area of operations. North African insurgents raided a gas plant with an ambush on local land transportation, and seizure, murder, and hostage-taking of plant workers.

Another TTP by a small insurgent cell in Syria included a dismounted raid on a tank platoon. Basic tactics in reconnaissance, surprise, and violent execution of an

assault resulted in successful raid of a tank platoon defensive position. Similar TTP are being incorporated into **Training Circular 7-100.3, Irregular Opposing Forces**, to be published in 2013.

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

and

Mrs. Angela M. Wilkins, Chief Editor, BMA CTR
angela.m.wilkins7.ctr@mail.mil

TC 7-100.3
Irregular Opposing Forces
TC 7-100.3 Coming Soon!
HEADQUARTERS
DEPARTMENT OF THE ARMY

WE are at WAR!
...on TERROR

Trained
Ready
Adaptive
Decisive

Access AKO with password
<https://us.army.mil/suite/doc/30837459>

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

Know the Threat - Know the Enemy

Complex Threat

TRISA
Complex Operational Environment
and Threat Integration Directorate

TRISA WOT Poster No. 07-13
U.S. Army TRADOC
G2 Intelligence Support Activity
(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

The front page announcement of this TRISA *Red Diamond* on *Regionally Aligned Force Training Environment (RAFTE)-Africa* spotlights the next significant phase of TRADOC G2 training support as a follow-on to the *Decisive Action Training Environment (DATE)*. With the U.S. Army accepting *DATE* as a primary source-tool for **conditions** related to tasks and standards of performance, a *RAFTE* [pronounced “raft”] is an adaptable source of **conditions** in a particular region for training readiness. The *DATE* and a *RAFTE* are a companion set and require tandem use to achieve an effective outcome.

The *RAFTE-Africa* provides the Army training community and unit commanders with the complex and dynamic conditions for an African operational environment (OE). The *RAFTE-Africa* identifies conditions to be present in an African OE that are not already present in the *DATE*, and notes conditions in the *DATE* that are not applicable to an African OE.

To use *RAFTE-Africa*, commanders must first understand the *Decisive Action Training Environment (DATE)* as the U.S. Army’s baseline conditions document for training events that range from Combat Training Center (CTC) rotations to individual home station training (HST) events. The *RAFTE-Africa* is flexible, scalable, and adaptable to a unit commander’s partnering and training objectives and U.S. Army support to bilateral and multinational military exercises in Africa.

Implementing the Regionally Aligned Force (RAF) concept fully will take several years to complete. As the Army aligns brigades to support combatant command theater requirements, the Army Training and Doctrine Command G-2 will continue to incorporate contemporary conditions into the *DATE* and produce regionally focused *RAFTE* to support RAF brigades, Army Service Component Commands (ASCCs), and combatant commands (COCOMs) with **conditions** for continuity across the training and education communities in live, constructive, virtual, and gaming (LCVG) simulations. Conditions will accent leader development in the complex and dynamic nature of PMESII-PT variables--political, military, economic, social, information, infrastructure, physical environment, and time.

Jon

jon.s.cleaves.civ@mail.mil

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 LONG REACH OF TRISA-WETED

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

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



TRISA's Wargaming, Experimentation, Testing and Evaluation Directorate (WETED), on any given day, is engaged in all manner of activities in Army and even Joint labs, field sites, classrooms, and other venues. Highly trained experts in threat emulation, current doctrine, and threat TTP are being used to stress Army leaders as they consider equipment, force design, and training options for the near and long term.

Formed around 2002 as part of several TRADOC G2 initiatives aimed at providing "World Class" Red Teaming to the training base, deployed and deploying forces, and the testing and experimentation element, TRISA WETED is THE source of trained and ready opposing forces and leaders in those activities. Where applicable, the Red Forces are driven by the doctrinal provisions of the [FM/TC 7-100](#) series and other CTID products. It must be noted here that the connection between WETED and CTID under the TRISA umbrella is broad and deep; much Red success over time began with detailed CTID analysis of what potential adversaries can and will do.

The current TRISA WETED structure is austere but is fully capable of delivering on its chartered mission, all day every day. At this writing TRISA WETED, through its contracted "force provider," ThreatTec, LLC of Yorktown, Virginia is engaged in OPFOR missions at the following venues:

- ASAT (Advanced Situational Awareness Training), Fort Benning Maneuver Center of Excellence
- NIE (Network Integration Evaluation), Fort Bliss, Texas
- AEWE (Army Expeditionary Warfare Experiment), Fort Benning, Fort Sill, Fort Rucker, and others
- A Seminar Wargame for the Maneuver Center of Excellence, Fort Benning examining the R and S Brigade
- ARCIC (Army Capabilities Integration Center and Mission Command Battle Lab), Fort Eustis and Fort Leavenworth. It also conducts activities at the Army War College exercise facility at Carlisle Barracks, PA.

WETED Impact on Readiness

Each of the TRISA WETED sponsored and monitored venues is noteworthy in one or more aspects of what it does, how it got to be what it is, and its potential for future refinement. Some examples:

ASAT. Established at a long underused range facility at Fort Benning, the ASAT site is literally a living, breathing Middle Eastern village that confronts a Blue Force of up to platoon size with every conceivable challenge in developing a tactical situation. The site and its training value is now embedded in all junior officer and NCO leader development POIs at the MCOE and has recently been added to the training regimen of the USA Sniper School.



Figure 1. RPG gunners prepare for "Swarm" strike

NIE. Running at a field site deep in the Bliss/WSMR range area, this effort is a cooperative enterprise between TRISA WETED and those responsible for building the Army combat brigade of the future. Red Team Emulators and Cadre serve as the opposing force in field exercises by up to company-size formations conducted over long distances and multiple days in Major Combat Operations scenarios.

SPIRAL Technologies Experiments. These short-term, highly-focused experiments assess the utility and battlefield functionality of off-the-shelf equipment. Red Team subject matter experts provide insights and supervise OPFOR activities designed to stress the equipment and potential users in multiple dimensions.

JFEWE. TRISA WETED designated subject matter experts have typically served as “Red Force Commanders” and simulation interface operators in a series of experiments at Forts Benning, Leavenworth, Sill, Rucker, Huachuca, and others. In every case, the rigor and reality of the opposing force TTP have provided the Army with extremely valuable insights and data as it prepares itself for the challenges to come in 2020 and beyond.

Unified Quest. For many years TRISA WETED has provided the OPFOR planners and “commanders” for the CSA’s primary annual force development and national military strategy exercise. Every year the findings cite lessons and insights derived from Red activities that have served and will serve to save precious lives and resources for the Nation’s Army.

The way ahead for TRISA WETED is filled with challenges as the many elements adapt to the needs of an Army facing ever evolving threats, a daunting but not unprecedented constraint on resources, and even some reasons to relearn some eroded training management processes and techniques. The embedded subject matter expert group is likely to be heavily engaged in assisting with all of the above as the Emulators and OPFOR Cadre evolve to become the “new and improved” Red Team.

Wherever and whenever the Red Team is engaged, there are several long established and often validated (GAMOA, JFE, UQ, AEWE Spiral, etc.) TTP that serve to confound BLUFOR success. Some of those TTP are referred to as the “Dirty Dozen:”

WETED “Dirty Dozen”

1. NEVER cede access to BLUFOR units. Contest every inch of ground if only by ensuring friendly civilian populations are complicating use of routes and “ports.” A little counter-mobility goes a long way in halting BLUFOR momentum before it gets started.

2. Consider MSRs, LOCs, and FOBs as opportunities for selective application of fires and other effects. The “Disruption Zone” fight is a constant.

3. NEVER let BLUFOR dictate where and when main forces do battle.

4. Use decoys, spoofing, deception, civilian masking, humanitarian activities, and protected sites for every advantage.

5. Use highly decentralized command and control (C2) mechanisms to ensure continuity of operations and to confound BLUFOR ISR.

6. Develop and selectively apply “swarms” of relatively low tech, high impact weapons, tactics, and fires at BLUFOR high value C2 and logistics targets.

7. Use information operations to every advantage. If BLUFOR claims success in any dimension, find ways to turn it into a “lie or delusion.”

8. If available (it almost always is available in some form!) maintain the “WMD option” at all costs.

9. Target soft BLUFOR and BLUFOR Coalition homeland targets relentlessly.

10. Use NGOs and international organizations as “sympathetic” targets for information operations.

11. UASs and UAVs are increasingly available to Red Forces. They are easily procured, very effective as ISR tools, and turn BLUFOR air superiority into a myth. They can also be used as in the attacking swarms described in #6 above.

12. The BLUFOR is casualty averse. Every dead member of the BLUFOR is “Headline News.” A BLUFOR strike that kills sympathetic Red civilians is “Breaking News.”

WETED

Note. Future issues of the *Red Diamond* will provide updates and emerging insights and observations from TRISA WETED’s many ongoing activities. Stay tuned!

KACHIN INDEPENDENCE ARMY'S AMBUSH TTP

Irregular Forces in an Insurgency

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

In June 2011, after a seventeen-year ceasefire, the Kachin Independence Army (KIA) resumed fighting against the government of Burma. While the two sides have since stopped active combat actions against each other, the KIA and the Burmese government have not yet reached a ceasefire agreement. The Threat Report, [Kachin Independence Army \(KIA\)](#), not only examines the insurgent group's tactics, techniques, and procedures (TTP), but informs the Army training community of one of the largest insurgent groups in Burma. The Threat Report also provides a short history of the ethnic division within the country and the status of the other insurgencies within Burma.

While the KIA uses many of the same TTP as insurgent groups in other parts of the world, the two examples in the Threat Report involve an ambush of a moving target and the destruction of bridges to prevent the advance of government troops along a high-speed avenue of approach. The Threat Report makes use of several diagrams like the one below to demonstrate KIA TTP. Other insurgent TTP can be found in the [TRISA G2 Handbook No. 1.07 C3](#), *A Soldier's Primer to Terrorism TTP: Tactics, Techniques, and Procedures in Complex Operational Environments*.

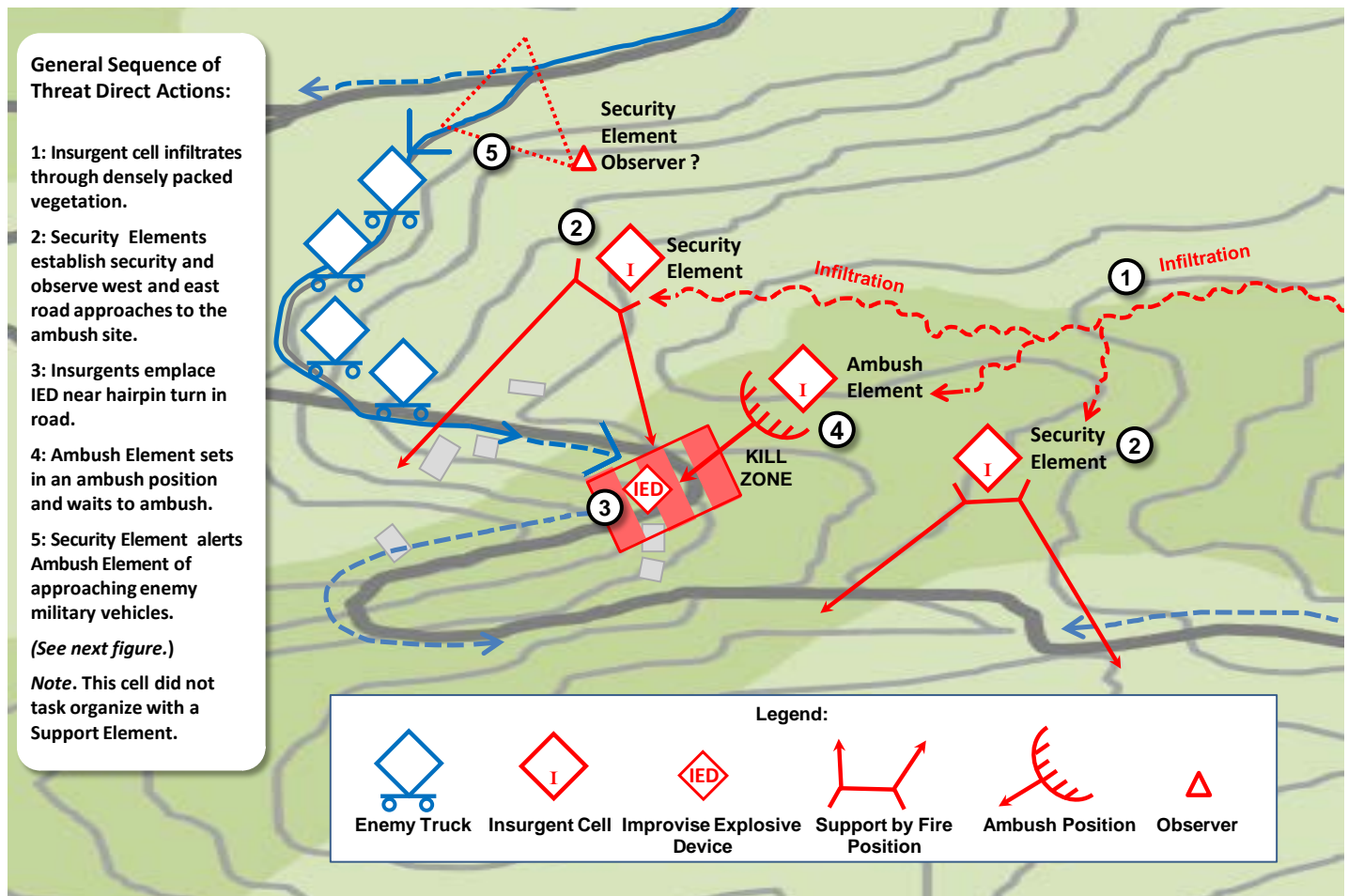


Figure 1 of 2. Setting an ambush for truck convoy

SUBMARINE FIBER OPTIC CABLES

Asymmetric Approaches in an Operational Environment

by Penny L. Mellies, CTID Deputy Director (DAC)

A recent article by Alexandra Chang in *Wired* magazine focused on the vulnerabilities of undersea (submarine) fiber optic cables, which provide most of the world's digital connectivity. Chang specifically wrote of these cables' susceptibility to attacks by terrorists, who know that damaging the undersea cable framework would significantly hinder telecommunications and data transfer.

Currently nearly 200 undersea fiber optic cables make up this maze of global connectivity.¹ Loss of just one of these cables – whether intentionally or unintentionally disrupted or damaged – can dramatically slow down or completely cut off a country's or region's access. A 2002 RAND study called these cables “a critical element” of most countries' access to global information infrastructure.² Like *Wired*, RAND's study postulated that the significance of these cables “could conceivably make them a potential target or target for other states or terrorists.”³

Given the world's dependency on this transoceanic information infrastructure, it is important to not only understand the components of the system, but to evaluate just how vulnerable to attack these deep undersea cables actually are. The *Wired* article suggests that due to poor monitoring and lack of basic security, these cables resting deep on the ocean floor are vulnerable to sabotage and potential terrorist attacks. A conceivable target does not necessarily equal a probable target, though. A closer look at the undersea or submarine cable networks reveals that there may be more tempting targets than the cables themselves. No matter which element of the system proves to be most vulnerable, any analysis of an operational environment (OE) should include a detailed discussion of these cables and their associated landing stations.

History

The first transoceanic fiber optic cable was installed in 1988 between the US and Europe.⁴ By the mid 1990s, the demand for increased communications bandwidth was taxing the capabilities of satellites. Industries and governments looked with increasing interest to undersea fiber optic cable as an alternative to satellites. Not only was it cheaper to use fiber optic cables, but the cables carried a significantly higher volume of data and provided a higher degree of data security.⁵ By 2000, undersea cable use had grown to 80% of all transoceanic data and voice transmissions.⁶ Current estimates indicate that over 95% of all US transoceanic communications travel across undersea fiber optic cables.⁷ Undersea fiber optic cables have become the backbone of the US's and the world's global information infrastructure.

Components of an Undersea Fiber Optic Cable Network

In order to gauge the probability of an attack, and thus the vulnerability of undersea cables, it is important to understand the key components of the system. For the purposes of this discussion, the four key components are identified as the *Undersea Cables*, the *Landing Trenches or Termination Points*, the *Landing Stations*, and *Carrier Houses/Data Centers*. There are other components farther inland that are connected to this infrastructure, but these present the greatest level of vulnerability.

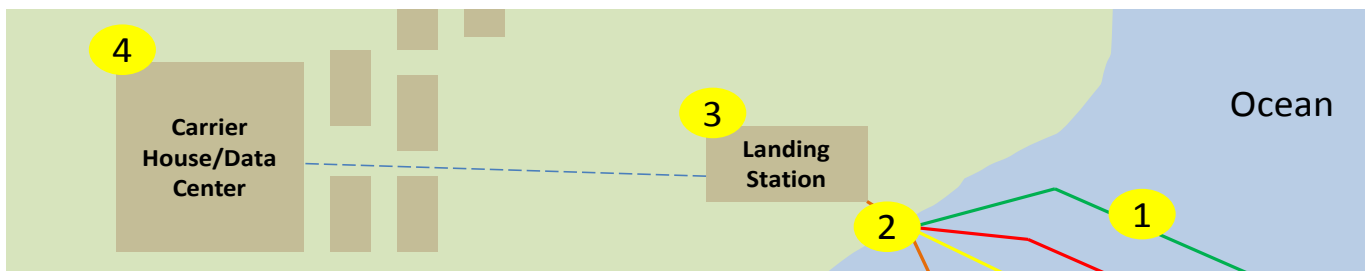


Figure 1. Basic components of undersea fiber optic cable network

1. *Undersea Cables* – Up to 150 small fiber optic lines are contained in each undersea cable, which provides a water-tight barrier made of layers of petroleum jelly, copper or aluminum tubing, polycarbonate, an additional layer of aluminum, stranded steel wires, mylar tape, and polyethylene. Though they vary in size, the cables typically range from 1.5 to 2.5 inches in diameter. Typically, cables resting closer to shore tend to be larger due to extra layers of galvanized wire to protect the fiber optic strands. Each cable provides up to several terabits of capacity.⁸ For example, one cable connecting the US and the UK typically carries 3.2 terabits of data per second, which means that a journey of 7,600 miles takes only 0.00072 seconds to complete.⁹

Placing the cables on the ocean floor requires equipment to dig trenches in the ocean floor and specialized cable-laying ships to feed the cable into trenches of varying depth. Cables far from shore are typically placed at a depth of a few feet, while cables closer to shore can reach a depth of 30 feet or more.¹⁰ This is done as a protective measure against coastal erosion, fishing entanglements, human tampering, and maritime traffic. The greater burial depth close to shore makes it more difficult – although not impossible – to conduct a disruptive or damaging physical attack against the cable.

Cables placed miles off shore are obviously harder to reach in terms of both the required diving capabilities and skills as well as the transportation and sensor equipment needed to locate the cables. In the future, remotely piloted undersea vehicles might help overcome some workability issues, but such capabilities will most likely remain only an option for more sophisticated state actors in the near term. Although terrorist groups could conceivably obtain such capabilities in the future, the cable networks offer more vulnerable elements in the present: the three network components closer to shore. The Landing Trenches or Termination Points, Landing Stations, or the Carrier Houses/Data Centers may provide ease-of-access vulnerabilities that the cables themselves do not. Even so, as the sampling of disruptive events below indicates, undersea cables are most vulnerable to natural phenomena and accidental disturbances, rather than intentional acts of destruction.

2. *Landing Trenches/Termination Points* – Cables approach the shore in a trench reaching a termination point. Many cable companies use the same location as a cost-saving measure as well as ease of access to the landing station. These tunnels are dug into the shore and many times contain multiple cables, effectively creating a choke point. Such choke points could present a target of opportunity for those seeking to strike multiple lines. Physical destruction attacks against sites could have major impact the undersea cable network. Locations of termination points and associated cables can easily be found on a variety of Internet sites and in industry literature. TeleGeography, a telecommunications and market research firm, has produced a free [interactive submarine cable map](#) listing each submarine cable and pin-pointing landing stations. Potential adversaries can easily locate this information and use it to plan for an attack. While not a terrorist attack, the April 2011 event discussed below highlights the ease at which such an attack can and has occurred.

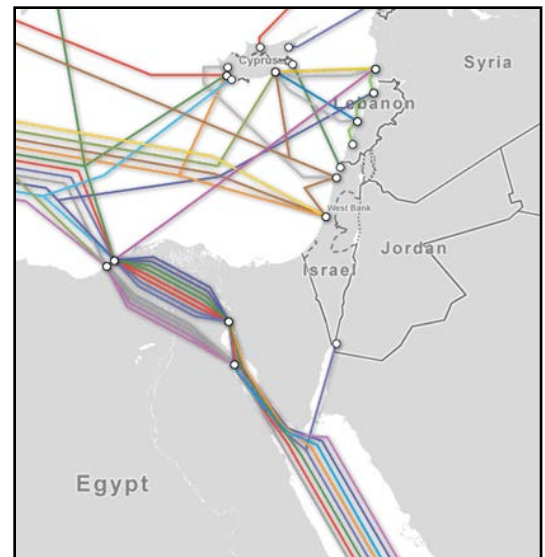


Figure 2: Screen shot of TeleGeography's interactive submarine cable map

Note. See the potential cable choke point in the Middle East.

3. *Landing Stations* – Landing stations receive and collect the information from the fiber optic cables and transmit the data to Carrier Houses/Data Centers farther inland. While some landing stations have begun increasing security measures, most remain relatively unsecured. And, as previously mentioned, many landing stations serve multiple cables, rendering them easy and lucrative targets. For example, the landing station in Manasquan, New Jersey has six associated cables. Staging an attack against such landing station could effectively damage multiple cables and impact a wide region, if not the entire coast. It would be relatively easy for a terrorist organization to stage an attack at such a landing station.
4. *Carrier House/Data Center* – Data moves from the landing station to Carrier Houses/Data Centers farther inland. From here it is routed to other networks and distributed across long distances. Carrier Houses/Data Centers are typically located in key populations centers. These facilities are also potentially the most lucrative targets in the network. Attacks against these centers would likely have the most-widely felt impact as data centers serve as major hubs of data from various landing stations. A well placed bomb, mortar, or rocket attack could shut down large swaths of a country's information infrastructure.

Disruptive Events

Despite the fact that the networks of cables are designed to be robust, resistant, and at times redundant, disruption of data flows has occurred and will likely continue to occur. A single ship dropping its anchor in the wrong place can cause millions to lose data and voice transmission capabilities. Current research indicates that about 200 cable disruptions occur each year, the vast majorities (77%) of which are caused by fishing accidents or misplaced anchor drops.¹¹ The following list of events highlights the range, type, and location of some of the attacks. This list is not all-inclusive, but shows the range of potential disruptions.

Natural Disaster – Taiwan (December 2006): An earthquake in the Luzon Strait damaged several cables, cutting off communication to Hong Kong, Southeast Asia, and China.¹² The earthquake caused submarine landslides resulting in the fracture of nine cables. Repair took multiple ships and lasted for close to 50 days.¹³

Confirmed Theft – Vietnam (March 2007): Several Vietnamese pirates cut two cables in search of copper.

Unknown cause, possible theft or anchor drop – Egypt (December 2008): Three fiber optic cables were damaged in the Mediterranean Sea off the coast of Alexandria, Egypt. Data flows between Europe and the Middle East were severed. Egypt, India, Pakistan, and Kuwait were left cut off from Internet traffic. While no clear understanding of what caused the damage was ever published, one report indicated the possibility of attack to harvest copper.¹⁴ Some speculate a stray anchor. The three cables carried 75% of all the traffic between the Middle East, Europe, and the US. According to one news report at the time of the event, “55% of voice traffic in Saudi Arabia, 52% in Egypt and 82% in India was out of service.”¹⁵

Unknown cause – Dubai (February 2008): One cable was cut 50 km off the coast of Dubai.¹⁶ Traffic flows from India to Egypt were slowed, and no official statement as to the cause of the event was released.

Unconfirmed, one source states a terrorist attack – Philippines (June 2010): In June 2010, terrorists in the Philippines hit a cable landing station.¹⁷ The attack was on a manhole close to the landing station and not the cable. No information is available on the extent of communication disruption that occurred as a result.

Confirmed theft – Georgia (April 2011): A Georgian woman attempting to scavenge copper along the coast by Tbilisi cut through a cable, resulting in most of Armenia losing access to the Internet. Georgia provides close to 90% of Armenia's Internet connectivity. Areas of Georgia and Azerbaijan also lost connectivity.¹⁸

Confirmed anchor – Kenya (February 2012): A stray anchor drop cut Internet access to wide areas of Kenya, Rwanda, Burundi, Tanzania, Ethiopia, and South Sudan.¹⁹ The responsible ship was waiting to enter the port of Mombasa when it entered a restricted area and hit the cable.

Unknown cause – Australia and Singapore (January 2013): The SEA-ME-WE-3 cable linking Australia and Singapore was damaged. Reports indicate that the cable was severed.²⁰

Unknown cause, possible theft – Egypt (March 2013): News reports claim a disruptive attack by three divers who were subsequently arrested by the Egyptian Navy. Reports claim that the three were found trying to cut an undersea cable near the Alexandria. The cable was identified as the SEA-ME-WE-4. This cable is one of eight that links Egypt to Europe. It also carries data and voice among 14 countries – Egypt, Algeria, Tunisia, India, Italy, Singapore, Malaysia, Thailand, Bangladesh, Sri Lanka, Pakistan, the United Arab Emirates, Saudi Arabia, and France.²¹ Reasons for the attack are unknown. Seacom, the undersea cabling company involved in the incident, issued a press release on 27 March 2013 which stated, “We think it is unlikely that the damage to our system was caused by sabotage. The reasons for conclusion are the specific location, distance from the shore, much greater depth, the presence of a large anchored vessel on the fault site, which appears to be the cause of the damage and other characteristics of the event.”²² The Egyptian military has not commented further on the event.

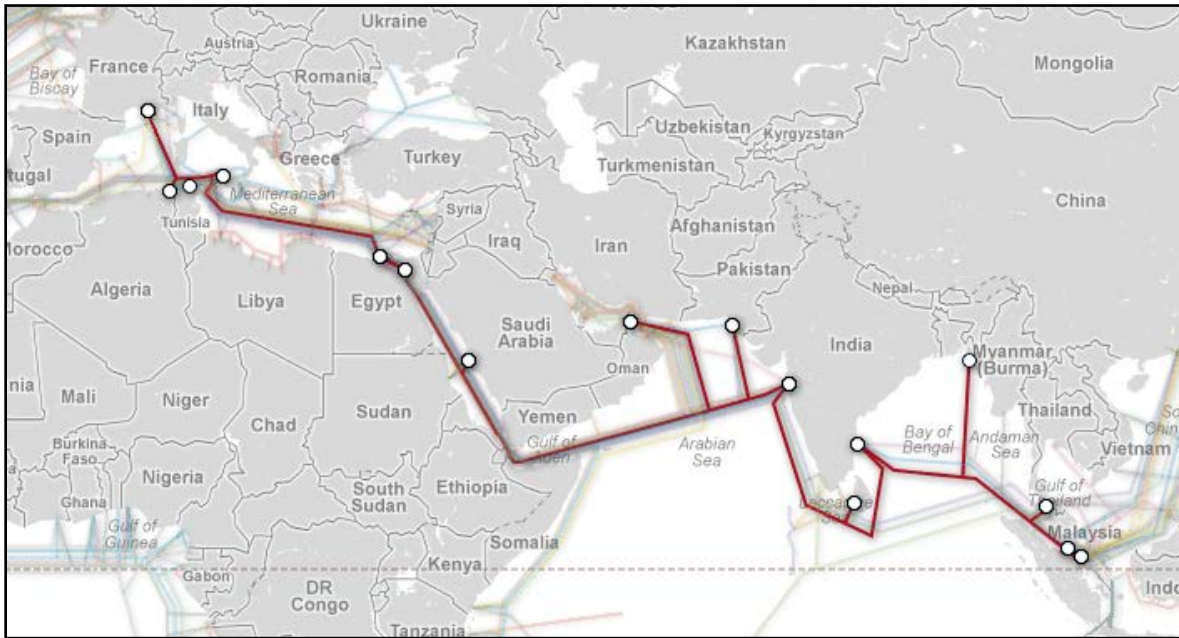


Figure 3: Path of the SEA-ME-WE-4 cable from TeleGeography’s interactive submarine cable map

As the disruptive events above show, cables have been damaged or disrupted by a range of actors with a range of motivations. Natural disasters, individuals seeking cash-generating materials, sailors dropping an anchor in the wrong place and a terrorist seeking to cripple a landing station have all helped to reveal the importance and vulnerability of these undersea fiber optic cables and their land-based infrastructure. Yet, despite this range, the majority of cable disruptions are caused by human accidents.²³ Despite the obstacles to attacking the cables, the threats and their potential and capability to target other sections of the network must be better understood and evaluated. While it is unlikely to see terror groups employing scuba divers to strategically attack a deep-sea fiber optic cable, other elements of the network are vulnerable to attack and would create both the physical destruction effects and perception management storylines sought by many terrorist organizations. Current and future potential adversaries could potentially stage attacks, most likely targeting landing stations or carrier houses/data centers. Therefore, the analysis of any potential OE should include a detailed discussion of this critical form of information infrastructure.

Endnotes

¹ Alexandra Chang, “[Why Undersea Internet Cables Are More Vulnerable Than You Think](#),” *Wired*, April 2013.

² RAND, “[A Concept of Operations for a New Deep-Diving Submarine](#), 2002.

³ RAND, “[A Concept of Operations for a New Deep-Diving Submarine](#), 2002.

⁴ International Protection Committee, [Submarine Cable Network Security](#), 13 April 2009.

⁵ Douglas Burnett, “Cable Vision,” Proceedings, 2011.

⁶ RAND, “[A Concept of Operations for a New Deep-Diving Submarine](#), 2002.

- ⁷ International Protection Committee, [Submarine Cable Network Security](#), 13 April 2009; Douglas Burnett, "Cable Vision," Proceedings, US Naval Institute, 2011.
- ⁸ Mail Online, ["The Deep Web: Incredible new map of the Undersea Cables that keep 99% per cent of the world clicking."](#)
- ⁹ Mail Online, ["The Deep Web: Incredible new map of the Undersea Cables that keep 99% per cent of the world clicking."](#)
- ¹⁰ eHow Online, ["How is Fiber Optic Cable Laid on the Ocean Floor?"](#)
- ¹¹ Douglas Burnett, "Cable Vision," Proceedings, US Naval Institute, 2011.
- ¹² Alexandra Chang, ["Why Undersea Internet Cables Are More Vulnerable Than You Think,"](#) *Wired*, April 2013.
- ¹³ International Protection Committee, [Submarine Cable Network Security](#), 13 April 2009.
- ¹⁴ Alexandra Chang, ["Why Undersea Internet Cables Are More Vulnerable Than You Think,"](#) *Wired*, April 2013.
- ¹⁵ Bloomberg, ["Severed Cables in Mediterranean Disrupt Communications \(Update 4\),"](#) 19 December 2008.
- ¹⁶ CNN.com, ["Third undersea Internet cable cut in Mideast,"](#) 1 February 2008.
- ¹⁷ Squire Sanders, ["The 1884 International Convention for Protection of Submarine Cables Provisions Not in UNCLOS Deserve Attention Now,"](#) Squire Sanders.
- ¹⁸ ["Georgian woman cuts off web access to whole of Armenia,"](#) *The Guardian*, 6 April 2011.
- ¹⁹ ["East Africa Internet access slows to a crawl after anchor snags cable,"](#) *The Guardian*, 28 February 2012.
- ²⁰ Itnews, ["Perth-Singapore cable severed,"](#) 15 Jan 2012.
- ²¹ ["Dude, what's wrong with my Internet speed?"](#) The Hindu.
- ²² ["Dude, what's wrong with my Internet speed?"](#) The Hindu.
- ²³ Seymour Shapiro, James Murray, Robert Gleason, Stuart Barnes, Brian Eales and Paul Woodward, "Cables," No date given.

OE THREAT ASSESSMENT SERIES: FOCUS ON YEMEN

Complex Operational Environments

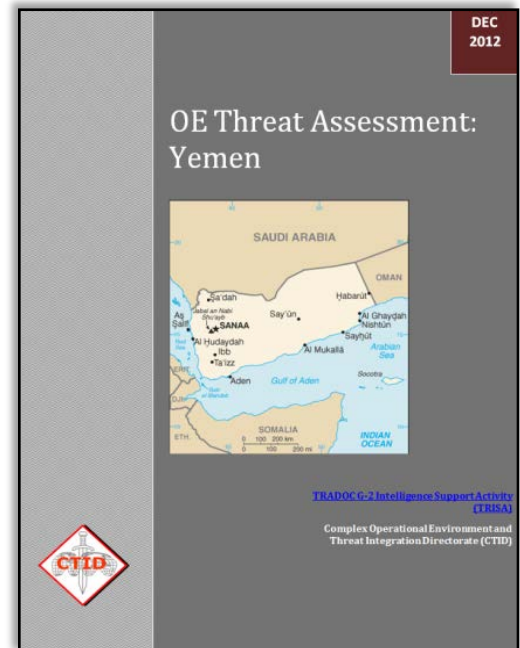
by Laura Deatrack, OE Assessment Team (ISC Ctr)

Yemen is a small but geographically important country in the Middle East. Several U.S. national security interests manifest in Yemen. Issues ranging from open access to the Bab el Mandeb strait, to exporting hydrocarbons to the U.S., to a direct threat posed by terrorist groups in Yemen could potentially challenge U.S. national security interests. In addition, the State has high incidents of human rights abuses, political instability, food insecurity, and high probability for terrorist acts that could trigger events leading to U.S. action in the OE. For Yemen, the most likely U.S. mission is counterterrorism.

Yemen is a republic headed by a president and assisted by a vice president. The president is the head of State while the prime minister is the head of the government and appoints members of the cabinet. The country has a bicameral parliament, with the president appointing members of the Shura Council and the people electing members of the House of Representatives.

Large protests broke out against President Saleh during the "Arab Spring" of 2010-2011 that he unsuccessfully attempted to quell by force. The UN and the Gulf Cooperative Countries (GCC) eventually stepped in and brokered a deal in which Saleh resigned and passed power to Vice President Hadi, and a new coalition government was formed.

The most pressing political issue in Yemen at present is the election scheduled for 2014. The election will be a litmus test for a country that verged on civil war in 2011. The coalition government also must deal with secessionist politics from the South where the country's major oil resources reside. Another dominant political issue is the restoration of stability in a country with a history of tension between North and South since the two regions united in 1990. Strife also exists between the majority Sunni and minority Shia populations and between different tribes, particularly important since



Yemeni tribal chiefs hold greater influence than the government. Terrorist organizations within Yemen are also a concern, drawing attention from the government as well as from other nations. The United States in particular is troubled by al-Qaeda elements in Yemen.



Yemen is seen as a safe haven for Muslim extremists and terrorists, prompting the U.S. and other key international players to concentrate on formulating strategies to help eradicate terrorism in the country. Many Yemenis consider the presence of U.S. unmanned aerial vehicles and counterterrorism officials to be intrusive; hence a contemptuous attitude toward the U.S. is prevalent.

Terrorist activities, civil unrest, and violent crime pose a danger to U.S. troops deployed to Yemen. The U.S. State Department assesses the security threat level in the country to be extremely high and encourages U.S. citizens to avoid the country.

Several attacks against U.S. citizens and interests have occurred during 2012, including two murders, one killing by AQAP, and a mob attack on the U.S. Embassy. Any U.S. forces present in the country would provide a highly desirable target for terrorists, insurgents, and criminal actors. Heightened anti-terrorism and force protection measures, such as those followed in Afghanistan and Iraq, would apply.

View the [OE Threat Assessment: Yemen](#) for more detail on all the PMESII-PT variables.

IN AMENAS, ALGERIA GAS PLANT ATTACK

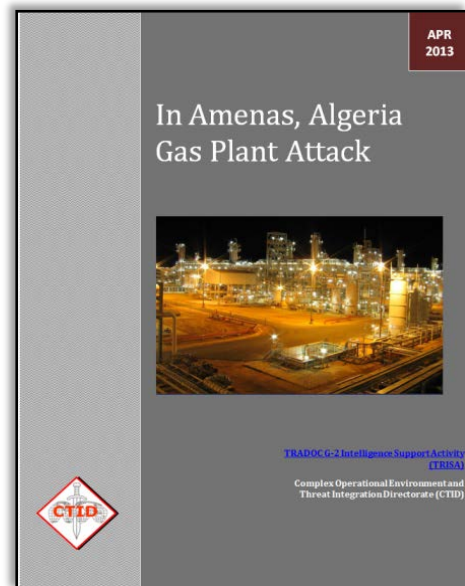
Irregular Force TTP in an Operational Environment

by Rick Burns, OE Assessment Team (BMA Ctr)

On the morning of 16 January 2013, thirty to forty terrorists affiliated with former al-Qaeda in the Islamic Maghreb (AQIM) member Mokhtar Belmokhtar attacked an oil and gas facility near the city of In Amenas, Algeria. This remote facility is close to the volatile Libyan border. The facility is jointly operated and serviced by British Petroleum, Norwegian-owned Statoil, the Algerian state oil company Sonatrach, and Japanese-owned JGC Corp. The In Amenas gas plant lies approximately 825 miles southeast of Algiers and 60 miles west of the Libyan border.

Mokhtar Belmokhtar claimed his new group, “Signers with Blood” (Muaqiin bil Dam), carried out the attack in response to the French intervention in Mali. The degree of planning and logistics required for this attack suggest that preparation began long before the French intervention in Mali the week before. Belmokhtar’s referral to the French intervention shows a skillful use of information operation targets of opportunity.

The attack on the 16th was multi-faceted and involved insider intelligence. The operation began with an attack on two buses carrying employees headed for the In Amenas airport. It is unclear whether this was part of the original plan or a target of opportunity. The



terrorists then divided into two teams; one occupied the residential camp (RC) and the second occupied the main gas plant (MGP). Operations at both sites involved searching for foreign employees with the likely intent of ransom, as Belmokhtar has a long history of kidnapping for ransom. The primary intent behind occupying the

MGP was to blow it up. The quick reaction of one of the employees in sounding the alarm in the initial moments of the attack allowed some employees to shut down the

flow of explosive gas through the plant, and others to hide. After sounding the crucial alarm, this employee was immediately killed.

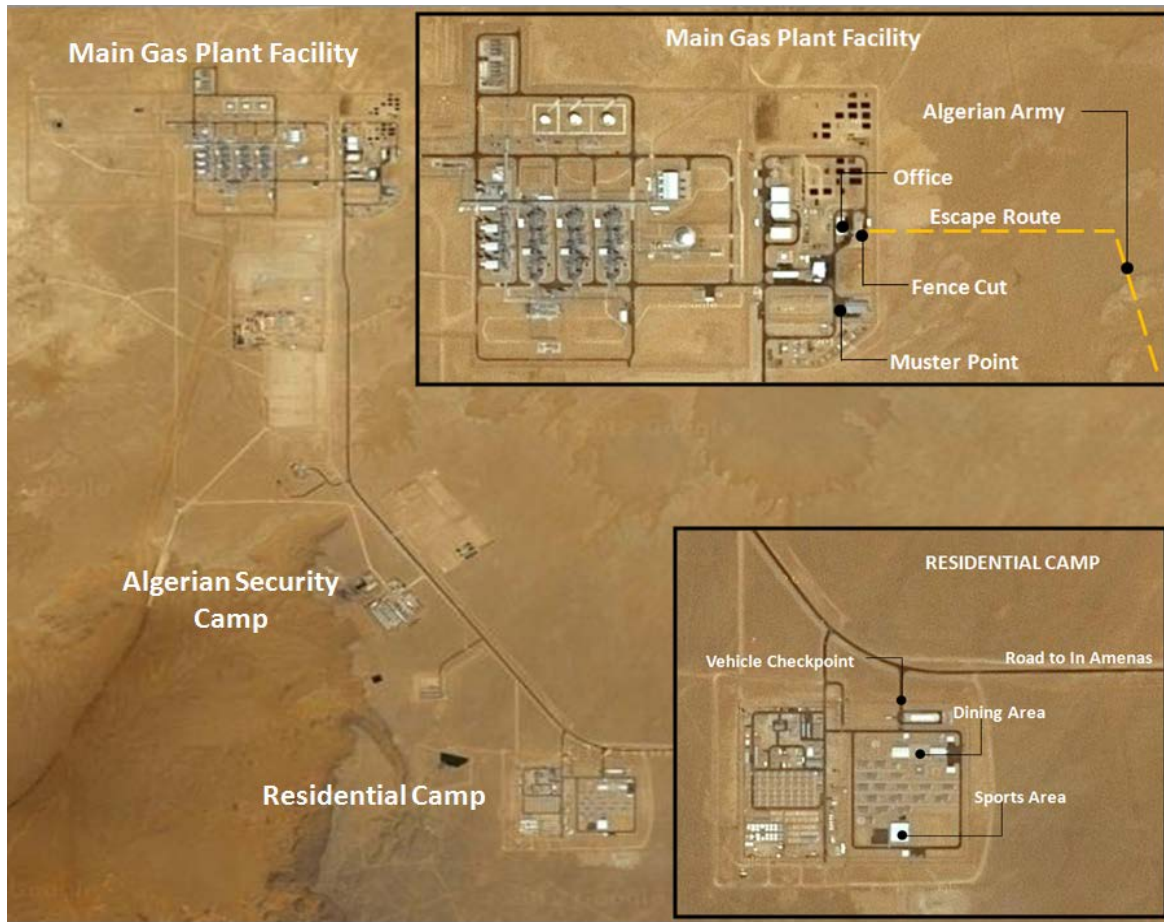


Figure 1. Modified maps of main gas plant facility and residential area, [Google Maps](#), 2013

Algerian security forces killed nearly all of the terrorists at both sites. On Thursday afternoon, 17 January 2013, terrorists at the RC loaded five vehicles with hostages and began movement. It is unclear whether the intent was to consolidate at the MGP or move the hostages to the group's base in northern Mali as hostages for ransom. When the Algerian military detected the movement, it sent in HIND helicopters to attack the convoy. All but one of the vehicles were destroyed and their occupants killed. On Saturday, 19 January 2013, Algerian Special Forces, believing the militants were going to kill the seven hostages they held, attempted to rescue the hostages. Eight of the terrorists were killed in the assault. The seven hostages, however, had been killed the night before. As many as three terrorists were captured alive.

The attack on the In Amenas facilities indicates insider intelligence, extensive planning, training, and logistics. At least one of the terrorists had worked at the plant, and eleven others are currently being investigated by the Algerian government for complicity. The plant will always suffer from a calculated vulnerability due to the large number of local

Algerians needed to make it function. The militants increased confusion by wearing uniforms and driving company-disguised vehicles. The ease of entry and the intimate knowledge of the layout of the plant aided them in quickly entering and rounding up hostages. The large number of explosive vests points to the fatalistic intent of the operation. The one flaw in their plan involved their inability to blow up the MGP. Quick and fatal actions by one employee allowed the plant to be shut down in a way that prevented the plant from being blown up.

While the tactical operation was a failure, Belmokhtar will reap strategic benefits from the attack. The immediate impact was that security costs and concerns immediately went up for similar plants in Algeria, Libya, and other remote areas of

Africa as each plant considered its current security protocols. The audacity of the attack will increase the prestige and narrative of Belmokhtar as a man of action, enhancing his ability to recruit for future operations. Although the attack had been planned for many months, Belmokhtar used the French invasion of northern Mali the week before as the reason for the attack. The French invasion gave a current, relevant, and substantive reason for the attack.

Countries with citizens being held hostage at the two sites expressed significant concern over the unilateral operations of the Algerian government and its security forces. Algeria, after a decade-long civil war, was determined to prove to terrorist organizations, and the world at large, its ability to act alone to repel terrorists. The Algerian security forces refused to negotiate with the terrorists and acted decisively when it appeared the militants were going to kill hostages. There were some complaints about the attack on the convoy containing hostages that resulted in all but a few plant employees killed. Either the militants were being moved to consolidate with the other force at the MGP or the hostages were being moved to Mali to be held for ransom. In either case, the bombs strapped to the hostages pointed to little hope that all would be allowed to live. From all accounts, it appears that the decisive actions of the Algerian security forces contributed to saving the lives of many of the hostages by decisively engaging and killing the terrorists.

For more details, please refer to the Threat Report, [In Amenas, Algeria Gas Plant Attack](#).

HYBRID THREATS ON THE ARMY TRAINING NETWORK

Training Readiness for Complex Operational Environments

by Jerry England, Threat Integration Directorate (TID) (DAC)

Complex Operational Environment and Threat Integration Directorate (CTID) has a new presence on the Army Training Network (ATN) Portal. The easy-to-use 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 for Home Station Training (HST).

New products are being developed, so it is a good idea to check the portal periodically for updates. A link that will direct users to the [Decisive Action Training Environment \(DATE\)](#) as well as a variety of Operational Environment Assessments (OEAs) and *Threat Reports* are scheduled to come online in the near future. Additionally, data for the *Regionally Aligned Force Training Environment (RAFTE)* will also be added.

Once CTID site is fully resources with Opposing Force (OPFOR) and Hybrid Threat references, Soldiers involved in planning and designing training exercises will have a one-stop shop from which to build Operational Environment conditions and a Hybrid Threat Order of Battle. This data will assist commanders in providing the realism and capabilities needed for a variety of training objectives.



Figure 1. [ATN main page](#)

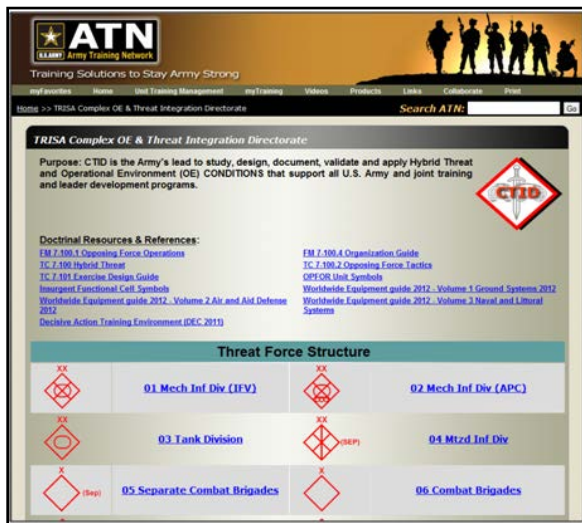


Figure 2. [TRISA CTID ATN page](#)

Note. Figure 2 illustrates the organization of OPFOR and Hybrid Threat with listings, military symbols, and descriptive text to present easy-to-find references. The illustration of Threat force structure section displays the initial major unit organizations such as—

- Mechanized infantry division (IFV).
- Mechanized infantry division (APC).
- Tank division.
- Separate combat brigade.
- Motorized infantry brigade.
- Combat brigades.

Several source documents are listed as part of the Army's *Opposing Force Program* as stated in AR 350-2.

HISTORY AND PROLIFERATION OF THE HIND HELICOPTER

Weapon Systems in an Operational Environment

by LTC Terry Howard, Training, Education, and Leader Development Team (TELD) (USAR)

The Mi-24 (NATO designation “Hind”) attack/transport helicopter is manufactured by the Mil Moscow Helicopter Plant in Moscow, Russia. It first entered service with the Soviet Union in 1979, and since that time more than 2,500 have been produced. The Hind has been used in numerous conflicts around the world, including 1979 Soviet war in Afghanistan. The original model, the Hind-A, was designed to carry eight combat troops, and was later reconfigured to take on the gunship role, the Hind-D.

The design of the Mi-24 is based on a conventional pod and boom, with a five-blade main rotor and three-blade tail rotor. It has retractable tricycle nose-wheel landing gear. The two crew members (pilot and weapons operator) are accommodated in a tandem armored cockpit with individual canopies and flat, bulletproof windshield. The main cabin can accommodate eight troops or four stretchers.

Later versions, Mi-24P and the exported Mi-35P, are also armed with anti-tank rocket systems for the engagement of armored targets, weapon emplacements, and slow-moving air targets.



Figure 1. Mi-24 “Hind-D” Helicopter in flight

Source: 2012 Edition of the [Worldwide Equipment Guide](#), Volume 2, Chapter 2, page 2-9

Later versions of the Mi-24P are armed with anti-tank missile systems. All versions retain the troop transport carrying capability.

The helicopter is powered by two Isotov TV3-117VMA turbo shaft engines, delivering 2,200 horsepower each. The air intakes are fitted with deflectors and separators to prevent dust particle intake when taking off from unprepared sites. An auxiliary power unit can also be fitted.

The internal fuel capacity is 1,500 kg, with an additional 1,000 kg in an auxiliary tank in the cabin or 1,200 kg on four external tanks. The fuel tank has a self-sealing

cover and porous fuel tank filler for increased survivability, and the exhaust is fitted with an infrared suppression system.

Avionics

The Mi-24D is equipped with the KPS-53A electro-optical sighting pod. The most recent Mi-24V and P variants have a digital PNK-24 avionics suite and multifunction LCD cockpit displays, and night-vision goggles, with an NVG compatible lighted cockpit. Both helicopters are fitted with the Urals Optical and Mechanical Plant GOES-342 TV/FLIR sighting system and a laser rangefinder. Countermeasures include infrared jammers, a radar warning system, and flare dispensers.

Weapons

The helicopter has six suspension weapon units on the wingtips. The Mi-24D (Mi-25) and the Mi-24V (Mi-35) are equipped with a four-barreled, 12.7-mm, built-in, flexible mounted machine gun, with a rate of fire of 4,000-4,500 rounds a minute. The Mi-24P is fitted with a 30-mm, built-in, fixed gun mount; the Mi-24VP with a 23-mm, built-in, flexible mounted gun.

The Mi-24P and Mi-24V have four under wing pylons for up to 12 antitank missiles. The Mi-24V (Mi-35) can be armed with the Shturm antitank guided rocket system. Shturm is a short-range rocket with a semi-automatic,

radio command guidance. The 5.4 kg high-explosive fragmentation warhead is capable of penetrating up to 650-mm of armor. Maximum range is 5 km.

The Mi-24V can also carry the longer-range Ataka antitank rocket system (NATO designation AT-9), as well as the Mi-24P. Maximum range of the rocket is 8 km. The average target range is between 3 and 6 km. The rocket has a shaped charge with 7.4 kg of explosives, with a tandem charge for penetration of up to 800-mm of armor. All Mi-24 helicopters can also be armed with rockets and grenade launchers.

Proliferation of the Hind helicopters

The Mi-24 is currently in service in Russia and countries of the ex-Soviet Union, and has been sold to other countries, including Afghanistan, Algeria, Angola, Bulgaria, Cuba, Czech Republic, Hungary, India, Indonesia, Iran, the Ivory Coast, Libya, Mozambique, Nicaragua, North Korea, Peru, Poland, Vietnam, South Yemen, and Venezuela. Because of the relatively low cost of the Mi-24, along with its lethal firepower and worldwide proliferation, the Hind will most likely be a favorite military helicopter in developing countries for the foreseeable future.

THE PUMA INFANTRY FIGHTING VEHICLE

Worldwide Equipment Guide (WEG) and Threats in Complex Operational Environments

by John Cantin, Threat Integration Team (BMA Ctr)

Germany recently decided to replace its ageing fleet of Marder 1 Infantry Fighting Vehicles (IFV) with the Puma Armored Infantry Fighting Vehicle (AIFV). Germany has ordered 405 new Pumas that will be integrated into the German Army. The Puma is air deployable and compatible with other armored systems and is designed to enable numerous modifications. This makes it a prime candidate for significant proliferation in the next several years. Britain, The Netherlands, Norway, Canada and the United States have expressed interest in the Puma or variants of it.

The Puma is a thirty-one ton tracked IFV with a crew of three that can transport six to eight troops, depending on configuration. It offers protection for the occupants from both mines and projectile charges from the ground, and when enhanced with add-on armor, can withstand mortar and artillery bomblets.

Additional armor can be installed to protect the tracks and top of the vehicle once it is off loaded from air transports. The additional armor makes the IFVs total weight approximately forty-three tons. The front glacis of the Puma is nearly flat, giving it protection against hollow charge rounds. The sides are protected against 14.5mm kinetic energy rounds and RPG-7 rocket propelled grenades.



Figure 1. [Infantry fighting vehicle Puma](#)

Source: Sonaz, Wikimedia Commons, April 2013,

The vehicle has three gas tanks that are mounted outside of the hull, installed in the running gear carriers and protected by heavy armor. The Puma also has an optical system that allows for 360 degree coverage and six zoom settings that are displayed to the entire crew. The optics system has laser range finders, thermal vision cameras, and an image intensifier. The main gun is a 30mm Mark 30-2 Auto Cannon that can fire 700 rounds per minute with a range of up to three kilometers. The main gun is augmented with a HK MG4 Machine Gun and two Euro-Spike LR Missile Launchers that can range out to four kilometers.



Figure 2. [Rheinmetall 30-mm MK 30-2/ABM \(air burst munitions\) autocannon](#)

Source: Sonaz, Wikimedia Commons, April 2013,

The crew occupies a single hull and the turret is an unmanned, double-asymmetrical turret that sits slightly off-center. The Puma's turret is on the left-hand side of the vehicle, while the main cannon is mounted on the right side of the turret and on the middle axis of the hull when the turret is in the forward position. Another feature is an NBC system, along with a fire suppression system.

The squad compartment can carry six to eight soldiers. This presents a problem for the U.S. Army, since the current Bradley IFV can hold nine troops, allowing for an entire squad to move on the battlefield in tandem. If the U.S. Army was to field the Puma, a platoon would have to go from four to five vehicles and the issue of squad integrity would have to be addressed.

The Puma appears to be another emerging IFV that will be mass produced, copied, and modified by threat and friendly forces. It was developed to be modular and can be modified to become a command vehicle, fire support platform, air defense platform, troop transport, and the like. As the reality of economics and budget constraints force militaries, insurgent groups and terrorist groups to acquire an IFV that can be inexpensively operated and maintained, the Puma may become one of the primary platforms for friendly and threat forces alike.

Specifications:

Weight: 31.5 tons (63,000 lbs), 43 tons (86,000 lbs) with add-on armor
 Length: 7.4 M (24.28 ft)
 Width: 3.7 M (when up armored), (12.14 ft)
 Height: 3.1 M (10.17 ft)
 Crew: 3 (Commander, Gunner, Driver) plus 6-8 troops
 Armor: Modular AMAP composite armor
 Main Armament: 30mm Mark 30-2/ABM autocannon
 400 rounds
 Secondary Armament: 5.56 mm HK MG4 machine gun,
 76mm grenade launcher, 2 x 4 smoke grenade launchers
 Engine: MTU V10 892 diesel, 800 kilowatts (1,110 hp) at 4250 rpm
 Suspension: Hydroneumatic
 Operational Range: 600km (373 miles)
 Speed 70 kilometers per hour (43 miles per hour)

References

Beacon, Lance. "Cost Cutting May Kill Ground Combat Vehicle." *Army Times*. 9 April 2013.
 Bertucca, Tony. "Army Contractors Come Out Swinging at CBO Report Questioning GCV." *InsideDefense.com*. 5 April 2013.
 Halcom, Chad. "Local Defense Contractors Question Data, Criteria Used In Critical CBO Report." *Crain's Detroit Business*. 5 April 2013.
 Puma IFV. [Military Today](#). 11 April 2013.

THE PK SERIES OF GENERAL PURPOSE MACHINE GUNS

Weapon in an Operational Environment

by Mike Spight, Training, Education, and Leader Development Team (TELD) (ISC Ctr)



Figure 1. CAMP YASSIR, AL ASAD, Iraq – Iraqi Army Soldiers spend a day at the range, firing the PK machine gun as part of the School of Infantry

Photo by: Cpl. Adam Johnston, [Photo ID: 2007442010](#), Submitting Unit: 2nd Marine Division

There is little doubt that Germany's work in firearms development prior to and during WW2 has and continues to influence the development of military small arms in both the latter half of the 20th century and well into the 21st century. This influence can be seen in weapons designed in both the former Soviet Union and within Western nations and NATO.

Not only Germany's development of the StG-44 (Sturmgewehr 44 – Assault Rifle-44, the inspiration for Mikhail Kalashnikov's AK-47), Germany would (with their MG-42 (Maschinengewehr-42—Machine Gun-42) also provide the design foundation for a series of Soviet General Purpose Machine Guns (GPMG), culminating with Kalashnikov's design of the Pulemyot Kalashnikova, ("Kalashnikov's Machine Gun" – PK) in the early 60s which was accepted for issue by the Soviet Ministry of Defense in 1965. To date, in excess of one million PK series machine guns have been manufactured and issued to Russian military and security forces.

Designed with the intent to fill multiple roles, GPMG are belt fed, and primarily utilized from their organic bi-pod, but can also be mounted on a tripod, and used in conjunction with a Traversing and Elevation (T&E) Mechanism from fixed defensive or overwatch positions. But the most common use is as part of an Infantry Platoon, from the bi-pod, where the firepower and increased effective range of the GPMG can greatly improve a unit's overall ability to deliver suppressive fire against either point or area targets. They are typically chambered for full-sized rifle caliber cartridges (7.62x51mm NATO, 7.62x54mm Rimmed, 7.92x57 Mauser). Modern examples include the M-60, the M-240, and the PK/PKM series of medium machine guns. This is a distinct difference from "Squad Automatic Weapons" (SAW) or "light machine guns" which are normally of the same caliber as the individual Soldiers Assault Rifles (5.56x45-mm NATO, 5.45x39-mm, 7.62x39-mm). Examples of these would be the FN manufactured "MINIMI"/M-249 or the Soviet/Russian RPD, RPK, and RPK-74M.

Specifically, the PK series of Russian GPMGs are chambered for the 7.62x54-mm Rimmed cartridge. This round has been in service since the 1890s when Czarist Russia adopted the Moisin-Nagant bolt action rifle as their standard issue weapon for the Infantry. It is a proven cartridge capable of acceptable accuracy, greater effective range, and the ability to penetrate barriers with greater effect than the 7.62x39-mm or 5.45x39-mm rounds used by the AK series of Assault Rifles or the RPD and RPK series of light machine guns.

The significant points of performance for the PK family of machine guns are as follows:

- Rate of fire (cyclic): 650 rounds per minute.
- Practical or combat rate of fire: 200-250 rounds per minute.
- Effective range: 1,000 meters (point targets); 1,500 meters (area targets).
- Weight: PK 19.84lbs; PKM 16.53lbs; PKP 19lbs.
- Feed system: Belt fed from right side, from detachable box containing 100, 200, or 250 linked rounds. **Note:** Soviet/Russian machine guns typically feed from the right hand side and eject on the left hand side of the receiver.
- Gas operated: 3-position gas regulator, rotary bolt system, fires from open bolt position.
- Chrome plated bore.
- Air cooled: Quick change capable barrel (PK and PKM basic issue items include a spare barrel). **Note:** the quick change feature of the PK series of machine guns is not as efficient or fast as those of Western nation GPMGs.



Figure 2. [Finnish Army issue PKM machine gun](#) Source: "MKVI"

By 1965, an improved variant had been tested, approved, and issued to the Soviet Army. The PKM (the “M” meaning “Modernized”) featured product improvements that primarily lowered the weight from almost 20 pounds to 16.5 pounds (PK to PKM). This was done by replacing some machined steel parts with stamped parts, and by replacing the PK’s heavier fluted barrel with a lighter, non-fluted barrel on the PKM. Otherwise, performance remains identical in both weapons. This weapon remains in current service with Russian Army, Naval Infantry, and Airborne forces.

As with the PK machine gun, the PKM can be mounted on a tripod, mounted on a pintle mount for use up top on tanks, Infantry Fighting Vehicles (IFV), Recon Vehicles, and rotary wing aircraft (when fitted with spade grips) for use as door guns. It is also used as a coaxial machine gun on Russian MBTs and IFVs (when fitted with an electrical solenoid).

Brought into service in 1999, the most recent variation on the basic PK/PKM them is the PKP or “Pecheneg.” This variant is also the result of product improvements that, in this case, were driven by Soviet Army experiences in Afghanistan, and later in the Caucasus.



Figure 3. [PKP \(Pecheneg\) from the Recon Company, 4th Separate Tank Brigade, Russian Federation](#)

Source: Vitaly Kuzman

Primarily used by SPETSNAZ and other elite Russian military or Ministry of the Interior forces, the PKP’s performance points are basically the same as the PK and PKM. In terms of weight, it comes in at 19 pounds, as it is equipped with a heavier barrel that is manufactured from higher quality ordnance steel.

This totally eliminates the need for a quick change barrel capability, and an extra barrel and tripod are not included with issued PKPs. Its only role is to provide heavy, sustained firepower to squad/team level, without the need to change barrels. In theory, the PKP is capable of firing up to 600 rounds per minute (basically sustained cyclic fire) without overheating the barrel. This is considerably more than the 200-250 rounds per minute of practical or combat rate of fire for the PK/PKM.

Besides the heavier, high quality ordnance steel barrel, the PKP features radial cooling fins machined onto the barrel’s surface and it is surrounded by steel jacket, which provides forced air cooling. In theory, air enters the jacket through

cuts at the rear of the barrel close to the receiver, and exits the jacket where it terminates, midway down the length of the barrel, just before the gas port. Additionally, a fixed carrying handle is attached to the top of the barrel jacket, and the PKP has sling swivels that allow the gunner to move forward and fire the weapon from the assault position (slung, and fired from the hip) if necessary. The PKP also has a mount on the left side of the receiver for attaching optical and night vision devices.

One additional modification over the PK/PKM is the location of the bipod. The PKP bipod is located just behind the muzzle of the weapon, which provides a steadier firing platform than the PK/PKM bipod, located on the gas tube. The only disadvantage offered by the PKP's bipod, is that it is too far forward for the gunner to grasp when standing/advancing, and firing from the hip.

The PK series has also been sold directly to many nations around the world, or licenses were granted for rights to manufacture. It is estimated that in excess of 50 nations currently use the PK/PKM or their domestically manufactured copy as their issued GPMG. The weapon's reliability and performance are such that some former Warsaw Pact members (Poland, for example), now manufacture a PKM clones that are chambered in 7.62x51mm NATO.

This level of distribution clearly indicates that like the AK-47/AK-74M and other Soviet era/Russian Federation weapons systems, the potential for future Threats and their allies to be equipped and armed the PK/PKM/PKP is very, very high. Knowing and understanding its capabilities is essential for every tactical leader in the US Army.

INSURGENT DISMOUNTED RAID ON A TANK PLATOON

Insurgent Threat TTP

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

A *raid* is an attack against a stationary target for the purposes of its capture or destruction that concludes with the withdrawal of the raiding force to safe territory. U.S. Army Training Circular 7-100.2, [Opposing Force Tactics](#), states that a raid can also be used to secure information and/or deceive the enemy. Keys to successful accomplishment of a raid include—

- Surprise.
- Massed firepower.
- Violent conduct.

Raid objectives can include—

- Destroy or damage key enemy systems or facilities.
- Deny critical information to the enemy.
- Disrupt enemy operations and/or support.
- Distract enemy attention from other Threat actions.
- Secure hostages or prisoners.
- Seize critical weapon systems and/or materiel.
- Support the Threat information warfare (INFOWAR) plan.

Command and Control of a Raid

A raid can be conducted by Threat elements that are autonomous in an OE but are typically associated and/or affiliated with a higher regular or irregular force unit or organization. Although a raid can be supported with operational assets, raids are primarily conducted by task-organized units, cells, or organizations at the tactical level of operations.



Figure 1. Insurgent video surveillance of enemy tank platoon position

Functional Organization for a Raid

Reconnaissance and surveillance provide the foundation for planning and conducting a raid. Resources may be as sophisticated as unmanned aerial vehicles (UAV) or satellite imagery to the simplicity of posting observers at critical points in an operational environment (OE). See the enclosed set of three figures for an example of sequential and concurrent tasks in conduct of a raid.

The size of the raiding force depends upon its mission, the nature and location of the target, and the enemy situation. The raiding force may vary in size and capability from a large mechanized task-organized force such as a Threat brigade tactical group (BTG) to a small irregular force of insurgents. Regardless of unit, cell, or organization size, a raiding force typically consists of three elements: raiding, security, and support. It may involve other functional elements such as a breaching element or a fixing element (see [TC 7-100.2](#), para. 3-174 to 3-192).

Raiding Element(s)

The raiding element executes the main task that ensures success of a raid in the destruction or seizure of the target in the raid. This element accomplishes its task through direct actions in a rapid and violent manner. Surprise is critical to mission success.

Security Element(s)

The primary threat to all elements of a raid is being discovered and defeated by enemy forces prior to execution of the raid. The security element within a raid focuses primarily on fixing enemy security and response forces or containing the enemy's escape from the objective area. The security element is equipped and organized to detect enemy forces and prevent or disrupt them from contacting other enemy forces that might influence the raid.

Security elements deploy to locations where they can disrupt the enemy freedom of movement along ground or air avenues of approach and delay reinforcement of the enemy on the objective. The security element operating within a small insurgent cell, regular force, or guerrilla unit mission may be only capable of providing early warning to the raiding and support elements. The security element also covers the withdrawal of the raiding element, and when necessary, acts as a rear guard for the raiding force. The size of the security element depends upon the size of the enemy's capability to intervene and disrupt the raid.

Support Element(s)

The support element has several enabling functions and assists in setting the conditions for the success of the raid. The support element provides fire support, logistics support, and/or reinforcement to the raiding and security elements. TC 7-100.2 states that a commander or leader of a raid typically controls a raid from within the support element. However, the commander or leader determines where to locate for best command and control (C2) the raid.

If needed, support elements may assist the raiding element(s) in reaching the objective and/or target of the mission. They can execute one or more complementary tasks such as—

- Eliminating enemy guards.
- Breaching and removing obstacles to and/or at the objective.
- Conducting diversionary or holding actions.
- Canalizing enemy forces.
- Providing fire support.

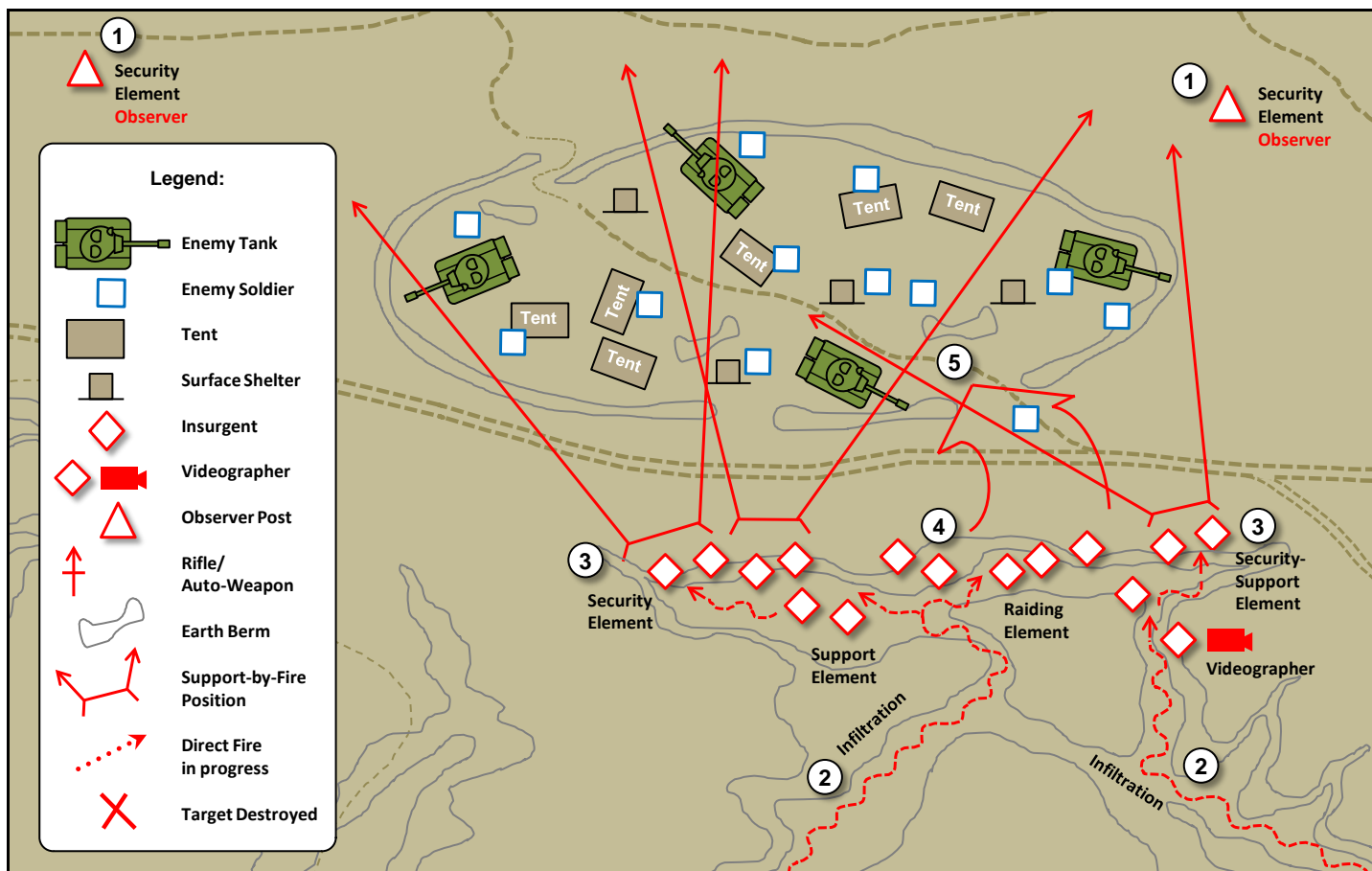


Figure 2. Insurgent plan for raid on tank platoon in defensive position

Tactical Example: Raid

The following example of a raid is based on a recent tactical action in Syria by insurgent forces on the regular forces of their enemy. Some tactical aspects have been amplified or modified to emphasize tactical principles.

Movement to the Assault Position

① See figure 2. Insurgent reconnaissance and surveillance observe an enemy tank platoon since it occupied a defensive position along an avenue of approach in farmland area near an urban center. Berms are prepared as a hasty circular perimeter with several gaps to allow vehicle movement in and out of the position. The only vehicular traffic for several days is a periodic arrival of a small cargo truck that appears to deliver rations and containers of water. Surprisingly, no other obstacles are constructed and no attempt has been initiated to improve the platoon defenses. Several tents and manmade shelters within the position indicate that the platoon-size force will remain in the area.

② Active supporters of the insurgent cell report on concealed approaches to the enemy position through severe ravines caused by erosion. Site reconnaissance and rehearsals confirm the infiltration routes for small groups of insurgents and where the insurgents will rendezvous near the enemy position. Insurgent observers report that the enemy has conducted no patrolling outside their perimeter and security measures are lax. Enemy soldiers walk individually or in pairs with no weapons, no load bearing equipment, and wear a mixed dress of military and civilian clothing. They appear to be casually talking rather than paying attention to or observing from the immediate perimeter.

No regular preventive maintenance has been performed on the tanks in the past days, turret-mounted machine guns remain under canvas, and all tanks have remained in the same position since their arrival.



Figure 3. Insurgents infiltrating into their raid assault position

③ Insurgent support elements move to the flanks and occupy support-by-fire positions while some insurgents also perform a security element function. The right flank support element will initiate the assault on order of the cell leader by killing any enemy soldiers at or near the gap in the berm selected for the assault penetration. The left flank support element prepares to provide support-by-fire small arms fire (SAF) to suppress or contain any enemy soldiers in the western half of the defensive position.

④ The initial raiding element positions on-line just below the crest of the ravine wall and close to the gap in the berm. The insurgent cell leader confirms final preparations and cell readiness. Specific tanks, tents, shelters, and designated areas have been assigned to insurgents with the task to quickly seize the tanks and kill any enemy soldiers. The insurgent cell is prepared to assault on-line and rush through the gap in the berm.

⑤ Insurgent observers report no enemy activity along the roadway east or west of the tank platoon. An insurgent in the right flank security element sees only one soldier without a weapon at the penetration point. The insurgent leader gives the signal to assault.

Assault

⑥ See figure 3. The right flank security element immediately shoots two soldiers at or near the gap in the berm as the initial raiding element of six to eight insurgents rushes the gap from the ravine. Surprise is complete.

⑦ The left flank support element covers its designated sectors with SAF and contains several enemy soldiers attempting to emerge from their tents or shelters. The SAF also keeps individual soldiers in tanks down inside the turrets. No soldiers attempt to operate individual or crew-served weapons in the tanks and any SAF from enemy soldiers on the ground is sporadic and ineffective. The speed of the assault and massed direct fires of the insurgents is achieving its intended purpose.

⑧ As the initial raiding element races through the gap in the berm and down the center path, insurgents quickly fan out left and right of the path to seize the two nearest tanks. They also quickly yet methodically clear each tent or shelter with SAF. Small arms fire from the enemy is nil.

⑨ The left flank support element shifts its SAF to the western part of the tank platoon position as the lead raiding element continues to assault through the position. The insurgent leader directs the support element to join the assault as these insurgents follow through the gap in the berm.

⑩ The insurgent cell seizes the tank platoon position within several minutes. Each support element designates one insurgent to act as security to the west and east along the main trail as early warning. The insurgent observers also report from their vantage points farther to the north.

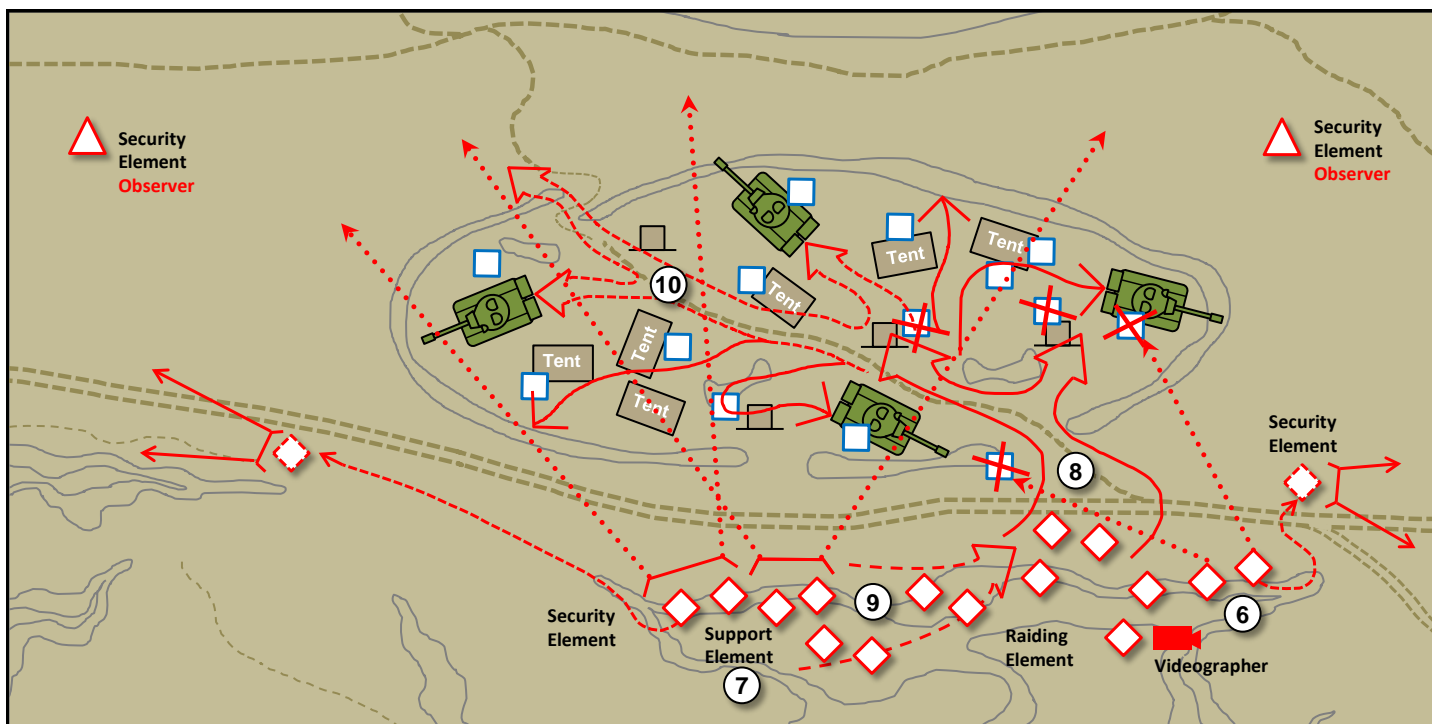


Figure 4. Insurgent conduct of raid on tank platoon in defensive position

Reorganization and Exfiltration

- ⑪ The insurgent leader directs that each tank is manned immediately and prepared for movement out of the berm position. Other reorganization tasks are limited to verifying the status of all insurgents and reallocating small arms ammunition. Casualties are limited to two insurgents with minor gunshot wounds. Meanwhile, insurgents gather several enemy weapons and distribute equipment as they organize for their exfiltration.
- ⑫ The videographer has recorded scenes during the entire raid and takes particular interest in how unprepared the tank platoon was in its defensive position. He walks among the insurgents and films the destruction of equipment, tanks being prepared for movement, and enemy dead to be abandoned in the position.



Figure 5. Insurgents seize a tank platoon defensive position in a raid

Note. Once the insurgent cell has arrived at its urban safe haven, the videotape and audiotape coverage of the raid is provided to an intermediary who transfers the recordings to local-regional media outlets and an INFOWAR cell of the local insurgent organization. The video and audio recordings are publicized on the Internet within hours of the raid and exploited to demonstrate enemy weaknesses in morale, lack of tactical discipline, and absence of force protection

measures. The insurgent organization uses the same video and audio recordings as a training aid in orienting recruits on how to successfully conduct tactical operations.



Figure 6. Insurgents moving captured tanks from raid objective

⑬ Insurgent groups start to exit the position and exfiltrate on routes different from the routes used for infiltration. The ravines to the south provide excellent concealment and soon the insurgents disappear as the last insurgent descends into the ravines.

Several insurgents exfiltrate to the northwest, link up with one of the observers, and move to an urban complex battle position (CBP). In the west, an insurgent exfiltrates parallel to the main trail and continues to report to the insurgent leader who is on one of the tanks.

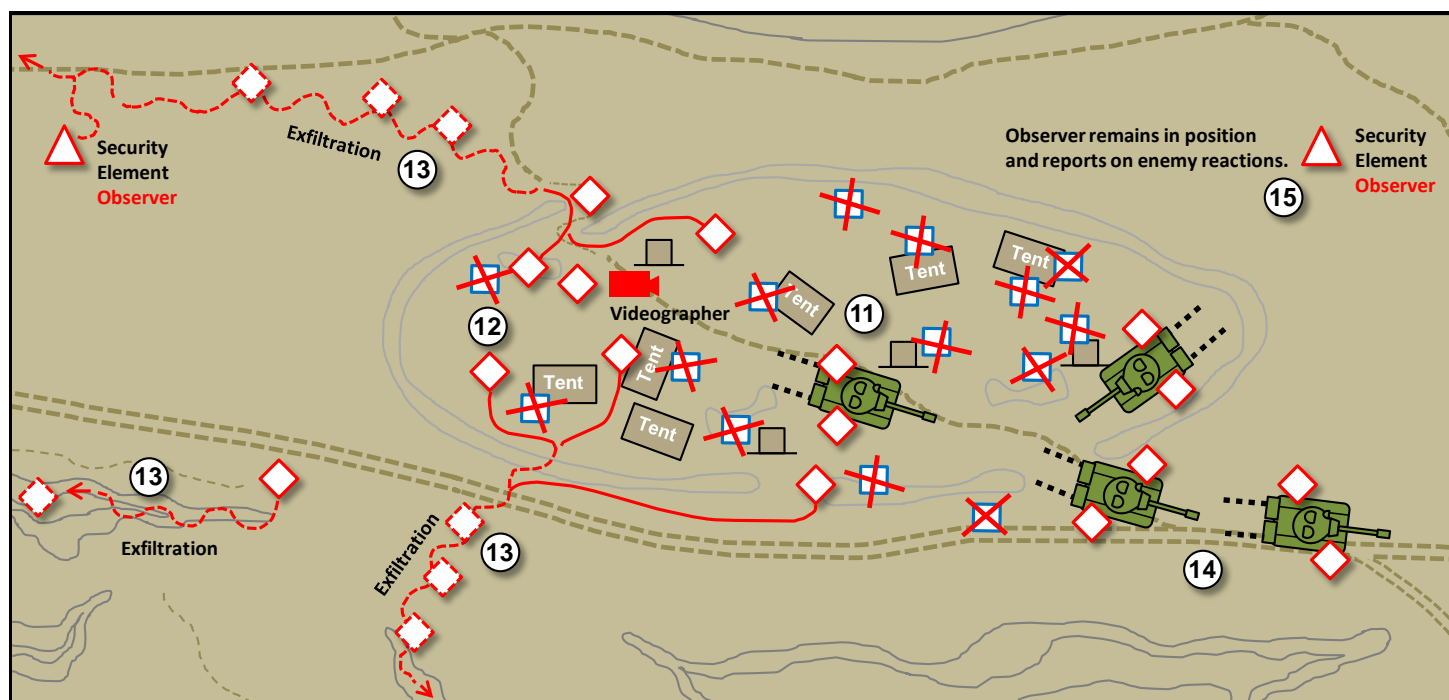


Figure 7. Insurgents moving captured tanks to urban hide positions

⑭ All four tanks are operational and are ordered by the insurgent leader to move east. During rehearsals, the insurgent cell leader identified hide positions near probable ambush sites in the restrictive network of urban streets. The local insurgent organization had already prepared multiple routes and ambush positions for use of tank main guns for flank or rear shots into enemy armored vehicles.

⑮ One insurgent observer remains concealed in a position to the northeast. He continues to send periodic reports to the local insurgent organization leader on how the enemy response forces act when they arrive hours later at the bermed position. Enemy soldier remains were removed and the site was not reoccupied by enemy forces.

Support of a Raid

A raid typically requires several types of support. These capabilities can include reconnaissance, armor, fire support, air defense, engineer, logistics, and INFOWAR. The primary reconnaissance task in a raid is to locate and monitor the target of the raid until the raiding element is in contact. Reconnaissance also monitors possible or probable enemy responses to a raid.

In the tactical example of this article, no armor vehicles are available to the insurgent organization. No indirect fires are in support of the raid. Air defense is prepared to use a Threat all-arms air defense tactic (see [TC 7-100.2](#), para. 11-72 to 11-78) with available small arms and automatic weapons.

A detailed reconnaissance of the enemy position determines that no physical breaching element is required for the assault. All logistics for this raid are carried with the insurgents in their infiltration to the attack position.

INFOWAR is a regular – if not constant – support task to military operations such as a raid. INFOWAR can support a raid by concealing the intended action through deception and perception management. The videographer in the tactical example of this article records the movement and maneuver of the insurgent cell as it—

- Infiltrates from a tactical assembly area.
- Coordinates elements for the raid in an assault position.
- Conducts the assault through a gap in the enemy berms.
- Seizes the enemy platoon position.
- Secures the enemy main battle tanks and equipment.
- Reorganizes for tactical movement.
- Exfiltrates dismounted insurgents on multiple routes.
- Moves captured main battle tanks to urban hide positions.

Observations for Training Readiness

This real-world example of a raid spotlights the importance of reconnaissance and surveillance to find and confirm enemy critical weaknesses. When enemy security measures are lacking and enemy soldier and leader discipline is not observable, a dismounted infantry-like insurgent cell *can* plan and conduct an assault to defeat and/or destroy a stationary enemy force of main battle tanks in a platoon-size defensive position. For more visual details on what was recorded by an insurgent videographer in an insurgent raid on an armor platoon defensive position in Syria, see [Dismounted Raid on a Tank Platoon](#).

No indirect fire support or heavy weapons were available for the raid. Rehearsals and coordinated teamwork among the insurgent elements emphasized surprise and violent execution of the assault. Using only small arms and automatic weapons, an insurgent cell of twelve to twenty insurgents raids an enemy armor platoon in a defensive position, kills all enemy soldiers, and seizes four main battle tanks for insurgent urban operations against a corrupt governing authority.

Worldwide Threat Assessment of the US Intelligence Community 2013 (U)

Syria and the Nusrah Front

Almost two years into the unrest in Syria, we assess that the erosion of the Syrian regime's capabilities is accelerating. Although the Asad regime has prevented insurgents from seizing key cities—such as Damascus, Aleppo, and Homs—it has been unable to dislodge them from these areas...prolonged instability is also allowing al-Qa'ida's Nusrah Front to establish a presence within Syria.

Honorable James R. Clapper

Director of National Intelligence (12 March 2013)

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 April. U.S.: [The Texas Department of Public Safety releases its "Threat Overview" for 2013, with Mexican Cartels at No. 1 spot](#)
DPRK: [North Korea declares "state of war" with South](#)
- 03 April. ROK: [U.S. deploys warship as tensions over North Korea rise](#)
- 05 April. DPRK: [North Korea moves missile with 'considerable range' to east coast](#)
Myanmar: [Shan villagers flee army abuses](#)
- 08 April. Afghanistan: [Six Americans, including one young diplomat, killed in Zabul province](#)
Nigeria: [12 police missing after Bayelsa attack](#)
- 10 April. Kuwait: [20,000 U.S. M-16s stolen from unguarded warehouse in Kuwait](#)
South China Sea: [Psychological warfare in the South China Sea](#)
- 12 April. Lebanon: [Syrian air forces raid Lebanese border town, 5 injured](#)
Syria: [60+ die in shelling and executions in al-Sanamein, Deraa](#)
- 15 April. U.S.: [Explosions reported at the Boston Marathon; dozens injured](#)
Syria: [Chemical warfare looms over Syria. Israel passes atropine to rebels](#)
- 17 April. U.S.: [Ricin letter sent to POTUS](#)
China: [China issues white paper on national defense](#)
- 19 April. U.S.: [Death toll unknown, 160+ injured: Texas plant explosion](#)
- 22 April. Nigeria: [Fighting between JTF and Boko Haram in Baga kills 185, destroys 2000 homes](#)
Sweden: [Russian fighter jets practiced attacks on Sweden](#)
- 24 April. Syria: [Clashes escalate on Syria-Lebanon border](#)
China: [Violence erupts in Xinjiang province, 21 dead](#)
- 26 April. Venezuela: [Venezuela detains American accused of fomenting violence](#)
India: [Chinese troops erect tents 19Km inside Indian territory](#)
- 29 April. Pakistan: [Suicide bomber attacks bus in Peshawar, eight killed, 45 wounded](#)
Israel: [Israeli jets bomb Syrian chemical weapons depot outside Damascus](#)

CTID Points of Contact

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

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

