



Red Diamond

Complex Operational Environment and Threat Integration Directorate

Fort Leavenworth, KS Volume 4, Issue 1 JAN 2013

INSIDE THIS ISSUE

Describing RAFTE...2
OEs Overview3
Assault TTP5
Aircraft Threats8
Iran SAM12
Suicide Vest TTP...15
Director's Notes....21
CTID POCs25

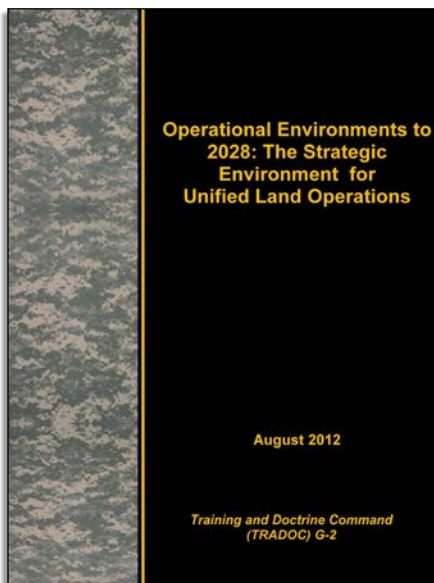
Red Diamond is a newsletter published each month by TRISA at CTID. Send your suggestions to CTID on article content.

ATTN: Red Diamond
Dr. Jon H. Moilanen
CTID Operations, BMA
and
Mrs. Angela Wilkins
Chief Editor, BMA



OPERATIONAL ENVIRONMENTS AND THE FUTURE

by Complex Operational Environment and Threat Integration Directorate



The Army does not have the luxury of focusing on any one potential adversary or any one mission type across the range of military operations. Instead, leaders and Soldiers must be exposed to the multiple conditions representing threats that exist across the globe. Potential threats will range from standing conventional or unconventional forces, to irregular militias and paramilitaries, to terrorist groups and criminals. Training, education, and capabilities and concept development should reflect this reality. The strategic environment (SE) to 2028, with its combination of tough enduring problems and emerging OE conditions and characteristics, adds complexity to this challenge.

We must strive to understand the complex future and prepare our Army to operate and adapt in any environment. As we prepare our Soldiers, leaders, and units for the future, this document provides a foundation for us to design training and education, build leader development programs, and develop required capabilities for our Army. The operational environments we will encounter in the future will differ from Iraq and Afghanistan. Although there may be similarities, the multitude of different actors, interests, and conditions in each conflict create unique and complex environments.

Robert W. Cone
General, U.S. Army
Commanding General's Foreword, [Operational Environments to 2028](#)

RED DIAMOND TOPICS OF INTEREST

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

This issue of the TRISA Red Diamond spotlights several articles on current events concerning real-world Threats and variations on tactics, techniques, and procedures. Of note, *The Operational Environment to 2028: The Strategic Environment for Unified land Operations*, describes the key CONDITIONS manifesting across the strategic environment through 2028. This document also addresses military implications of both OE conditions and potential adversary strategies.

The current and future strategic environment will be characterized by uncertainty, complexity, and increasingly nuanced relationships. The conditions of the strategic environment must be understood, captured, and factored into Army decision making. Only then can realistic training, the correct combination of systems and capabilities, and adaptive approaches to leader development and education be identified, examined, and implemented across TRADOC and the Army in general.

See <https://www.us.army.mil/suite/doc/3764173> for *The Operational Environment to 2028: The Strategic Environment for Unified land Operations*.

ACTIONS in 2013

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

Submit your concept for consideration in a 2013 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

DESCRIBING A REGIONALLY ALIGNED FORCES TRAINING ENVIRONMENT (RAFTE)

by CTID Operations

A Regionally Aligned Forces Training Environment (RAFTE) is a supplement to the [DATE](#) [Decisive Action Training Environment] that will contribute information specific to a regional operational environment (OE). A particular RAFTE will focus on and use the geography within a COCOM for training readiness of regionally aligned forces. It will be different but not separate from the DATE.

The Decisive Action Training Environment is the comprehensive OE document, and—

- Is the *source* for OE conditions and OPFOR structure for Army training events.
- Presents a *complex OE* with a *Hybrid Threat* that can be employed to challenge unit training objectives.
- Provides the *baseline conditions* for *scenario continuity* across the training community.

RAFTE

Each RAFTE will provide information in two main categories. One section of the RAFTE will describe conditions that are present in a specific regional OE that are not already present in the DATE. The other section will detail conditions that are present in the DATE that should be removed from regional considerations in order to set appropriate conditions for a specific regional OE.

- Explains PMESII-PT variables [Political, Military, Economic, Social, Information, Infrastructure, Physical Environment, and Time] that are indicative of capabilities and limitations to five states in the DATE OE. The DATE states of Ariana, Atropia, Gorgas, Minaria, and Donovia present a wide range of characteristics and conditions to support training objectives for a decisive action operation.

Each RAFTE, as a complement to the DATE, eliminates the requirement to develop an OE for each training venue. Resources and time can be programmed and used more effectively in support of training exercise objectives. The information provided in a RAFTE will be presented in two main categories. One section of the RAFTE will describe conditions that are present in a specific regional OE that are not already presented in the DATE. The other section will detail conditions that are present in the DATE that should be removed from consideration while training for a specific regional OE.



The first RAFTE will be an OE of Africa. The Complex Operational Environment and Threat Integration Directorate (CTID) of the TRADOC G2 Intelligence Support Activity (TRISA) is developing information in a RAFTE-Africa according to PMESII-PT variables with “bullet lists” and concise explanations. The document will assist an exercise planner with guidance on what CONDITIONS to add to, emphasize, or delete from the DATE. The amount of OE-specific information will highlight significant issues for that specific OE and RAF training readiness requirements.

CTID is currently soliciting input and feedback from key senior leaders on a draft of RAFTE-Africa 1.0. Each RAFTE will be built through collaboration between CTID and the Army Service Component Command (ASCC) staff. The ASCC staff will identify the key conditions that must be replicated in regionally aligned force brigade combat team (BCT) training for that region. CTID will then integrate these conditions into an informational package using the DATE framework. The RAFTE will provide exercise planners with the tools and conditions necessary to provide realistic challenges and opportunities across all OE variables. Another focus will be conditions specific to the region covered by a particular RAFTE. The RAFTE-Africa 1.0 will be published later this year.

In the future, CTID will likely produce RAFTEs for other regional OEs based on guidance and priorities of effort from senior Army leaders. All DATE and RAFTE products will be available through Army Knowledge Online (AKO).

OE THREAT ASSESSMENTS OVERVIEW

Threat Assessments in an OE

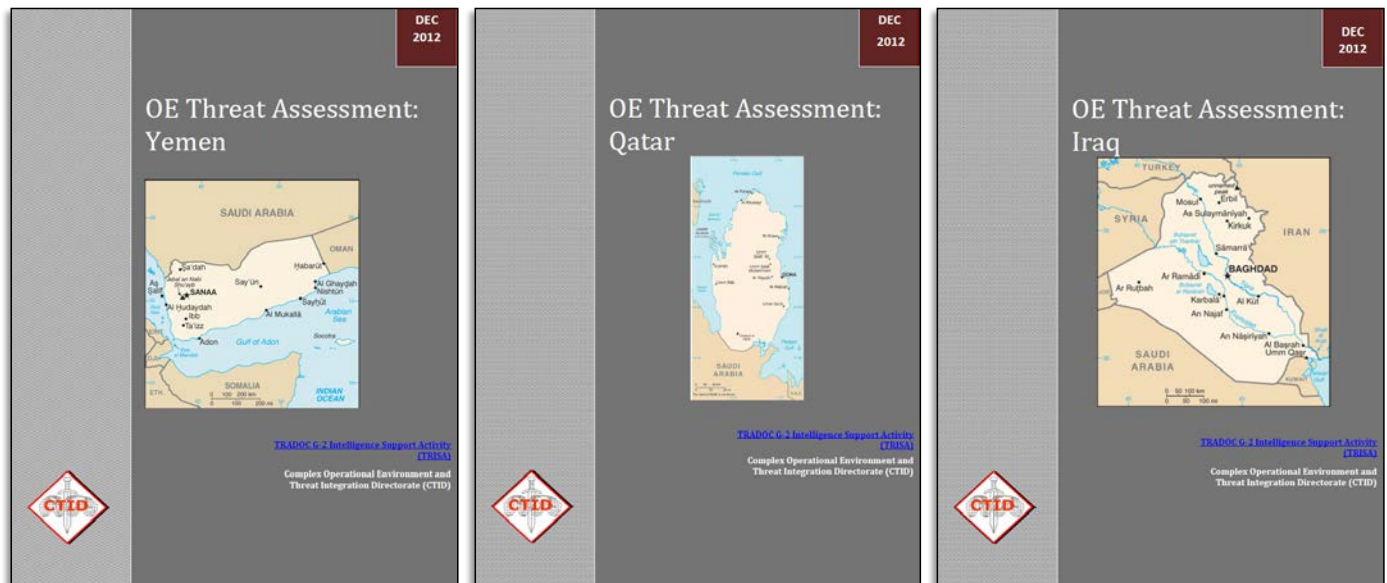
by H. David Pendleton, OE Assessment Team (ISC-CG CTR)

The OEA team produced ten [Operational Environment \(OE\) Threat Assessments](#) in response to an RFI from the 135th Expeditionary Sustainment Command (ESC) who requested a threat product that focused on military, criminal, terrorist, foreign intelligence service, and other force protection-related issues for ten countries

in the United States Central Command’s (CENTCOM) Area of Responsibility (AOR). In less than a month, the OEA Team produced the Threat Assessments for Bahrain, Egypt, Iraq, Jordan, Kuwait, Oman, Qatar, Saudi Arabia, the United Arab Emirates, and Yemen. These products range from 12 to 20 pages and, while they

cover all eight PMESII-PT (political, military, economic, social, information, infrastructure, physical terrain, and

time) variables, the primary focus is squarely on the military section.



After a general discussion of the country’s military, the OE Threat Assessment looks at all three services—army, air force, and navy—by type of units, equipment use, major bases, and capabilities. The OE Threat Assessment also covers any governmental forces that possess paramilitary capabilities along with any foreign troops located in the country. The product then examines the country’s military through the lens of the seven military functions: mission command, maneuver, INFOWAR (Information Warfare), RISTA elements (reconnaissance, intelligence, surveillance, and target acquisition), fire support, protection, and logistics.

Other potential military threat actors also receive careful examination if they operate in the country. These groups can include non-state paramilitary forces such as insurgent groups, guerrilla forces, criminal organizations, private security organizations, and nonmilitary armed combatants. If any of these groups presents a significant presence in the country, the potential threat actors also receive an assessment based on the seven military functions.

The OE Threat Assessment includes a section on force protection issues that American military personnel could face in the country and increases the attention paid to any governmental intelligence agencies under the information variable. While not as detailed as the standard Operational Environment Assessment (OEA) that takes four to six months to produce, the OE Threat Assessment provides a quick synopsis of seven of the PMESII-PT variables and an enhanced assessment of the military variable for the OE.

TRISA CTID analysts respond to RFIs from all our customers. If there is something you need, please contact us. The last page of this *Red Diamond* lists contact information for CTID.

OE Assessments by CTID

The OEA team at TRISA-CTID produced ten Operational Environment (OE) Threat Assessments in response to an RFI from the 135th Expeditionary Sustainment Command (ESC). They requested a threat product that focused on—

- Military
- Criminal
- Terrorist
- Foreign intelligence service, and other Force protection-related issues for ten countries in the United States Central Command’s (CENTCOM) Area of Responsibility (AOR)

INSURGENT ASSAULT ON A COALITION TRAFFIC CONTROL POST

Threat Assault Tactics, Techniques, and Procedures (TTP)

by Dr Jon H. Moilanen, CTID Operations (BMA CTR)

Insurgent Assault on a Coalition TCP

Insurgents select the offensive action best suited to accomplishing their mission. Cells at this level of organization typically execute one combat mission at a time. Therefore, it would be rare for such a unit to employ more than one type of offensive action simultaneously. Insurgent cells are dynamic and adapt very quickly to the situation.

An assault is an attack that destroys an enemy force through firepower and the physical occupation and/or destruction of his position. An assault is the basic form of irregular OPFOR tactical offensive combat. Therefore, other types of offensive action may include an element that conducts an assault to complete the mission; however, that element will typically be given a designation that corresponds to the specific mission accomplished. For example, an element that conducts an assault in the completion of an ambush would be called the ambush element.

Irregular OPFOR do not have a separate design for “mounted” and “dismounted” assaults since the same basic principles apply to any assault action. An assault may have to make use of whatever cells can take advantage of a window of opportunity. Irregular OPFOR view all assaults as combined arms actions.

Functional Organization for an Assault

See figure 1 [on page 6] for an example of an insurgent cell assault. An insurgent cell conducting an ambush typically is organized into three elements:

- Assault
- Security
- Support

Assault Element

The *assault element* is the action element. It maneuvers to and seizes the enemy position, destroying any forces there.

Security Element

The *security element* provides early warning of approaching enemy forces, and when applicable, prevents enemy forces from reinforcing the assaulted enemy unit. Security elements often make use of terrain choke points, obstacles, ambushes and other techniques to resist larger forces for the duration of the assault. The insurgent cell leader may (or may be forced to) accept risk and employ a security element that can only provide early warning that is not strong enough to block or delay enemy reinforcements. This decision is based on the specific situation.

Support Element

The *support element* provides the assault element with one or more of the following:

- Threat mission command
- Combat service support (CSS)
- Supporting direct fire (such as small arms, grenade launchers, or infantry antitank weapons)
- Supporting indirect fire (such as mortars)
- Mobility support

Executing an Assault

An assault is the most violent course of action (COA) a military force can undertake. Indeed, a simple direct assault has a very low chance of success without some significant mitigating factors. Decisive irregular OPFOR assaults are characterized by—

- Isolation of the objective (enemy traffic control post (TCP) in the example) so that it cannot be reinforced during the engagement.
- Early warning and/or other security measures by the insurgent security element of any approaching enemy reinforcements.

- Effective suppression of the enemy by the insurgent support element prior to the assault element maneuvering on the enemy position.
- Violent fire and maneuver against the enemy position.

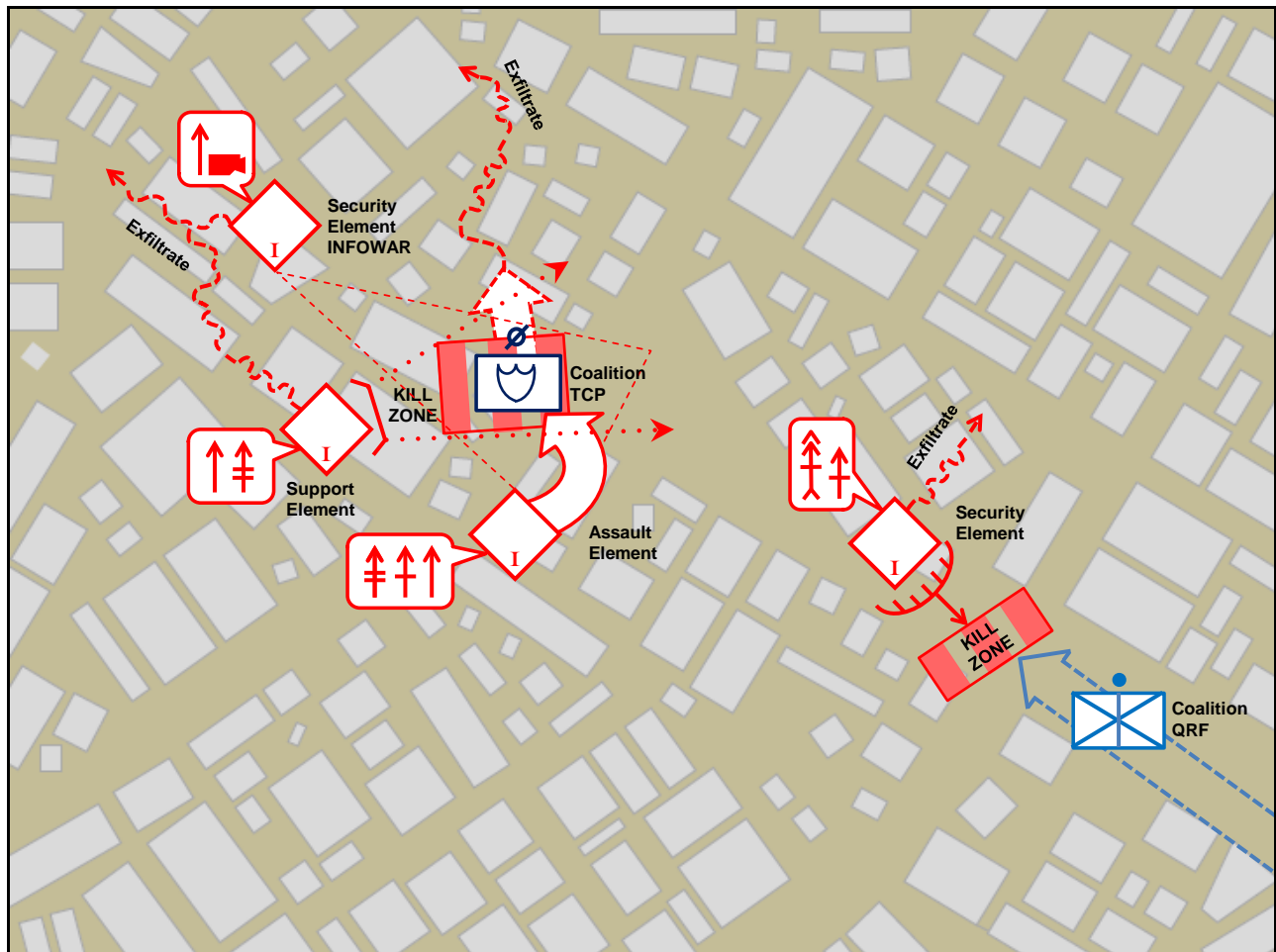


Figure 1. Insurgent assault on a coalition traffic control post

The assault element maneuvers from its assault position to the objective and destroys the enemy located at the objective. It can conduct attack by fire, but this is often not an optimal method and should be used only when necessary. Typical tactical tasks of the assault element are—

- Clear
- Destroy
- Seize

Irregular OPFOR normally do not assault to secure as this task indicates an intention to prevent the loss of an objective to subsequent enemy reaction. Any occupation of an objective is typically temporary to minimize the ability of an enemy force to mass

overwhelming combat power against irregular OPFOR. Speed of execution and surprise are critical to an assault

The security element is equipped and organized to detect enemy forces that may be able to react to an irregular OPFOR assault on an objective. Security tasks may include the requirement to isolate the objective from any reinforcement by enemy forces with tasks such as block, contain, or delay while the assault is in progress. The security element may be directed to conduct similar tasks that allow the assault and support elements to exfiltrate.

The insurgent cell leader typically exercises mission command from within the support element. He can also lead the assault element when he determines that his personal presence in the assault is critical to mission success.

The support element controls all combat support (CS) and CSS functions as well as any supporting fires. Tasks expected of support elements in the assault are normally attack by fire and/or support by fire. These direct and/or indirect fires are often intended to deceive the enemy's attention in support of maneuver by the irregular OPFOR assault element.

Threat Mission Command of an Assault

Mission command of the irregular OPFOR assault masses insurgent capabilities in time and space for rapid and violent attack on a selected objective. The irregular OPFOR normally plans an assault in detail to improve tactical execution with surprise and deception and in order to achieve temporary superior combat power against an enemy force. However, irregular OPFOR will often take advantage of an unexpected opportunity as it occurs in order to assault an enemy force.

Fighting in complex terrain can be a significant tactical advantage for irregular OPFOR. In the offense, combat actions in urban areas by irregular OPFOR can use the civilian community and its infrastructure for shielding and obstacles against enemy forces. Irregular OPFOR may decide to not comply with international conventions and law of war restrictions that are complied with normally by traditional military forces and governing authorities with whom irregular OPFOR are in conflict.

Complex Terrain

Complex terrain for the irregular OPFOR Threat is a topographical area consisting of an urban center larger than a village and/or of two or more types of restrictive terrain or environmental conditions occupying the same space. (Restrictive terrain or environmental conditions include but are not limited to slope, high altitude, forestation, severe weather, and varied degree of rural and/or urban development.)

TC 7-100.2 Opposing Force Tactics

Channelized corridors of urban traffic networks and the vantage points of multi-story buildings and/or surface or sub-surface infrastructure can be demoralizing to an enemy force attempting to counter an irregular OPFOR. Beyond the human and facilities cover and concealment provided in urban areas to irregular OPFOR, enemy forces often operate within a relevant population that

they do not want to alienate due to excessive civilian casualties, restrictions, and/or damage to their facilities and livelihoods. In comparison, rural complex terrain may have less people within designated areas but can be used to similar cover and concealment advantage by irregular OPFOR for deception, surprise, and assault tasks. The civilians that reside in such rural areas can be influenced to support irregular OPFOR voluntarily or involuntarily through an effective INFOWAR campaign.

Support of the Assault

Support norms to an irregular OPFOR assault include reconnaissance and INFOWAR. When required for a particular mission, actions such as fire support, air defense, and/or other functions can be added to the insurgent cell capabilities to conduct an assault. Aspects of reconnaissance and INFOWAR include—

Reconnaissance

Reconnaissance effort for an irregular OPFOR assault is continuous in the objective area in order to confirm and/or adjust information collection and intelligence previously collected and analyzed. The insurgent cell leader uses active supporters in the relevant population to observe and report on enemy activities at the planned objective area. Insurgents are often positioned in the local community and in vicinity of the objective posing as innocent civilians conducting normal commercial or social actions. These reconnaissance and surveillance reports, combined with the reports from active supporters, assist the insurgent cell leader in finalizing his assault plan to shape, assault, and exfiltrate. Once infiltration and exfiltration routes are planned, the irregular OPFOR maintain these routes under constant surveillance prior to and during the assault. Secrecy of irregular OPFOR locations and activities is essential to tactical survival. Locations of keen interest for reconnaissance and surveillance include—

- Caches
- Infiltration routes
- Assault position
- Support position
- Objective
- Exfiltration routes
- Safe houses

INFOWAR

INFOWAR support of an irregular OPFOR assault considers the rapid and violent nature of an assault and the intention to temporarily and psychologically isolate the enemy force. Isolation of the enemy may also use physical means such as simultaneous assaults on multiple objectives to overload the enemy's ability to respond and/or effectively reinforce an enemy force at a particular irregular OPFOR objective (see Appendix A).

Other INFOWAR activities that can limit enemy force effectiveness can include—

- Deceiving enemy forces at the objective with recurring and apparent non-threatening community activities in the vicinity of the objective.
- Exploiting enemy information collection with false intelligence provided by active supporters of the irregular OPFOR and/or insider threat insurgents.
- Disrupting enemy information collection through coercion and extortion of the relevant population to not cooperate with enemy forces.
- Influencing enemy forces with misinformation and/or manipulated claims against the governing authority to which the enemy forces belong.
- Influencing a local, regional, and/or global audience with near real-time media coverage of irregular OPFOR assaults and successes against an enemy force.

TTP Note: A simple, effective, and successful assault technique employed often by irregular OPFOR is to surprise the enemy by focusing enemy attention in one direction and then assaulting from a different direction. This deception complements the nearly simultaneous action of massing firepower and maneuver on the objective. The support element shifts and/or lifts its small arms fire across the objective as the assault element assaults through the objective. Security element(s) prepare to protect other irregular OPFOR elements and/or ambush any coalition response forces. On order of the insurgent leader, support and security elements exfiltrate from the area. In this example, an INFOWAR cell positioned with a security element records the successful assault. The INFOWAR cell relays the video-audio coverage to an intermediary for delivery to local media outlets with added narrative by the higher insurgent organization spokesperson.

AIRCRAFT THREATS

Aerial Threats in a Complex Operational Environment

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

"If it flies, it dies" is the adage of the air defense branch and one that holds uncomfortable truth for aviators. The U.S. goes to great lengths to ensure it has air superiority in conflict zones, and this includes air-to-air combat as well as neutralizing ground-to-air capabilities through suppression of enemy air defense (SEAD) missions. Some of the threats to our aircraft are ground fire from small arms, man portable air defense systems (MANPADS), and gun-missile systems. Relatively recently, the threats have included laser "dazzlers" fired at cockpits and high-energy laser systems for countering rockets, artillery, and mortar shells (C-RAM).

C-RAM

Since the invention of the laser, military application has been the goal of many researchers. However, the energy requirements for such a weapon have been considered too high. In October 2012, MBDA Germany completed a further major step toward a laser weapon system capable of providing air defense. For the first time, the company's high-energy laser demonstrator was used to demonstrate the complete deployment sequence in C-RAM. Using 40 kilowatts (kW) of laser power, the laser demonstrator successfully acted on

airborne targets at a range of over 2,000 meters. For these tests, MBDA Germany's laser demonstrator was equipped with a new, improved performance, significantly more compact and lighter optical system which was integrated in a transportable container. During the tests, the illumination and effect laser was pre-targeted using a radar (SPEXER™ 2000) and an IR optronics system (MEOS II) supplied by Cassidian. A multi-stage control system, incorporating an in-house developed image processing system, was used to lock onto the target at close range.¹ This was tested against multiple artillery shells in a wide variety of flight paths at an altitude of 1,000 meters. This implication is that it will also be effective against manned aircraft within range.

In November 2012, Rheinmetall successfully tested a 50kW laser weapon in Switzerland against steel girders, nose-diving target drones, and 3.2-inch steel projectiles moving at 50 meters per second. Designed for air defense, asymmetric warfare, and C-RAM operations, the Rheinmetall laser isn't a single weapon, but two laser modules mounted on Oerlikon Revolver Gun air defense turrets with additional modules for the power supply. The lasers are combined using Rheinmetall's Beam Superimposing Technology (BST) to focus a 30kW and a 20kW laser on the same spot. This gives it the destructive power of a single 50kW laser. Rheinmetall claims this laser works in snow, dazzling sunlight, ice, and rain. Currently this is a stationary system which could be used for static air defense of military installations and forward operating bases. Rheinmetall looks to develop a mobile system in the future.²

On 12 December 2012, Lockheed-Martin successfully tested a tactical-level system named Area Defense Anti-Munitions (ADAM). Providing short-range defense of high-value areas including forward operating bases, the ADAM system is designed to track targets at a range of more than 5 kilometers and to destroy targets at a range of up to 2 kilometers. It is specifically designed as defense against rocket and unmanned aerial systems (UAS), but may also prove effective against manned aircraft.³

Dazzlers

Lasers are especially dangerous to human eyes and there are multiple cases of people shining them at pilots while in flight or on final approach. In June 2011, three men in their 20s were arrested in Chicago for shining a green laser at a police helicopter.⁴ According to the FBI, there were 10 reported laser incidents in Virginia Beach

during 2011 and 98 in Virginia. January 25, 2012 marked the first felony conviction in a laser-pointing case in Virginia.⁵

Russia has developed harsh laws concerning the use of laser pointers against airplanes. The Criminal Code provides three years in prison or an 80,000 ruble fine (approximately \$2,600) for "laser hooliganism." If the airplane's crew is blinded by laser pointers, which may disorient pilots, those responsible will face up to seven years in prison. If laser hooliganism causes the jet's crash, the sentence will increase to 10 years in prison.⁶ There were 50 such cases in Russia in 2011.

Air Threats

Threats to aircraft include ground fire from small arms, man portable air defense systems (MANPADS), and gun-missile systems. In relatively recent attacks, the threats have included laser "dazzlers" fired at cockpits and high-energy laser systems for countering rockets, artillery, and mortar shells (C-RAM).

Gun Systems

"Small arms" in air defense parlance includes heavy machineguns such as the U.S. M2 .50 caliber and the Russian DsHK 14.5mm machinegun. Small arms were extremely effective against rotary wing aircraft in the Vietnam War, and were responsible for multiple aircraft downings and damage in Operation Urgent Fury (Grenada), Operation Just Cause (Panama), Operation Gothic Serpent (Somalia), and the Battle of Najaf in 2003 (Iraq). Not classed as an air defense weapon, the RPG-7 has been proven effective against low flying or hovering aircraft when fired in volley. During the Vietnam War, enemy squads were drilled in downing low-flying U.S. helicopters using nothing more than AK-47s.

The current rebellion in Syria has provided video evidence of ground fire downing both rotary wing and fixed wing aircraft. The Free Syrian Army (FSA) has used anti aircraft weapons, such as the ZU-23-2, to bring down Syrian aircraft. For more information on the ZU-23-2 weapon system, refer to the [Worldwide Equipment Guide, Vol 2: Airspace and Air Defense Systems](#), p. 6-49.

Below are examples of successful FSA attacks on Syrian aircraft. (Compilation from the CTID OEA Team Threat Report, [*The Free Syrian Army: Rifles to MANPADS*](#), November 2012.)

June 26, 2012

A helicopter was shot down in Maardebseh, Idlib. The Suqour al-Sham Brigade and the Shuhada Jebel al-Zawiyah Battalion both claimed responsibility. [Video Source](#)

July 7, 2012

A surveillance aircraft was shot down by members of the Jafar al-Tayyar Battalion in Deir Ezzor.

August 13, 2012 A MiG jet was shot down in the town of Mohasan, Deir Ezzor. [Video Source](#)

August 27, 2012

A helicopter was shot down in the vicinity of the Jobar neighborhood. [Video Source](#)

August 31, 2012

A MiG jet was shot down by the Shuhada Jebel al-Zawiyah Battalion during a week-long attack on the Abu Dhuhur airport. [Video Source](#)

September 4, 2012

A second MiG jet was shot down by the Shuhada Jebel al-Zawiyah Battalion during the week-long attack on the Abu Dhuhur airport.

September 5, 2012

A helicopter was shot down over Damascus by the Saif al-Islam Battalion of the al-Islam Brigade.

MANPADS

Man-portable air defense systems (MANPADS) were originally developed in the 1940s to provide air defense to ground troops (German *Fliegerfaust*). The first generation of missiles was infrared guided, developed in the 1960s, which lock-in on an aircraft's exhaust plume. These include the American Redeye, the Chinese HN-5, and Soviet SA-7 and were referred to as "tail chasers" or "revenge weapons." Second generation MANPADS including the Russian SA-14 and Chinese FN-6 permit head-on and side engagements, and the U.S. Stinger includes a UV target-detection mode. Third generation MANPADS include the French Mistral, Russian SA-18, and U.S. Stinger B. These can recognize and reject decoy flares. Fourth generation missiles (Stinger Block 2) use advanced sensor systems and have greater range.

Command line-of-site (CLOS) missiles require a gunner to visually acquire a target and "fly" the missile to that target. These include the British Blowpipe, Javelin, and Starburst. Laser guided missiles require a highly trained gunner to keep a laser trained on the target while the missile flies the beam. These include the Swedish RBS-70 and the British Starstreak.

Twenty-five countries, including the United States, produce man-portable air defense systems. Possession, export, and trafficking of such weapons are officially tightly controlled, due to the threat they pose to civil aviation, although such efforts have not always been successful. This was especially true following the Russia-Afghan War when the U.S. provided Stinger missiles to Afghan mujahedeen. Use of MANPADS against civilian aircraft is an especially sensitive issue and not without precedence as the incidents listed below show.



Figure 2. MANPADS Hit, Iraq (2003)

Known civilian aircraft incidents:

03 September 1978: A Rhodesian Vickers Viscount was struck by a Soviet-made Strela 2 fired by Zimbabwe People's Revolutionary Army (ZIPRA) cadres near Karoi. 38 killed in the crash, another 10 killed on the ground by guerrillas.

12 February 1979: Air Rhodesia Flight 827 was shot down by ZIPRA guerrillas using a Strela-2 surface to air missile (SAM). 59 killed (55 passengers, four crew). After this incident, Air Rhodesia modified the exhaust pipes of their aircraft and painted aircraft with low-radiation paint.⁷

21 September 1993: A Transair Georgia airliner on final approach was shot down by a SAM fired by rebels in Sukhumi, Abkhazia, Georgia. 27 killed (22 passengers, five crew).

29 September 1998: Lionair Flight 602 from Sri Lanka was shot down by a MANPAD fired by Liberation Tigers of Tamil Eelam (LTTE). 55 killed (48 passengers, 7 crew).

28 November 2002: Two SA-7b Mod 1 “Grail” SAMs were fired at an Arkia Airlines Boeing 757 as it departed Mombasa, Kenya. Both missiles missed and the aircraft continued its flight to Israel with Israeli Air Force fighter escort. Police found the launcher assemblies and missile casings 2 km from the airport.⁸

22 November 2003: A DHL Airbus A-300B was hit by a SA-7 SAM at 10,000 feet over Iraq. The crew managed to land the aircraft at Baghdad International Airport (see figure 1 on previous page).

23 March 2007: A TransAVIAexport Airlines Ilyushin Il-76 aircraft was shot down outside Mogadishu, Somalia. Eyewitnesses reported seeing a SAM strike the aircraft. The MANPAD was reported to be a Strela-3 (SA-14). 11 killed (4 passengers, 7 crew).

Training Readiness

Threats to aircraft remain a significant aspect of uncertain-complex environments.

Threats against U.S. aircraft are numerous and must be replicated in training. Allowing aircraft to operate freely in a hostile area is unrealistic and teaches the wrong lessons to air crews. At the same time, the weapons systems deployed against aircraft must be realistic. This means no less lethal, and no more lethal, than the real-world systems they replicate.

Known military aircraft incidents:

17 November 1991: A USAF F-16 and an RAF Tornado GR1 were shot down by Strela-3 SAMs during Operation Desert Storm in Iraq.

06 April 1994: A SAM shot down a Dassault Falcon 50 carrying the Rwandan and Burundian presidents in Kigali, Rwanda. 12 killed.

16 April 1994: A RAF Sea Harrier was shot down by a MANPAD during Operation Deliberate Force in Serbia while attacking two Bosnia Serb tanks.

27 May 1999: AmiG-21 and a MiG-27 of the Indian Air Force were shot down during the Kargil Conflict by a Pakistani Anza Mark II MANPAD.

19 November 2000: A Su-27 was shot down by a Strela-3 in Angola fired by UNITA forces during final approach.

19 August 2002: An Igla SAM hit a Russian Mi-26 helicopter in Khankala, Chechnya. 127 killed.

27 November 2012: [Videos](#) from Syria appear to show first confirmed hit of aircraft by surface-to-air missile by Syrian rebels (see figure 3).

Anti-Aircraft IEDs

Just like IEDs are used against troops and ground vehicles, there have been instances of anti-aircraft IEDs. In 2006 the Army’s Aviation center was discussing insurgent use of devices being fired into the air and exploding with proximity fuses at U.S. helicopters. On 15 May 2009, a scout helicopter operating near Mosul, Iraq was damaged and forced to land by an anti-aircraft IED.⁹ These are used to deny landing access and to disrupt flight patterns for rotary wing aircraft.¹⁰ While not common, they have the potential of becoming more effective in a long term counterinsurgency environment.



Figure 3. MANPADS Kill, Syria (2012)

Application in Training

The threats against U.S. aircraft are numerous and must be replicated in training. Allowing aircraft to operate freely in a hostile area is unrealistic and teaches the wrong lessons to air crews. At the same time, the weapons systems deployed against aircraft must be

realistic. This means no less lethal, and no more lethal, than the real-world systems they replicate.

This can be controlled by the number of air defense systems in the training area and ensuring the hit-to-kill indicators match real-world capabilities. Recognizing

the abilities of conventional systems requires pilots to be experts on their counter-systems and will reinforce the need to adapt their tactics as the opposing forces shift theirs.

References

1. [MBDA Germany's laser demonstrator proves its air defence capabilities](#), accessed 15 November 2012.
2. [Rheinmetal successfully tests 50kW high-energy laser weapon](#), accessed 06 January 2013.
3. [Lockheed Martin's New Killer Laser Puts Israel's Iron Dome to Shame](#), accessed 19 December 2012.
4. [UPI.com, 3 arrested for pointing laser at helicopter](#), accessed 17 May 2012.
5. [FBI, Virginia Beach man pleads guilty to using laser to endanger aircraft](#), accessed 17 May 2012.
6. [ITAR-TASS, Duma seeks criminal responsibility for "laser hooliganism"](#), accessed 17 May 2012.
7. Peter Petter-Bowyer, "Winds of Destruction," Trafford Publishing.
8. David A. Kuhn, "Mombasa attack highlights increasing MANPADS threat," Jane's Intelligence Review, February 2003.
9. [Daniel W. Smith, Iraq Slogger; Mosul: US helicopter hit by "anti-aircraft IED"](#), accessed 20 May 2009.
10. [Small Wars Journal](#), accessed 04 December 2012.

IRAN'S "THUNDER" SAM

Surface-to-Air Missile Developments in Iran

by Steffany Trofino, Threat Integration Team

During a military parade in September 2012, the Iranian Revolutionary Guard unveiled a new, domestically developed medium range surface to air missile (SAM) referred to as the Ra'd system (which means thunder in Farsi). On 2 January 2013 during Iranian Naval exercise *Velayat 91*, Iran test fired the system which successfully hit its designated target.

Origins: Iranian Ra'd SAM System Versus the Russian Buk M2 SAM System

The Iranian Ra'd SAM system is a variant of the Russian Buk M2 SAM system which uses the 9M317 missile. The 9M317 missiles used in conjunction with the Buk M2 SAM system is an upgraded variant from the older Buk M1 system's 9M38M1 missiles and is reported to have an advanced fire and control system. Additionally, the engagement envelope has been expanded from 22 km to 25 km in altitude and from a 35 km range to a 45 km range. In detail, the Russian 9M317 missile is capable of engaging tactical ballistic missiles up to 20 km in range and from 2 km to 16 km in altitude. Furthermore, it is capable of engaging anti-radiation missiles up to 20 km

in range and from 100 m to 15 km in altitude, cruise missiles up to 30-35 km in range, sea-surface targets (destroyer size) from 3-25 km, and ground targets up to 10-15 km in range.

In the below picture, the Russian 9M317 missile closely resembles the Iranian Taer 2 missile used in conjunction with Iran's Ra'd SAM system. The exception however is the placement of the center fins on each system. On the Iranian Taer 2 missile the center fins are placed more toward the rear of the missile perhaps due to the center of gravity of the missile moving backward. The reason for this may be the density of the rocket engine as Iran's Taer 2 missile may have a more advance propulsion system than that of its predecessor, Russia's 9M317 missile. Enhancing the propulsion system of the Iranian Taer 2 would account for the greater range the missile is claimed to have. Also note the difference in the larger tail fins of the Taer 2 missile verses the Russian 9M317 missile, which would enhance maneuverability of the Taer 2 missile.



Figure 4. Russia's 9M317 missile (upper image); Iran's Taer 2 missile (lower image), Photos: www.Mashregnews.ir

Known Specifications of Iran's Taer 2 Missile

Little is known to date of the specifications of Iran's Ra'd system other than what is reported by Iranian news or various blogs posting messages regarding the system. What Iran has claimed thus far however can be compared to the Ra'd systems closest resemblance which is Russia's Buk M2E air defense system. Various news reports or blog posts impart the following: the propulsion system is assessed to be different than the Russian Buk M2's 9M317 missile due to the Taer 2 missile design being slightly different than Russia's 9M317 missile, as well as the enhanced range capability Iran claims with the system. Iran claims the range of the Ra'd system has the ability to trace and hit targets up to 50 km and in altitudes from 25-27 km (75,000 feet). While little is known to date of the guidance system, Iran has stated it is comparable to the Russian Buk M2E.

Differences between Russia's Buk M2 and Iran's Ra'd Systems

In assessing Russia's Buk M2 system using the Russian 9M317 missile versus the Iranian Ra'd System using the Taer 2 missile, a notable difference is the missiles design which may be due to the propulsion system. With the Buk M2 9M317, the maximum altitude is 25,000 ft. The Iranian Ra'd system's Taer 2 missile is reportedly capable of altitudes from 25-27 km (75,000 feet). Clearly with upgrading the propulsion system, the Iranian Ra'd system is more advanced than its Russian predecessor. Another difference between the two systems is the Russian BUK M2 platform can house four 9M317 missiles while the Iranian Ra'd platform is only able to house three Taer 2 missiles.



Figure 5. Photo (left): Iranian Ra'd system; Photo (right): Russian Buk M2E TELAR
Photo sources: Ra'd system, www.presstv.ir; Buk M2E TELAR, www.wikipedia.org

Note. The guidance system is missing from the Iranian Ra'd system photo (left).

Known Specifications of Russia's BUK M2 SAM System

Russian SAM System Buk-M1-2 (SA-11 FO) and Buk-M2E (SA-17)

		Weapons & Ammunition Types	Typical Combat Load
Buk-M1 Launcher with 9M38M1 Missiles		System/Complex Total	72
		Self-Propelled Launcher	8
		TELAR	4
		Onboard Reload	4
		Loader-launcher	8
		On launch rails	4
		On transport rails	4
SYSTEM Alternative Designations: 9K37M1-2 In OPFOR this is a Tier 1 system. Date of Introduction: 1997 Proliferation: At least 3 countries, export Target: FW, heli, TBM, CM, ASM, UAV, artillery rocket, ships, ground targets Primary Components: System is a modernized version of the SA-11/Buk-M1 system. It adds elements of the SA-17/GRIZZLY system (missile, LRF fire control) to the system. Battalion/Complex: CP vehicle, radar, 6 transport, maintenance, mobile test vehs. Chassis: GM-569 armored tracked for CP, radar, TELAR, launcher-loader	Dimensions: 5.5 m length, 400 mm diameter Weight (kg): 715 Max target speed (m/s): 1,200 Max missile Speed (m/s): 1,200 Propulsion: Solid fuel Guidance: RF command, inertial correction, Semi-active radar homing Warhead Type: Frag HE Warhead Weight (kg): 70 Warhead lethal radius (m): 17 Fuze Type: Proximity RF or contact Probability of Hit (Ph%): 70 TBM, 80 other Simultaneous missiles: 2 per target Other Missile: 9M317A is an anti-radiation homing missile/attack missile interceptor	data with other units in the IADS net. Assets include FOs and ELINT, e.g., Orion (pg 6-17). Launcher-loader (LL): 9A39M1-1, see 9A38M1, pg 6-71. C ² Vehicle: 9S470M1-2, see 9S470M1, pg 6-71.	
Launcher Vehicle: Name: 9A310M1-2 Description: TELAR Crew: 4 Combat Weight (mt): 32.34 Description: TELAR Dimensions (m) : 9.3 length x 3.25 width 3.8 travel/7.72 deployed height	PROTECTION/COUNTERMEASURES Jam ECCM: Noise jam 240-330 w/MHz Passive Jam ECCM: 3 Packets/100m Measures: One launcher operates radar, while others are passive. Other guidance modes reduce radar illumination time. IFF: Pulse-doppler	VARIANTS Predecessors, Buk and Buk-M1 , see pg 6-71 China is working on a Buk-M1-2 upgrade version called HQ-16 .	
Automotive Performance: See SA-11 Radio: INA Protection: Armor protection: Small arms (est) NBC Protection System: Collective	FIRE CONTROL Laser Range-finder: New addition to FCS. This permits system to engage ground targets to 15 km, waterborne targets 25 km. Sights: TV optical auto-tracker Acquisition range (km): 20, permits passive missile guidance, day and night Navigation systems: Available on all	SA-N-12: Naval version with 12 x 9M17M/ Shtil-1 missiles in a vertical-launch canister.	
ARMAMENT Launcher: Missiles per launcher: 4 Reaction Time (min): 0.25-0.5 0.1 for low-flyers Time Between Launches (sec): 2 Reload Time (min): 12 Fire on Move: No Emplace/Displace time (min): 5 Emplace time, reposition (sec): 20 for a 100-200 m survivability move.	Onboard Radar: Name: FIRE DOME, see pg 6-72 Radar: Name: 9S18M1-1/SNOW DRIFT Note: It is similar to 9S1M1 on pg 6-72.	SA-17/GRIZZLY/Buk-M2E/URAL: Russian redesign/follow-on of SA-11. It uses 9M317 missiles and 2 new radars. The system has 2 Giraffe vehicles (with dual mode radars on telescope arms), 4 TELARs, 8 LLs, Orion RF intel system, and a support coordination vehicle. All battery radars are CHAIRBACK phased array with 160 km detection, 120 for low flyers. System simultaneously tracks 10 targets and engage 4 (or 24/bn). Effective range is 45 km with Ph of 90% for FW/heli, 80 TBMs. Minimum altitude is 0 m with 80% P-hit. It now has limited fielding in 1 country.	
Missile: Name: 9M317 Range (km): 3-42, 15 with TV sights Altitude (m): Max. Altitude: 25,000 Min. Altitude: 0 with degraded Ph	Other Radars: Brigade will have EW/TA radars, such as Kasta-2E2 (pg 6-69), or one similar to Giraffe AMB (pg 6-16). Upgrade options include radars and support vehicles from the SA-17 System. Other Assets: The SA-11 digitally links to the IADS (e.g., aircraft, intel , and other SAM units. SA-10/20/11 FO radars share	A wheeled version of SA-17 is Buk-M2EK on a 6x6 Belorussian cross-country chassis.	
			
		Buk-M3: An upgrade in testing for all previous Buk-M systems with a new radar, and TBM intercept capability to Mach 4.	

Note. Buk-M1-2 is a multi-role system for SAM and surface-to-surface missile (SSM) ground/sea target attack missions.

Proliferation

While it is known the Buk M2E (export variant of Buk M2) system was not sold to Iran directly, the system was sold to Syria in 2010 and Syria may have provided the technology to Iran. Advancements made by Iran in the development of the Ra'd system also may be a result of the failure of Russia in delivering the controversial Russian S-300 SAM system to Iran. At the time Russia canceled its contract with Iran, Iran recognized the need to develop a comparable system, indigenously. Although Iran may have acquired the Russia Buk M2 system from Syria it may also have acquired further technical assistance from Belarus's AGAT Company who oversees a Russian S-300 overhauling plant in Belarus.

Ra'd Radar and Control System

Iran has not publically provided details on the Ra'd system's radar and control capabilities but suggested the capabilities "are similar to that of the Buk-M2 system." In viewing various *YouTube* videos available via open source, several photos include a radar system which is clearly visible on the forward chassis. However, during large scale public ceremonies, the radar system is noticeably absent from display.

Iranian Naval Variant: NASR

On the fourth day of Iranian Naval exercise, Iran successfully tested a naval version of the Ra'd system and dubbed the short range missile, Nasr (meaning Victory). According to Iran's Defense Minister Ahmad Vahidi, Nasr cruise missile is capable of destroying vessels up to 3,000 tons, and can be launched from both inland bases and offshore military vessels. Advancements are ongoing to the system which will include the capability to launch Nasr missiles from both helicopters as well as submarines. Rear Admiral Amir Rastegari of the Iranian Navy stated this new system had been modified by Iranian Naval experts to be installed on warships, and further indicated the system will undergo future advancements providing for the capability to be launched from helicopters as well as submarine platforms.

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.

MAIMANA MOSQUE BOMBING

Suicide Vest Attack TTP

by Laura Deatrick, OE Assessment Team (ISC-CG CTR)

On 26 October 2012, a suicide bomber wearing an Afghan National Police (ANP) uniform approached the Eid Gah mosque in Maimana. It was the first day of Eid al-Adha and people were just leaving the heavily-attended prayer service. The bomber reached the gate to the mosque complex and then detonated his explosives, killing 41 and injuring 56. The new OEA Team Threat Report, [Maimana Mosque Bombing](#),

examines the details of the attack and possible training implications.

Friday, 26 October 2012, marked the beginning of the Muslim holiday of Eid al-Adha – the Feast of Sacrifice – in Maimana. Men and boys had turned out in droves for the morning prayer services that were traditionally held in mosques on the first day of the Feast. The Eid Gah Mosque, located in the center of town, was no

exception. As it was Maimana's largest mosque, many provincial officials – including the governor, ANP chief, and several Members of Parliament – had chosen to worship there. Security was tight due to the high-profile visitors, with mosque attendees gaining entrance only after proceeding through multiple checkpoints.

The service at the Eid Gah Mosque concluded at around 0900 local time, and the hundreds of attendees began to make their way out of the mosque complex. Buildings in the region are usually surrounded by a tall fence containing a minimal number of gates, and Eid Gah was no exception. The provincial head of the ANP, Abdul Khaliq Aqsai, prepared to leave, and his vehicle had just pulled up to the northern gate. As Aqsai was exiting the mosque complex, a teenager wearing an ANP uniform approached the gate on foot. Just seconds after Aqsai entered his vehicle, the teenager detonated his ball bearing-filled suicide vest.

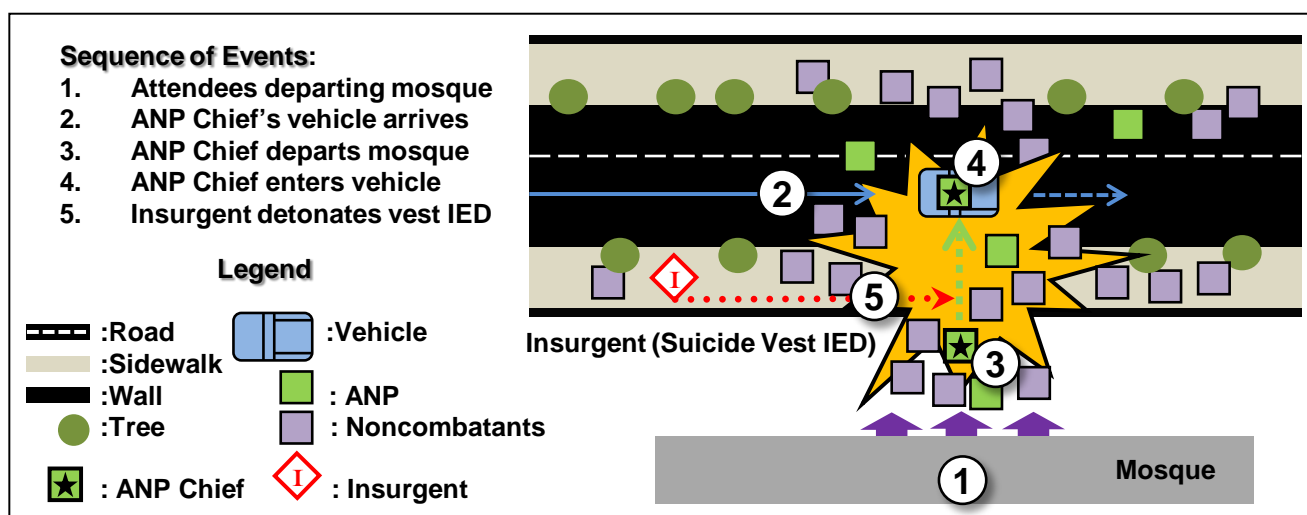
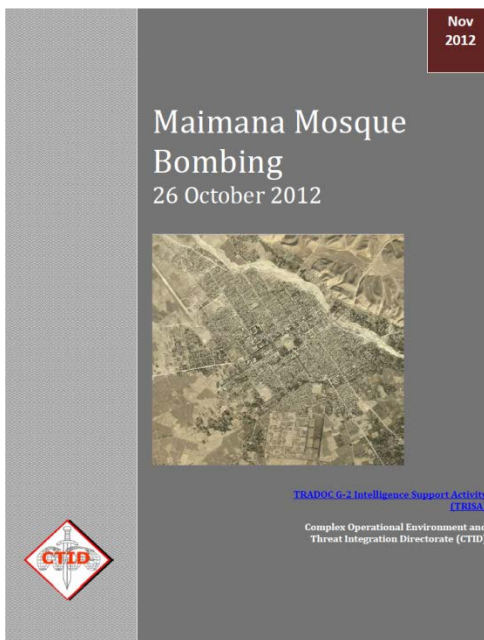
Forty people died in the resulting explosion, approximately half of which were security force personnel, including members of the ANP, Afghan National Army (ANA), and National Directorate of Security (NDS – the Afghan intelligence agency). The remainder of the casualties were civilians, including five or six children. Fifty-seven were wounded – many critically – and at least one subsequently died of his injuries. The provincial governor was still in the mosque at the time of the blast

and escaped injury, as did the Faryab Members of Parliament. Other high-ranking officials were not so fortunate. At least two ANP commanders were killed, and Aqsai was wounded in the blast. He was initially reported as killed, though this was corrected in later reporting.

Several aspects of this event will make it of interest to trainers and scenario writers. First, it is an excellent scenario of first responder and mass casualty training, and would be easy to mimic in the home-station training environment. It tests troop adherence to basic

security protocols such as ID checks and body searches, and can be used to probe for weaknesses in planned security measures. Such an event is also an excellent cause-and-effect scenario, as the attack can be easily thwarted by a single alert Soldier.

The [Maimana Mosque Bombing](#) Threat Report provides information to the Army training community on the October attack. It contains a detailed review of the event with accompanying diagram and a discussion of mosque security. In addition, it considers the likely target and possible actors, provides an analyst assessment of the attack, and examines training implications.



DECISIVE ACTION IN COMPLEX CONDITIONS

by CTID Operations

Know the Threat -- Know the Enemy

*Trained
Ready
Adaptive
Decisive*

WE are at WAR!
...on TERROR

Operational Environments to 2028: The Strategic Environment for Unified Land Operations
August 2012
Training and Doctrine Command (TRADOC) G-2

US ARMY TRADOC
KNOW THE ENEMY
TERROR THREAT INTEGRATION
TRISA

- ◆ Regular Forces
- ◆ Irregulars
- ◆ Terrorists
- ◆ Criminals
- ◆ Affiliates
- ◆ Adherents

Complex Operational Environment and Threat Integration Directorate

Decisive Action in Complex Conditions

TRISA WOT Poster No. 04-13
U.S. Army TRADOC
G2 Intelligence Support Activity

Get Your Copy of "Operational Environments to 2028"
Access AKO with password
<https://www.us.army.mil/suite/doc/37694173> (Photo: Sgt Barnes)

OE THREAT ASSESSMENT: KUWAIT

Operational Environment Assessment within Complex Conditions

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

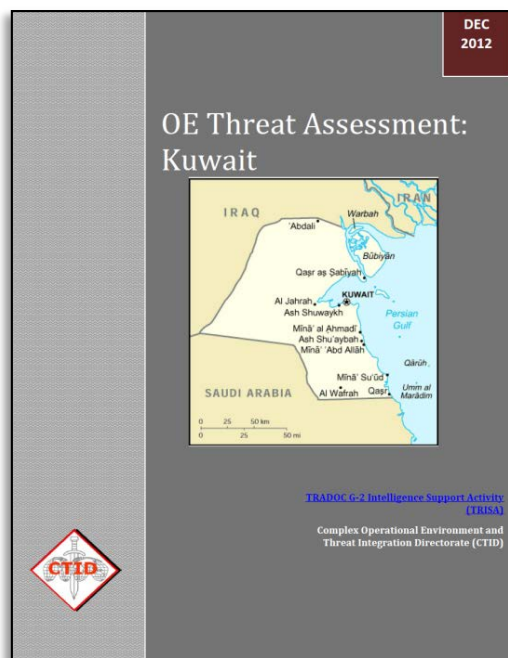
One of the first [Operational Environment \(OE\) Threat Assessments](#) completed by the Operational Environment Assessment (OEA) Team was on Kuwait, an important American ally in the Middle East. While all eight PMESII-PT (political, military, economic, social, information, infrastructure, physical terrain, and time) receive some coverage, the lion's share of the product concentrates on the military variable.

The Kuwait military contains about 16,000 active duty and 23,700 reserve force personnel in all three service branches—army, air force, and navy. While military

service has been voluntary for some time, Kuwait is considering the reinstitution of conscription.

The Kuwaiti army of 12,000 active duty personnel uses primarily Western equipment including M1A2 Abrams main battle tanks. Most of the units are mechanized and include three armored brigades, two mechanized infantry brigades, and one mechanized recon brigade. There is also one reserve mechanized brigade. Most likely the Kuwaiti army could only delay an enemy for 48 hours to allow other countries to come to its aid.

There are approximately 2,500 active duty personnel in the Kuwaiti air force that fly primarily American airframes supplemented by other Western equipment. Fixed winged units include two fighter/ground attack squadrons and one transportation squadron.



squadron and a helicopter training squadron. The Kuwaiti air defense command is subordinate to the air force commander.

About 1,500 naval personnel, 500 coast guardsmen, and 600 civilians serve in the Kuwaiti navy. Their primary purpose is to protect the country's 310-mile coastline, the sea line of communication, and any offshore hydrocarbon infrastructure.

The Kuwaiti National Guard is the largest paramilitary organization in the country at 5,000 active duty personnel, and is responsible for Kuwait's internal security.

There are few threat actors in Kuwait with no known major insurgent forces or guerrillas currently operational. While the Kuwaiti government denies that there is organized crime in the country, there are instances of human trafficking. Most private security organizations, usually hired to protect VIPs or provide advice to the Kuwaiti military, will be supportive or at least neutral to the Western military presence in the country.

View the *OE Threat Assessment: Kuwait* for more detail on all the PMESII-PT variables.

Kuwait fields one attack helicopter squadron with Apache helicopters and one transportation squadron. The Kuwaiti air force operates both a fixed-wing training

OE THREAT ASSESSMENT: EGYPT

Operational Environment Assessment within Complex Conditions

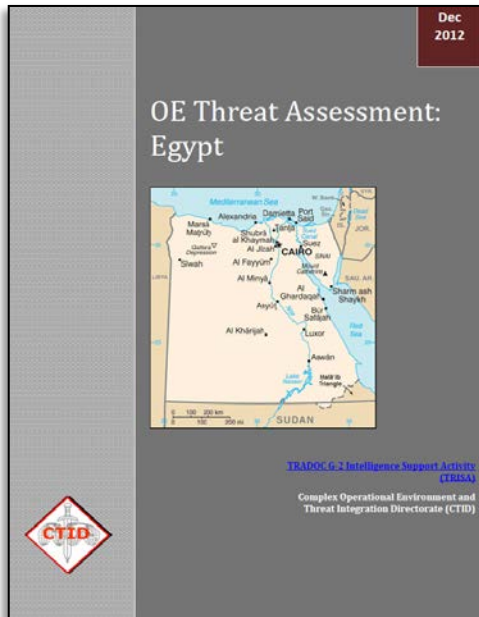
by Laura Deatrick, OE Assessment Team (ISC-CG CTR)

The Operational Environment Assessment (OEA) Team recently completed an [Operational Environment \(OE\) Threat Assessment on Egypt](#), an historical American ally in the Middle East. While all eight PMESII-PT variables (political, military, economic, social, information, infrastructure, physical terrain, and time) receive some coverage, the majority of the product concentrates on the political and military variables.

The Egyptian nation is located at an important crossroad, both geographically and politically. Physically, the country possesses the land on both sides

of the Suez Canal, thus controlling a vital chokepoint for global maritime commerce. Politically, it is still attempting to develop a new constitution and a functioning government since the resignation of President Hosni Mubarak in early 2011. While the country faces many challenges including natural disasters, unemployment, terrorist activity, and drug trafficking, the absence of a stable government that is legitimate in the eyes of its own people overrides all other concerns.

Egypt's current political system is in a state of transition that began on 25 January 2011. At that time, the "Arab Spring" manifested in the country in the form of large protests and demonstrations against the government that only grew in size and intensity with each passing day. Long-time President and U.S. ally Hosni Mubarak resigned under pressure on 11 February 2011 and handed power to the Supreme Council of the Armed Forces (SCAF), which immediately dissolved the Egyptian parliament and suspended the constitution.



The SCAF put forth an interim constitution, approved by voters and put into force in March 2011 that outlined steps to achieve a new, permanent constitution. The document called for the creation of a constituent assembly to draft the new constitution, and also included reforms such as presidential term limits and an independent judiciary. Elections for a new Parliament were held November 2011-January 2012, and both houses convened shortly thereafter. The presidential election of May-June 2012 resulted in Mohammed Morsi, the Muslim Brotherhood candidate, winning the poll and taking office on 30 June 2012.

The most pressing issue in the country is political instability. The president and the judiciary are at loggerheads, as are the Islamist parties against the moderate and liberal parties. Examples of these conflicts include the following events:

- The Supreme Constitutional Court dissolved the People's Assembly on 14 June 2012, which President Morsi subsequently attempted to

reinstate – unsuccessfully – by presidential decree.

- The first constituent assembly was also dissolved by the Court, which deemed it to be "unrepresentative." A second assembly was then appointed, but was later boycotted by moderate and liberal political parties, who viewed it as being dominated by Islamists.
- President Morsi issued a decree on 22 November 2012 granting himself new powers and removing the Supreme Constitutional Court's right to overturn any of his decisions. Popular demonstrations immediately broke out, at one point forcing Morsi to flee the presidential palace. Morsi subsequently annulled the decree on 9 December after continuous protests, some of which turned violent.
- Thousands of judges went on strike after Morsi's 22 November decree. As it is judges who oversee popular elections in Egypt, it was possible that the December 2012 constitutional referendum either would not be able to occur due to the refusal of the judiciary to oversee it, or that it would occur despite lack of judicial oversight and then be declared null and void by the courts.
- The remaining members of the second constituent assembly rushed the completion of a proposed constitution. Despite repeated requests by opposition members, Morsi refused to delay the December 2012 referendum. Moderate and liberal parties protested the vote, stating that the proposed constitution is unrepresentative and will impede on the rights of women and minorities. Despite their objections, the referendum occurred as scheduled, and the constitution won approval.

As these incidents show, Egypt remains politically unstable nearly two years after the resignation of Mubarak. Despite the progress that has been made, there is the real possibility that the country will fall back into fighting and undergo yet another revolution.

View the *OE Threat Assessment: Egypt* for more detail on all the PMESII-PT variables.

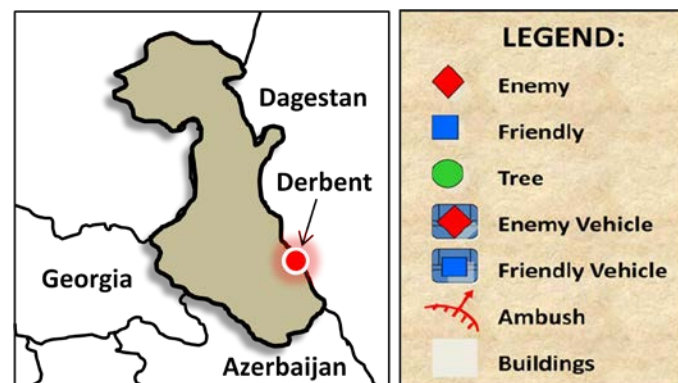
ASSASSINS TARGET IMAMS IN DAGESTAN

Threat TTP

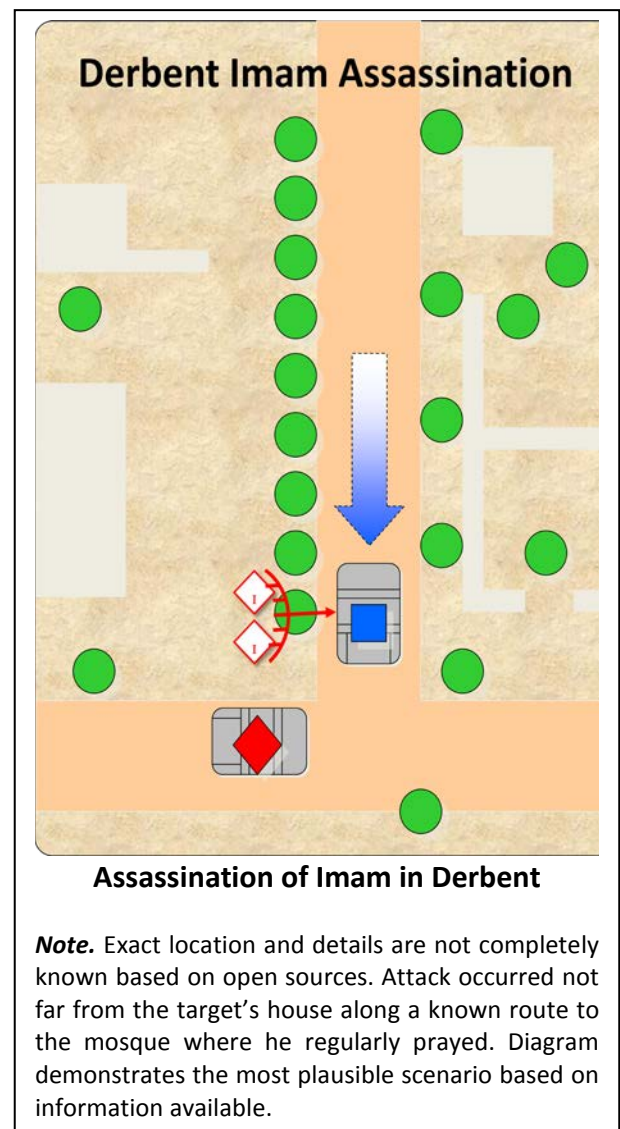
by H. David Pendleton, OE Assessment Team (ISC-CG CTR)

On 30 October 2012, two assassins killed a Salafist imam in Derbent, Dagestan, Russia with small arms fire as he was traveling in his car from his home to a mosque for morning prayers. The assassins also killed the imam's 82-year old father and his older brother in the attack. This was the fifth attack on a religious cleric in Dagestan during 2012. In the last six years, over 37 imams and muftis have been killed in the North Caucasus region of Russia.

The plan was very simplistic, but the imam made it easier for assassins. Kalimulla Ibragimov, an unregistered Salafist imam, traveled basically the same route every morning to attend morning prayers. Knowing the victim's set routine, the attackers waited with small-arms weapons along Ibragimov's primary route where the automobile would need to slow down. As the vehicle slowly passed by, the attackers fired their weapons into the vehicle, killing all three occupants before the assailants escaped in their own vehicle.



Many of the attacks on religious figures in Dagestan can be attributed to a conflict between the Sufi and Salafi sects of the Muslim faith in the region. While most of Dagestan's residents practice the Sufi version of Islam, the more radical and conservative Salafi branch continues to make inroads into the country. Because the attack on the Salafist cleric occurred within days of the one-year anniversary of the assassination of Sufi Sheikh Sirajuddin Israilov, it is possible that the motive was religious.



It is also possible, however, that many of these attacks are not actually based on religious ideological differences, but are simply revenge killings. In a Dagestani culture where retribution for slights or perceived slights is important, many of the killings could be revenge by one family against another with religion masking the true motive for the attack.

This assassination is an excellent example of *Small Arms Fire (SAF): Moving Target* attack. Details of this type of attack and others can be found in the [TRADOC G2 Handbook No. 1.07 C3](#), *A Soldier's Primer to Terrorism*

TTP: Tactics, Techniques, and Procedures in Complex Operational Environments.

The Threat Report, "[Religious Assassination in the North Caucasus](#)," provides additional details on the Ibragimov assassination, the analyst's assessment, personal

security techniques to reduce the likelihood of being an ambush victim, and the Russian response to the to the assassinations that are partially related to the insurgency in the region.

Director's Corner: Thoughts for Training Readiness



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

DATE and DATE Implementation

The [Decisive Action Training Environment \(DATE\)](#) is a composite model of real-world environments we may face in the future. All of the conditions and actors within DATE are real. Fictitious names are used for two reasons. First, the DATE, like any environment created for unclassified training, must be compliant with AR 350-2, *Opposing Force Program*. Second, the need to fit a composite model of many varied conditions into a relatively small portion of the globe means that no country or actor cell, unit, activity, or group will be an exact match for its collective real-world counterparts. The U.S. Army has chosen the South Caucasus physical environment for DATE for a host of reasons as TRISA captures the essential nature of actors from around the world and fits them into the mosaic of DATE. No actor set in DATE is a one-for-one match with a real-world physical environment so the use of actual names for countries would be misleading.

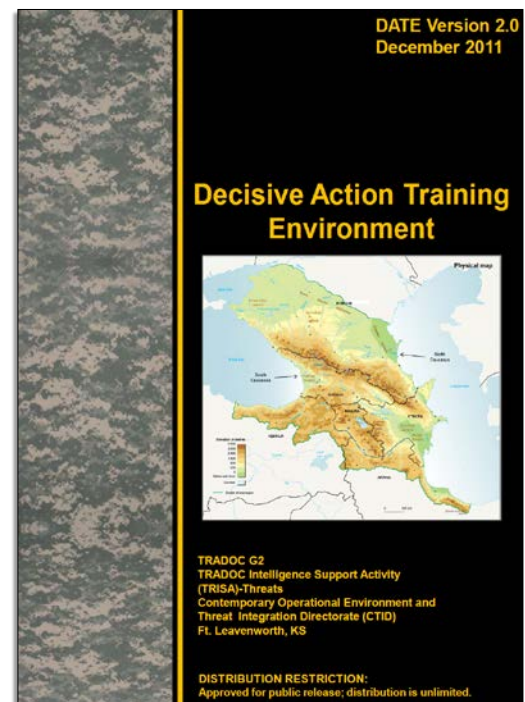
DATE—an Operational Environment Enterprise (OEE) Product

The DATE is an Operational Environment Enterprise (OEE) product that is created, researched, updated, and maintained by the Complex Operational Environment and Threat Integration Directorate (CTID) of U.S. Army TRADOC G2. If there is something about the DATE that you would like to see changed or adjusted, please contact us. We also provide oversight of the DATE document. CTID ensures that that DATE is used properly by exercise planners and scenario developers. If changes are required to support training readiness, CTID makes the change to the DATE document. In order to maintain the ability to do linked exercises and enforce training standards, DATE must remain consistent across training venues.

DATE—Implementation is Different

DATE *implementation* is something different. The CTID at TRISA is responsible for maintaining the DATE currency of relevant Hybrid Threat (HT) and operational environment (OE) CONDITIONS.

In order to implement DATE, terrain must be loaded into simulation centers, operations orders (OPORDS) must be produced and coordinated, "roads to war" established, courseware developed, etc. The simple way to keep it all straight is—



When you develop your training plans and conduct your exercises, CTID is your one-stop shop for the “red” and “green” conditions of the DATE.

For the “blue” aspects of DATE, the entry point is the U.S. Army Combined Arms Center (CAC) and its Combined Arms Center-Training (CAC-T). If your training issue is having trouble finding the “right condition set” for a training objective, we will fix that for you. If your training issue is finding an existing scenario to support your training objective, we will work with you to help locate what you want, if available, on the Common Framework of Scenarios (CFoS) repository. Also, until the (CFoS) is populated with more DATE-based scenarios, we will put you in touch with those who have already developed DATE scenarios and associated materials (OPORDs, master scenario events lists (MSELs), data sets, biometrics, role player instructions, etc.).

DATE—Who creates the *CONDITIONS* of “Red” and “Green” for the DATE?

A key point to remember is that the DATE (“red” and “green”) conditions are made here, at Fort Leavenworth, by CTID. DATE scenarios (“blue”) are made by a number of organizations: Combat Training Centers (CTCs), Centers of Excellence (CoEs), units, etc. Regardless of which part of DATE implementation involves your organization, you can always call us or email us for assistance. If it’s not our (CTID’s) role to directly fix an issue, CTID will help you find the correct action agent. My directorate’s point of contact info is listed at the back of this *Red Diamond*.

Jon

TRISA-CTID PRODUCTS FOR THREATS AND AN OPERATIONAL ENVIRONMENT

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 v. 1.0
*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>

TRISA THREATS TERRORISM TEAM ADVISORY-QUARTERLY REVIEW

Threat Fusion and Antiterrorism Awareness

by CTID Operations

U.S. Army Training and Doctrine Command G2

TRADOC G2 Intelligence Support Activity
Antiterrorism - Counterterrorism

Terrorism

T3 Advisory

Threat Fusion – Situational Awareness

You are key = Report Suspicious Activity!

The eGuardian Process:
The Military Police (MP)/Provost Marshal – Directorate of Emergency Services (PM/DES) or Criminal Investigation Division (CID) receive a report of suspicious activity and enter information into eGuardian.
The report goes to Headquarters CID where trained law enforcement analysts and CID agents review the information for potential nexus to terrorism and refer report into the eGuardian system. Law enforcement personnel across the Army can review the report and incidents in their area.
Task Force (JTTF) is the report in the system.

Look Listen Report

Report suspicious activity to local Provost Marshal or CID.

WAR on TERROR

See Army Knowledge Online.
Access: www.army.mil/suite/doc/25952049
Enter: www.army.mil/suite/doc/25952049
See Army Knowledge Online Threat for training.

OCT 2012 No. 01-13

U.S. Army Training and Doctrine Command G2

TRADOC G2 Intelligence Support Activity
Antiterrorism - Counterterrorism

Terrorism

T3 Advisory

Support Threat Fusion–Create Situational Awareness

Everyone has a Protection Role!

Report Suspicious Activity?

- Possible Surveillance
- Theft of Badges-Uniforms
- Misrepresentation-Identification Card
- Attempted Intrusion
- Vandalism-Tampering
- Testing of Security

Report suspicious activity to Provost Marshal or MPs.

WAR on TERROR

See Army Knowledge Online.
Access: www.army.mil/suite/doc/25952049
Enter: www.army.mil/suite/doc/25952049
See Army Knowledge Online Threat for training.

NOV 2012 No. 02-13

HQDA Antiterrorism Themes FY 2013

1st Quarter theme was:

Threat Fusion

- ◆ Report Suspicious Activity.
- ◆ Everyone has a role.
- ◆ Create Situational Awareness!

Report Suspicious Activity or Behavior

iWATCH ARMY

iREPORT **iKEEP US SAFE**

See Something Say Something

U.S. Army Training and Doctrine Command G2

TRADOC G2 Intelligence Support Activity
Antiterrorism - Counterterrorism

Terrorism

T3 Advisory

Threat Fusion–A Collective Action for Security

What is YOUR ROLE?

- Detect
- Deter
- Dissuade

Everyone has a Active Role to Report!

Report Suspicious Activity?

- Odd Questioning
- Recurring Photography
- Attempted Intrusion?
- Cell Phone Found
- Testing of Security?
- Possible Surveillance?
- Odd Questioning?
- Suspicious Containers?
- I.D. Card Found

Report suspicious activity to Provost Marshal or MPs.

WAR on TERROR

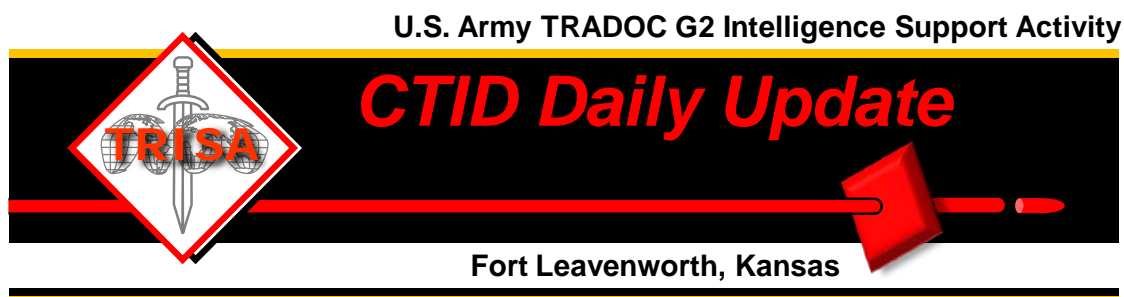
See Army Knowledge Online.
Access: www.army.mil/suite/doc/14886365
Enter: www.army.mil/suite/doc/14886365
See Army Knowledge Online Threat for training.

DEC 2012 No. 03-13

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.



- 02 January. [Seven aid workers shot and killed in Pakistan](#)
- 03 January. [Free Syrian Army claims chemical weapons capability](#)
- 04 January. [Warehouse stock of anti-tank missiles found in northern Sinai](#)
- 07 January. [Myanmar government forces shell HQ for the Kachin rebels](#)
- 14 January. [French warplanes hit central Mali in fierce fighting between Soldiers, Islamist guerrillas](#)
- 15 January. [U.S. fighters join Japan's F-15s over the disputed East China Sea islands](#)
- 16 January. [Qaeda-linked group claims seven Americans among 41 hostages held in Algeria](#)
- [Wave of attacks erupts in Iraq, 33 dead, 218 wounded](#)
- 17 January. [Algerian forces launch operation to break desert siege](#)
- 18 January. [Kurd-jihadist firefights rage in Syria; French journalist killed in Aleppo](#)
- 22 January. [Turkish Army launches large offensive against PKK](#)
- 23 January. [The rise of Islamists in the Sahara](#)
- 24 January. [Boko Haram threatens the African continent, says Nigerian President](#)
- 27 January. [Clash of militants leaves 53 killed in Pakistan](#)
- 28 January. [Egypt: President Morsi declares state of emergency, 48 killed in police clashes](#)
- 29 January. [80 bodies found in Aleppo, Syria](#)
- 30 January. [Israeli warplane 'struck target on Syria-Lebanon border' amid weapons fears](#)
- [Israeli warplanes bombed research center near Damascus](#)
- 31 January. [Syria, Iran warn of consequences to Israeli strike](#)

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 Force 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

All CTID products can be found on AKO. Use our products at:

www.us.army.mil/suite/files/11318389

