



Red Diamond

Threats Newsletter



TRADOC G-2 Operational Environment Enterprise
ACE Threats Integration

Fort Leavenworth, KS

Volume 7, Issue 04

APR 2016

INSIDE THIS ISSUE

TTR: Iran.....	1
Director's Corner.....	3
ATGM Threats Primer	4
Threats on ATN.....	9
Leclerc MBT & WEG.....	10
DATE Concepts	13
Disrupt OPFOR Task.....	20
CbT Poster	28
Threats ACE-TI POCs.....	29

OEE *Red Diamond* published
by TRADOC G-2 OEE
ACE Threats Integration

Send suggestions to:
ATTN: *Red Diamond*
Jon H. Moilanen (IDSI Ctr),
Operations, G-2 ACE-TI
and
Laura Deatrick (CGI Ctr),
Editor, G-2 ACE-TI
and
Angela McClain-Wilkins
Guest Editor
(DAC)

THREAT TACTICS REPORT: IRAN—COMING SOON! 2016

by [Kristin Lechowicz](#), TRADOC G-2 ACE Threats Integration (DAC)

The TRADOC G-2 ACE Threats Integration directorate will soon publish a Threat Tactics Report (TTR) focused on the Islamic Republic of Iran's military. The TTR: Iran is the next installment within a series of products that supports the US Army's training community.

The TTR: Iran is currently in the editing phase of production and is projected to be released in the summer of 2016. This product is part of the TTR series that includes reports on North Korea, China, Syria, Boko Haram, Russia, and the Islamic State of Iraq and the Levant (ISIL). The [TTR series](#) examines either a country of interest, such as Iran, or a potential threat actor, such as the Islamic State of Iraq and the Levant (ISIL). The primary purpose of TTRs is to convey to the training community how a group or country conducts military operations. The reports contain information on military doctrine, force structure (order of battle), weapons and equipment, and the warfighting functions. The training community can then use TTRs to better replicate similar threat tactics and capabilities using the [Training Circular \(TC\) 7-100 series](#) and actor-specific conditions found in the [Decisive Action Training Environment \(DATE\)](#).



Hybrid Threat

The diverse and dynamic combination of regular forces, irregular forces, terrorist forces, and/or criminal elements unified to achieve mutually benefitting effects.

ADRP 3-0 *Unified Land Operations* (2012)



RED DIAMOND TOPICS OF INTEREST

by [Jon H. Moilanen](#), TRADOC G-2 ACE Threats Integration, Operations, *Red Diamond* Newsletter (IDSI Ctr)

This issue of *Red Diamond* creates a special moment in the Directors' Corner. We recognize, in memoriam, the passing of "Rick" McCall—a former teammate and intelligence senior analyst in the TRADOC G-2 ACE Threats Integration Directorate.

The lead article in this *Red Diamond* is a threat primer on anti-tank guided missiles (ATGMs), and provides an introduction to threat capabilities and the increasing availability of these weapons systems in current operational environments throughout the world. This ATGM primer is a collaborative effort between the TRADOC G-2 ACE Threats Integration Directorate and the Defense Intelligence Agency's Missile Space Intelligence Center (MSIC).

An article on the French Leclerc main battle tank (MBT) presents information on system capabilities and performance, and states training implications. Deployed in peacekeeping operations in Kosovo and Lebanon, the Leclerc has been used in combat for the first time in Yemen by the United Arab Emirates, as part of the Arab Coalition led by the Kingdom of Saudi Arabia. The Leclerc MBT will be included in the 2016 update to the TRADOC G-2 *Worldwide Equipment Guide*.

The [Decisive Action Training Environment \(DATE\)](#) provides conditions for operational environments, threats, and

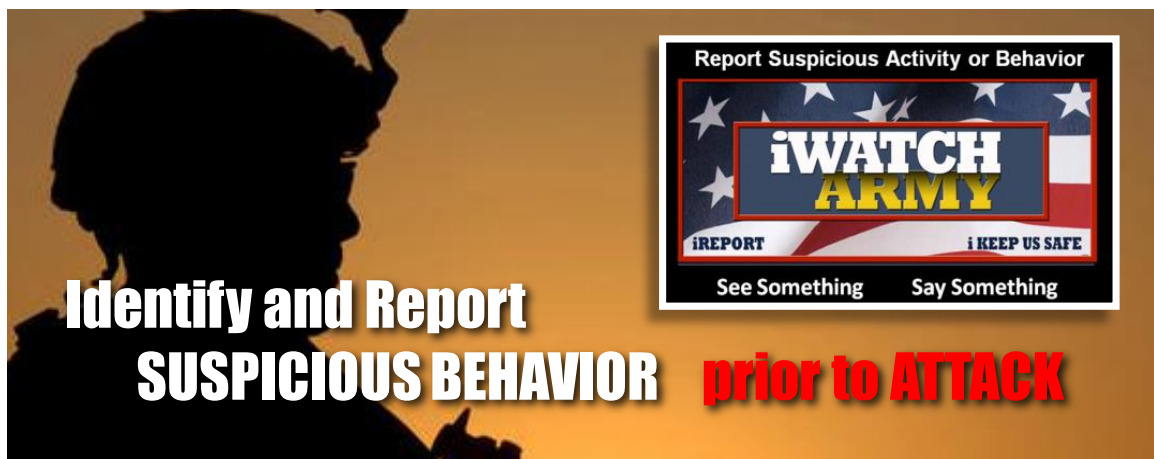
hybrid threats for training, professional education, and leader development venues. The DATE is not a scenario, but can be adapted by scenario designers to develop challenging environments for US Army readiness.

The OPFOR Tactical Task List, published in [TC 7-101, Exercise Design](#), is specific to an opposing force (OPFOR). This list of tasks is undergoing a significant update at TRADOC G-2 ACE Threats Integration (ACE-TI), and will be incorporated in the next update to [TC 7-100.2, Opposing Force Tactics](#). This article describes *disrupt* as a tactical task to upset an enemy's formation or tempo, interrupt the enemy's timetable, cause an enemy to prematurely commit combat power, and/or cause an enemy to attack in piecemeal manner. The task and subtasks are a baseline for training this OPFOR task to standard.

A point of contact list for TRADOC G-2 ACE Threats Integration provides email and telephone information to assist in OE and threats support to training, professional education, and leader development.

To be added to the *Red Diamond* e-distribution list, contact:

Dr. Jon H. Moilanen (IDSI Ctr)
TRADOC G-2 ACE Threats Integration, Operations
jon.h.moilanen.ctr@mail.mil





Director's Corner

Thoughts for Training Readiness



In Memoriam

Sergeant Major Richard G. McCall (US Army, Retired)

We bid farewell to "Rick" McCall—an intelligence senior analyst in the TRADOC G-2 ACE Threats Integration Directorate for over twenty years before his recent retirement. He passed away on March 14, 2016. Having entered the US Army as an infantryman, he served a tour in the Vietnam War and then transitioned during his distinguished career to military intelligence and achieved the rank of sergeant major before retiring from active duty. He continued significant contributions to the US Army as a Department of the Army Civilian intelligence senior analyst. His analytic expertise, practical experiences, and ability to accurately describe the organizations, doctrine, tactics, and techniques of a hybrid threat were integral to a small team of TRADOC G-2 experts at Fort Leavenworth, Kansas as we analyzed and documented the many threat challenges facing the United States Army of the 21st Century.



Rick was instrumental to the development and publication of the innovative and groundbreaking US Army Training Circular 7-100 series on regular force and irregular force threats as baseline guidance to the US Army's Operational Environment and Opposing Force (OPFOR) Program. He demonstrated particular expertise and skill in describing threat force structure for regular and irregular forces and defining the details of weapon systems, equipment, and other materiel for OPFOR tactical to strategic echelon units and task organizations.

His invaluable contributions to US Army readiness is an enduring accolade to his professional excellence as a leader, teammate, and friend. Rick McCall is gone but he will never be forgotten.

[Jon Cleaves](#), Director, TRADOC G-2 ACE Threats Integration (DAC)



by [MAJ Michael Trujillo](#), (US Army) Defense Intelligence Agency's Missile Space Intelligence Center and [Kristin Lechowicz](#), TRADOC G-2 ACE Threats Integration (DAC)

This article provides an introduction to antitank guided missiles (ATGMs) and illustrates the potential threat along with scenario replication for the training community. This ATGM primer is a collaborative effort between the TRADOC G-2 ACE Threats Integration Directorate and the Defense Intelligence Agency's Missile Space Intelligence Center (MSIC). This article addresses ATGM characteristics, warhead types, usage, proliferation, and the potential for doctrinal opposing force (OPFOR) replication. The ATGM threat to US and coalition forces is not a new phenomenon in the strategic environment. Many systems are increasing in lethality and are being proliferated, making the ATGM available to regular and irregular forces worldwide.

ATGMs have been used in nearly every major conflict since the end of WWII. Their precision, mobility, and penetration capability make for a lethal weapon system that is highly sought after among both state and non-state organizations. Although the ATGM is intended to increase the lethality and protection of combined arms formations in peer-to-peer conflict, availability, ease of use, and mobility make the ATGM an excellent weapon for a hybrid threat. ATGMs are considered one of the greatest land-based threats for armor in a current complex threat environment.¹

Recent videos from the Syrian conflict reveal significant trends and techniques with regards to ATGM usage against a wide variety of targets. As mentioned earlier, ATGMs as a threat are not a new development on the modern battlefield. The evolution of the ATGM followed the moderate success of unguided rockets against armored targets in World War II. The German military developed the X-7, or *Rotkappchen*, that was specifically designed for the anti-armor role.² The concept of the X-7 was simple: delivery of a formidable warhead, capable of penetrating armor, with increased range, accuracy, and lethality; however, these early anti-armor weapons were not guided to the target.

ATGMs are distinguished from other antitank weapons in that their missile is guided to the target. The concept is that an operator holds crosshairs on the target and the missile tracker directs the missile to that point.³ The tactical versatility of the ATGM makes it more of an all-purpose guided missile, with the ability to engage varying targets from long distances. With engagement ranges of up to 5,500 meters and precision-guided munitions, the ATGM is a combat multiplier for any maneuver formation, whether regular, irregular, criminal, or a hybrid threat.

As of December 2014, the Small Arms Survey organization estimates that within the Middle East and North Africa region there are 27-44 active non-state groups that possesses 11 different types of ATGM capabilities.⁴ The likelihood of the US and coalition forces entering an operational environment with some sort of ATGM threat is highly likely and the importance of understanding the basic threats is critical.

ATGM Design and Characteristics

The ATGM's inherent design includes a missile body, boost motor, aerodynamic control, guidance, and warhead. The basic composition of the ATGM system includes the missile and the launch platform/guidance system.

- **Guidance:** ATGMs use two categories for precision guidance, which takes the missile from its launch platform to the intended target. ATGMs use homing and line of sight guidance with variations for each.
- **Homing** guidance for ATGMs includes passive, active, semi-active, and command. These types of homing guidance typically involve the integration of a seeker into the head of the ATGM.

- **Passive homing** involves seeking the radiant energy of its target, whereas active homing emits energy against its target and homes in on the reflection. Although passive and active homing involve what is commonly referred to as “fire and forget,” semi-active homing requires the gunner to mark the target, thus guiding the missile. An ATGM enabled with command homing offers the gunner the ability to “see” what the missile sees through a television or infrared (IR) transmitter. Command homing is a very versatile guidance type, as it can integrate a preplanned flight until the gunner is ready to assume control and initiate the attack on the intended target.
- **Line of sight (LOS)** guidance is typical of most ground-based ATGM systems in use. This involves a clear and unobstructed view between the gunner and his intended target. There are three basic types of LOS guidance, with advantages and disadvantages for each.
- **Manual command to line of sight (MCLOS)** guidance ATGMs require a very high level of skill and proficiency to operate. MCLOS ATGM systems require the gunner to not only maintain observation of the target, but to control the missile flight profile. MCLOS guidance typically involves a sight and joystick, allowing the gunner to maintain visual contact of the target while comparing it to the missile in flight, thus guiding the missile to its target. Due to the high training threshold for these systems, active development of MCLOS systems has ceased among countries that develop ATGMs.⁵
- **Semi-automatic command to line of sight (SACLOS)** ATGMs offer improved integration between gunner and missile, while only requiring the gunner to maintain visual contact of the intended target. SACLOS launchers incorporate tracking mechanisms that allow the launch guidance system to track the missile through an IR source such as a flashing light (beacon) or a high temperature flare. As the gunner maintains his crosshairs on the target, missile flight adjustments transmit through a wire connected directly to the missile.
- **Laser beam riding (LBR)** ATGM systems use the same tenants as SACLOS systems; however, the link between the missile and launch guidance system occurs through a laser beam, which guides the missile onto the intended target. The launcher projects a laser cone, which a rearward-looking receiver on the missile uses to maintain the correct flight profile to the target.

ATGM Warhead Types

The destructive power of the ATGM lives within the warhead. There are several warhead variants and uses for each. The ATGM warhead types are as follows:

- **Shaped Charge (SC):** SC warheads are the most common, as they offer the armor-penetrating capability required of an ATGM. Unitary SC warheads achieve penetration through the explosive re-formation of an inverted metallic cone. The explosive charge reforms the inverted cone warhead into a metallic jet that penetrates the armor of its intended target. Additionally, some ATGMs contain tandem SC warheads, which operate fundamentally the same but are designed to defeat reactive armor. A smaller precursor inverted cone initiates first and creates the penetrating jet ahead of the main warhead, which continues penetration after the reactive armor’s defeat.
- **Explosively Formed Penetrator (EFP):** The initiating process for the EFP mimics that of the SC warhead, with one notable exception. The EFP typically involves creating an explosively-formed slug versus a penetrating jet. Although the EFP has limited penetrating capability, it can cause devastating behind-armor effects. Additionally, the EFP warhead is very useful in ATGMs that use a top-down attack profile, taking full advantage of the thin armor on the top of armored vehicles.
- **Blast/Thermobaric Warheads (TB):** SC warhead ATGMs are useful for destroying heavy or armored targets; however, given the all-purpose nature of ATGMs, there must exist a capability to target softer targets, such as bunkers and dismounted personnel. Blast fragmentation warheads are the “shotgun shell” of the ATGM warhead variety. The explosive charge initiates high-speed fragmentation, which is highly useful against personnel in the open and slow-moving airborne threats such as rotary wing aircraft. TB warheads essentially create enormous overpressure and heat upon detonation. They are highly effective against urban structures and rotary wing aircraft.

ATGM Launch Platforms

ATGMs are designed for employment from multiple platforms, again demonstrating the versatility of this highly-lethal weapon system. The main categories include portable (launched from a tripod or ground-based configuration), vehicle borne (wheeled or tracked), gun-launched (launched through the main gun of a tank or towed direct fire weapon), airborne (fixed or rotary wing aircraft), or waterborne.

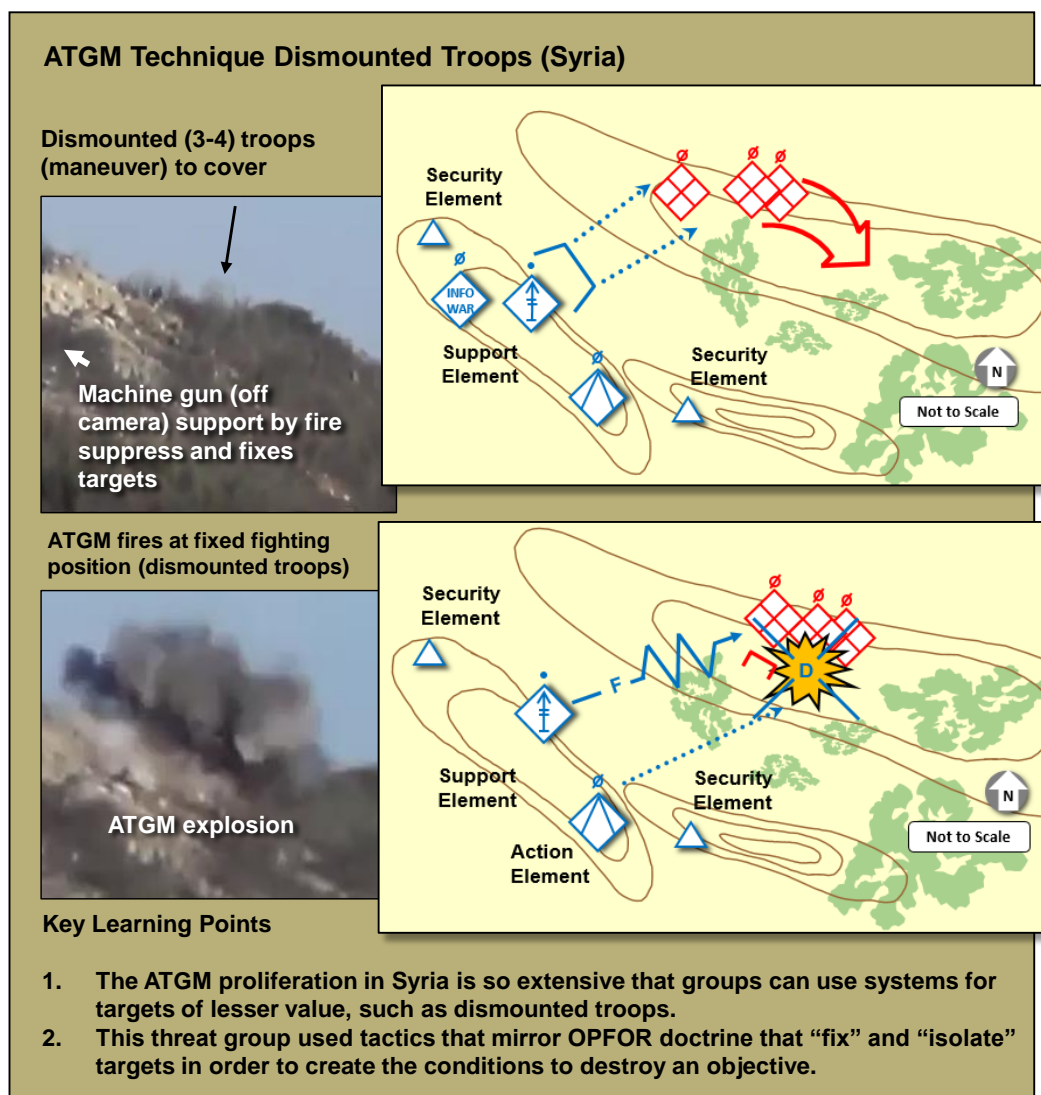


Figure 1. ATGM assault diagram and [graphic](#)

ATGMs in Modern Conflict

An applicable example of hybrid ATGM usage dates back nearly 10 years to the 2006 Israel-Hezbollah War. Following cessation of hostilities, the Israeli Defense Force (IDF) became painfully aware of the requirement to develop its manpower, training, and anti-ATGM protection in light of the swarm techniques prosecuted by Hezbollah ATGM teams. Learning from experience that small mobile teams equipped with antitank weapons are a decisive force against a heavily-armored adversary, IDF was forced to increase the armor balance within its frontline units. The effective use of dispersed and highly-mobile ATGM teams during this conflict resulted in as many as 20 Israeli tanks destroyed, with an estimated 48 tanks engaged by ATGMs.⁶ Similarly, at the onset of the Syrian Civil War, Syrian opposition elements captured various

types of Russian- and European-made ATGMs. The opposition began posting ATGM firings on social media, such as YouTube, for propaganda and training aids in early 2012, and continues postings to present day. The opposition's use of mobile and highly-dispersed ATGM teams is reminiscent of the tactics employed by Hezbollah in 2006. The pictures and a diagram at figure 1 represent an ATGM attack in Syria.

ATGM Proliferation to Insurgent Groups

ATGM proliferation to jihadist groups changes the tactical landscape of the complex operational environment. Insurgent groups including the Islamic State of Iraq and the Levant (ISIL) and Al Nusrah Front (ANF) possess ATGMs, and demonstrate skill and tactical competency in their employment. Through unknown means, ANF acquired the US TOW 2A ATGM in April 2014 and posted videos on social media of attacks against Syrian Arab Army targets.⁷ Although there is no definitive indication in open sources that ISIL possesses TOW 2A ATGMs, the group certainly possesses a variety of Russian-made ATGMs including the Konkurs (AT-5) and Kornet (AT-14). ATGM proliferation to ISIL provides its formation with a new level of lethality and protection via weapon standoff, with numerous examples of attacks against US military platforms provided to the Iraqi Security Forces (ISF) in open sources and social media.

Proliferation of modern ATGMs to non-state groups is not confined to the Syrian conflict or to groups operating in Iraq. The current conflict in Yemen demonstrates non-state use of ATGMs by the Houthi rebel groups operating in the southwestern regions bordering Yemen and Saudi Arabia. Similarly, there is evidence in open sources of Houthi rebel using Kornet (AT-14), Konkurs (AT-5), and Metis (AT-7) ATGMs to target M1 Abrams and M-60 Patton variant tanks.

OPFOR Implications and Training Support

The modern use of ATGMs lends itself to the hybrid warfare fight, capitalizing on the highly-mobile nature of these weapon systems, particularly in their dismounted configuration. Examples derived from real world ATGM threats should be incorporated into the training environment. As an example, live OPFOR employment of replicated ATGMs at the combat training centers (CTCs) should take into account the various means of employment by both regular and irregular forces. The following picture from the Joint Multinational Readiness Center (JMRC) shows a dismounted OPFOR soldier firing an ATGM at a rotational training unit.



Figure 2. [OPFOR 1/4 soldier fires an ATGM during JMRC's Combined Resolve exercise](#)

The ATGM issue presents a daunting challenge for training or deploying units. The question arises as to how a unit successfully mitigates the risk of a precision-guided munition launched from multiple kilometers away. A CTC scenario developer can use the AT-14 Russian Kornet ATGM that is included as a Tier 1 OPFOR weapon system in the latest WEG. This system can be replicated in all available configurations during [Decisive Action Training Environment \(DATE\)](#) exercises to challenge a rotational training unit. This ATGM system—capable of achieving catastrophic effects against a maneuver formation, hard to locate, and highly-proliferated among non-state groups—is essential in enabling OPFOR units to raise the bar as they support realistic training based on real-world events.



Figure 3. US Army training material for hybrid threat scenario development (sample)

Training Circular [\(TC\) 7-100.2](#) and [TC 7-100.3](#) support the CTCs by referencing the usage of tactics that include ATGMs for both regular and irregular elements/forces. Scenario developers can find additional information on ATGM units, organization, or weapons systems in [TC 7-100.4](#), its associated [Threat Force Structure](#), and the [Worldwide Equipment Guide \(WEG\)](#). The [Red Diamond](#) also includes articles on real-world threats such as ATGMs to inform and stimulate the training community.

Notes

- ¹ US Army, TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. [Worldwide Equipment Guide – Volume 1: Ground Systems](#). December 2015. Pg 5-2.
- ² Wehrmacht History, [X7 Rotkappchen Anti-Tank Missile](#). Accessed February 2016.
- ³ US Army, TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. [Worldwide Equipment Guide – Volume 1: Ground Systems](#). December 2015. Pg 5-2.
- ⁴ Small Arms Survey. [Armed Groups and Guided Light Weapons: 2014 Update with MENA Focus](#). December 2014.
- ⁵ Janes. [Anti-tank Guided Missiles](#). 26 October 2015.
- ⁶ Anthony H. Cordsmen. [Lessons of the 2006 Israeli-Hezbollah War](#). Center for Strategic and International Studies. 2007. Pgs 108–119.
- ⁷ Liveleak. [DShK & BGM-71 TOW Missile attack SAA checkpoint](#). Posted 6 April 2014. (Video is no longer accessible.)

Find the Threats/Opposing Force Products on **ATN**

<https://atn.army.mil/>

Leader Development

Soldiers Skills

Training for Operations

- Cyber Electromagnetic Activities (CEMA) Resources
- Deputy Commanding General Course

- SHARP Training
- Warrior Tasks and Battle Drills
- Mandatory Training (AR 350-1)
- U.S. Army Physical Readiness

- Personal Protection
- Traumatic Brain Injury (TBI) Training Support Package
- TRADOC G2 ACE Threats Integration



TRADOC G-2 ACE Threats Integration

Operational Environment and Training Products

TRADOC G-2 ACE is the Army's lead to study, design, document, validate, and apply Hybrid Threat and Operational Environment (OE) CONDITIONS that support all U.S. Army and joint training and leader development programs. These pages include Operational Environment Products, Threat Tactics Products Opposing Force (OPFOR) Doctrine, and the Red Diamond Newsletter. Threat Tactics Course Material is also housed here.

Browse the e-Folders

Home

DATE/RAFTEs

OPFOR/Threat Doctrine

Threat Tactics Course

Threat Tactics Reports

Operational Environment (OE) Estimate

Opposing Force (OPFOR)/Hybrid Threat Doctrine

Decisive Action Training (DATE) and Regionally Aligned Forces Training Environment (RAFTEs)

Red Diamond Newsletter

Threat Tactics Reports

Worldwide Equipment Guide (WEG)

OE Assessments (OEAs), OE Quick Guides and OE Threat Assessments

Threat Reports and Handbooks

Combatting Terrorism Posters (Cbt) and Threats Terrorism Team (T3) Advisories

Threat Tactics Course

Hosted Materials

TRADOC G-2 *Worldwide Equipment Guide*: French Leclerc Tropicalized Main Battle Tank Leclerc EAU

by [Marc Williams](#), TRADOC G-2 ACE Threats Integration (ThreatTec Ctr)



The French Leclerc Tropicalized Main Battle Tank (MBT) Leclerc EAU is sometimes called the AMX-56. It is a class 69—in combat order with jettisonable fuel drums—heavy track-laying armored MBT and is extremely mobile. It can operate in a nuclear/biological/chemical (NBC) environment and can fire while moving, in all weather, on stationary or moving targets.

The Leclerc has been operationally deployed in the past for peacekeeping operations in Kosovo and Lebanon. However, since 2015 it has been used in combat for the first time in Yemen by the United Arab Emirates, as part of the Arab Coalition led by the Kingdom of Saudi Arabia.

System Capabilities and Characteristics

The Leclerc EAU is a relatively light MBT (<57 tons) with a cruising range of 470 km. This can be extended to 620 km using external jettisonable tanks. It is powered by a V-12 1,500 horsepower diesel engine and can cruise up to 71 km/hr on roads. Despite its excellent off-road capability, it does not swim and can ford only one meter of water.

The armament of this MBT includes a 120-mm smoothbore stabilized main gun, a 12.7-mm coaxial machinegun slaved to the main gun, a 7.62-mm roof weapon, and 27 80-mm grenade launchers. The main gun is an autoloader and can be fired on the move. It has both thermal and infrared capability. Appliqué armor is available for protection, and the tank has an NBC protection system.

Employment

The Leclerc EAU deployed in April 2015 for use in Yemen as part of the Saudi-led coalition of nine Arab states to reinstate the Yemeni government. The primary enemies are Houthi rebels, pro-Houthi Yemeni Army units, and al-Qaeda in the Arabian Peninsula (AQAP).

The Leclerc EAU operates in 4-tank platoons in coordination with infantry in armored fighting vehicles. An Emirati armored brigade spearheaded the coalition breakout from Aden and captured al-Anad Air Base in July 2015. More analysis on the effectiveness of the Leclerc EAU and associated tactics will take place as the conflict progresses.

System Proliferation

France and the United Arab Emirates have this MBT.

Training Implications

Logistics trainers using this system must plan for a fuel consumption rate of 146 liters per hour, plus all associated petroleum, oils, and lubricants. Ammunition will be consumed quickly during battles. The main gun fires six rounds per minute and carries 40 rounds onboard.

Personnel replacements will be slightly better, with a crew of three vice four due to the use of the main gun autoloader. The rangefinders reach to 8,000 meters, adding significantly to line-of-sight engagements. Tactics trainers must plan for infantry, artillery, and attack air units to support Leclerc units, as well as sizeable mobile trains. Probability hit-to-kill tables will have to be developed, as well as survivability tables based on the use (or not) of reactive armor add-ons.



Figure 1. UAE and geographic region

FRENCH LECLERC TROPICALIZED MAIN BATTLE TANK **LECLERC EAU**



SYSTEM	SPECIFICATIONS	SYSTEM	SPECIFICATIONS
Alternative Designations:	AMX-56	ARMAMENT-MAIN GUN	Smoothbore gun
Date of Introduction:	1996	Caliber, type, name:	120-mm GIAT CN120-26/52
Proliferation:	France, United Arab Emirates	Rate of Fire (rd/min):	6
Crew:	3	Loader Type:	Autoloader
Combat Weight (mt):	56.95	Ready main gun rounds:	22
Chassis Length Overall (m):	7.96	Stowed rounds:	18
Height Overall (m):	3.04	Elevation (°):	-10/+20
Width Overall (m):	3.62	Fire on Move:	Yes
Ground Pressure (kg/cm2):	INA	ARMAMENT-AUXILIARY WEAPON	Turret coax to main gun
AUTOMOTIVE		Caliber, type, name:	12.7-mm GIAT M693
Engine Type:	V-12, 1500-hp Diesel	Max Eff Range-Day (m):	INA
Cruising Range (km):	470/620 with aux fuel tanks	Max Eff Range-Night (m):	INA
Max Road Speed (kph):	71	Fire On Move:	Yes
Max Off-Road Speed (kph)	55	Rate of Fire (rd/min):	600
Average Cross-Country (kph):	50	ARMAMENT-AUXILIARY WEAPON	Roof armament
Max Swim:	n/a	Caliber, type, name:	7.62-mm FN HERSTAL
Fording Depth (m):	1 (without preparation)	Max Eff Range-Day (m):	INA
COMMUNICATIONS		Max Eff Range-Night (m):	INA
Radio:	Voice and data transmission	Fire On Move:	Yes
External Intercom Device:	Yes. Telephone handset	Rate of Fire (rd/min):	900
PROTECTION		ARMAMENT-AUXILIARY WEAPON	Grenade launchers
Applique Armor:	Available	Caliber, type, name:	80-mm grenade GALIX
Explosive Reactive Armor:	No	Max Eff Range-Day (m):	30-50
Active Protection System:	Yes	Max Eff Range-Night (m):	30-50
Mine Clearing:	No	Fire On Move:	Yes
Self-Entrenching Blade:	No	Rate of Fire (rd/min):	INA
NBC Protection System:	Yes	FIRE CONTROL	
Smoke Equipment:	Smoke grenade launchers; smoke generator	FCS Name:	Fire Control Computer (CCT)
		Thermal: TC-Gunner:	Yes (5,700 m)
		Main Gun Stabilization:	Yes
		Infrared:	Yes (video)
		Sights w/magnification day (m):	5,700
		Sights w/magnification nt (m):	INA

NOTES

THE LECLERC TROPICALIZED MBT IS A CLASS 69 (IN COMBAT ORDER WITH JETTISONABLE FUEL DRUMS) HEAVY TRACK-LAYING ARMORED MBT AND IS EXTREMELY MOBILE. IT CAN OPERATE IN AN NBC ENVIRONMENT AND CAN FIRE WHILE MOVING, IN ALL WEATHER, ON STATIONARY OR MOVING TARGETS. IT'S FUEL CONSUMPTION RATE IS 146 LITERS PER HOUR. SITUATIONAL AWARENESS IS MAINTAINED THROUGH THE LECLERC BATTLE MANAGEMENT EQUIPMENT (LBME). THE COMMANDER AND GUNNER HAVE LASER RANGEFINDERS RANGED TO 8,000 METERS. THE LECLERC EAU INCLUDES AN AUXILIARY POWER UNIT.

WEAPONS & AMMUNITION TYPES AND TYPICAL COMBAT LOAD

120-MM SMOOTHBORE GUN	40 total mix
APFSDS, APFSDS-T, HEAT TP, and HEAT MP	
12.7mm coax MG	700
Ball, tracer	
7.62X51 cupola MG (FN HERSTAL)	1,600
Ball, tracer	
80-MM grenade launchers (GALIX)	27
Smoke, AP, HE, Decoy	

VARIANTS

LECLERC T3 THROUGH T11, AZUR, EPG, DNG, AND MARS. FUTURE UPGRADES INCLUDE THE "CONTACT" TACTICAL RADIO SYSTEM AND THE "SCORPION" INFORMATION AND COMMAND SYSTEM.

MAIN ARMAMENT AMMUNITION

CALIBER, TYPE, NAME:

120-MM APFSDS, APFSDS-T

MAXIMUM AIMED RANGE (M): 4,000

MAXIMUM EFFECTIVE RANGE (M):

DAY: INA

NIGHT: INA

ARMOR PENETRATION (MM KE): INA

120-MM HEAT TP, HEAT MP

MAXIMUM AIMED RANGE (M): 3,000

MAXIMUM EFFECTIVE RANGE (M):

DAY: INA

NIGHT: INA

ARMOR PENETRATION (MM KE): INA





by [Angela M. Wilkins](#), TRADOC G-2 ACE Threats Integration (DAC)

A charter of TRADOC G-2 ACE Threats Integration (ACE-TI) is to produce and maintain the [Decisive Action Training Environment \(DATE\)](#). DATE establishes a common operational environment (OE) with hybrid threat elements for training. Although it is not within ACE-TI's purview to design scenarios, the organization's analysts have provided ideas and guidance to scenario designers. The conditions within DATE allow for the creation of a multitude of scenarios to challenge all training tasks, and this article will describe several prospective ideas for scenarios.

DATE's Road to War Example

Within Appendix D of DATE 2.2 is an *example* Road to War (RTW). The decision was made to include this as an aid to scenario designers and/or to provide an easy starting point for joint exercises; it was never intended to be the "one and only" nor the best-possible road to war. The opening paragraph of Appendix D clarifies the purpose:

The DATE Road to War (RTW) is intended to serve as a common starting point for all Army CTCs and TRADOC Schools and Centers to draw upon in formulating their scenarios and other supporting documentation for training events and exercises. This RTW is not the only possible narrative to assist in the generation of scenarios. Each CTC has the flexibility and freedom to adapt, change, or modify this RTW to fit the specific needs of each training event.

Figure 1. Excerpt from DATE 2.2, Appendix D: Road to War

It is ultimately up to each training center to determine whether to use this RTW or another one. The DATE countries and their conditions are written in such a way that exercise designers could choose any state or actor to attack any other state or actor in any part of the OE.

To help with ideas for conflict, also included in DATE is an events section (Section 3). It provides 77 ideas for conflict along with related mission-essential task list (METL) items for training. These events are written generically, meaning that they can be applied to the DATE OE that works best for a particular training exercise. See Figure 2 for a sample DATE event.

Recently, TRADOC G-2 ACE-TI produced a briefing with several "scenario starter" ideas. Included in the briefing were ideas already implemented at the combat training centers (CTCs), but several new ideas were also proposed. What follows is a description of these ideas, which can be modified as needed to be used at CTCs, at home station, or even in the classroom.

Of note is that each idea reflects recent/real-world events, which is in line with the DATE concept being a composite of real-world conditions. ACE-TI has processes that overlap with its other tasks to ensure that DATE remains relevant with each iteration, which enables all DATE-based training to prepare soldiers to fight robust and challenging threats in a variety of conditions.

Event		Local Army Helicopter Shot Down by Insurgents	
1. Related Activity	➤ Host nation army responds with air support.		
➤ Possible Variable Conditions	<ul style="list-style-type: none">○ Military○ Political	<ul style="list-style-type: none">➤ Host nation military is able to scare off the insurgents.➤ Government authorities challenged by insurgent group, tensions increase. Assassination attempts likely.	
2. Related Activity	➤ Insurgent group uses this as a threat. Uses INFOWAR to tell the locals that their government and military are weak.		
➤ Possible Variable Conditions	<ul style="list-style-type: none">○ Political○ Social	<ul style="list-style-type: none">➤ HN government must counter the insurgent's message and show the people that the insurgent is wrong.➤ Locals are frightened by the show of power by the insurgents and begin to question their government's ability to protect them and keep the peace.	
3. Related Activity	➤ Host nation government request assistance from US to stage a defense against insurgents against further attacks.		
➤ Possible Variable Conditions	<ul style="list-style-type: none">○ Political & Military○ Social	<ul style="list-style-type: none">➤ Government unable to amass enough troops throughout the area due to low numbers; requests assistance from US forces.➤ Social unrest increases. Locals are made uneasy by the troops throughout the area.	
4. Related Activity	➤ Insurgents capitalize on social unrest through continued use of INFOWAR tactics, reminding the people that their government can't handle the situation on its own, and as soon as US troops leave, the insurgents threaten to strike again.		
➤ Possible Variable Conditions	<ul style="list-style-type: none">○ Social○ Political & Information	<ul style="list-style-type: none">➤ Locals are frightened by the threats from the insurgents, begin questioning their government.➤ The government attempts to quell the anxiety and to ensure the people that they are safe. Messages are sent through TV and radio messages, primarily.	
Possible Related METL Tasks	Conduct Command and Control (ART 5.0) <ul style="list-style-type: none">➤ Execute the Operations Process (ART 5.1)➤ Integrate Information Engagement Capabilities (ART 5.3.1)		
	Conduct Offensive Operations (ART 7.1) <ul style="list-style-type: none">➤ Conduct an Attack (ART 7.1.2)➤ Conduct Air Assault (ART 1.2.1.1.2)		
	Conduct Security Operations (ART 6.7.3) <ul style="list-style-type: none">➤ Conduct Area Security Operations (ART 6.5.3)		
	Conduct Stability Operations (ART 7.3) <ul style="list-style-type: none">➤ Provide Essential Civil Service (Immediate Response) (ART 7.3.3.1)➤ Coordinate Public Order and Safety (Immediate Response) (ART 7.3.2.1)		

Figure 2. Sample event from DATE 2.2, Section 3: Events

Atropia v Ariana (A)

Conditions and events leading to conflict—

- Ariana lays claim to Atropian oil reserves in the Caspian Sea.
- Ariana conducts a 10-day military exercise along the Atropian border.
- Both countries exchange mortar fire, during which one Arianian soldier is killed in action.
- The US and EU impose sanctions against Ariana.
- Ariana ceases all oil exports to Atropia.
- Ties between Ariana and Atropia are severed.

- Atropia requests NATO intervention.
- NATO authorizes enforcement of resolution that maintains Atropian territorial integrity.
- Atropia welcomes international show of support with a multinational combined exercise.
- Atropian and Arianian forces occupy positions along the border.

Real-world related situation: Russia claims natural resources on the Arctic continental shelf that technically lie in international waters; Russia bolsters its military in the Arctic (conducts military exercises, etc.), which provokes a NATO response to protect the Global Commons.



Figure 3. Atropia v Ariana (A)

Atropia v Ariana (B)

Conditions and events leading to conflict—

- Ethnic Atropians begin to flee western Atropia in fear of increased activity by the South Atropian Peoples' Army (SAPA).
- Ariana reportedly provides financial and military support to SAPA.
- US condemns Ariana's support to SAPA; issues travel warning to Atropia.
- UN issues a resolution on humanitarian and security situation in Atropia.
- The international community condemns actions of Ariana crossing into Atropia after Ariana builds up forces on Atropia's border.

- US President signs nonlethal Presidential Finding authorizing covert other governmental agency (OGA) support to Atropia, closely followed by the authorization of lethal OGA support to resistance forces and OGA unconventional warfare operations.
- A ceasefire agreement is followed by reports of Arianian forces committing various atrocities in Atropia.
- US Special Forces deploy to Gorgas in order to prevent further escalation of war.

Real-world related situation: Iran/Iraq War in 1970—OR—Kurds and other ethnic groups in northern Syria stampede north toward the Turkish border (fleeing the ISIL/Kurdish fighting in Kobani) and stress Turkish capacity to accommodate the heavy flow of refugees.



Figure 4. Atropia v Ariana (B)

Limaria v Atropia

Conditions and events leading to conflict—

- A high-ranking Limarian official visits the Lower Janga region and gets killed by a Free Lower Janga Movement (FLJM) sniper.
- Limaria immediately accuses Atropia of having trained and supported the sniper, which Atropia denies.
- Rising tensions cause the UN to agree to approve insertion of forces in order to restore peace.
- Variations (optional)
 - Donovan (a strong supporter of Limaria) sends troops into Limaria on the Atropian border, or

- Fabricate a recent agreement with Atropia that benefits Donovia economically, so Donovia chooses to stay out of the conflict.

Real-world related situation: Recently, high-ranking Justice and Development Party (AKP) officials have been visiting Turkey's southeastern provinces, where a huge military pacification effort is currently underway. Since the region is close to civil war anyway, the assassination of one of these figures, such as a member of parliament or cabinet member, could ignite a level of violence sufficient to warrant insertion of a peacekeeping force to maintain order.



Figure 5. Limaria v Atropia

Gorgas v Atropia

Conditions and events leading to conflict—

- Gorgas decides to build three major hydropower plants to help offset its electrical needs: one north of Akhmeta on the Alazani River; one north of Tskhinvali on the Liakhvi River; and one south of Kvishkheta on the Kura River.
- Atropia fears that the reduced flow of water into the Mingachevir Reservoir will compromise its associated power plant.
- A diplomatic dispute rapidly escalates, with Gorgas accusing Atropia of trying to hinder its efforts to be more independent. A small Salasyl cell, to make things more difficult for the Atropian government, crosses the border into Gorgas and bombs a small church. Gorgans, for whom being Christian is the same as being Gorgan, immediately interpret the attack as one against God and country.

- SAPA uses the controversy as an opportunity to conduct further targeted attacks against religious buildings in Gorgas and publicly attribute them to Salasyl.
- Attacks rise and cause civil unrest and civilian deaths.
- Gorgas pleads for Western intervention to quell the unrest.
- Optional: Limaria—a Christian country that hates Atropia, feels discriminated against, and is acutely aware of its lack of regional allies—could join Gorgas against Atropia. Donovia would choose to stay out of it in either case, as the country doesn't like either Gorgas or Atropia and would benefit regardless of who “wins.”

Real-world related situation: Sudan building dams on the upper Nile River that prevent the flow of water to Egypt.

Atropia v Donovia (A)

Conditions and events leading to conflict—

- The Atropian electrical grid is taken down by unknown hackers, with Donovia being highly suspected as the culprit.
- A humanitarian crisis results, along with chaos and revolt against the Atropian government for not being able to protect its citizens.
- Atropia seeks assistance from the US, and a brigade is deployed for humanitarian purposes and to maintain stability and order in the region.

Real-world related situation: Cyberattack across regions in Ukraine: Malware targeted at a major power supplier in Ukraine caused a power outage for 200,000 homes and businesses that lasted six hours.¹

Atropia v Donovia (B)

Conditions and events leading to conflict—

- The oil market crashes, taking the Donovanian economy with it.
- The Donovanian government tries to lessen its burden by committing atrocities against the minority Atropians to reduce their population.
- The US intervenes.

Real-world related situation: Enclaves of ethnic Turks currently live in the lower Caucasus region. Historically they have been the victims of Soviet deportations, and they still suffer hostility at the hands of ethnic Russians. Russian economic suffering caused by a combination of the oil market crash and US/EU sanctions could trigger a resurgence/intensification of anti-Turkish ethnic hostility that could warrant humanitarian intervention by an outside military force.

Arianian Civil War

Conditions and events leading to conflict—

- The people rise up in Ariana and begin a civil war led by insurgents.
- US assists the rebels.

Real-world related situation: Arab spring revolutions, specifically including Tunisia, Syria, and Libya, and current national aspirations of ethnic Kurds—the world's largest ethnic minority (approx. 20–25 million) without a country—that spread across four countries: Iraq, Iran, Syria, and Turkey.



Figure 6. Gorgas v Atropia

Ariana and Donovia v Atropia

Conditions and events leading to conflict—

- Ariana and Donovia attack Atropia for oil resources.

Real-world related situation: Chinese expansion of its “nine-dash-line” in the South China Sea in order to encroach on the region’s natural resources and gain an advantage in trade (shipping lanes, etc.).

Donovia v Gorgas

Conditions and events leading to conflict—

- Donovia attacks Gorgas because of its desire to be more Western, which Donovia views as a threat.

Real-world related situation: Russia v Ukraine 2014, i.e. Russian’s annexation of the Crimea and recent incursions in Ukraine.

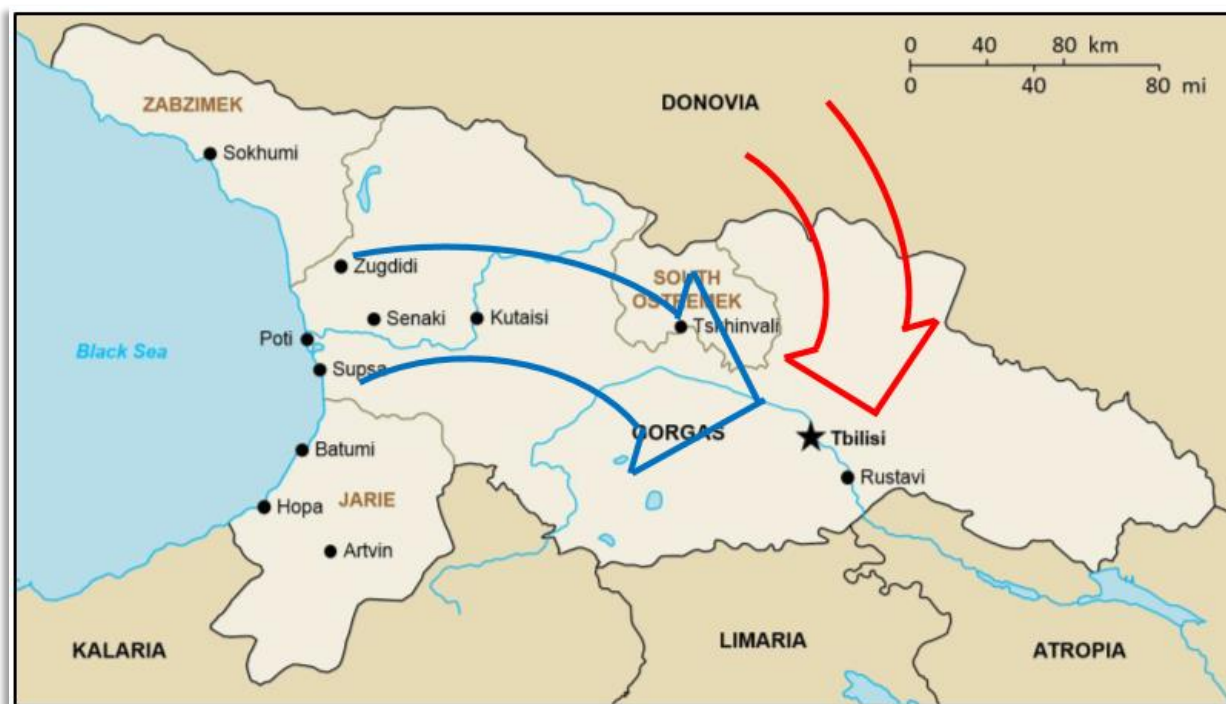


Figure 7. Donovia v Gorgas

It should be clear from the above examples that any DATE country can be the threat, and any DATE country can require US assistance to face conflict in the OE. Flexibility is one of the principle functions of the DATE environment. These examples can assist exercise planners and scenario designers, but other ideas could be used as well. If more detail is needed on any of the conditions in DATE to aid in the development of a specific scenario, that can be added and is considered part of DATE’s flexibility, as long as no changes are made to the baseline conditions. The current version of [DATE \(2.2, April 2015\)](#) is available on the Army Training Network (ATN), along with all of ACE-TI’s products. Since the first version of DATE was released in 2010, ACE-TI has modified it several times based on user feedback and leadership guidance. All feedback is welcome and will be carefully considered for the next version. Currently, DATE 3.0 is expected to be complete by the middle of 2017.

Note

¹ US Department of State, Overseas Security Advisory Council (OSAC). “[Analysis & Implications of Cyberattacks on Ukraine’s Critical Infrastructure Systems](#).” 29 February 2016

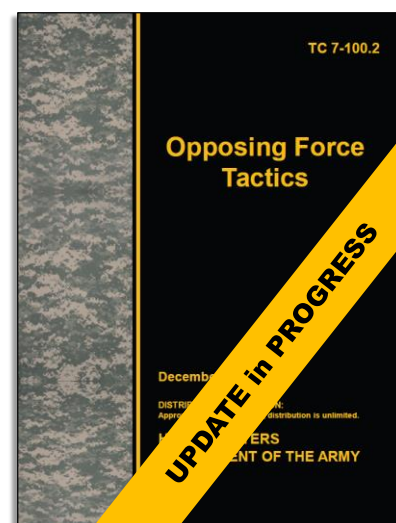


by [Jon H. Moilanen](#), TRADOC G-2 ACE Threats Integration (IDSI Ctr)

An opposing force (OPFOR) conducts tactical operations with a number of tactical tasks that are trained to standardized conduct and successful execution. *Disrupt* is a tactical task with a purpose to “upset an enemy’s formation or tempo, interrupt the enemy’s timetable, cause the enemy to commit his forces prematurely, and/or cause the enemy to attack in piecemeal fashion.”¹ Successful disruption degrades enemy combat system capability and prevents the enemy from conducting an effective operation.²

The OPFOR Tactical Task List, published in [TC 7-101, Exercise Design](#), is specific to an opposing force. This list of tasks is undergoing a significant update at TRADOC G-2 ACE Threats Integration (ACE-TI), and will be incorporated in the next update to [TC 7-100.2, Opposing Force Tactics](#). OPFOR tactical organizations and individuals perform these tasks instead of comparable tasks in the [Army Universal Task List \(AUTL\)](#). However, an OPFOR might conduct this task quite differently from US Army elements. An OPFOR will often have less restrictions and not necessarily comply with international conventions on conflict and/or law of war protocols. An OPFOR may even employ acts of terrorism.

OPFOR organizations and individual actors perform tactical tasks in order to provide challenging conditions for the training of Army mission essential and/or designated tasks by units, organizations, and individuals. The OPFOR Tactical Task List serves as the primary source for most tasks the opposing force must perform to a standard. Exercise planners, curriculum developers, soldiers, and leaders refer to this list first when conducting countertask analysis in training, professional education, and leader-development venues. If the OPFOR Tactical Task List does not contain an appropriate task for a particular OPFOR requirement, a task is selected for the OPFOR from the US Army AUTL.³



Note: The OPFOR tasks, when approved by TRADOC G-2 ACE Threats Integration, are added to the G-27 resources of the TRADOC G-2 Virtual OPFOR Academy (VOA). With common access card (CAC) entry you can visit the VOA resources, which support training, professional education, and leader development, at <https://tbr.army.mil/voa/>. This disrupt task is in a review process as of April 2016.

OPFOR Disrupt Task

Actions can be centralized or purposely decentralized in order to mass OPFOR combat power at a designated time and location or to cause an enemy to address multiple independent threats throughout an operational area. Disrupt tasks can be conducted anywhere in an OPFOR area of operations.

Reconnaissance and counterreconnaissance defeat enemy reconnaissance and security operations. Countermobility obstacles channel the enemy into disadvantageous terrain and kill zones, and long-range indirect fires and direct fires degrade enemy formations. Information warfare (INFOWAR) components such as deception, perception management, and electronic warfare are OPFOR combat multipliers employed to limit effective enemy command and control (C2) in defensive and offensive operations. Destruction of a designated combat system equates to the system being combat

ineffective until that capability is reconstituted. Any OPFOR level of command and any type of elements that are conducting a disrupt task have the same basic subtasks.

Functional action determines an OPFOR force or element designation. For example, a disruption element generally disrupts, but also may need to fix a part of an enemy element or force. The functional designation then becomes *fix* rather than *disrupt*. This article uses an OPFOR battalion detachment (BDET) in the tactical diagram example. The BDET commander focuses on how to best accomplish the disrupt task with considerations to:

- Known, probable, or possible enemy avenues of approach,
- Sufficient elements allocated to disrupt the enemy,
- Directional positioning and repositioning of elements,
- Engineer effort prioritized to camouflage, cover, concealment, and deception (C3D),
- Countermobility actions focused to protect friendly elements and channel or contain the enemy into kill zones,
- Massed on order indirect and direct fires, and
- Flexible movement and maneuver options to prioritized contingencies.

Forces and Elements

An OPFOR commander specifies in his combat order the initial organization of forces or elements within his level of command, according to the specific *functions* he intends his various subordinate units to perform. At brigade or BTG and above, the subordinate units performing these functions are referred to as *forces*, while at battalion or BDET and lower echelon units are called *elements*.

US Army Training Circular 7-100.2, *Opposing Force Tactics* (2011)

The BDET commander recognizes that enemy action and battlefield conditions may make the originally-selected mission order inadequate and require timely adaptation in order to achieve the mission. The tactical conditions may provide an opportunity to not only contain and destroy lead enemy elements in a coordinated kill zone, but exploit success with counterattacks to defeat follow-on enemy elements and/or sustainment capabilities. Task organization could adjust quickly, and the commander could allocate a part of the BDET as an exploitation element and/or reinforce combat power of a fixing element to canalize an enemy's main effort into an apparently lightly-defended avenue of approach.

The tactical example and diagram in this article presents an OPFOR defensive operation. A general organization of an OPFOR to disrupt, by function, can include the following elements:⁴

- *Security element* to provide reconnaissance, surveillance, and/or security.
- *Disruption element* to prevent an enemy from influencing OPFOR mission accomplishment, and/or prevent the enemy from conducting effective tactical operations. Specific functional designations within disruption could be tasked, such as *fix*, *containment*, and/or *exploitation*.
- *Support element* to provide combat and combat service support and C2.
- *Reserve element* to provide tactical flexibility to the commander as an uncommitted capability of combat power.

The BDET commander must disrupt enemy attacking elements in his assigned zone of a brigade tactical group (BTG) disruption zone. He executes his mission to break up the enemy formations as they approach the BTG battle zone, delay effective enemy massing of combat power, canalize enemy lead echelons into prepared kill zones, and destroy key enemy systems contained within the disruption zone.⁵ These actions allow more time and situational understanding by the BTG commander to defend his battle zone and/or consider counterattack options in the defense.

Disrupt Example

Current intelligence from OPFOR reconnaissance, intelligence, surveillance, and target acquisition (RISTA) assets inform BDET reconnaissance and surveillance of the approaching enemy. Security actions in the BDET zone shape enemy situational understanding to encourage an enemy main effort to cross the west river in the north with a supporting effort on the southern approach. Combined arms actions suppress enemy advances at the southern bridge site while the OPFOR purposely applies less combat power in the north. A sequenced OPFOR delay in the north convinces the enemy to reinforce this northern axis. Once lead enemy elements are committed east of the bridge site, effective C3D in the north surprises the enemy with an extensive OPFOR countermobility effort, combined with direct and indirect fires, that blocks the enemy advance. In the south, OPFOR elements conduct a withdrawal under pressure that gradually accelerates to the east to imply that OPFOR defenses are failing along the southern axis. This deception convinces the enemy to shift its main effort to the south and rapidly advance eastward. OPFOR defenses in the northern avenue continue to fix any enemy advance as the enemy starts shifting follow-on elements to find a bypass to the southeast.

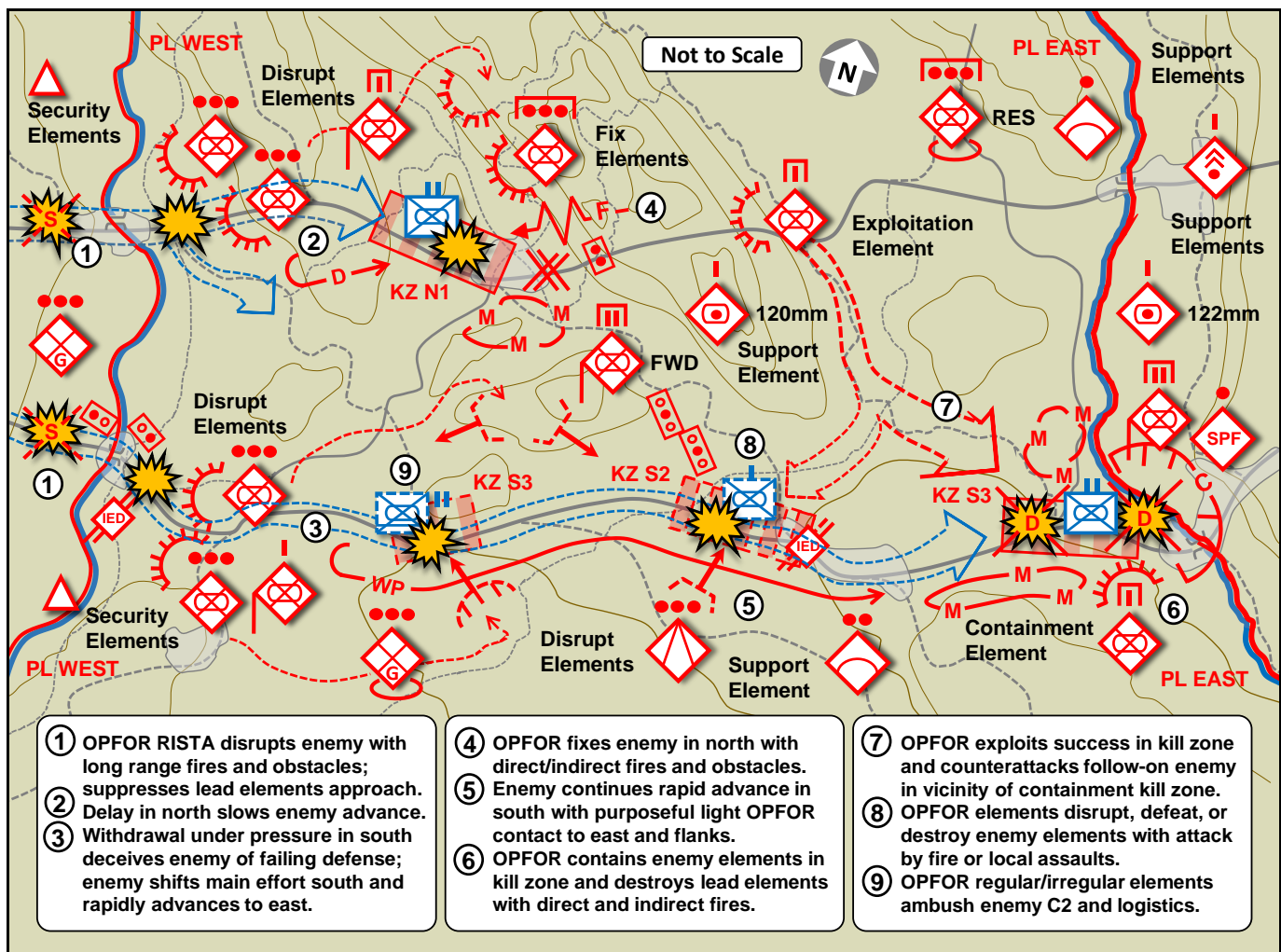


Figure 1. OPFOR task to disrupt

Contact with the OPFOR in the southern axis lessens and reinforces enemy momentum toward the southern bridge sites on the east river. The OPFOR continues sporadic direct and indirect fires and allows lead enemy elements to enter the urban area of the bridge site. Guerrilla elements in the urban area of the southern bridge site, in coordination with the BDET commander, are prepared to disrupt enemy elements and block access to the bridge. On order indirect fires, in conjunction with execution of countermobility demolitions and other obstacles, contain lead elements in and along the

main road network. OPFOR integrated air defenses of the BTG suppress enemy air attempting to influence the attack. INFOWAR element support by special purpose forces activates electronic warfare capability to degrade enemy C2 at this critical phase of the disruption and defense. The enemy lead echelon enters the kill zone west of the east river. The combined effects of direct and indirect fires, reinforced with camouflaged minefields, contain the enemy. Enemy attempts to maneuver to either flank are quickly defeated. Antitank systems concentrate on vehicles near the rear of the lead echelon and block any egress to the west.

As the enemy attack stalls along the western bank of the east river, the BDET counterattacks into the flank of the enemy to complete destruction of the enemy lead echelon. Given the successful fix of enemy elements on the northern approach, the BDET commander alerts his subordinate commanders for a possible counterattack to defeat enemy sustainment and/or follow-on echelon elements along the southern approach. His reserve element remains uncommitted.

Guerrilla elements and BDET reconnaissance elements keep the BDET commander informed on enemy concentrations on the northern and southern axes into the disruption zone. Other guerrilla elements in urban areas and along both axes emplace improvised explosive devices (IEDs) and are prepared to arm the IEDs in support of the BDET disrupt task. The BDET commander updates the BTG commander and continues security actions in his zone of the BTG disruption zone.

Training Conditions and Standards

Actions normally represent all measures associated with organizing and implementing an undetected posture within an assigned area of responsibility (AOR). When designated OPFOR are prioritized to a disrupt task, systems warfare or other support, such as INFOWAR systems, can be integrated in support of an overarching deception objective. INFOWAR elements can be used to manipulate enemy situational understanding of an operational environment (OE).

For example, a tactical environment could present the following conditions as a mission task. The OPFOR is conducting operations as part of a larger element or force and receives an operation order or fragmentary order to disrupt at a location and time specified. The order includes all applicable overlays and/or graphics. Task organization provides the combat power capabilities to accomplish the task. The OPFOR has communications with higher, adjacent, subordinate, and supporting elements. Friendly forces, enemy coalition forces, noncombatants, government agencies, nongovernmental organizations, and local and international media may be in the OE. The OPFOR is not constrained by standardized rules of engagement and does not necessarily comply with international conventions or agreements on the conduct of warfare.

As an Army standard, the OPFOR conducts disrupt actions in accordance with tactics and techniques in [TC 7-100.2, *Opposing Force Tactics*](#), and [TC 7-100.3, *Irregular Opposing Forces*](#), the order, and/or higher commander's guidance. The OPFOR leader acknowledges the mission order, conducts reconnaissance and/or surveillance to accomplish security requirements, and executes the mission. Stay-behind elements, on order, conduct follow-on tasks that can include but are not limited to reconnaissance, surveillance, and coordination to disrupt, delay, suppress, neutralize, defeat, and/or destroy designated enemy elements and/or capabilities. The OPFOR continues the mission. The disrupt task and subtasks from initial plans to mission completion include six main tasks with several subtasks. A guide for selecting priorities of effort in OPFOR disrupt training tasks to standard is as follows:

PLAN

- Identify reconnaissance and counterreconnaissance objectives.
- Identify deception objectives.
- Collect current information on enemy element/force capabilities and limitations and OE information to be obtained or confirmed in an AOR.
- Analyze *action*, *enabling*, and *support* functions that must be performed to achieve mission success. Consider tasks to deceive, disrupt, suppress, neutralize, delay, fix, contain, breach, defeat, and/or destroy.
- Determine the functional tactics to be applied by *action*, *enabling*, and *support* elements.

- Identify situational awareness and understanding requirements for collection and analysis by ground maneuver, aviation, and/or other technical capabilities.
- Task-organize elements by function in accordance with TC 7-100.2 and TC 7-100.3.
- Determine how and when functional elements act, enable, and/or support the reconnaissance and counterreconnaissance, and transition to disrupt task and/or other tasks/subtasks.

PREPARE

- Evaluate ongoing reconnaissance, surveillance, and counterreconnaissance actions to provide situational understanding and/or shape the OE conditions required for destruction of enemy reconnaissance elements, forces, and capabilities.
- Coordinate the combined arms integration of available RISTA assets for continuous and overlapping coverage of designated areas, counterreconnaissance zones (CRZs), reference zones (RZs), routes, predicted enemy locations (PELs), kill zones, and/or special objectives in a disruption zone, battle zone, and/or support zone of an assigned AOR.
- Coordinate for situational awareness and understanding among friendly elements in an AOR and its zone of reconnaissance responsibility (ZORR), such as long-range reconnaissance; special purposes forces; mounted, aerial, and dismounted elements operating in the same AOR/ZORR; and signals reconnaissance intelligence.
- Assess current counterreconnaissance actions to prevent enemy RISTA from obtaining situational understanding of OPFOR intentions.
- Conduct mission and task rehearsals of *action*, *enabling*, and *support* elements.
- Confirm secure communications requirements and capabilities.
- Execute INFOWAR in support of the mission.

FIND

- Coordinate reconnaissance and counterreconnaissance ground maneuver, fixed-wing and rotary-wing aviation, unmanned aerial vehicles, and/or other technical collection or disruption/electronic warfare assets of OPFOR RISTA to locate, monitor, and set the conditions for actions against designated enemy elements, and/or capabilities.
- Conduct undetected and sequenced movement and maneuver by reconnaissance elements through and/or into an AOR to locate enemy reconnaissance, surveillance, and/or other security elements in CRZs, RZs, routes, PELs, kill zones, and/or special counterreconnaissance objectives. Report enemy security elements, main forces, reserves, combat service support, and C2.
- Conduct undetected and sequenced movement and maneuver by counterreconnaissance elements through and/or into an area occupied by enemy elements in an AOR to locate and/or act on intelligence as tasked in mission order.
- Conduct actions with counterreconnaissance elements in order to deceive, disrupt, suppress, delay, fix, contain, breach, neutralize, defeat, and/or destroy enemy security or response elements as part of assigned counterreconnaissance tasks.
- Report regular, periodic, and/or situational collection updates in a timely manner to satisfy the commander's critical and/or recurring reconnaissance, surveillance, and counterreconnaissance information requirements that support the mission intent.
- Destroy enemy RISTA.
- Recommend if current tactical conditions require an adjustment to the time and/or tempo ordered for tasks to disrupt the enemy operation.

- Conduct security tasks to provide early warning and protect. [Other tactical tasks may include but are not limited to: block, canalize, contain, delay, destroy, disrupt, fix, interdict, suppress, or neutralize.]

CONTAIN

- Use surprise, limited visibility, complex terrain, emplaced obstacles, C3D, and fires to restrict and channel the enemy combat system into kill zone(s).
- Conduct INFOWAR perception management activities to convince the enemy commander/leader that he cannot move or decides not to move from the present location.
- Employ, when appropriate, INFOWAR electronic warfare activities to block or disrupt enemy C2 of the enemy element, force, or combat system being disrupted.
- Employ, when appropriate, relevant populations in the target area to physically block, contain, or disrupt an enemy element/force in support of fix.
- Deliver lethal and/or nonlethal suppression effects on enemy elements, forces, or combat system to isolate the combat system from contact with other enemy elements.
- Conduct direct and indirect fires and associated INFOWAR actions to suppress and/or neutralize designated targets.
- Execute selected mobile countermobility obstacles in conjunction with direct and indirect fires and obscuration.
- Block, fix, or surround enemy elements to contain the combat system in the kill zone(s) and cause enemy elements to center their activity to a given front and prevent them from withdrawing any part of the element for use elsewhere.
- Deny enemy elements freedom of movement and maneuver in a designated location or kill zone for specified period of time when in concert with mission intent.
- Degrade designated enemy elements to temporarily prevent them from assisting the isolated enemy element.
- Position a reserve element for rapid movement/maneuver, on order of the OPFOR commander, to support the mission.
- Deny the enemy freedom of movement and maneuver along ground or air avenues of approach.

DESTROY

- Attack with sudden and massed effects by action, security, and support elements.
- Destroy enemy designated combat systems.
- Destroy enemy designated elements.

CONTINUE MISSION

- Consolidate and reorganize OPFOR elements to minimize the impacts of combat losses and functional capabilities.
- Reorganize OPFOR elements quickly when order directs continued offensive actions in zone.
- Reorganize OPFOR elements quickly into small elements when order directs exfiltration along designated lanes.

- Reorganize OPFOR elements quickly into small elements when order directs withdrawal or withdrawal under pressure along designated exfiltration lanes.
- Retain a reserve element/force.
- Conduct timely undetected movement from or into areas under enemy control by stealth, deception, surprise, or clandestine means.
- Execute tasks with stay-behind elements, when required, that can include but is not limited to: surveillance, disrupt, delay, suppress, neutralize, defend, defeat, and/or destroy tasks.
- Conduct continuous element/force reconnaissance and counterreconnaissance in designated zones and/or areas.
- Report information and intelligence updates to satisfy the commander's mission intent.
- Coordinate for logistics linkup points for combat support and combat service support in support of rapid offensive or defensive momentum and objectives.
- Recommend if current tactical conditions require an adjustment to the time and/or tempo ordered for tasks to disrupt the enemy operation. Continue the mission.

Table 1. OPFOR tactical task drill: Disrupt

TACTICAL TASK: DISRUPT		
No.	Scale	Measure
01	Yes/No	Reconnaissance locates and targets high value targets.
02	Yes/No	Key operational environment factors confirmed.
03	Yes/No	Counterreconnaissance destroys high value target RISTA.
03	Time	OPFOR security operations provide 360-degree coverage.
04	Yes/No	INFOWAR deceives enemy.
05	Yes/No	Countermobility obstacles emplaced to block or canalize.
06	Time	Position action, enabling, and support elements.
07	Yes/No	Camouflage, cover, and concealment effective.
08	Yes/No	Designated combat systems contained in kill zone(s).
09	Yes/No	Long-range indirect fires effective in kill zone(s).
10	Yes/No	Direct fires effective in kill zone(s).
11	Yes/No	All-arms air defense effective against fixed/rotary aircraft.
12	Yes/No	Relevant population used as combat multiplier.
13	Yes/No	Reserve in position and ready for immediate action.
14	Yes/No	Elements destroy key combat systems.
15	Yes/No	Elements effectively disrupt enemy momentum.
16	Percent	Combat effectiveness of enemy formation.
17	Percent	Friendly elements available to continue mission.
18	Yes/No	Report mission task success to higher headquarters.
19	Yes/No	Recommend if mission task requires adjustment.
20	Time	Conduct logistic linkup, consolidate, and reorganize.

TACTICAL TASK: DISRUPT		
No.	Scale	Measure
21	Yes/No	Stay-behind elements achieve mission tasks.
22	Yes/No	Continue mission.

OPFOR Training for Readiness

The TRADOC G-2 is the “responsible official for the development, management, administration, integration, and approval functions of the OE and OPFOR program across the US Army.”⁶ An OPFOR is a “plausible, flexible, and free-thinking mixture of regular forces, irregular forces, and/or criminal elements representing a composite of varying capabilities of actual worldwide forces and capabilities (doctrine, tactics, organization, and equipment). The OPFOR is used in lieu of a specific threat force for training and developing US forces,” and can be configured to represent a hybrid threat.⁷ TRADOC G-2 ACE Threats Integration serves as the US Army lead for the TRADOC G-2 to design, document, and integrate threat or OPFOR and OE conditions in support of all Army training, education, and leader development programs.⁸

An OPFOR must be a realistic, robust, and relevant threat that challenges the capabilities and limitations of these forces in the execution of their military missions. TRADOC G-2 ACE-TI is refining the task, condition, and standard for an OPFOR disrupt task and its use in learning venues of training, professional education, and leader development. Current operational considerations and emergent threats since the publication of OPFOR tasks in [TC 7-101, Exercise Design](#) require this current evaluation and update of how to best portray threat and OPFOR tasks in learning conditions that span the live, virtual, constructive, and gaming environments of the US Army, allies, and partners.

Training Implications

A trainer, curriculum developer, soldier, or unit leader can use this OPFOR training literature on the disrupt task to support US Army readiness. This baseline of tactical information and guidance can be adjusted to satisfy specific requirements in live training at combat training centers; major exercises in constructive and virtual simulations; regional field training with allies and partners; and/or home station training, Army professional education venues, and individual professional development.

Opposing Force

An OPFOR is a plausible, flexible, and free-thinking mixture of regular forces, irregular forces, and/or criminal elements representing a composite of varying capabilities of actual worldwide forces and capabilities (doctrine, tactics, organization, and equipment). The OPFOR is used in lieu of a specific threat force for training and developing US forces, and can be configured to represent a hybrid threat.

AR 350-2, Operational Environment and Opposing Force Program (2015)

As the ACE Threats Integration directorate continues to refine and update the tasks, conditions, standards, and measures of performance for an OPFOR in US Army learning venues, the TRADOC G-2 is presenting easy on-line access to OPFOR readiness resources, such as the TRADOC G-2 Virtual OPFOR Academy (VOA) with

instructional vignettes and virtual simulations of OPFOR tactical actions. Other resources include updated OPFOR tasks, conditions, standards, and measures of performance posted to the Army’s Combined Arms Strategies (CATS). Future articles in the TRADOC G-2 *Red Diamond* monthly newsletter will describe these and other aids in providing a realistic, robust, and relevant OPFOR to challenge specified and implied mission requirements for US Army readiness.

References

- Headquarters, Department of the Army. Training Circular 7-100.3, Irregular Opposing Forces. TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. January 2014.
- Headquarters, Department of the Army. Training Circular 7-100.4, Hybrid Threat Force Structure Organization Guide. TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. June 2015.

Headquarters, Department of the Army. Training Circular 7-102, Operational Environment and Army Learning. TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. November 2014.

US Army, TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. Decisive Action Training Environment. Version 2.2. April 2015.

Notes

- Headquarters, Department of the Army. [Training Circular 7-101, Exercise Design](#). TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. November 2010. Pg B-11. This TC appendix is being updated and will be incorporated into the 2017 update to TC 71-00.2, *Opposing Force Tactics*.
- ² Headquarters, Department of the Army. [Training Circular 7-101, Exercise Design](#). TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. November 2010. Pg B-11.
- ³ Headquarters, Department of the Army. [Training Circular 7-101, Exercise Design](#). TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. November 2010. Pg B-1.
- ⁴ Headquarters, Department of the Army. [Training Circular 7-100.2, Opposing Force Tactics](#). TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. 9 December 2011. Para. 4-39.
- ⁵ Headquarters, Department of the Army. [Training Circular 7-100.2, Opposing Force Tactics](#). TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. 9 December 2011. Para. 4-24.
- ⁶ Headquarters, Department of the Army. [Army Regulation 350-2, Operational Environment and Opposing Force Program](#). 19 June 2015. Para 2-8a.
- ⁷ Headquarters, Department of the Army. [Army Regulation 350-2, Operational Environment and Opposing Force Program](#). 19 June 2015. Para 1-5b.
- ⁸ Headquarters, US Army Training and Doctrine Command. [TRADOC Regulation 10-5-1, Organization and Functions](#). 20 July 2010. Para 8-18c(1)(a).

Personal Protection—Antiterrorism Situational Awareness

Determine how to respond to an active shooter incident based on your immediate local environment. Your training is essential to decisions in moments of active shooter crisis for your personal protection, safety, and survival.



Know the Threats

Know "How To" Respond:

- 1 Escape-Evacuate**
- 2 Hide-Seek Cover**
- 3 Fight to Survive**

We are Combating TERRORISM

Personal Protective Measures: Active Shooter Incident

TRADOC G-2 ACE Threats

Be ALERT!

US Army TRADOC G-2 Operational Environment Enterprise

Combating Terrorism (CbT) Poster 07-16

For more on Threats and Opposing Forces (OPFOR) Go to <https://atn.army.mil/> Click "Training for Operations"-"TRADOC G-2 ACE Threats Integration" and "DA Training Environment"- "TRADOC G-2 ACE Threats Integration OPFOR & Hybrid Threat Doctrine"

ATN Army Training Network

for Training (Photo: US Army)

What ACE Threats Integration Supports for YOUR Readiness

- ◆ Determine Operational Environment (OE) conditions for Army training, education, and leader development.
- ◆ Design, document, and integrate hybrid threat opposing forces (OPFOR) doctrine for near-term/midterm OEs.
- ◆ Develop and update threat methods, tactics, and techniques in HQDA Training Circular (TC) 7-100 series.
- ◆ Design and update Army exercise design methods-learning model in TC 7-101/7-102.
- ◆ Develop and update the US Army *Decisive Action Training Environment (DATE)*.
- ◆ Develop and update the US Army *Regionally Aligned Forces Training Environment (RAFTE)* products.
- ◆ Conduct Threat Tactics Course resident at Fort Leavenworth, KS.
- ◆ Conduct Threat Tactics mobile training team (MTT) at units and activities.
- ◆ Support terrorism-antiterrorism awareness in threat models and OEs.
- ◆ Research, author, and publish OE and threat related classified/unclassified documents for Army operational and institutional domains.
- ◆ Support Combat Training Centers (CTCs) and Home Station Training (HST) and OE Master Plan reviews and updates.
- ◆ Support TRADOC G-2 threat and OE accreditation program for Army Centers of Excellence (CoEs), schools, and collective training at sites for Army/USAR/ARNG.
- ◆ Respond to requests for information (RFIs) on threat and OE issues.

ACE Threats Integration POCs

DIR, ACE Threats Integration jon.s.cleaves.civ@mail.mil	Jon Cleaves 913.684.7975
Dep Director DSN:552 jennifer.v.dunn.civ@mail.mil	DAC Jennifer Dunn 684.7962
Military Analyst/Operations jon.h.moilanen.ctr@mail.mil	Dr. Jon Moilanen IDSI 684.7928
Intelligence Specialist jerry.j.england.civ@mail.mil	DAC Jerry England 684.7934
Senior Threats Officer james.d.hunt50.mil@mail.mil	MAJ Jay Hunt 684.7960
Intel Specialist-NTC LNO kristin.d.lechowicz.civ@mail.mil	DAC Kris Lechowicz 684.7922
(UK) LNO matthew.j.tucker28.fm@mail.mil	Warrant Officer Matt Tucker 684-7994
Intelligence Specialist-DATE angela.m.mcclain-wilkins.civ@mail.mil	DAC Angela Wilkins 684.7929
Intelligence Specialist walter.l.williams112.civ@mail.mil	DAC Walt Williams 684.7923
Threat Tactics nickolas.m.zappone.mil@mail.mil	CPT Nikolas Zappone 684.7939
Military Analyst james.r.bird.ctr@mail.mil	Dr. Jim Bird IDSI 684.7919
Military Analyst richard.b.burns4.ctr@mail.mil	Rick Burns BMA 684.7897
Military Analyst & WEG john.m.cantin.ctr@mail.mil	John Cantin BMA 684.7952
Military Analyst-Editing laura.m.deatrick.ctr@mail.mil	Laura Deatrick CGI 684.7925
Mil Analyst-MCTP LNO patrick.m.madden16.ctr@mail.mil	BMA Pat Madden 684.7997
Military Analyst henry.d.pendleton.ctr@mail.mil	H. David Pendleton CGI 684.7946
Mil Analyst-JMRC LNO michael.g.spight.ctr@mail.mil	Mike Spight CGI 684.7974
Mil Analyst-JRTC LNO Threat Tec james.m.williams257.ctr@mail.mil	Marc Williams 684-7943
Military Analyst (Vacant)	CTR (TBD)
Intel Specialist-Analyst (Vacant)	DAC (TBD)