



Red Diamond Threats Newsletter



TRADOC G-2 Operational Environment Enterprise
ACE Threats Integration

Fort Leavenworth, KS

Volume 7, Issue 02

FEB 2016

INSIDE THIS ISSUE

BN/BDE S-2 and TTC.....	3
TTR: Syria	4
Urban Crime	7
WFX 16-2	10
Canada and DATE	17
TAR: Sinjar Preview	20
OPFOR Fix Drill	23
Threats on ATN.....	29
ACE-TI POCs.....	30

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

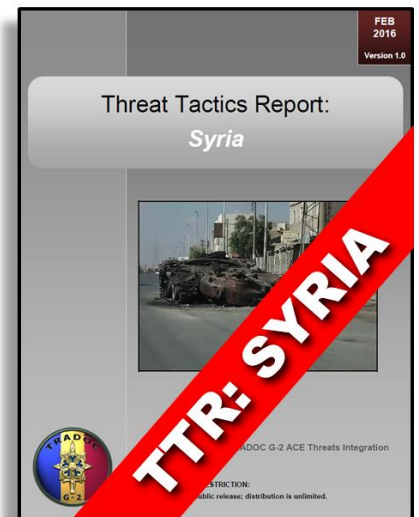
Send suggestions to:
ATTN: *Red Diamond*
Jon H. Moilanen (IDSI Ctr),
G-2 ACE-TI Operations
and
Laura Deatrck (CGI Ctr),
Editor

THREAT TACTICS REPORT: SYRIA—PUBLISHED FEB 2016

by [Jerry England](#), TRADOC G-2 ACE Threats Integration (DAC)

TRADOC G-2 ACE Threats Integration released the Threat Tactics Report (TTR) on Syria earlier this month and has posted the [report](#) on its [Army Training Network \(ATN\)](#) website.

The TTR explains how a threat actor—either a country or insurgent group—fights and operates to include its doctrine, force structure, weapons and equipment, and warfighting functions. A TTR identifies where similar conditions of the actor are present in the Decisive Action Training Environment (DATE) and other US Army training materials for easy access and use across Army Learning Model venues. This TTR describes the Syrian Arab Army (SAA) and its proxies' strategy and goals, key political and military leadership, and major alliances. The report also discusses the organizational size and structure of the SAA and its subordinate organizations of the Syrian Air Force and the Syrian Navy. The TTR examines SAA strengths and weaknesses, current unit dispositions, tactics and techniques, and defensive and offensive military strategies.



The US Army training community can use the Syria TTR to gain insight into SAA methods and operations. Exercise and curricula developers can incorporate tactics and techniques into training events and educational experiences to provide a realistic portrayal of a threat in complex operational environments.

The Syrian regime and most of the opposition are participating in UN-mediated talks that started in early February...Both sides probably have low expectations...
DNI *Worldwide Threat Assessment* (9 February 2016)



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* leads with an article on the *Threat Tactics Report: Syria*, published in February 2016. This TTR describes the Syrian army's tactics and illustrates how real-world events can be tailored to create relevant and timely training events using threat doctrine and the *Decisive Action Training Environment* (DATE).

An article on crime as an opposing force (OPFOR) tactical task informs analysis and use of crime, fear, and disorder as training conditions across a range of complex operational environments. This second part of a two-part series orients primarily on urban population centers.

MCTP WFX 16-2 was a distributed, simulation-supported, corps-level, command-post warfighter exercise conducted in November 2015. Observations from an OPFOR threats perspective note the value of a competitive and multi-echelon component joint training environment, with commanders executing effective mission command.

The Canadian Army is currently integrating the US Army's [Decisive Action Training Environment \(DATE\)](#) as its common environment for training. To assist Canadian

exercise developers/planners, TRADOC G-2 ACE Threats Integration delivered a Threat Tactics Course (TTC) via a mobile training team to the Canadian Army. Close coordination continues in 2016.

The *Tactical Action Report: Sinjar* contains information about ISIL's Nineveh province offensive, its occupation of Sinjar, and the use of subterranean facilities, as well as the adaptive nature of a hybrid threat.

An article on the tactical *fix* drill is one in a series of articles on the ongoing update of OPFOR tasks by TRADOC G-2 ACE Threats Integration. This series of updated tasks/drills is being integrated into the TRADOC G-2 Virtual OPFOR Academy (VOA) instructional vignettes, VBS3 visualizations, and other training and educational resources.

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

Red Diamond Disclaimer

The *Red Diamond* newsletter 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 US Army position and does not change or supersede any information in other official US 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 US Army for information contained therein.





Director's Corner

Thoughts for Training Readiness



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

Intelligence staff officers must understand myriad contemporary and emergent threats and be effective knowledge integrators of other complex and uncertain conditions in operational environments. The intelligence officer supports a commander's ability to execute mission command by collecting, creating, and maintaining relevant knowledge and intelligence products for team situational understanding and visualization.

However, comments from the field continue to highlight a performance gap by many battalion and brigade intelligence staff officers (S-2) in providing timely and accurate analysis of threat courses of action for commander and staff collaboration, recommendations, and decision points. Operational mission critiques and training after-action reviews note intelligence products are often inadequate in analysis of threat tactical options.

The intelligence staff officer, applying professional experience and decisionmaking, must be a proficient and confident team member in enabling a commander to balance the art of command and science of control for successful operations. He or she must be a critical and creative thinker, disciplined and self-reflective, and a positive contributor to effective organizational teamwork.

The TRADOC G-2 ACE Threats Integration Directorate provides an opportunity to learn or hone these tactical intelligence skills in a five-day Threat Tactics Course conducted twice a fiscal year at Fort Leavenworth, Kansas. Attendees include US Armed Forces active and reserve component officers, noncommissioned officers, and enlisted members; Department of the Army Civilians; contractors; and representatives from ally and partner nations. The course focuses on a composite threat model of worldwide best practices of potential adversaries and compliments instruction with vignettes of recent and ongoing military operations, as well as considering operational and strategic impacts.

The small group seminar includes doctrinal presentations based on the US Army [Training Circular 7-100 series](#), OPFOR role-playing, and table-top or computer-assisted practical exercises. Topics include but are not limited to the following:

- **Threat concepts and functional tactics,**
- **Operational environment (OE) variables and sub-variables,**
- **Hybrid threat in complex and persistent conflict,**
- **Threat actors: regular and irregular forces and elements,**
- **Offensive and defensive tactics and techniques, and**
- **Emergent threats.**

For planning dates, the next course after our March 2016 course is mid-August 2016, with the specific dates still to be determined. State your interest now, as ACE Threats Integration may scope a five-day course for current and selected battalion and brigade S-2s. We are currently developing a course program for acceptance into the HQDA G2 Foundry Program; currently, Foundry funds can be used to attend the Threat Tactics Course. A mobile training team to your location is also available, and can be tailored to your organizational requirements. For more information, contact Mr. Kris Lechowicz, kristin.d.lechowicz.civ@mail.mil, 913-684-7922.

JON



by [Jerry England](#), TRADOC G-2 ACE Threats Integration (DAC)

The [Threat Tactics Report \(TTR\): Syria](#) describes in broad terms the situation in Syria and the factors that seem to have the most direct impact on the military of Assad's government. The TTR also shows how the Syrian government was able to conduct both offensive and defensive operations against a variety of opposition groups to defend its cities and other infrastructure in an effort to maintain control over the country and emerge as the only legitimate power worthy of governing the region. The purpose of this TTR is to describe the Syrian army's tactics and illustrate how real-world events can be tailored to create relevant and timely training events using threat doctrine and the Decisive Action Training Environment (DATE). This article contains a summary of some of the material found in the Syria TTR .

Syria's Arab Spring Legacy

When protests began in 2011 the US saw reasons to be hopeful for a regime change. Nevertheless, the regime of President Bashar al Assad met the protests with countermeasures that were meant to suppress any kind of civil disobedience. Cities throughout the Sunni heartland of Syria became occupation zones as the protestors radicalized and militarized through a combination of extremist ideology and foreign military assistance. The regime fought to maintain control by imposing martial law throughout the country and using aggressive tactics and techniques to root out the opposition groups and their means of support.

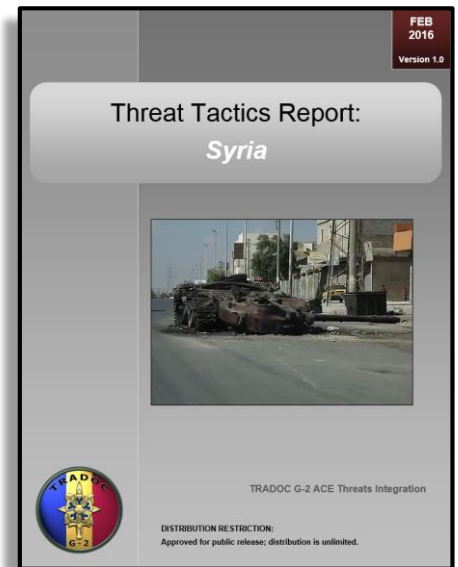


Figure 1. [A demonstration in the city of Banyas](#)

Meanwhile, the mostly Sunni-Arab conscripts of the Syrian Arab Army began to desert, taking their weapons and training with them. In late 2012 the rebels, with significant help from a number of government Army deserters, held the strategic border town of al Qusayr. The prospect for conflict threatened every corner of the Orontes Valley and destabilized major sections of Homs province. The Syrian government forces, aided by the Shia radical group Hezbollah, came in and cleared al Qusayr and solidified control of the eastern part of the province. By adapting to the urban combat zone, the Syrian government forces and Hezbollah used coordinated maneuver and fires to isolate the city and eventually drive the rebels out of the area. The forces loyal to the Assad regime formed a coalition and tried to replicate the success in al Qusayr throughout the country, especially in cities along the main highway from Damascus to Aleppo. The lack of a trustworthy offensive force, however, resulted in failure to produce decisive

results in a variety of battle zones. The situation turned the counterinsurgency into a war of attrition as forces tried to gain an advantage while protecting their territories. The Syrian army is prepared to fight using tactics designed to preserve its strength until it is confident that it can succeed in a decisive battle. Use of modern technology and personnel provided by Syrian government supporters such as Russia and Iran is significant, but has failed to defeat the varied groups that make up the opposition.

Game-Changing Weapons and Techniques

With areas around the capital and other major urban areas locked in a stalemate, the Syrian regime struggled to find a silver bullet to turn the tide and restore order. The use of fires for psychological effect became a low-risk high-payoff technique for the Syrian government forces. Barrel bombs, which were crude improvised explosive devices dropped from military aircraft, became a weapon of choice against areas that provided stiff resistance. Additionally, the Syrian government's use of chemical weapons against its own citizens directly challenged the notion of Western intervention in the conflict and proved to the world the limited extent to which the international community would be able to influence events within the country.

Besides the frequent use of weapons of mass destruction against its own citizens, the Syrian government established an unprecedented police state within the country. The use of monitoring systems designed to track the communications of opposition groups throughout the country allowed interior security forces to identify, exploit, and target anyone who relied on public information and communications technology to coordinate operations. Software and cyber security systems were repurposed by the regime to monitor and censure dissenting views. Additionally, the Assad regime's narrative of counter-extremism playing across the global media created enough leeway for serious breaches of liberty and rights against Syrian citizens and provided plausible deniability for Syria's allies to mobilize across the region.

Syria's allies provided technical and tactical support throughout the country and across the spectrum of combat operations. Iranian military and ministry of interior forces provided law enforcement and counterterrorism assistance. Hezbollah fighters provided training and support to Syria's security apparatus and directly participated in operations in

key battles. Videos of Iranian unmanned aerial vehicles (UAVs) have been posted to social media sites, providing further evidence of Iranian-Syrian technology-sharing. Iranian advisors have also provided technical expertise and have made recommendations as to the structure of Syrian forces.

Hezbollah support was also noted throughout the country, especially in the west along the Lebanese border. Direct assistance of Hezbollah forces in al Qusayr in the form of infantry and sapper operations was instrumental in securing the city and denying its use to the opposition forces. Along the mountains of southern Syria, Hezbollah provided support to Syrian government forces in disruption efforts against the opposition's supply lines running over the border.

Both regional and Western media sources report the Assad government is supported by troops from Iran as well as religiously-aligned Afghan fighters. The inclusion of regional actors among the Syrian coalition increased the number of soldiers for defensive



Figure 2. [Barrel bombs on their way to a target \(video link\)](#)



Figure 3. [A Syrian T-55 tank](#)

operations and provided freedom of movement to the Syrian government forces for surge operations in contested areas such as Damascus and Aleppo.

In addition to its regional partners, the Syrian government received assistance from the Russian government. It was widely known that the Russians maintained a naval base at the port town of Tartus and intended to retain its control even after major hostilities subsided. But in 2015 the Russians pushed beyond the coastline and began to upgrade Syrian airports for an intense bombing campaign. The expansion of Russia's role is focusing on maintaining the country's influence in the region and defeating terrorism.

Conclusion

Before the current civil war, the Syrian army's main capability was in its armored forces, which were not optimized for urban combat. Conducting counterinsurgency operations from armored vehicles and tanks is difficult and sends the wrong message when the intent is to influence the population to reject opposition narratives and accept central government authority. Syrian forces also preferred to attack population centers using aerial bombing, antiaircraft guns, and tanks to destroy suspected enemy positions, with little regard for the civilians in the area. This type of heavy-handedness isolated populations and increased their resolve to fight against Syrian regular forces. Additionally, heavy weapons lacked the maneuverability to pursue lightly-armed insurgents in an urban battlefield. Hezbollah provided experienced fighters with recent combat experience against Israel to assist the Syrian army in areas where it was lacking the experience necessary to root out rebels in complex battle positions. The foreign assistance to Syrian forces has influenced the Syrian army's techniques and highlighted the need for more skilled and specialized fighters. In addition to filling the need for tactical specialists, the Syrian army must address the complex stability issues that were at the heart of the conflict. The ability to safely and securely implement reforms across the country will be a key effort as the winner of the Syrian conflict emerges and reconstruction begins. The fighting force that effectively provides for the civilian population under its control will have the most support and will be successful in bringing stability to Syria.

The [Syria TTR](#) is published on the Army Training Network. To read more about the Syrian military and military support to Bashar al Assad's regime see our webpage on the Army Training Network at https://atn.army.mil/dsp_template.aspx?dpID=377.

US Army TRADOC G-2 Operational Environment Enterprise
TRADOC G-2 ACE Threats
Combating Terrorism (CbT) Poster No. 05-16

Know the Threats

- Review **YOUR Social Media**
- Educate **YOUR Family**
- Be Alert

We are Combating TERRORISM

Personal Protective Measures for Readiness

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

Observations on the Contemporary Urban Crime Environment

Part 2 of 2

by [CPT Nickolas Zappone](#), TRADOC G-2 ACE Threats Integration

This article is the second of a two-part series on crime, fear, and disorder. The basis for this series was observations made during my three weeks with the Kansas City Police Department's Street Crimes Unit (SCU) tactical squads (TAC). My observations of Kansas City's inner city will serve as the foundation for articulating crime as an Opposing Force (OPFOR) tactical task and will also help inform future analysis of the manifestations and impacts of crime, fear, and disorder across a range of operational environments, predominantly urban population centers. Part one of this series can be found in the [January 2016 edition](#) of [Red Diamond](#) on the TRADOC G-2 ACE Threats Integration [website](#) within the Army Training Network.

The Benefits of Street Crime

Street crime serves as a resilient and enduring revenue stream for threat actors. Some of the most prevalent criminal activities conducted at the street level are sex-industry crimes, theft, and drug trafficking. These are low-risk markets that run-of-the-mill criminals can access easily relative to more complex criminal activities such as counterfeiting, protection rackets, or smuggling. Sex-industry crimes are especially appealing to unaffiliated street criminals because they do not require large sums of startup capital and the commodity (in this case the prostitute or trafficked party) is an enduring asset, unlike drugs or stolen goods. Bank robberies have been used by nefarious actors as a funding source for decades. In 1978, the Basque nationalist group Euskadi Ta Askatasuna (ETA) conducted approximately fifty bank robberies, netting it around \$4 million.¹ There is, however, a cost for doing business. More-powerful threat actors within the criminal demimonde will levy taxes on those criminal entrepreneurs operating on their terrain and/or under their umbrella of protection. The imposition of taxes serves as a consistent passive revenue stream that enables organized-crime groups to sustain operations and invest in legitimate and illegitimate business ventures.

Street crime enables material procurement in two ways: it generates the capital and operating funds required to cover expenses and purchase items like weapons, munitions, vehicles, technology, real estate, et cetera. It also directly procures those items through criminal activities such as theft and extortion. For example, a cell of crafty car thieves may be sub-contracted by a street gang or organized-crime group to steal sport utility vehicles, which are then sold to a local insurgent group or used as assets to be traded for automatic weapons. In turn, the insurgent organization may manufacture the newly-acquired vehicles into vehicle borne improvised explosive devices (VBIEDs). At face value, vehicle theft may not appear to be of considerable concern to host nation police forces and Army units fighting an insurgency. However, once the proverbial onion is peeled back, one can start to see how street crime is part and parcel of the diverse illicit networks used by threat actors to conduct attacks and sustain hostilities.



Figure 1: [Pro-Russian rioters intimidating a journalist](#)

Street crime—particularly extortion—helps criminals exert influence over the relevant population by creating and maintaining fear. Extortion at the street level is often dependent upon a group’s ability to have a monopoly on power within a geographic area (e.g. Ndrangheta’s grip on isolated Calabrian mountain villages). The monopoly on power is amplified considerably in diaspora communities as criminals leverage language and sociocultural barriers to their advantage. At times, engendering fear or anxiety may be the desired effect of a targeted criminal act. For example, if a local business owner refuses to pay protection money to the local street gang or organized-crime group, he or she will be coerced through force or the threat of force. Of greater concern, however, is the cumulative effect of fear within an area of operations. A fearful and anxious citizenry will undoubtedly be apprehensive about supporting people, groups, or organizations that are incongruent with the status quo. This problem is severely compounded when the indigenous criminal justice system is—or is perceived to be—incompetent or, even worse, irreparably corrupt.

Orchestrating Street Crime

Russia’s actions in the Donbass region of Eastern Ukraine and Crimea exemplify how state actors can orchestrate street crime in pursuit of military and political objectives. Prior to discussing specific threat actions, one must be mindful of the pre-existing sociocultural and political conditions on the ground in Donbass and Crimea. Both regions are predominantly comprised of ethnic Russians—largely a result of Stalin’s importation of Russians into the area pursuant to an orchestrated famine that killed millions of Ukrainians.² Politically speaking, both regions are ideologically aligned with the Party of Regions—the Russia-leaning political party of former Ukrainian President Viktor Yanukovich, who has dubious connections with oligarchs, politicians, and mobsters alike. When you couple the sociocultural and political disposition of the citizenry with the triumvirate of oligarchs, politicians, and organized-crime figures, one can begin to see how a Russian takeover was met with such little resistance.

In secessionist environments in which threat actors wish to retain the cloak of anonymity, employing provocateurs to train, equip, fund, and direct criminals is an effective, yet still clandestine, way of conducting operations. Operatives from

Russia’s Federal Security Service (FSB) and Main Intelligence Directorate (GRU) leverage existing relationships with corrupt politicians—probably members of the Party of Regions—and organized crime figures like gangster-turned-politician, Sergey Aksyonov, to make contact with Donetsk and Simferopol-based crime groups like the Salem group



Figure 2: [Pro-Russian mob storms Horlivka Police Station \(video link\)](#)

or Bashmaki group.³ Of note, it is probably not coincidental that Sergey Aksyonov is the current Prime Minister of the Republic of Crimea. After these links are established, FSB and GRU operatives may “orchestrate pro-Russian sentiment” in concert with crime-group provocateurs by mobilizing both armed and unarmed noncombatants to conduct disorder, such as rioters attacking police stations and government buildings.⁴ These crime groups may also be employed by FSB and GRU operatives to coerce and/or intimidate opposition dissenters to ensure that the strategic narrative propagated by the Kremlin remains undisputed. Lastly, they may also assist proxy forces when consolidating gains after tactical victories by establishing road blocks and securing key infrastructure, as was seen in Slovyansk.⁵

Implications for the Brigade Combat Team (BCT)

Crime, fear, and disorder help threat actors create end-state conditions that are antithetical to the BCT’s desired end-state conditions. For example, “established rule of law” is the desired end-state condition of the “justice and reconciliation” stability sector.⁶ By conducting criminal activities, sowing disorder, engendering fear, and creating anxiety amongst the relevant population, threat actors can drastically alter the calculus of the citizenry in their favor. If the criminal justice system is—or is perceived to be—underperforming, incompetent, corrupt, or a mixture thereof, citizens within the

BCT's area of operations will not rely on the criminal justice system to provide fair, impartial, and accountable justice. Paradoxically, the citizenry will rely on the very threat actor that is the source of instability to mete out justice through the use of more culturally-relevant grievance-solution processes like shadow courts or tribal councils.

Crime and disorder help create windows of opportunity for threat actors. This innovative technique can be expressed as fix, neutralize, or isolate by other means. For example, to provide an *enabling* function during the execution of a functional tactic, a threat actor could pay a cell of criminals to sneak into the BCT's brigade support area and sabotage the quick reaction force's vehicles, thereby "*fixing* enemy forces so they cannot interfere with the primary action."⁷ Additionally, crime and disorder help mitigate BCT overmatch. For example, episodic events like riots and public unrest in a BCT's area of operations would most likely result in the BCT commander committing combat power to help host nation security forces monitor, contain, or quell the disturbance and restore order. Cognizant of a fleeting opportunity to exacerbate tensions, threat actors may employ criminal provocateurs to precipitate violence in an attempt to draw in friendly forces. Taking full advantage of their increasing communications and media acumen, threat actors may then embellish, skew, or fabricate the event as part of their information warfare campaign, thus exploiting a perceived BCT misstep and mitigating the BCT's overmatch in the human domain.⁸



Figure 3. [Crime in a complex operational environment](#)

Committing combat power to fight street crime helps the BCT commander in a number of ways. First, by reducing street crime, the BCT commander can disrupt and degrade a threat actor's ability to generate revenue, procure material, and exert influence within the BCT area of operations. Second, by targeting street crime the BCT can reduce a threat actor's ability to fix, neutralize, or isolate by other means. Lastly, by mitigating the effects of crime, fear, and disorder, the BCT commander has a better chance of achieving his or her desired end-state conditions. It is of the utmost importance to remember that crime, fear, and disorder do not solely impact the BCT during Phase IV Stabilize operations, as this is a common misconception held by many. Crime, fear, and disorder have diverse manifestations and impacts within an operational environment that transcend phasing models and battlefield frameworks.

Notes

¹ Louise Shelly. [Dirty Entanglements: Crime, Corruption, and Terrorism](#). Cambridge University Press. 2014. Pg 183.

² Eve Conant. "[How History, Geography Help Explain Ukraine's Political Crisis](#)." National Geographic. 31 January 2014.

³ Jamie Dettmer. "[The Mafia Ruling Ukraine's Mobs](#)." The Daily Beast. 22 March 2014.

⁴ Jamie Dettmer. "[The Mafia Ruling Ukraine's Mobs](#)." The Daily Beast. 22 March 2014.

⁵ Andrew Kramer "[In Ukraine's East, Russians Are Blending Right In](#)." The New York Times. 14 April 2014.

⁶ Headquarters, Department of the Army. [ADRP 3-07, Stability](#). August 2012. Pg 2-7.

⁷ Headquarters, Department of the Army. [Training Circular 7-100, Hybrid Threat](#). TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. November 2010. Pg 5-6.

⁸ United States Special Operations Command. [Operating in the Human Domain Version 1.0](#). 3 August 2015. Pg 8.

Scenario Design

The road to war scenario leading up to the start of the exercise involves a dispute between Ariana and Atropia. Ariana accuses Atropia of stealing its oil reserves and threatens military reprisals. This is followed by the United Nations imposing two rounds of sanctions on Ariana and the US evacuation of its embassy in Baku. Ariana responds by deploying its military units along the Ariana/Atropia border under the guise of conducting training exercises. An agreement is then made between the US and Atropia to deploy US forces to deter further Arianian aggression. US forces arrive at the port of Poti in Gorgas and begin movement to Tbilisi for joint reception, staging, onward movement, and integration (JRSOI). Without warning, Ariana responds by invading Atropia with an operational-strategic command (OSC) comprised of four division tactical groups (DTGs). Ariana is successful in seizing most of Atropia with the exception of the northwestern region, small area in the far northeast, and the Tramaz peninsula, which includes the capital of Baku. Ariana forces also captured a significant portion of the Trans-Caucasus Petroleum Pipeline. In response, the US issues Presidential Decision Directive 35 to expel Arianian forces from Atropia.

As a result of US military force authorization, shaping operations commence and Combined Joint Task Force (CJTF) 12 is created to intervene on behalf of Atropia. Led by US forces, CJTF 12 completes JRSOI and begins movement into western Atropia in order to attack, defeat, and force the withdrawal of OSC 2 back into Ariana. Also located in Atropia are remnants of brigades from Field Group Atropia defending terrain in order to buy time for CJTF 12 forces to arrive. In the northeastern portion of Atropia, remnants of the Northern Command and Capital Defense Command also remain in order to defend against OSC attempts to capture Baku. When the exercise begins, ground forces from CJTF 12 complete a forward passage of lines with two Atropian Army brigades. These two brigades transition with a follow and support mission of CJTF 12. Initially, the main effort is led by the US 101st Airborne Division (Air Assault) in the north and supported by the 29th Infantry Division in the south.

Training Units

The evaluated training divisions for this exercise were the 101st Airborne and the 29th Infantry Division (ID) from the Army National Guard. Supporting the 101st were four brigade combat teams (BCTs). Also supporting the 101st were an Atropia Motorized Brigade and three additional US brigades consisting of artillery, maneuver enhancement, and rotary wing aviation. Training objectives for the 101st were the following:

- Conduct multiple brigade task force-sized air assault operations to defeat a complex hybrid threat.
- Employ division mission command posts, maintain continuity of operations and common operational picture, and validate mission command systems.
- Organize, synchronize, and integrate intelligence, surveillance, and reconnaissance/collection management functions to facilitate the division targeting cycle.
- Integrate the division artillery into the division mission command structure, exercising the targeting process throughout each planning horizon.
- Validate 101st Sustainment Brigade's land/air operations supporting the division for ground and air assault missions beyond 72 hours.
- Conduct a deliberate wet-gap crossing of a brigade task force-sized element over complex terrain.
- Conduct operational assessments to inform the commander's decision cycle.
- Conduct stability operations in coordination with host-nation and joint partners to establish a safe and secure environment.
- Integrate and synchronize the division targeting process for stability operations between host-nation and joint partners.

Supporting the 29th were three BCTs. Also supporting the 29th were an Atropian armor brigade and three additional US brigades consisting of artillery, maneuver enhancement, and rotary wing aviation. Training objectives for the 29th were the following:

- Exercise mission command using the operations process to employ forces in unified land operations. Execute decisive action (offense, defense, and stability tasks) by means of combined arms maneuver and wide area security to defeat a hybrid threat.

The exercise for training units was planned as a five-phased CJFLCC operation. Execution of the exercise was limited to Phase III, which was divided into three sub-phases (see figure 2). Phase II, Seize the Initiative, had already occurred prior to the beginning of the exercise. Phase II focused on setting the conditions to allow coalition forces to conduct successful offensive operations during Phase III. Phase II included shaping operations from the CFACC and other long-range fires. At the start of Phase III, Access, the 101st attacked in zone in the north to defeat Arianian forces. The purpose was to link up and relieve forces in Baku or conduct supporting attacks to isolate Arianian forces and compel their surrender or withdrawal. At the same time the 29th ID, supporting CJFLCC forces in the south, would attack in zone to defeat the enemy's defenses, interdict the enemy lines of communication, and force a withdrawal or complete the isolation of Arianian forces in Atropia. Critical to the CJFLCC offensive throughout Phase III was the rapid seizure of key terrain to gain operational depth in order to create multiple dilemmas for Arianian forces. Phase IIIC, Defeat, ended once the Arianian forces withdrew from Atropia and the southern Atropian border was restored. The CJFLCC would then transition to Phase IV, Stability Operations, which was the final phase of the operation.

Unique features of this exercise were two competitive training divisions, increased offensive tempo, and an opposing force (OPFOR) synchronization group. Normally during warfighter exercises there is only one division that is a competitive, evaluated division. The other division is scripted, controlled by MCTP, and not evaluated by an operations group. It is essentially a "wrap-around unit" that provides the necessary force structure for the corps CJFLCC or another designated joint task force. Associated with this unique feature was the aggressive, offensive nature of both divisions, especially the 29th ID. From the beginning of the exercise until it ended, both divisions were exceptionally aggressive during offensive operations and sustained heavy losses, as did the WCOPFOR. Fortunately for the WCOPFOR, there was a daily OPFOR synchronization group meeting that was held each morning and designed to discuss and coordinate with various operations groups or neutral/white cell organizations.

The purpose of this daily event was to help minimize exercise confusion and ensure that training objectives were being met. It also helped other participants like media, irregular forces, Atropian leadership, and operations groups to voice their issues, discuss solutions, and get a larger, current picture of all sides of the ongoing conflict. This relatively new synchronization group has been growing in attendance and has significantly helped to reduce confusion as well as to synchronize the WCOPFOR future actions with all other applicable MCTP organizations.

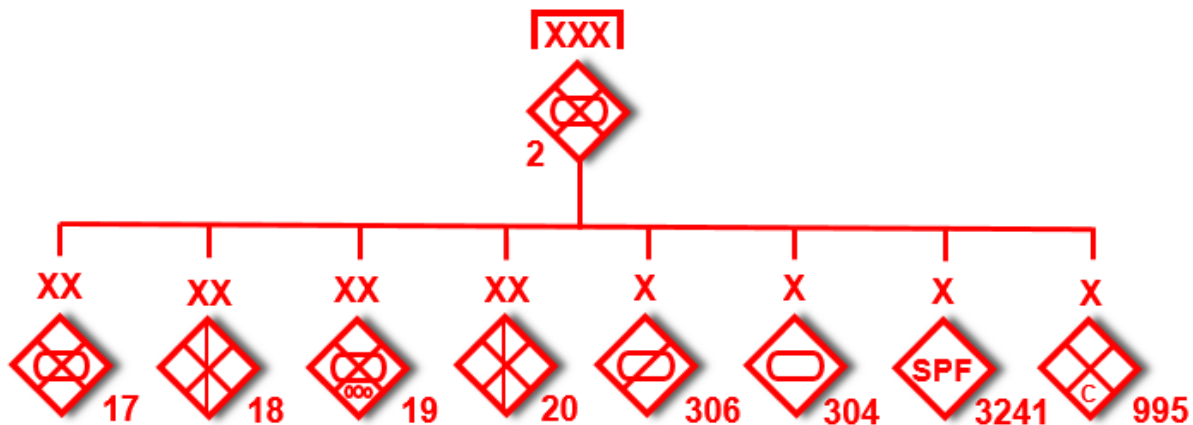


Figure 3. OSC 2 maneuver forces

Opposing Force

WCOPFOR continues to plan and operate competitively as an OSC during WFXs, with approximately four subordinate divisions and three separate brigades. The Supreme High Command (SHC) is part of the MCTP exercise control group and is not a simulated unit, with the exception of its strategic reserves. The SHC writes and publishes its strategic campaign plan for WCOPFOR implementation. It also operates as a white hat organization that attends OPFOR synchronization and white cell meetings, receives guidance from MCTP leadership, and coordinates with the OSC. The OSC and SHC are intentionally separated during exercises since the WCOPFOR is competitive.

During this exercise, OSC 2 opposed XVIII ABC and its two subordinate divisions. Constituent maneuver units from OSC 2 were four division tactical groups (DTGs) consisting of the 17th, 18th, 19th, and 20th. Also constituent was the 306th Reconnaissance Brigade (-), as well as the 304th Tank Brigade, which was initially designated as part of a strike force and later as the OSC reserve. The 3241st Special-Purpose Forces (SPF) Brigade and 995th Commando Brigade were constituent and dedicated units respectively for OSC 2 (see figure 3). Included in this force structure was the integrated support command (ISC) with three dedicated militia brigades and a motorized infantry brigade in order to provide protection in the OSC support zone. The OSC 2 also utilized an integrated fires command that consisted of long range artillery, air defense artillery, and fixed and rotary wing aircraft.

The mission of OSC 2 was to retain key terrain including the Sangachal Oil Terminal and bridges across the Aras, Agshu, and Kura rivers, to include defeating coalition forces in order to set the conditions to seize Objective EBI (Baku). Operational success was defined as destroying coalition forces west of phase line Reno, retaining control over the Sangachal Oil Terminal, and seizing Baku.

At the beginning of the exercise, the overall strength of OSC 2 units was approximately 60-70%, resulting from previous attrition from the invasion of Atropia and subsequent CFACC shaping operations. Coalition forces attacked with units at approximately 100% strength. OSC 2 maneuver units used both defensive and offensive tactics throughout most of the exercise. Offensive tactics included several planned and executed counterattacks in attempts to block or stall the coalition offensive.

OPFOR Defense

In order to retain its captured Atropia territory, the OPFOR divided its OSC 2 area of responsibility (AOR) into disruption, battle, and support zones and assigned key tasks. The key task for the 306th Reconnaissance Brigade (-) in the OSC 2 disruption zone was to disrupt and delay coalition forces, as well as conduct counter-reconnaissance. To the east of the 306th disruption zone were the 19th and 20th DTGs. Both divisions were tasked to conduct an area defense as well as seize key bridges in their AOR in order to retain key terrain and deny coalition wet-gap crossing sites along the Agshu and Aras Rivers respectively.

Located south of the 20th DTG battle zone was the OSC 2 support zone. Positioned in this zone in assembly areas were the 17th and 18th DTGs. The primary on order mission for the 17th DTG was to reinforce the 19th or 20th DTG area defenses with a secondary enabling mission of isolating Baku in the northeast. The 18th DTG mission was to function as an exploitation force and attack to seize Objective EBI (Baku). Also located in the support zone was the 304th Tank Brigade that functioned as the OSC 2 reserve. The ISC, with its four militia brigades and one motorized brigade, was tasked with providing freedom of movement of sustainment forces by conducting counter-reconnaissance and securing lines of communication, major supply routes, and bridging sites. The purpose of this task was to prevent US Special Forces from interdiction and targeting.

In addition to the WCOPFOR regular forces described in previous paragraphs, there was an extensive effort throughout the exercise to use SPF, commandos, and irregular forces throughout the XVIII ABC area of operations. Irregular warfare continues to be a very effective affiliated asset to WCOPFOR. The most effective organizations were the South Atropia Peoples' Army (SAPA) and the commando units. Their success enabled SPF to focus on other missions, such as operational reconnaissance, without having to be used exclusively for direct action missions. WCOPFOR uses its SPF to support SAPA and closely coordinates their operations. SAPA and commando direct action attacks are focused on soft targets, such as logistical units along major supply routes, maneuver enhancement brigades, airfields, and forward arming and refueling points, all of which have a significant impact on training units' ability to conduct wide area security. These attacks were planned and successfully executed throughout Atropia during the exercise. This combined support helped enable the WCOPFOR to focus on the maneuver units attacking it.

OPFOR Defensive Operations

At the beginning of the exercise, the 29th ID and 101st Airborne attacked to the east. Unlike previous exercises, both divisions advanced at a much faster pace. This led to the creation of initial gaps between the two division boundaries but

a concerted effort by both divisions closed the gaps, which were not as significant relative to previous exercises. It should be noted that it is much more difficult to keep adjoining boundaries tight when you have dissimilar types of divisions.

During the same time the 306th, 19th, and 20th all moved simultaneously into their defensive positions as the coalition forces attacked eastward. Typically the WCOPFOR is already set in defensive positions at the start of the exercise. The WCOPFOR purposely intended to be maneuvering at this time in order to encourage the two US divisions to attack at the beginning of the exercise, rather than wait in defensive positions for days before ground maneuver attacks commenced. Within 24 hours the OSC disruption zone had collapsed, although it did provide enough time for the 19th and 20th DTGs to move into defensive positions. Nevertheless, the WCOPFOR did achieve some inadvertent success due to some internal planning confusion when its rotary wing attack aviation was sent out to test the reaction of the 101st units, which it thought would be looking for a plausible landing zone. The units turned out to be a significant target and the OSC 2 attack aviation was able to destroy a battalion's worth of combat power. This deep attack upset the 101st plans by delaying its air assault. Instead, the 101st conducted a rotary wing movement of 1/101st to Objective Florida just southeast of the Mingachevir Reservoir.

As a result of the aggressive attack by the 29th and the 101st, both divisions suffered heavy losses. They did not set the successive conditions for the offense, which prevented their ability to exploit success. The 29th was forced to pause and go through the process of reconstitution, which slowed the offensive for approximately 24 hours. The 101st also slowed its offensive. A temporary ceasefire was declared, which OSC 2 took advantage of and began counter-mobility efforts to prevent coalition forces from conducting successful river crossings. The OSC 2 also used this time to move its 304th Tank Brigade reserve—undetected—from the ISC support zone to the rear of the 20th DTG main battle zone and slightly south of the Kura River. All militia brigades from the ISC were moved just south of the 20th DTG boundary to provide direct and indirect fires in order to prevent the 29th from flanking OSC 2. Heavy losses were also incurred by the 19th and 20th DTGs. The majority of losses occurring in OSC 2 were from USAF fixed wing and Army attack helicopters, not ground forces.

As the exercise continued, the 101st began crossing the Agshu River in the north in order to continue its eastward attack to achieve link-up with coalition forces in Baku. This time the 101st was moving faster than the 29th since the former it had already successfully completed an air movement closer to the Agshu River in the north. The 29th ID also moved eastward but had more ground to cover. Nevertheless, both divisions succeeded in collapsing the DTG disruption zones of the 19th and 20th, respectively. This led to the eastern withdrawal of both DTGs across their respective rivers. During this time period the 304th Tank Brigade, centered between the two DTGs, was allowed to attack north across the Kura River into the southern flank of the 101st.

The intent was to distract the XVIIIth ABC, slow down the 101st wet-gap crossing of the Agshu River, and prevent OSC 2 lines of communication from being severed. The 304th successfully crossed the Kura and did cause some units from the 101st to pull back from their crossing site in the south and attack in order to prevent the 304th from causing significant damage. The attack also slowed down some of the 101st progress in crossing the river, even though fixed aircraft destroyed the 304th soon after it crossed over.

As a result of the 19th DTG attrition, the 17th DTG was ordered to move from the OSC 2 support zone to the northeast battle zone of the 19th to reinforce its collapsing defense. The 17th also had the mission of reinforcing the 19th DTG's Ariana Naval Infantry (ARNIN) Regiment efforts to retain the Sangachal Oil Terminal, located southwest of Baku, and prevent coalition forces from severing its lines of communications. This change of mission resulted in the 17th being unable to be the enabling force for the 18th DTG planned attack and seizure of Baku. The 92nd Mechanized Infantry Division (SHC strategic reserve) was also moved up near the OSC support zone in the south, to be committed if necessary.

During this same period extensive deception units, including surface-to-surface missile decoys, were moved forward and were beginning to be attacked by coalition long-range fires. OSC artillery units also fired smoke rounds in an effort to simulate chemical gas and cause confusion as well as defensive chemical reaction procedures from coalition forces. Both of these deception methods were largely successful.

The 17th DTG was successful in moving from the Ariana border area to reinforce ARNIN and remnants of the 19th DTG. Of significance was that the 17th DTG was not attacked during its entire movement from the Ariana border to the 19th DTG battle zone. All coalition air assets were focused instead on destroying the 20th DTG, which was rendered combat

ineffective. As a result, trail maneuver units of the 17th were shifted to reinforce the 20th DTG. At approximately the same time period, the 101st conducted a successful air movement of a battalion with C-130s to Baku. WCOPFOR was prevented from attacking this unit with indirect fires. However, the 101st did not coordinate the details with the Atropia Capital Defense Command, which presented several problems when it landed unannounced. In addition, the XVIII ABC's remaining reserve force traveled east through the evening and reached Baku. The 29th ID in the south resumed its efforts to cross the Aras River after recovering from long-range artillery losses.

Towards the end of the exercise, both the 101st Airborne and the 29th ID had completed or had elements of their divisions across their respective wet-gap crossing sites. In the south the 29th ID was successful in crossing two river sites with two brigades but did not have the capacity to exploit this success, despite the fact that it was unopposed during the river crossing. In response, OSC 2 committed one brigade of the 18th DTG to reinforce the 20th DTG, which only had one brigade left. The remaining 18th DTG units traveled north to reinforce the 17th, which had suffered significant losses from coalition rotary and fixed wing aircraft.

Atropia, and later the XVIII ABC units, counterattacked from the north to try to seize the Sangachal Terminal area and prevent the 18th from reinforcing the 17th. Confusion by the XVIII ABC over the objective opened up an uncontested area that allowed the 18th to take advantage of a gap in the eastern portion of the objective. This allowed OSC 2 to hold onto retained terrain in this area with the timely reinforcement of the 18th DTG. In the southwest, the 92nd Mechanized Infantry Division strategic reserve was also employed to protect the 20th DTG, which only had two battalions remaining, from becoming flanked by the 29th ID. The 92nd then began to piecemeal its brigades into Atropia to support this effort in order to preserve its forces if needed elsewhere. However, during the last day of the exercise the 18th and 92nd were ordered to conduct a tactical withdrawal from Atropia in order to preserve combat power and set the conditions for ceasefire negotiations. During the withdrawal, these units were ordered to destroy Atropian infrastructure, including the Sangachal Terminal and bridges, in order to delay coalition offensive ground maneuver operations.



Figure 4. [Small unit leadership in field training](#)

In conclusion, the WCOPFOR was successful in challenging training units throughout this fast-paced exercise. Both sides fought hard throughout the exercise. Most, if not all, of the evaluated training units achieved all or the majority of their training objectives. It is important to note that close coordination between the WCOPFOR and MCTP leadership, exemplified by the daily OPFOR synchronization group, continues as these exercises grow in size and complexity in an ever-changing and challenging training environment.



by [WO2 Matthew Tucker](#) (UK LO) and [Kristin Lechowicz](#) (DAC) of TRADOC G-2 ACE Threats Integration, and the Canadian Army Doctrine and Training Centre G5

In January 2016, the Canadian Army began the phased adoption of TRADOC’s [Decisive Action Training Environment \(DATE\)](#) as its common environment for training. To help educate exercise developers and planners in making optimal use of DATE, the Canadian Army delivered a Threat Tactics Course (TTC) at Canadian Forces Base Kingston from 2–6 November 2015. The following article discusses ACE Threats Integration’s (ACE-TI’s) mobile training team (MTT) support to the Canadian Armed Forces, and includes an excerpt from a previously-published piece in the magazine of the Canadian Armed Forces, “The Maple Leaf,” that provides insight into the rationale behind DATE adoption in the Canadian Army. This article finishes by discussing the benefits of collaboration and associated future endeavors.

Two ACE-TI members travelled to Kingston, Ontario, Canada, in November 2015 to provide an MTT in support of the Canadian Armed Forces’ initial program to educate their exercise developers and planners. The training was coordinated by two instructors from the Canadian Army Doctrine and Training Centre (CADTC), both of whom were graduates from the Threat Tactics Course at Fort Leavenworth, KS. The primary objective of the five-day block of classroom instruction was to introduce the students to DATE (with focus on the Military variable), teach hybrid threat principles, and explain the methodology from the [Training Circular \(TC\) 7-100](#) series of documents.



Figure 1. Selected US Army Training Circular 7-100 series documents

DATE contains five operational environment assessments (OEA) using the PMESII-PT construct (political, military, economic, social, information, infrastructure, physical environment, and time) and allows scenario developers to modify the variables in order to present the correct level and type of challenge for the training audience. The Military variable is expressed by describing the armed forces of each of the OEAs to include national command authority, strategy, size, and structure.

The detail provides exercise designers with the ability to provide a scalable, high-intensity, dynamic, near-peer regular force with niche capabilities that also includes irregular forces such as insurgents, guerrillas, and criminal elements to challenge a training audience. Scenario developers can also find details elsewhere within DATE that relate to and enrich the Military variable, such as:

- National infrastructure capabilities,
- National-level human intelligence, open-source intelligence, and signals intelligence programs,
- Information on communications capabilities,

- Details of nuclear capabilities and facilities, if relevant, and
- Details regarding the location, type, and purpose of underground facilities.

The doctrine of the armed forces presented in the DATE Military variable is expressed in the US Army TC 7-100 series. The hybrid threat doctrine provides a flexible and complex threat that will use an ever-changing variety of conventional and unconventional organizations, equipment, and tactics to create multiple dilemmas. Hybrid-threat doctrine is a composite created with real world examples extracted from multiple threat actors.

In January 2016, the excerpt below was published in “The Maple Leaf” magazine and provides the CADTC G5 point of view regarding the Canadian Army’s decision to adopt DATE and hold the initial hybrid threat OPFOR tactics training.¹

Much of the training delivered over the past decade to the Canadian Armed Forces has been focused on mission requirements. Now that the operational tempo has slowed, the need to focus on a combat capable, flexible, and adaptable force must be brought to the fore. To address this requirement the Commander of the Canadian Army, Lt-Gen Hainse, has made the decision that the Canadian Army will adopt the Decisive Action Training Environment as the common training environment.

The Common Contemporary Training System, based upon WEST ISLE scenario, was not meeting the Canadian Army needs, particularly with regard to joint force development or international interoperability. The Canadian Army requires a modern, adaptable, realistic and relevant training environment to fully prepare commanders, staffs and individual soldiers to successfully conduct Adaptive Dispersed Operations throughout the Full Spectrum of Operations. Adopting a single Common Training Environment and associated threat model, permits a deeper understanding of the full range of Opposing Forces.

While the Canadian Army Simulation Centre has been using the threat models from the DATE for three years, they had not begun conversion of the entire training environment until the decision to adopt DATE was made. DATE incorporates a better designed and in depth set of factors within the training environment based on PMESII-PT factors (political, military, economic, social, infrastructure, information, physical, and time). The DATE is supported by the 7-100 series of Training Circulars which detail threat tactics and other elements of the training environment.

Elements from the DATE can be used for training for Domestic Operations (DOMOPS) given that scenarios involving lone wolf actors, terrorist threats, criminal threats to the Canadian Department of National Defense property as well as the media. The fact that Canadian terrain must be employed for DOMOPS does not mean that the other elements of DATE are not valid for exercise development, design and delivery.

To teach exercise developers and planners to make optimal use of DATE, the first Canadian Army delivered TTC was conducted at Canadian Forces Base Kingston 2-6 November 2015. This serial of 32 students was delivered by qualified instructors from Canadian Army Doctrine Training Centre (CADTC) and Canadian Forces School of Military Intelligence (CFSMI), supported by two instructors from the US Army TRADOC G-2 Analysis and Control Element Threats Integration. These graduates now form the initial cadre of instructors at the Canadian Divisions, and they will begin delivering the TTC over the coming months.

ACE-TI’s participation in the first Canadian TTC has fostered TRADOC G-2 Operational Environment Enterprise (OEE) and Canadian Armed Forces relations. Both sets of instructors benefited and learned from the experience, which in turn benefitted the students. ACE-TI’s instructors built rapport and networked with their Canadian counterparts, which has already proved to be of use beyond this course. The student group discussions widened the experience of ACE-TI’s instructors by providing a greater insight into Canadian Army capabilities and how they would contribute to multinational coalition operations.



Figure 2. CADTC crest (used with permission)

As the Canadian Army moves toward its first large-scale live DATE exercise, “Maple Resolve 17,” its partnership with the TRADOC G-2 OEE is growing strongly. A large contingent from the Canadian Forces, including Army, Air Force, and Navy personnel, contributed considerably to the DATE 3.0 Working Group meeting held at Fort Leavenworth in December 2015. The TRADOC G-27 Operational Environment Training Support Center has established an easily-accessible electronic shared working area and has also offered direct support to the Canadian’s upcoming exercises.



Figure 3. [Canadian TOC operating on warfighter exercise](#)

At the same time that the Canadian Army is implementing DATE at its Maneuver Training Centre, the British Army is making similar strides. The staff at the British Army Training Area Suffield, which is located in Alberta, Canada, is working towards its first live DATE exercise, “Prairie Storm,” which is to be held in May 2016. These exercises are very encouraging for the training community and, with time, will create many more opportunities for training interoperability with international partners.

The Canadian TTC was a success for many reasons, and the valuable training will be spread through the Canadian Army by the newly-trained officers and soldiers. The US Army TRADOC G-2 OEE recognizes that the Canadian Army is an active champion of DATE and looks forward to an enriched product through further international collaboration.

References

Major-General Lanthier. Canadian Army’s Phased Adoption of the US Army DATE 2016. 6 Aug 2015.

Notes

¹ The Maple Leaf. “[Army Trains for Real World Threats.](#)” January 2016. Page 13. Reprinted with permission. (Link is only accessible from a Canadian government computer.)

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)

Tactical Action Report: Sinjar Preview

by [Rick Burns](#), TRADOC G-2 ACE Threats Integration (BMA CTR)

A focal point of the Islamic State of Iraq and the Levant's (ISIL's) 2014 Nineveh province offensive was the town of Sinjar. The forthcoming *Tactical Action Report: Sinjar* will contain a more detailed account of the ISIL occupation of Sinjar, the resulting humanitarian crisis, and the subsequent regrouping of Peshmerga forces and retaking of Sinjar with the help of US and allied air strikes. This article contains information about ISIL's Nineveh province offensive and the occupation of Sinjar.

Sinjar is a strategically-located Iraqi town in northwestern Nineveh province. It lies along a major ISIL east-west supply route that connects Mosul in Iraq with Raqqa in Syria—two important ISIL-held cities. Sinjar is approximately 52 km east of the Syrian border and 117 km west of Mosul. It is positioned at the foot of the Sinjar Mountains, an east-west mountain range rising 1,463 m above the surrounding alluvial steppe plains.

Sinjar is populated primarily by a Kurdish religious minority called the Yazidis. The Yazidis are particularly vulnerable to violence and persecution, having been the object of hatred for centuries because of their religious practices. Yazidis are ethnically Kurdish, but their religion combines elements of Islam, ancient Persian Zoroastrianism, and Eastern Mediterranean Mithraism. While Yazidis are monotheists, they believe in a fallen angel who serves as an intermediary between God and man. To Muslims, this intermediary resembles the Quranic devil. Yazidis are, therefore, considered devil worshippers by their Muslim neighbors. With isolated geography and a history of persecution, the Yazidis rarely intermarry and do not accept converts, further distinguishing themselves.¹



Figure 1. Sinjar mountain terrain

In June 2014, ISIL began an offensive in Nineveh province and captured Mosul, the second largest city in Iraq, that same month.² This defeat gave momentum to a push throughout Kurdish Peshmerga-held Nineveh province. On 1 August 2014, ISIL attacked a Peshmerga unit in the town of Zumar, a small Kurdish-majority outpost 40 km northwest of Mosul. ISIL killed 14 Peshmerga soldiers, while the group sustained 100 casualties and 38 members were taken prisoner in the attack.³ On 2–3 August, in a serious setback for Kurdish Peshmerga soldiers, ISIL succeeded in taking three strategic towns: Zumar, Wana, and Sinjar. Zumar is an oil-rich area that also lies on a road leading to Syria; Wana is a town on the Tigris river within

striking distance of the Mosul dam; and Sinjar is a town on a major supply line that connects ISIL-held Mosul in Iraq with ISIL-held Raqqa in Syria. The towns form a triangle west from Mosul to the borders of Syria and Turkey. The capture of these towns gave ISIL both momentum and proximity to seriously threaten those protecting the Mosul dam, which was temporarily captured and then lost by ISIL between 7–18 August, in part due to US air strikes.⁴

ISIL forces continued throughout August 2014 to push Kurdish Peshmerga forces from positions in Nineveh province. On 6 August, ISIL moved to within 49 km of Erbil, the capital of the Kurdish autonomous region, threatening US military and civilian personnel. On 8 August, the US began conducting airstrikes against ISIL positions, beginning around Erbil, to stop ISIL's advance on that city.⁵ Starting on 9 August, the US began airstrikes around the Sinjar Mountains to relieve Yazidis and others trapped by ISIL.⁶

ISIL successes created a humanitarian crisis, with thousands being displaced from their homes, kidnapped, injured, and killed by ISIL fighters. In the Sinjar area, ISIL gunned down 5,000 Yazidi men in a series of massacres, detained over 5,000 Yazidi women to be sold into slavery or given to jihadists, and caused as many as 200,000 civilians to flee, with 50,000 retreating into the besieged Sinjar Mountains. Pictures of Yazidis surrounded and trapped by ISIL on Mount Sinjar put increasing international pressure on the US administration to act and on Peshmerga forces—who were stinging from multiple defeats at the hands of ISIL—to reclaim lost territory.⁷

By October 2014, Peshmerga forces began winning back territory lost in the initial ISIL offensive. Attention then turned to rescuing the Yazidis trapped in the Sinjar area. The Kurdish offensive against ISIL began with US air strikes. Launching from the recaptured cities of Rabiya and Zumar, 8,000 Kurdish fighters opened a corridor from Mount Sinjar northeast into Kurdish-controlled areas. This broke the siege, but still left Sinjar in the hands of ISIL. Kurdish fighters were able to capture part of Sinjar, but settled into a stalemate with ISIL fighters in the city.⁸

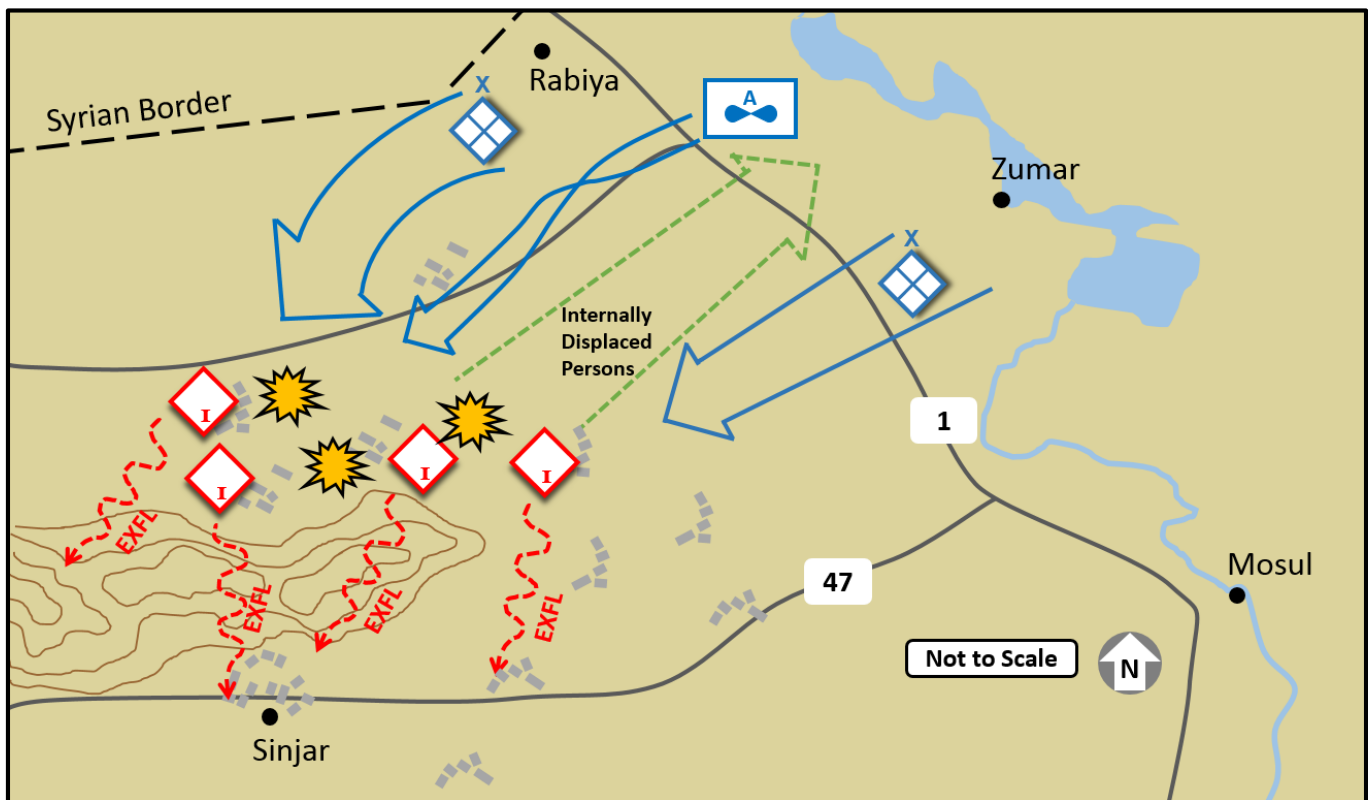


Figure 2. Kurdish Peshmerga attack on ISIL

ISIL encountered little resistance from Kurdish Peshmerga forces when it attacked Sinjar and the surrounding area in August 2014. It immediately took control of the population. Residents were told to either convert or be killed. While most

were able to escape, evidence of the extreme brutality brought to bear on those who remained has been found in mass graves uncovered after Sinjar was recaptured by Kurdish soldiers. Hundreds of Yazidis had been executed by ISIL and buried in mass graves.⁹ This served to both reduce the number of those not willing to adhere to the group's interpretation of Islam and to instill fear of noncompliance in those who remained.

Soon after ISIL took control of the city of Sinjar, US air strikes began to attack its positions. ISIL responded to this by building a network of tunnels that connected houses. These tunnels allowed protection and a means of subterranean command and control. The sandbagged tunnels, about the height of a person, contained ammunition, prescription drugs, blankets, electrical wires leading to fans and lights, and other supplies. In total, there were at least 30–40 tunnels.¹⁰



Figure 3. [ISIL tunnel in Sinjar \(video link\)](#)

At least two training points come from the invasion and occupation of Sinjar. First, ISIL is using violence against indigenous populations to both further its interpretive narrative of strict adherence to and protector of Islamic truth, and as a means of creating compliance through fear. The result is depopulation of whole towns and creation of humanitarian crises from fleeing, displaced people. A humanitarian crisis diverts attention and resources away from the hybrid threat, provides the enemy with human shield opportunities, and creates political and humanitarian pressures.

The second training consideration is the adaptive nature of the hybrid threat. Air strikes significantly limited ISIL's ability to maneuver and were critical to Kurdish success in gaining back lost territory from ISIL. ISIL responded to this new threat by going underground in Sinjar. Building a sophisticated network of tunnels that connected key buildings and provisioning those tunnels with supplies allowed the group to mitigate some of the effects of the bombing. Given time, the hybrid threat will continue to improve its subterranean expertise and find other ways to mitigate the effects of areas where it is threatened by superior technology.

Notes

¹ Avi Asher-Schapiro. "[Who Are the Yazidis, the Ancient, Persecuted, Religious Minority Struggling to Survive in Iraq?](#)" National Geographic. 11 August 2014.

² Al Jazeera. "[Rebels Seize Control of Iraq's Nineveh.](#)" 10 June 2014; for a more detailed description of the fall of Mosul see *Threat Tactics Report: Islamic State of Iraq and the Levant*.

³ Al Arabiya. "[Jihadists Kill Dozens as Iraq Fighting Rages.](#)" 2 August 2014.

⁴ Tim Arango. "[Sunni Extremists in Iraq Seize 3 Towns from Kurds and Threaten Major Dam.](#)" The New York Times. 3 August 2014; Tim Arango. "[Jihadists Rout Kurds in North and Seize Strategic Iraqi Dam.](#)" The New York Times. 7 August 2014; BBC News. "[Iraq Crisis: Mosul Dam Retaken from IS.](#)" 19 August 2014; for a more detailed description of the ISIL defense of the Mosul dam see *Threat Tactics Report: Islamic State of Iraq and the Levant*.

⁵ Julian E. Barnes, Jeffrey Sparshott, and Nour Malas. "[Barack Obama Approves Airstrikes on Iraq, Airdrops Aid.](#)" The Wall Street Journal. 8 August 2014.

⁶ Dan Roberts, Martin Chulov, and Julian Borger. "[Obama Authorises Air Strikes on ISIS to Help Iraqis Besieged on Mountain.](#)" The Guardian. 8 August 2014.

⁷ Mohammed A. Salih and Wladimir van Wilgenburg. "[Iraqi Yazidis: 'If We Move They Will Kill Us.'](#)" Al Jazeera. 5 August 2014; Steve Hopkins. "[Full Horror of the Yazidis Who Didn't Escape Mount Sinjar: UN Confirms 5,000 Men Were Executed and 7,000 Women Are Now Kept As Sex Slaves.](#)" Daily Mail. 14 October 2014; Martin Chulov. "[Iraq's Largest Christian Town Abandoned As ISIS Advance Continues.](#)" The Guardian. 7 August 2014.

⁸ BBC News. "[Mount Sinjar: Islamic State Siege Broken, Say Kurds.](#)" 19 December 2014.

⁹ Human Rights Watch. "[Iraq: Protect Mass Graves.](#)" 30 January 2016.

¹⁰ Associated Press. "[ISIS Dug Network of Tunnels under Conquered Iraqi City of Sinjar.](#)" 25 November 2015.



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

An opposing force (OPFOR) conducts tactical operations with a number of collective drills in support of accomplishing tactical tasks. One drill that occurs often is a requirement to fix an enemy element or force, which is integral to achieving a concurrent and/or subsequent task. A *fix* drill prevents the enemy from moving any part of its force from a specific location for a period of time.¹

A drill for the OPFOR is a collective task initiated by a situational cue that requires minimal leader orders to execute a prescribed group of actions. An OPFOR fix drill is often a subtask in other tactical tasks or drills. Actions can appear similar to tasks that isolate, block, and/or contain an enemy; however, a fix drill has a specified time period to fix actions at a specific location. Elements of information warfare (INFOWAR) such as perception management activities, deception techniques, and electronic warfare can be used to manipulate situational understanding of an operational environment (OE).

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/>.

OPFOR Collective Drill

An OPFOR applies a collective fix drill to deny an enemy force or element the ability to physically move from a location and/or psychologically convince an enemy leader to remain stationary in a geographic position. Tactical intelligence on the enemy situation, understanding of the natural conditions in an area of responsibility (AOR), and anticipated enemy tactical actions shape how an OPFOR leader uses available resources to fix an enemy.

OPFOR offensive actions typically apply a concept of fixing enemy forces to prevent their freedom to maneuver.² An enemy can be fixed by presenting, distorting, and/or deceiving situational understanding using conditions that include but are not limited to:

- Ineffective or no communication with its higher headquarters,
- Unclear or incorrect battlefield awareness,
- Loss of mobility and/or freedom to maneuver due to complex terrain, obstacles, or OPFOR combat power, and
- Belief that friendly elements or forces are about to become or are decisively engaged.

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* assigned to various subordinate units to perform. At brigade or brigade tactical group (BTG) and higher echelon units, the subordinate units of those headquarters performing these functions are referred to as *forces*. At battalion or battalion detachment (BDET) and lower echelon units, these units are called *elements*.

TC 7-100.2 Opposing Force Tactics (2011)

An OPFOR element or force that *enables*—by fixing enemy elements or forces so they cannot interfere with the primary action—is a *fixing* element or force.³ The functional action determines a force or element designation. For example, a disruption element generally disrupts, but also may need to fix a part of the enemy element or force. The functional designation then becomes fix rather than disruption.⁴ This article uses an element echelon in the tactical example. The element leader focuses on how to best accomplish this intent with considerations given to:

- Known, probable, or possible enemy avenues of approach,
- Elements allocated to fix the enemy,
- Directional positioning of enemy elements,
- Prioritization of engineer efforts for camouflage, cover, concealment, and deception (C3D),
- Countermobility actions focused to protect friendly elements and channel the enemy into kill zones,
- Massed on order fires, and
- Movement and maneuver.

In the following example, the OPFOR leader must fix an enemy element to prevent its interdicting several of his dispersed elements as they move along a restrictive valley corridor. Active reconnaissance and surveillance transition to security actions in a disruption zone to fix. INFOWAR systems exploit the fix drill in near real-time media releases for perception management and to degrade enemy morale.

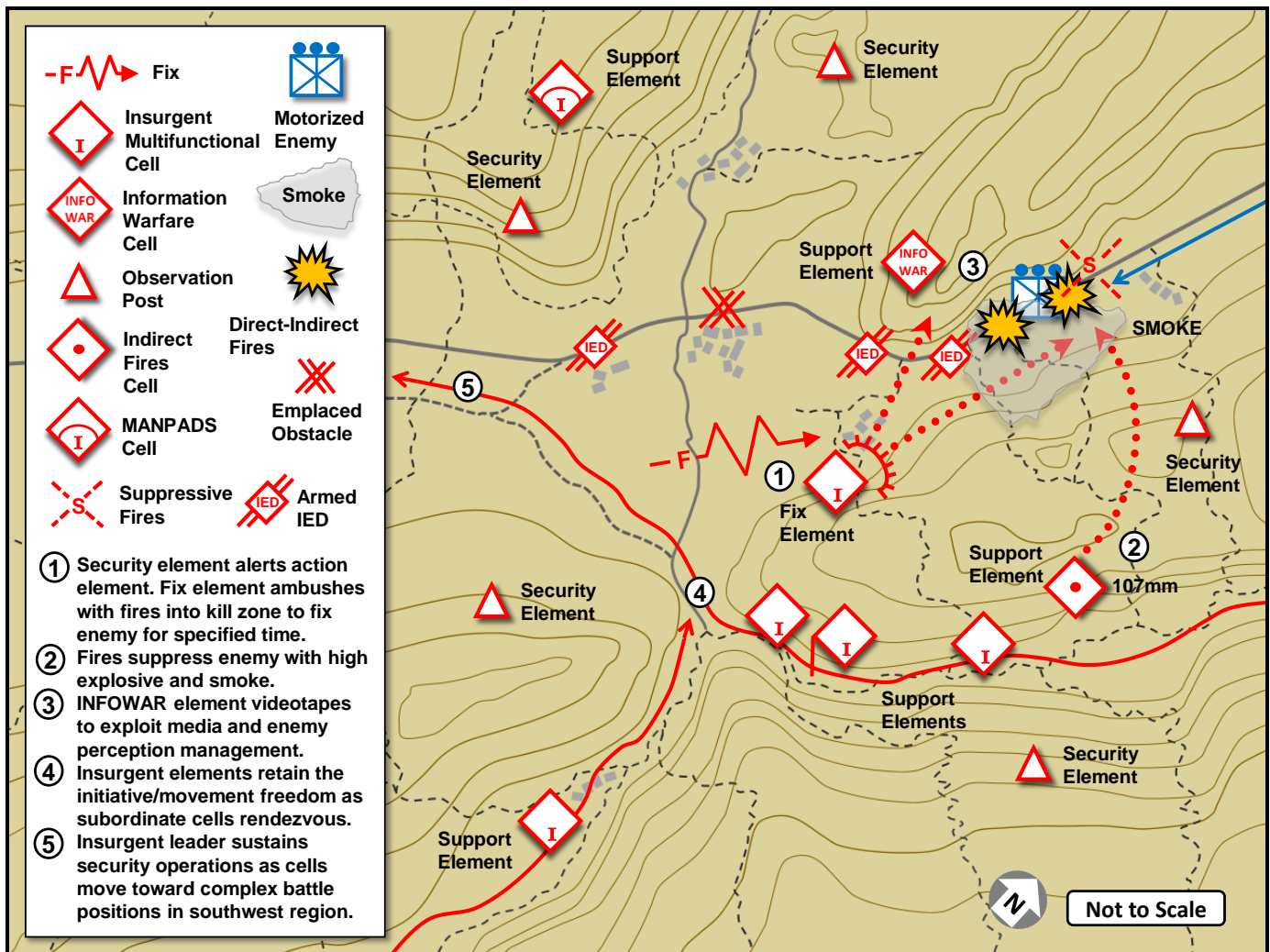


Figure 1. OPFOR collective drill to fix

An OPFOR leader recognizes that enemy action and battlefield conditions may make the originally-selected mission irrelevant and require an entirely new mission with minimal time to react. An example would be an OPFOR fixing element that finds itself the target of an enemy fixing action. To continue solely as a fixing element might actually assist the enemy in achieving its mission. The OPFOR leader could decide to change his task organization, allocating a part of the fixing element as an exploitation element and employing a smaller amount of combat power to keep the enemy fixing element from being able to influence the critical OPFOR tactical action.

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 fix drill, systems warfare or other support, such as INFOWAR systems, can be integrated in support of an overarching deception objective. A fix drill at any OPFOR level of command and with any type of elements and/or forces has the same basic subtasks. For example, a tactical environment could present the following conditions as a mission task. The OPFOR is conducting operations independently or as part of a larger element and receives an operation order or fragmentary order to fix 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 drill. The OPFOR has communications with higher, adjacent, subordinate, and supporting elements. Friendly forces, enemy coalition forces, noncombatants, government agencies, nongovernment 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 fix actions in accordance with tactics and techniques in [Training Circular \(TC\) 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 then continues the mission. The tasks and subtasks from initial plans to mission completion include five main tasks with several subtasks. A guide for selecting priorities of effort in training tasks to Army standard as an OPFOR is as follows:

PLAN

- Identify reconnaissance and surveillance objectives for collection and analysis in support of AOR situational awareness and situational understanding requirements.
- Identify elements that are to be fixed in support of the mission.
- Collect current information on enemy element capabilities and limitations, locations, and other operational environment information.
- Analyze *action* and *enabling* functions that must be performed to achieve mission and collective drill success for a fix drill.
- Determine the functional tactics to be applied by *action*, *enabling*, and *support* elements.
- Identify task organization requirements for elements by function in accordance with TC 7-100.2/TC 7-100.3.
- Determine how functional elements act or enable security tasks, *fix* the designated enemy element, conduct other offensive actions, provide combat support and combat service support, and/or transition to other tasks/subtasks.
- Identify time constraints and/or restrictions on accomplishing the mission and supporting requirements of a fix drill.

PREPARE

- Provide situational understanding of the enemy and operational environment from current reconnaissance, surveillance, and intelligence reports.

- Report regular, periodic, and/or unexpected information updates in a timely manner to satisfy the commander's critical information requirements and mission intent.
- Task-organize elements by function to fix the enemy in accordance with TC 7-100.2/TC 7-100.3.
- Coordinate the integration of available reconnaissance, intelligence, surveillance, and target acquisition assets for continuous and overlapping coverage of designated areas, zones, routes, and/or special objectives in the AOR and zone of reconnaissance responsibility (ZORR).
- Conduct counterreconnaissance actions that prevent enemy situational understanding of OPFOR intentions and/or offensive actions.
- Tailor each element's capabilities, taking into consideration anticipated complex terrain, survivability measures, and camouflage, concealment, cover, and deception (C3D).
- Conduct mission and task rehearsals of *action* and *enabling* elements and the action subtasks to fix an enemy element.
- Coordinate for required direct and indirect fires.
- Coordinate and prepare to emplace selected countermobility obstacles in conjunction with C3D.
- Confirm redundant command and control communication requirements and capabilities.
- Execute INFOWAR in support of offensive actions.

PREVENT MOVEMENT

- Confirm current enemy conditions at the enemy location and/or direction and speed or tempo of movement/maneuver of enemy elements to be fixed.
- Coordinate with friendly elements in adjacent AORs to ensure overlapping coverage of ZORRs and provide early warning of enemy activities and/or operational environment conditions that can impact on the fix drill.
- Conduct counterreconnaissance tasks to destroy or defeat enemy security elements that can influence the fix drill.
- Detect enemy elements along ground or air avenues of approach and coordinate to disrupt, delay, or deny access of those elements to the enemy being fixed.
- Maintain contact with the enemy to be fixed with observation and/or technical-sensor reconnaissance and surveillance means to sustain current situational information.
- Emplace selected stationary countermobility obstacles in conjunction with C3D.
- Position a reserve element for rapid movement/maneuver, on order of the OPFOR leader, to support the mission.
- Conduct undetected movement by *action* and *enabling* element(s) to occupy simple battle position(s) and/or support locations for security tasks and the fix drill.
- Execute actions that convince the enemy leader that he cannot move from the present location.
- Execute INFOWAR in support of the fix drill that convinces the enemy leader to not move his elements from their present location.

EXECUTE FIX

- Provide security for *action* and *enabling* element(s) that execute the fix drill.
- Engage enemy elements with direct and indirect fires in the fix location or kill zone.
- Suppress and/or neutralize enemy elements in the fix location or kill zone.
- Execute selected mobile countermobility obstacles in conjunction with direct and indirect fires and obscuration.
- Conduct INFOWAR perception management activities to convince the enemy leader that he cannot or should not move from the present location.

- Employ, when appropriate, INFOWAR electronic warfare activities to block or disrupt enemy command and control in support of fixing the enemy element.
- Employ, when appropriate, relevant populations in the target area to physically block, contain, or disrupt an enemy element in support of the fix drill.
- Deny enemy elements freedom of movement and maneuver in a designated location or kill zone for a specified period of time.
- Achieve the fix purpose, which can include intent to contain, isolate, suppress, neutralize, interdict, defeat, and/or destroy selected enemy elements.

CONTINUE MISSION

- Report regular, periodic, and/or unexpected information updates in a timely manner to satisfy the commander’s situational awareness and situational understanding requirements.
- Execute tasks with stay-behind elements, when required, that can include but are not limited to: surveil, disrupt, delay, suppress, neutralize, defend, defeat, and/or destroy tasks.
- Report reorganization and combat effectiveness of OPFOR elements.
- Recommend if current tactical conditions require an adjustment to the time and/or tempo for current and/or subsequent mission tasks.
- Continue the mission.

Table 1. Tactical drill: Fix

TACTICAL DRILL: FIX		
No.	Scale	Measure
01	Yes/No	Reconnaissance identifies enemy to fix
02	Yes/No	Counterreconnaissance actions effective
03	Yes/No	Report timely reconnaissance-intelligence
04	Yes/No	Deception actions are effective
05	Time	Select fix actions/method
06	Time	Position action and enabling elements
07	Time	Isolate enemy
08	Time	Execute fix actions
09	Time	Elements achieve fix task
10	Yes/No	Report effective fix of enemy
11	Percent	Friendly elements available to continue
12	Yes/No	Recommend if mission requires adjustment
13	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.⁵ Per Army doctrine, “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.”⁶ TRADOC G-2 Analysis and Control Element (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.⁷

An OPFOR must be a realistic, robust, and relevant threat that challenges the capabilities and limitations of Army forces in the execution of their military missions. TRADOC G-2 Analysis and Control Element (ACE) Threats Integration at Fort Leavenworth, Kansas, is refining the task, condition, and standard for an OPFOR fix collective drill and its use in learning venues in training, professional education, and leader development. Current operational considerations and emergent threats since the publication of OPFOR tasks in [TC 7-101, Exercise Design Guide](#) 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, and/or unit leader can use this OPFOR training literature on the fix drill to support OPFOR 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.

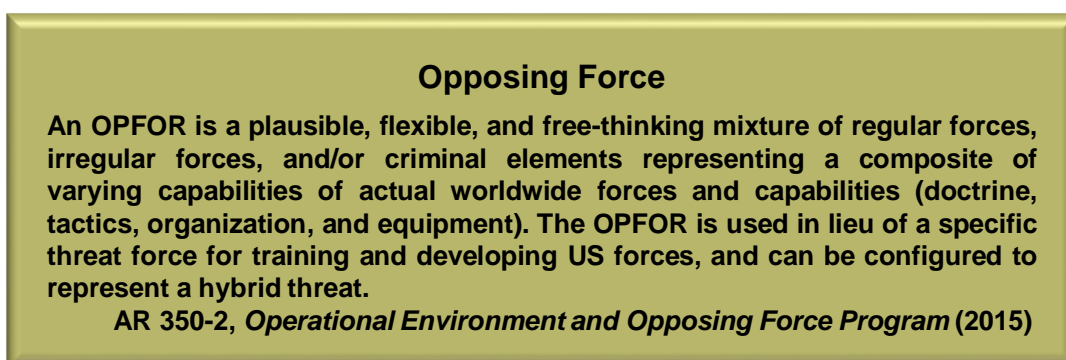


Figure 2. Opposing force for training readiness

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. 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.

Notes

¹ 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 5-40.

² 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 3-29.

³ 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 2-54.

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. Paras 2-50 and 2-55.

⁵ Headquarters, Department of the Army. [Army Regulation 350-2, Operational Environment and Opposing Force Program](#). 19 June 2015. Para 2-8a.

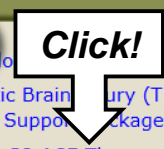
⁶ Headquarters, Department of the Army. [Army Regulation 350-2, Operational Environment and Opposing Force Program](#). 19 June 2015. Para 1-5b.

⁷ Headquarters, US Army Training and Doctrine Command. [TRADOC Regulation 10-5-1, Organization and Functions](#). 20 July 2010. Para 8-18c(1)(a).

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

 <https://atn.army.mil/> **1** 

Leader Development **Soldiers Skills** **Training for Operations**

- Cyber Electromagnetic Activities (CEMA) Resources
- SHARP Training
- Deputy Commanding General Course
- Warrior Tasks and Battle Drills
- Mandatory Training (AR 350-1)
- U.S. Army Physical Readiness
- **2** **Click!** 
- Traumatic Brain Injury (TBI) Training Support Package
- TRADOC G2 ACE Threats Integration

TRADOC G-2 ACE Threats Integration

3 **Browse the e-Folders** 

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.

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

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 DAC jennifer.v.dunn.civ@mail.mil	Jennifer Dunn 684.7962
Military Analyst/Operations jon.h.moilanen.ctr@mail.mil	Dr. Jon Moilanen IDSI 684.7928
Intelligence Specialist DAC jerry.j.england.civ@mail.mil	Jerry England 684.7934
Senior Threats Officer james.d.hunt50.mil@mail.mil	MAJ Jay Hunt 684.7960
Intel Specialist-NTC LNO DAC kristin.d.lechowicz.civ@mail.mil	Kris Lechowicz 684.7922
(UK) LNO Warrant Officer matthew.j.tucker28.fm@mail.mil	Matt Tucker 684-7994
Intelligence Specialist-DATE DAC angela.m.mcclain-wilkins.civ@mail.mil	Angela Wilkins 684.7929
Intelligence Specialist DAC walter.l.williams112.civ@mail.mil	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.deatricks.ctr@mail.mil	Laura Deatricks 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)