Red Diamond
Threats Newsletter

TRADOC G2 Operational Environment Enterprise
ACE-Threats Integration

Fort Leavenworth, KS Volume 6, Issue 4 APR 2015

INSIDE THIS ISSUE

OEE *Red Diamond* published monthly by TRADOC G2 OEE ACE-Threats Integration

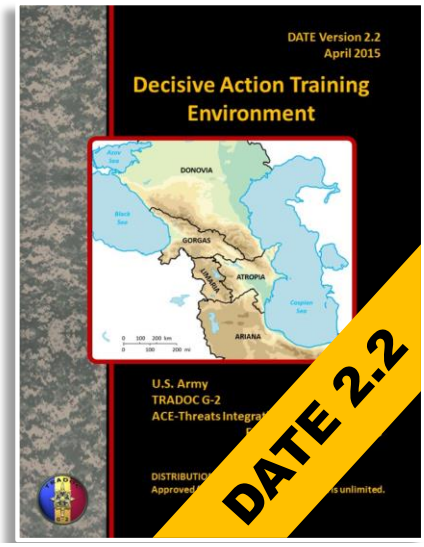
Send suggestions to:

ATTN: *Red Diamond*
Dr. Jon H. Moilanen
Operations
BMA Contractor
and
Angela Wilkins
Chief Editor and
Product Integration
BMA Contractor

DECISIVE ACTION TRAINING ENVIRONMENT 2.2 PUBLISHED

by Laura Deatrick, ACE-Threat integration (CGI Ctr)

The ***Decisive Action Training Environment*** (DATE), version 2.2, is now published and will soon be available on the Army Training Network (ATN) website. The DATE 2.2 provides the US Army with a common training baseline of detailed operational environments (OEs) that consist of five notional countries in a complex dynamic region. Hybrid threats include guerrilla units, insurgent organizations, criminal elements, and regular military forces. Acts of terrorism range from local incidents to international and transnational impacts.



Developed by the ACE-Threats Integration Directorate, DATE 2.2 is a product of the TRADOC G2 Operational Environment Enterprise (G2 OEE). Based on Chief of Staff of the Army guidance, the DATE applies to all US Army (Active Army, Army National Guard, and Army Reserve) units and integrates appropriate conditions in live training at home station, exercise locations, institutional organizations and activities, Combat Training Centers (CTCs), and constructive, virtual, and gaming simulations to improve leader and unit-team readiness.

The DATE offers challenging conditions through OE variables of political, military, economic, social, information, infrastructure, physical environment, and time (PMESII-PT). Commanders, exercise planners, and/or curriculum developers can integrate selected OE conditions into exercise design (TC 7-101) and/or Army learning (TC 7-102) for training, professional education, and leader development.

It is imperative that our Army adapts to the future Joint operating environment, one that consists of diverse enemies that employ traditional, unconventional, and hybrid strategies which threaten U.S. security and vital interests.

General Raymond T. Odierno (2015)

RED DIAMOND TOPICS OF INTEREST

by Jon H. Moilanen, TRADOC G2 ACE-Threats Integration, Operations and Chief, *Red Diamond* Newsletter (BMA Ctr)

This month's lead article spotlights a recent Warfighter exercise with the 38th Infantry Division supported by the 2nd Canadian Mechanized Brigade Group (CMBG). The WFX was in a Decisive Action Training Environment.

ACE-Threats Integration hosted 60 students for the March 2015 Threat Tactics Course at Fort Leavenworth. Students included active duty and reserve component military, Department of the Army civilians, contractors from as far as Ft. Shafter, Hawaii, and attendees from the Canadian Army.

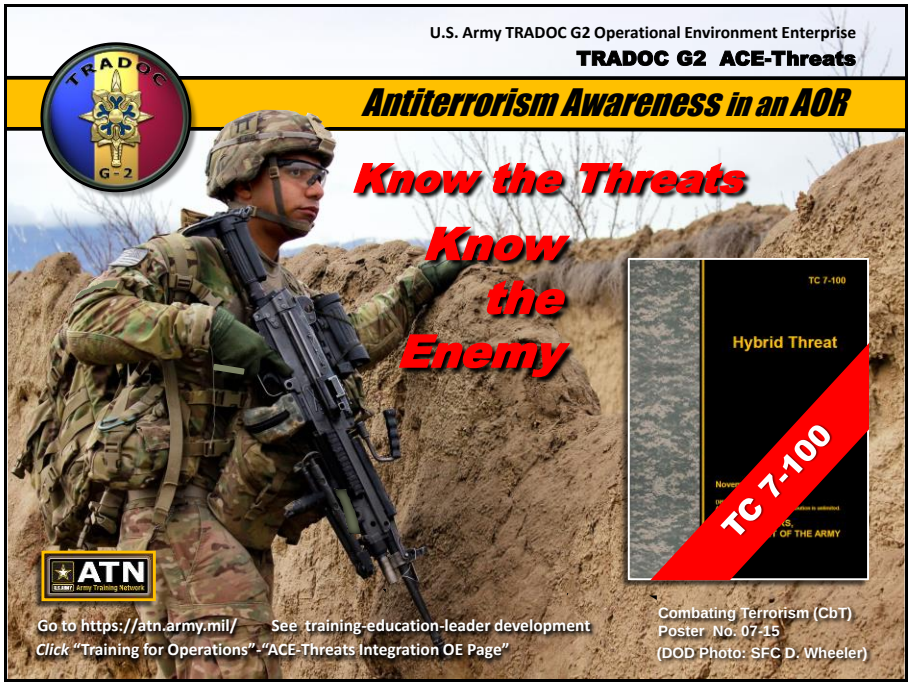
The intelligence staff officer must demonstrate technical skills competency and the ability to integrate intelligence architecture experiences to achieve expertise. Team proficiency in DCGS-A and other capabilities is a baseline tenet to optimize the Army intelligence enterprise.

An article on the RPG-28 rocket propelled grenade (125mm tandem warhead rocket) notes a disposable, non-extending launcher. This weapon is capable of a mobility or catastrophic kill on any main battle tank (MBT) known to be in current service with any nation, and can also be used in an anti-materiel role.

Military symbols is part 2 of a two-part article series. Threats and/or opposing forces (OPFOR) symbols are based on DOD and US Army doctrine in support of US Army training, professional military and civilian education, and leader development.

Email your topic recommendations to:

Dr. Jon H. Moilanen, ACE-Threats Integration Operations, BMA CTR
jon.h.moilanen.ctr@mail.mil
and
Angela M. Wilkins, ACE-Threats Integration Chief Editor and Product Integration, BMA CTR
angela.m.wilkins7.ctr@mail.mil



Director's Corner
Thoughts for Training Readiness

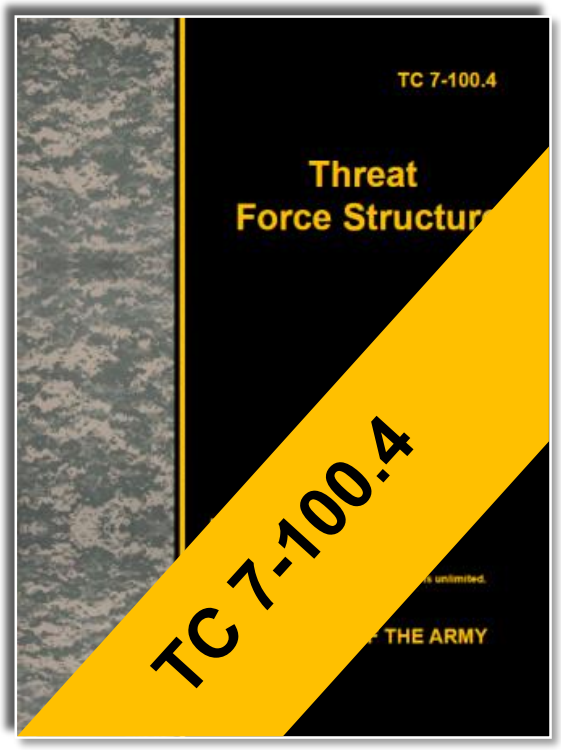
by Jon Cleaves, Director, TRADOC G2 ACE-Threats Integration

As part of the TRADOC G2 Operational Environment Enterprise (G2 OEE), the Analytic and Control Element (ACE)-Threats Integration Directorate continues to design, document, and integrate threats as opposing forces (OPFOR). The OPFOR are plausible, flexible military and/or paramilitary forces representing a composite of varying capabilities of actual worldwide forces (doctrine, tactics, organization, and equipment) used in lieu of a specific threat force for training and developing US military forces. We also conduct research on current threats operating in US areas of responsibility (AOR) to incorporate adversary and/or enemy capabilities, limitations, and constraints that could affect US mission success.

Threats and OPFOR are dynamic variables within conditions existing in any operational environment (OE), and are recurring considerations in the training literature we produce that supports US Army readiness—in training, professional education, and Army leader development. Regular review and analysis of threat incidents, apparent trends, and evolving patterns provide rationales for the periodic update of our publications on operational environments (OEs) and critical variables as they affect military operations.

A near-term update about to be released on the Army Publishing Directorate and the Army Training Network (ATN) is HQDA Training Circular 7-100 series. *Threat Force Structure*, TC 7-100.4. Originally titled *Opposing Force Organizational Guide*, this training circular updates threat force structures and associated online organizational directories to represent a realistic composite of known enemies and/or adversaries the US Army might encounter in near-term and midterm OEs.

Once published on the ATN website, the online organizational directories of TC 7-100.4 will be living documents and maintained with current weapon, system, and equipment data by the TRADOC G2 ACE-Threats Integration Directorate. Data in these directories is a sampling and is not intended to be a comprehensive listing of all available capabilities.



These OE conditions can be applied to the full-range of learning skills and organizational echelons in live, virtual, constructive, and gaming simulation experiences. Of course, if a US Army unit is preparing for a contingency or deployment mission with a probable threat or known threat environment, the unit commander uses that threat for his mission preparations.

If you search the directories and do not find a particular type of capability critical to your training objectives—contact us. We can address a flexible baseline of regular forces and irregular forces that can be adapted to meet a variety of different training, professional education, and leader development requirements. We will coordinate with you to obtain an appropriate level of threat understanding for realistic, robust, and relevant *conditions* that challenge your learning objectives on a path to achieving and sustaining Army standards.

JON

by Patrick Madden, TRADOC G2 ACE-Threats Integration (BMA Ctr)

MCTP WFX 15-3 was a distributed, simulation supported, corps-level, command post exercise. WFX 15-3 was held in Texas (Fort Hood), Indiana (Camp Atterbury), and Kansas (Fort Leavenworth) from 3 through 12 February 2015. WFX 15-3 is one of four corps and division-level exercises scheduled to be conducted by MCTP, Operations Group X-Ray during fiscal year 2015. The majority of WFXs are based on the Decisive Action Training Environment (DATE) and the Army Training Circular 7-100 series of publications.

The purpose of these exercises is to create a competitive and multi-echelon component training environment in order to provide commanders the opportunity to execute mission command in unified land operations (ULO). Each WFX is 10 days long and includes a comprehensive list of tasks in order for units to accomplish specific training objectives. (See figure 1 for WFX 15-3.) Based on this timeline and unit training objectives, the following discussion describes exercise design conditions, the unique features of WFX 15-3, and execution of this DATE-based exercise.

DAY#	1	2	3	4	MAAR	5	6	7	8	COM
DATE	3	4	5	6	7	8	9	10	11	12
III Corps	ATTACK TO PL GARY					ATTACK TO PL BILL		ATTACK TO PL VICTORIA		
176 ENG	MOBILITY					MOBILITY	WET GAP (KURA)		SURVIVABILITY	
1 CAB	DISRUPTION ZONE FIGHT / SCREEN					INTERDICTION / AIR ASSAULT / SCREEN				
38 ID	SEIZE OBJ JETS (CHEM)		ATTACK TO PL GARY			ATK to OBJ GIANTS	WET GAP (ARAS)	SEIZE OBJ RAMS BLOCK	TRANS	
2 CN	SECURE OBJ JETS (CHEM)		ATTACK TO PL GARY			ATK to OBJ GIANTS	WET GAP (ARAS)	SEIZE OBJ SEAHAWKS BLOCK	TRANS	
10 CAB	DISRUPTION ZONE FIGHT / SCREEN					AASLT		DISRUPTION ZONE FIGHT		
197 FAB	PROVIDE FIRES		ASSUME COUNTERFIRE			COUNTERFIRE		PROVIDE FIRES		
555 EN	MOBILITY					WET GAP		SURVIVABILITY / TRANSITION		
404 MEB	MANEUVER SUPPORT OPS / SUPPORT AREA OPS					MANEUVER SUPPORT OPS / SUPPORT AREA OPS			TRANS	
ESC	PROVIDE SUSTAINMENT MISSION COMMAND					PROVIDE SUSTAINMENT MISSION COMMAND				
15 SB	CONDUCT GS SUSTAINMENT ON AREA BASIS					CONDUCT GS SUSTAINMENT ON AREA BASIS				
230 SB	CONDUCT THEATER DISTRIBUTION					CONDUCT THEATER DISTRIBUTION				
LEGEND	ESC		38 ID					III Corps		AAR

Figure 1. Warfighter exercise 15-3 timeline and training environment priorities

Scenario Design

The scenario leading up to the beginning of the exercise involved a dispute between Ariana and Atropia. Ariana accuses Atropia of stealing oil reserves and deploys its military units along the Arianian/Atropian border under the guise of conducting training exercises. This is followed by the United Nations (UN) imposing two rounds of sanctions on Ariana and evacuation of US embassy personnel from Baku. Ariana responds by invading Atropia with an operational strategic command (OSC) comprised of four division tactical groups (DTGs). Ariana is partially successful in seizing most of Atropia with the exception of the western half of the country and a small area in the northeast, which includes the capital of Baku. In response, the US and the UN passed resolutions authorizing military force.

As a result of the military authorizations, Combined Joint Task Force (CJTF) 12 is created to intervene on behalf of Atropia. Led by US forces, CJTF 12 deploys to Gorgas and then moves east from the Black Sea Port of Poti into western Atropia in order to attack, defeat, and force the withdrawal of Ariana. When the exercise began, ground forces from CJTF 12 had already conducted a forward passage of lines (FPOL) with two Atropian Army brigades and began shaping operations against OSC forces. Initially, the main effort was led by the US 1st Infantry Division in the north and supported by the 38th Infantry Division in the south. In the northeast of Atropia, remnants of brigades from the Field Group and Capital Defense Command remained to defend against OSC 2 attempts to capture Baku.

Training Units

The evaluated training division for this exercise was the 38th Infantry Division from the Army National Guard. Supporting the 38th were three brigade combat teams (BCTs) as well as the 2nd Canadian Mechanized Brigade Group (CMBG). Also supporting the 38th was an Atropian armor brigade and four additional US brigades consisting of artillery, engineers, maneuver enhancement, and rotary wing aviation. Training objectives for the 34th were the following:

- Exercise mission command using the operations process to employ forces in unified land operations (ULO) and execute decisive action (offense, defense, and stability tasks) by means of Combined Arms Maneuver (CAM) and Wide Area Security (WAS).
- Exercise the intelligence process by managing information collection, supporting the targeting process, and providing intelligence support and situational understanding to the commander and staff.
- Synchronize lethal and nonlethal fires (including joint fires) using the targeting process in coordination with higher, lower, and adjacent unit fires.
- Refine the division's battle rhythm for decisive operations.
- Plan and execute division sustainment operations in coordination with corps and theater plans.
- Plan and execute effective stability tasks in coordination with host nation to establish a safe and secure environment.
- Refine division information and knowledge management systems and processes.

In addition to the training division, there was a higher command represented by III Corps as the coalition joint forces land component command (CJFLCC) of the notional CJTF 12. The III Corps staff was also participating as a training unit in preparation of their formal evaluation during WFX 16-4. The III Corps commander also functioned as the Exercise Director. Evaluated training units supporting III Corps consisted of two sustainment brigades, one rotary wing brigade, and one engineer brigade. Also supporting III Corps was an artillery brigade, maneuver enhancement brigade, and a Stryker cavalry regiment which functioned as the CJFLCC reserve. These III Corps units all operated as competitive response cells but were not part of the evaluated training audience. In total, there were nine competitive, evaluated training brigades which also had training objectives and were part of the formal after action review process.

Additional units that were part of a larger simulated, scripted supporting force for the overall exercise design were the 1st Infantry Division and remnants of Atropian forces. These forces and their subordinate units were also controlled by MCTP. For details, see figure 2 which highlights the training units in blue. All other units depicted in yellow, gray, green, and white respectively were either response cells, simulated by MCTP's movement control center, higher command, or not exercised but part of the overall exercise design. Also part of CJTF 12 were the coalition forces air component command (CFACC) and the joint forces special operations component command (JFSOCC). Response cells from these respective commands replicated the associated subordinate commands.

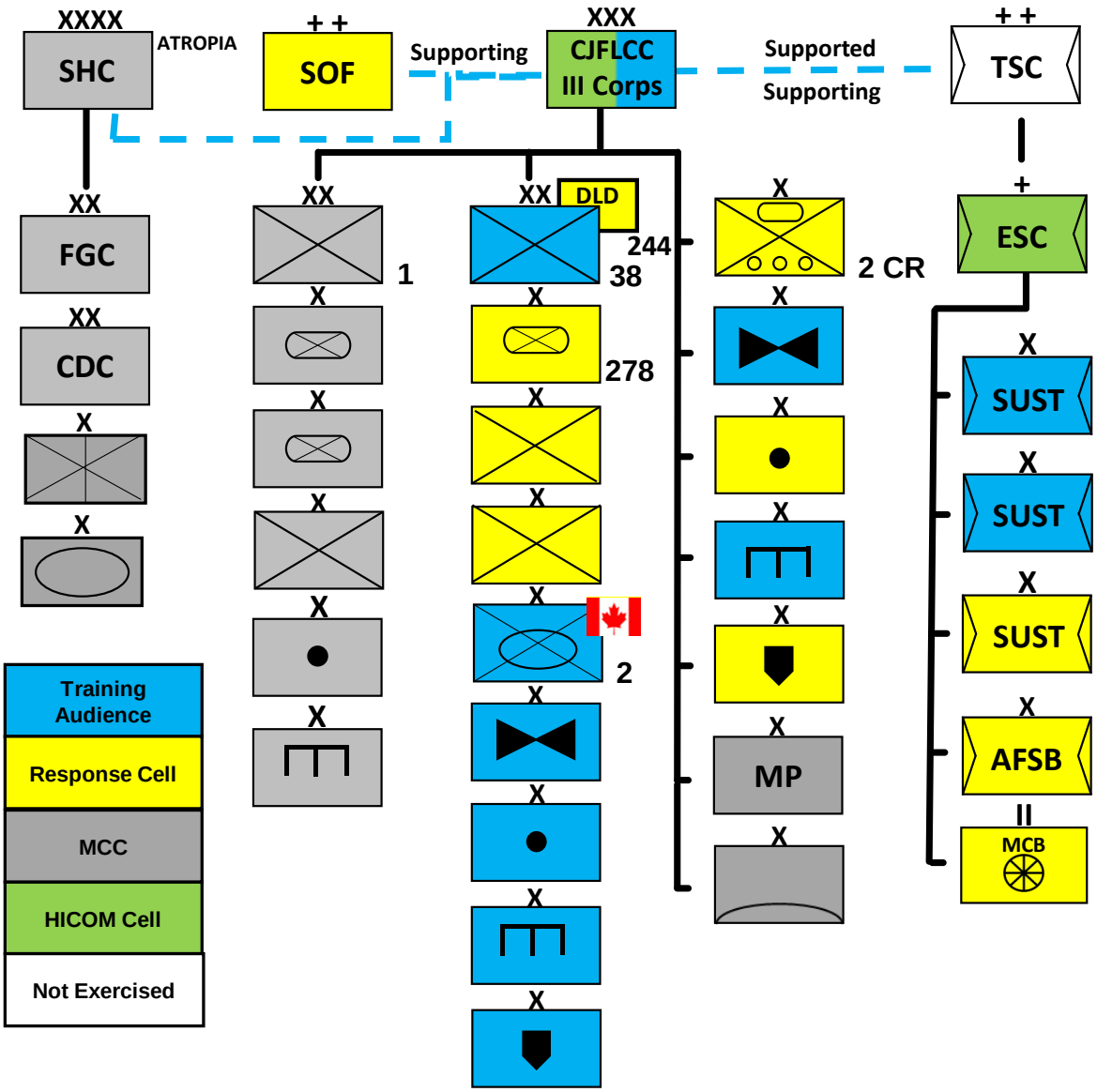


Figure 2. Training unit task organization (selected sample)

The exercise for training units was organized into three phases. Phase II was titled Shaping Operations which included a noncombatant evacuation operation. Phase III was divided into three sub-phases. Phase IIIA, Access, began with initiation of offensive operations and ended with the commitment of the CJFLCC reserve. Phase IIIB, Gain Position, included commitment of the corps reserve and ended with conditions set for wet gap crossings. Phase IIIC, Defeat, began with 1st ID seizing Objective Titans just east of the Agshu River and the 38th lead BCTs crossing the Aras River. Phase IIIC ends with the defeat of OSC 2 remaining DTGs and severing ground lines of communications. The final phase was titled Stability, which included the reestablishment of the Atropian-Arianian border.

Unique features of this exercise were the 244th Digital Liaison Team (DLT), 2nd CMBG, and WCOPFOR employment of Harpy unmanned aerial vehicles (UAVs), guided missiles, and commandos. The 244th DLT from the Illinois Army National Guard is a small team which has the mission of providing liaison capability to the Army forces with major subordinate commands including coalition units. They also work with many foreign armies as part of multinational exercises and are involved in exercise design. The 244th in this exercise assisted the 38th ID in ensuring that information exchanges between the 2nd CMBG and the division were accurate, clear, and timely. The 2nd CMBG was actively used by the 38th ID throughout the exercise. Both sides gained valuable lessons learned in coalition warfare such as interoperability and connectivity. Also

unique was the first employment of two power parachute commando companies and Harpy unmanned combat aerial vehicle (UCAV) designed to destroy radar emitters. These two assets were used as part of a counterattack discussed below. Significant damage and causalities resulted from their coordinated attacks during the latter part of the exercise.

Opposing Force (OPFOR)

MCTP's World Class Opposing Forces (WCOPFOR) now plan and operate competitively as an OSC during WFXs with approximately four subordinate divisions and separate brigades. This new requirement to operate at a higher echelon is a significant challenge since they are only manned for a division level exercise. The OSC is subordinate to a Supreme High Command (SHC) which is part of MCTP Exercise Control Group (ECG). The SHC plans and operates as a "white hat" organization that attends 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.

OSC 2 opposed III Corps and their two divisions. Supporting maneuver units from OSC 2 were the 306th Reconnaissance Brigade, four division tactical groups (DTGs) consisting of the 17th, 18th, 19th and 20th. Also supporting OSC 2 were two separate brigades, two militia brigades, and a naval infantry regiment. The mission of OSC 2 was to conduct a planned defense within their area of responsibility (AOR) in order to destroy Atropian Defense Forces, instigate regime change, and compel extra-regional forces to cease interference in Atropian national issues. Operational success was defined as destroying coalition forces when they advanced into Kill Zone Prancer. Strategic success was defined as seizing Baku and retaining critical hydrocarbon assets. For details on the initial composition of OSC 2 units, see figure 3.

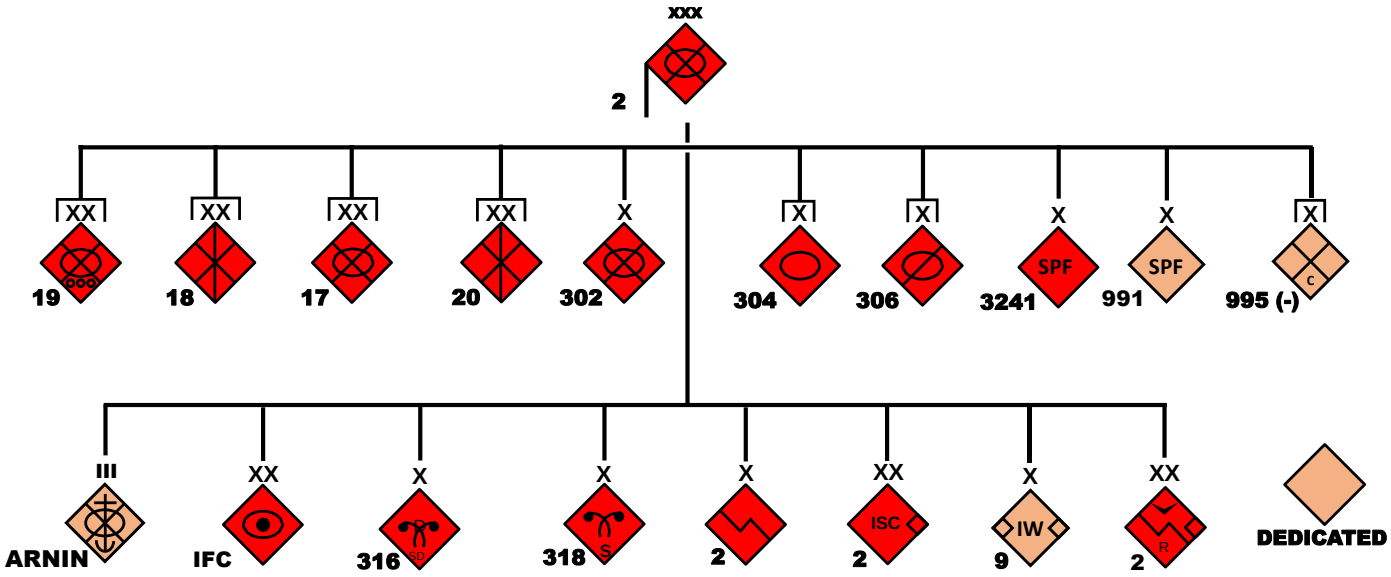


Figure 3. Operational strategic command initial composition of units

At the beginning of the exercise the overall strength of OSC 2 units were approximately 60-70% as a result of previous attrition from the invasion of Atropia. Since the coalition forces were attacking with units at approximately 100% strength, OSC 2 maneuver units used defensive tactics throughout most of the exercise. However, given the availability of complex terrain, OSC 2 planned counterattacks in attempts to block or stall the coalition offensive.

OPFOR Defense

As with most of the OPFOR offensive and defensive tactics, their AORs are divided into disruption, battle, and support zones. The key task for the 306th Reconnaissance Brigade in the OSC 2 disruption zone was to disrupt and delay coalition forces as well as report on their disposition, location and intent. To the northeast of the 306th was the 18th DTG which had seized a portion of the Baku–Tbilisi–Ceyhan Pipeline and then assumed defensive positions in the battle zone. To the east of the 18th was the 19th DTG also located in the battle zone and positioned southwest of Baku, having failed to seize the capitol. The 19th was given the difficult mission of continuing to attack to seize Baku in the east as well as establishing a defense along the Agshu River in the west. Located to the southeast of the 19th on the Caspian coastline was the Ariana

Naval Infantry Regiment with the mission to capture and retain the Sangachal Oil and Gas Terminal. For details on initial disposition of OSC 2, DTG units, see figure 4.

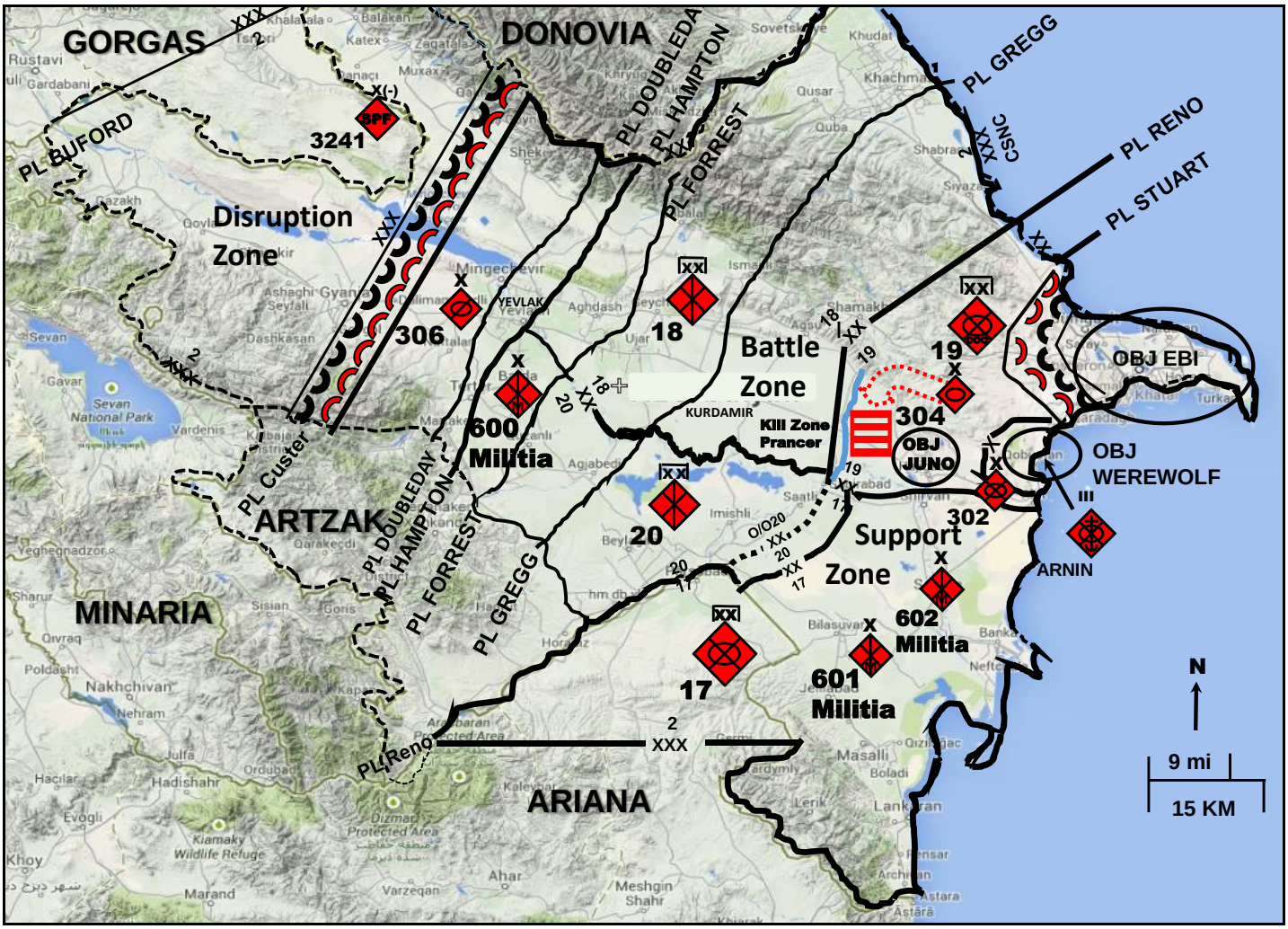


Figure 4. Initial disposition of operational strategic command 2

To the south of the 18th was the 600th Militia Brigade and the 20th DTG, both assuming defensive positions in the battle zone in order to prevent coalition forces from crossing the Aras River. To the east of the 20th was the 17th DTG and the 601st Militia Brigade, which were given the mission of securing the Arianian-Atropian border in the south, as well as the OSC support zone. The support zone also included logistics, long range fires, and the 302nd Mechanized Infantry Brigade which served as the OSC 2 reserve. The 304th Brigade Tactical Group (BTG) was designated as an assault force and was to be moved from the support zone to Attack Zone Sheba. The intent of the 304th was to be located in the central portion of the battle zone in order to destroy coalition forces in Kill Zone Prancer, located in the 19th DTG AOR.

In addition to the WCOPFOR regular forces described in previous paragraphs, there was an extensive effort to use special purpose forces (SPF) and irregular forces throughout the III Corps area of operations. The purpose was to challenge the training units' ability to execute wide area security (WAS). Soft targets such as airfields, major supply routes, and logistical support areas were attacked throughout the exercise. Both SPF and insurgent groups were also very effective in conducting reconnaissance, calling for indirect fires, and executing ambushes. These attacks were planned and executed throughout Gorgas and Atropia during the exercise.

OPFOR Defensive Operations

At the beginning of the exercise, the scripted 1st ID attack in the north advanced at such a fast pace that they created a significant gap on their boundary with the 38th ID in the south. The gap increased to approximately 100 kilometers which the WCOPFOR was not allowed to exploit. Also contributing to the gap was the significantly slow advance of the

competitive 38th ID, which was a deliberate ploy to focus the WCOPFOR on the 1st ID as the main effort. Creating unintentional confusion for the WCOPFOR were the non-competitive/competitive status and boundary changes of the 1st ID by MCTP. Initial WCOPFOR defensive plans were of little use as a result of these frequent changes. However, by the second day of the exercise the WCOPFOR commander correctly assessed the attempt by 1st ID to distract OSC 2 and portray itself as the main effort. The OSC 2 focus was quickly changed toward the 38th ID. The boundary gap was eventually closed as a result of coordination between the WCOPFOR commander and other key MCTP personnel as the exercise progressed.

Also early in the exercise, a critical decision was made by the exercise director to ensure that Ariana's strategic reserves from the 92nd DTG begin moving toward assembly areas along the southern Atropian border. This decision enabled OSC 2 to commit the 92nd in a timely manner if necessary. Another important decision was made by the director to ensure high to medium altitude air defense (HIMAD) coverage from SA-20s and SA-17s, in order to protect OSC 2 from USAF fixed-wing attacks.

At the end of the second day, the 306th Reconnaissance Brigade in the northern part of the disruption zone collapsed from significant losses, resulting from the 1st ID attack. Long range fires and fixed wing aircraft also contributed to the losses which resulted in all but remnants of the 306th in the north. In stark contrast, units from the 306th and the 600th in the southern portion of the disruption zone had almost no contact with the 38th ID. Most of the subsequent losses of the 306th and 600th opposing the 38th were also due to long-range fires from the high mobility artillery rocket system (HIMARS) and fixed/rotary-wing aircraft.

Throughout the exercise, WCOPFOR surface-to-surface missiles (SSMs) and fixed-wing aircraft reciprocal attacks were consistently destroyed by coalition air and air defense systems. The SS-21 and 26 SSMs required prior notice and approval from the exercise director during daily White Cell meetings. This process, in effect, restricted their use to fixed targets only.

For this exercise, all WCOPFOR and USAF fixed-wing aircraft were flown by an USAF air operations center using air warfare simulation (AWSIM), which is not compatible with the Army warfighter's simulation (WARSIM). As a result, all WCOPFOR 120 fixed-wing associated sorties during the exercise were destroyed in AWSIM, with the exception of support aircraft. This is compared to over 700 USAF sorties with minimal losses. USAF sorties included advanced aircraft, such as the F-35 Joint Strike Fighter, which has experienced design flaws and is primarily limited to testing bases. Admittedly, USAF sorties included support aircraft and had the mission of establishing air superiority as the CFACC. Nevertheless, WCOPFOR restrictions against any defensive counter-air sorties and the complete loss of competitive aircraft were unrealistic. These losses did not stress USAF participants and were debatably a waste of WCOPFOR planning time. However, allowing the exercise to start before USAF air superiority is achieved, including developing and documenting rules and procedures to compensate for the lack of simulated capabilities, could significantly improve the ability of the WCOPFOR and USAF to conduct reciprocal and meaningful shaping fires.

As the 1st ID continued to attack in the north, the 18th and 19th DTGs began to take casualties in the battle zone. The 18th, initially defending west of the Agshu River, was eventually forced to withdraw east of the river and reassume defensive posture. To the east of the 18th, the 19th was ordered to focus on defending against the Atropian forces in Baku. The Atropian Naval Regiment continued to defend in order to retain the BTC pipeline. In the south, the 38th ID began to advance with the 278th BCT in their northern sector. The 2nd CMBG also advanced in the south followed by light infantry brigades and a reconstituted Atropian armor brigade. As a result, the 20th DTG also began to take losses from coalition joint fires including HIMARS and Patriot missiles. The effects of the fires and attacks from fixed/rotary-wing aircraft forced the 20th to withdraw east under pressure across the Aras River. In the support zone, the 17th received minimal losses and continued to defend.

During this part of the exercise a decision was made by the exercise director to allow the reinforced 304th BTG to conduct a spoiling attack in the 38th ID sector against the 278th BCT, which was stalled on the western bank of Aras River. The 304th responded by successfully crossing the Aras River and attacking the 278th. The 278th suffered heavy losses with remnants withdrawing west in order to reconstitute. Following this success, the 304th also suffered significant losses from rotary wing aircraft and was subsequently unable to continue offensive operations.

As the exercise progressed the 18th, 19th, and 20th continued to suffer attrition from coalition forces. Atropia initiated an attack with two brigades from Baku. One brigade attempted to link up with 1st ID units in the north, while the other brigade attacked south in order to retake the Sangachal Oil and Gas Terminal. The link up initially failed but eventually

succeeded toward the end of the exercise. The attack south did succeed initially but was retaken by the Ariana Naval Infantry (ARNIN) Regiment.

Toward the end of the exercise, a two-phase OSC 2 counterattack against coalition forces was approved. The first phase was a successful counterattack by the 18th DTG to re-secure the Agshu River in order to force the withdrawal of 1st ID forces west of the river. The 19th DTG moved farther north to fix Atropian units in Baku in order to prevent a link up with 1st ID, reinforced the 18th DTG, and enabled the ARNIN Regiment to retake the terminal.

Phase II consisted of three successful counterattacks. The first was the infiltration of commandos, SPF, and Harpy UCAV attacks against the 38th ID and III Corps forces in the west. The infiltration was designed as a trigger for WCOPFOR remnants and the Southern Atropian People's Army (SAPA) to initiate attacks against III Corps logistical and command and control sites. At approximately the same time, 17th DTG launched a successful limited-objective attack to fix and contain first echelon units from the 28th ID which had crossed the Arus River. The final counterattack was from the 92nd DTG which successfully crossed the Arus River in the south and attacked into the southern flank of the 38th ID. The 92nd disrupted the operations tempo, significantly damaged several key targets, and shifted the focus of the 38th to the south. Overall, the counterattacks were very successful but resulted in high attrition. The 18th and 20th DTGs were effectively destroyed as well as SA-17 and SA-20 systems forcing OSC 2 to transition back to the defense and consolidate their positions. However, for the first time in several warfighters, the WCOPFOR still retained significant terrain in Atropia and was capable of defending it at the conclusion of the exercise.

In summary, the WCOPFOR successfully challenged the training units throughout the exercise. Most, if not all, of the evaluated training units achieved their training objectives. Many of the significant challenges that occurred during this exercise were related to MCTP's growing mission to include more sister services and coalition forces, to include diverse Army active, guard, and reserve units. As the size and complexity of these warfighters increase, the WCOPFOR must also increase in size in its new role as an OSC. It is important that close coordination between the WCOPFOR, MCTP leadership, and exercise directors continue as these very complex exercises continue to evolve.

Threat Tactics Courses (TTC) 2015

March TTC a Success

by Angela Wilkins, TRADOC G2 ACE-Threats Integration (BMA Ctr)

TRADOC G2 ACE-Threats Integration successfully hosted 60 students for the March Threat Tactics Course at TRISA on Fort Leavenworth. Active duty and reserve military, Department of the Army civilians, and contractors from as far as Ft. Shafter, Hawaii and Canada arrived on Monday, 9 March to begin the week-long course. Eight instructors taught the students the basics of threat tactics and functions through lecture, discussion, practical exercises, and a battle analysis activity.

Instructors educated the students on several concepts, to include the following:

- **Operational environment (OE) variables**
- **Threat concepts**
- **Functional tactics**
- **Hybrid threat**
- **Offensive and defensive tactics**
- **Threat designs**
- **Threat actors**

Students were shown where and how to access TRADOC G2 ACE-Threats Integration products on the Army Training Network (ATN) to use for further study. These products aid the exercise design process, development of training exercises at multiple venues, or to help individuals tasked to teach threat tactics to their colleagues. Training Circulars (TCs); the Decisive Action Training Environment (DATE); weapons and equipment data (Worldwide Equipment Guide); terrorism advisories; and articles, reports, and tactics handbooks describing all aspects of the threat are available on this site. These materials all inform the content of the Threat Tactics Course. The files from the course itself are available on ATN, too. Access ACE-Threats Integration products in two places:

TRADOC G2 ACE-Threats Integration Operational Environment Page or

TRADOC G2 ACE-Threats Integration Doctrine and Threat Force Structure Page

To help with the continual effort to improve the course, ACE-Threats Integration solicits feedback from students to determine level of learning and suggestions for improvement. For the March course, student feedback indicated a high level of understanding of the concepts by almost all students. For instance, 98% of students indicated a strong understanding of threat designs, and 100% claimed a strong understanding of functional tactics, threat offensive actions, and threat defensive actions. Also, some student found the battle analysis activity to be confusing. ACE-Threats Integration will look at ways to improve these areas. Overwhelmingly, though, the feedback was positive. One US Army captain commented: “Certainly worth the time away from work to ensure that we’re planning and executing in accordance with

OPFOR doctrine published by TRISA." A master sergeant stated, "Excellent course! This course has taught me a lot of how to approach an exercise." Feedback and questions about the course are welcome at any time.

The course contents did undergo significant updates from last March, to include a name change from Hybrid Threat Train-the-Trainer to Threat Tactics Course (TTC). The analysts spent time in particular evaluating the practical exercises. This time several tactical handouts were provided as homework to better prepare students for the practical exercise and the

newly added battle analysis on al Qasayr (see figure 1) and the Forest Camp. These changes sought to better demonstrate to students how the concepts are derived from study of real-world threats, and how to apply the concepts to training in the CTCs, at home station, and other venues.

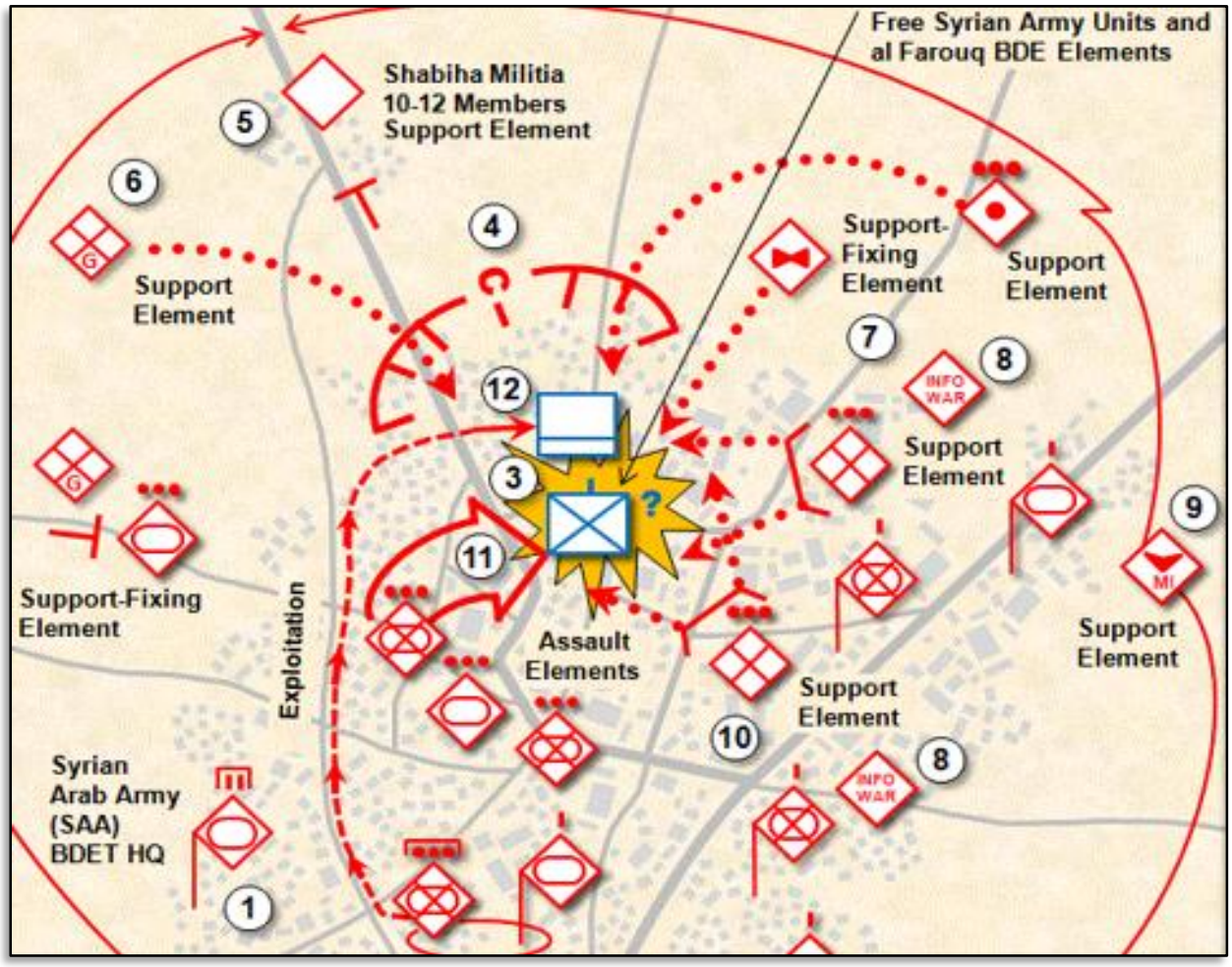


Figure 1. Tactical extract in al Qasayr small group discussions

The next Threat Tactics Course will be offered **24-28 August 2015** and is open to 48 students. If you would like to receive more information about or to register for the August course, please contact the course administrator, Angela Wilkins, at 913-684-7929, or angela.m.wilkins7.ctr@mail.mil.

by Jon S. Cleaves (DAC), Keith M. Hamlin (DAC), and Jon H. Moilanen (BMA Ctr)

The intelligence staff officer of the brigade combat team (BCT) must be an effective knowledge integrator of operational environment (OE) variables that far exceeds traditional priorities of effort to knowing an adversary or enemy for tactical operations. The Army conducts "operations in all environments and types of terrain."[1] Today's intelligence staff officer must know not only how an adversary will fight, but also understand the broader conditions within an OE that can be influenced to bring about Army mission success in accordance with the commander's intent.

The expectation of what the intelligence staff officer integrates across the missions of decisive action can be daunting in perspective. Notwithstanding, winning in a complex environment "requires a thorough understanding of the problem and the many facets, including cultural, economic, military and political; an understanding of all the players and the relationship between them, and an understanding of the variables that drive change."[2]

Intelligence is both a process and a function that enables the Army to conduct unified land operations. This function is inherently joint, interagency, intergovernmental, and multinational and leverages the intelligence enterprise.[3] The intelligence officer supports the commander's ability to execute mission command by collecting, creating, and maintaining relevant information and knowledge products of OE situational understanding and visualization.[4]

Technology and Intelligence Readiness

Technologies offer opportunities to improve the collection and collaboration of information to produce timely, accurate, and relevant intelligence to support a mission in a particular OE; however, Army capstone doctrine states that "the evidence overwhelmingly indicates that warfare remains a fundamentally human endeavor."[5] The Chief of Staff of the Army states that, "Our competitive advantage in today's complex strategic environment is not our high-tech weapon systems or adaptive military doctrine. It is our leadership development."[6]

Figure 1. Exploiting real-time intelligence

The intelligence staff officer must recognize the critical role of focusing on key aspects in an OE by study, analysis, and interpretation of many "conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander."[7] In typical dynamic situations before, during, and after a mission, the ability to act can be hampered by too much information, not enough information, and/or an enemy-centric focus in a continuum of intelligence preparation of the battlefield (IPB).

Experiences in Afghanistan (2009) present clear evidence that brigade and regional command analytic products were often inadequate in comprehensive analysis of an OE, and that a lethal targeting focus in tactical missions often acquired a

myopic view of operational or strategic impacts.[8] However, once a holistic approach capitalized on variables such as social and economic in near real time, coalition operations achieved successes not previously experienced. The Army continues to learn these lessons in theater and during recent collective training exercises. Actionable intelligence in a fast-paced OE must get to the action operator before tactical opportunities become irrelevant.[9] In another collective training example, lack of appreciating social variables can position a tactical task or mission for failure.[10] For example, displaying behavior that is culturally offensive can be a critical mistake when interacting with the local populace or conducting a key leader engagement.

To provide timely and effective intelligence results to the soldier and leader, "corps and divisions are now focused on integrating the intelligence architecture to support missions and exercise the critical linkages that connect them to national, joint, and multinational partners."[11] This aligns with a mission command system that acknowledges the diverse OE conditions of uncertainty, volatility, ambiguity, complexity, increasing technological change, greater connectivity and linked aspects of human and technological networks, convergence of land and cyberspace operations, and interaction with determined, adaptive adversaries, as well as numerous characteristics of the operational variables: political, military, economic, social, information, infrastructure, physical environment, and time (PMESII-PT).[12]

These OE variables and sub-variables support the decision-making process by providing the foundational detailed information and intelligence for mission analysis in the military decision-making process (MDMP). The Army uses mission, enemy, terrain and weather, troops and support available, time available and civil considerations (METT-TC) to focus mission planning and execution. A complementary operational environment framework of analysis (PMESII-PT) is the construct to achieve a holistic and detailed understanding of an OE in support of mission conduct. Each OE is dynamic. This characteristic is primarily the result of the ever-changing nature of operational variables, their interactions, and the cascading implications of such interactions.[13]

Intelligence Warfighting Function and Intelligence Enterprise

Intelligence warfighting function: The related tasks and systems that facilitate understanding the enemy, terrain, and civil considerations….The intelligence warfighting function is the Army's contribution to the intelligence enterprise that comprises all U.S. intelligence professionals, sensors, systems, federated organizations, information, and processes supported by a network-enabled architecture. The most important element of the intelligence enterprise is the people that make it work.

ADRP 2-0**,** *Intelligence* (2012) and ADRP 3-0, *Unified Lands Operations* (2012)

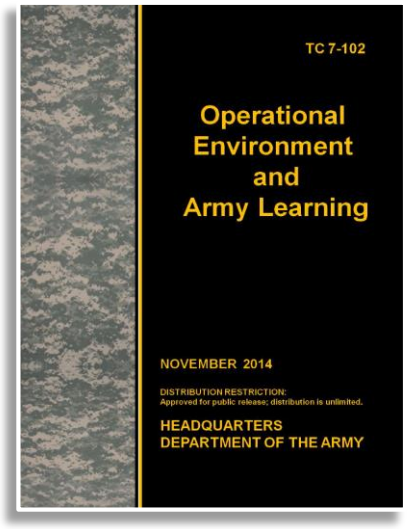
Army Intelligence Doctrinal Framework

Within the intelligence warfighting function, one of its essential tasks is "support to situational understanding—the task of providing information and intelligence to commanders to assist them in achieving a clear understanding of the force's current state with relation to the threat and other relevant aspects of the operational environment."[14] Intelligence reach is central to this function as an activity to proactively and rapidly access information from, receive support from, and conduct direct intelligence enterprise collaboration and information of sharing with other units and agencies, both within and outside the area of operations, unconstrained by geographic proximity, echelon, or command.[15]

Intelligence synchronization is the art of integrating information collection and intelligence analysis with operations to effectively and efficiently support leader decision-making. Knowledge management ensures that required information gets to the user in a useable format and is not redundant.[16] Primary questions the Army analyzes include: "What is the environment we think Army forces will operate in, and what is the problem we are trying to solve?"[17] The answer is perplexing. "The environment the Army will operate in is unknown. The enemy is unknown, the location is unknown, and the coalitions involved are unknown."[18] The remaining problem is how the Army is to succeed as a learning organization in contemporary operational environments while the Army plans for future operational environments.

Operational Environment and the Army Learning Model

The Army emphasizes an Army Learning Model (ALM) that merges training, education, and self-development for a common intellectual framework of leader development and readiness. The ALM must provide the comprehensive learning experiences necessary to enable adaptive critical thinking, adept use of technology advances, and to inculcate decisive leader decision-making in a "dynamic and uncertain security environment with challenges across every continent."[19] A recently published Army training circular, *Operational Environment and Army Learning*, presents concise and enduring doctrine-based guidance on how to integrate the variables of an OE in support of Army learning.[20] A companion HQDA document is *Exercise Design*. This Army training circular is a planning and design guide to produce robust, relevant, and realistic OE conditions that challenge achieving unit objectives.[21] The HQDA TC 7-100 series enhances how to shape OE variables and threats for the Army's institutional and operational domains.



The intelligence staff officer can charter professional self-development, institutional training and education, and operational experiences to understand and apply available OE resources of the intelligence enterprise. Intelligence staff officer expertise is a lifelong leader development requirement to understand the collective variables of an OE, and effectively synchronize and integrate an ever-increasing amount of technical resource networks, intelligence collection and analysis, and timely distribution to users at lower and higher tactical echelons in support of mission success.

Intelligence Enterprise Integration

The Army Training and Doctrine Command (TRADOC) G2 Operational Environment Enterprise (OEE) is a key asset of the intelligence enterprise. As an integrated training environment (ITE), technology-enabled presentations and other information-intelligence resources leverage understanding of individual and collective learning experiences and exercises, home station training, and operational missions. The G2 OEE is TRADOC's principal means to deliver OE products, services, and support to TRADOC's supported stakeholders. The G2 OEE resides in the institutional training domain, that is, the Army's institutional training and education systems, and partners in readiness with the Army's operational domain.[22]

Disseminating intelligence simultaneously to multiple recipients is one of the most effective, efficient, and timely methods, and can be accomplished through various means.[23] An example of a critical enabler to intelligence integration is the Army's Distributed Common Ground Sensor System-Army (DCGS-A)—a global intelligence network consisting of deployed and fixed sites that provides virtual connectivity among home station unit and activity locations and intelligence nodes throughout the Army. The DCGS-A is the Army's intelligence component of Mission Command. DCGS-A fuses "big data" and leverages strategic, operational, and tactical intelligence resources to support a BCT S2 in maintaining an accurate and timely understanding of all aspects of an OE. DCGS-A is an essential enabler to support of Mission Command and the Intelligence Warfighting Function (IWfF). It includes Multi-Function Workstations (P-MFWS), the Tactical Ground Station (TGS), GEOINT Workstations (GWS), Prophet, and CHARCS operating across multiple networks (NIPR, SIPR, JWICS).

The regionally aligned US Army Intelligence and Security Command's (INSCOM) Theater Intelligence Brigades (TIB) function as an "anchor point" or gateway connecting MI with tailored, multi-disciplined intelligence and intelligence capabilities at the tactical, operational, and strategic levels. The TIB is the hub that facilitates collaboration among not only the 17 Intelligence Community (IC) members but potentially thousands of data sources spanning the globe from local and regional social media to national level intelligence capabilities.

Commanders and their staffs must understand Cyberspace (Cyber) capabilities and restrictions as future Offensive Cyberspace Operations (OCO) and Defensive Cyberspace Operations (DCO) will be increasingly planned and coordinated, and possibly even conducted by cyber forces found within tactical formations, as organic capabilities and/or augmentation as external enablers. In existing tactical formations today, the Cyber-Electromagnetic Activities (CEMA) Cell serves as the link between the commander and the effects he or she requires on the battlefield. While the S2 is not inherently a part of the CEMA Cell, the S2 must integrate intelligence diligently with cyberspace effects. As the Army evolves Cyber

DOTMLPF (doctrine, operations, training, materiel, leadership and education, personnel, and facilities) strategies to meet Army requirements, networks are vulnerable to breaches. At brigade level, the S2 intelligence officer must wargame, analyze, and mitigate possible threat attacks to the intelligence knowledge network (IKN).

This distributed and integrated network increases the Army's ability for proactive planning, and when directed, rapid response. The network also represents a significant challenge when tasked to replicate these environments in support of leader development, training, and education. As the Intelligence Community Integrated Technology Enterprise (IC ITE) develops and is adopted throughout the DOD and Intelligence Community, new tradecraft and tools will be introduced to S2s affording them the ability to effectively navigate through big data. The OEE must be prepared to not only describe the complexity of an OE, but deliver it with the same level of complexity S2s have grown accustomed to in order to challenge them during training.

Implications for S2 Intelligence Readiness

- ***Doctrinal Acuity***

The intelligence staff officer knows that "As the Army transitions from a force shaped by counter-insurgency and stability missions, it will remain engaged in the current conflicts."[24] These contemporary and future engagements will likely be persistent and complex, and may appear with little advance warning prior to an Army mission. Army readiness requires effective use of available technologies to engage adaptive leadership and synchronized actions among actors, and as a norm, "include those that come together virtually in cyberspace unbounded by physical geography."[25]

- ***Intelligence Readiness***

Gaining OE situational understanding is an essential aspect of excelling to Army standards. Intelligence leaders prioritize learning to best support a unit mission essential task list (METL) or designated mission tasks from a higher headquarters and aim to achieve standards as published by the Army. Conditions are a statement of the learning environment in which tasks are experienced in a training framework of task/action-condition-standard.

The intelligence staff officer must demonstrate technical skills competency and the ability to integrate intelligence architecture experiences to achieve and sustain expertise. Team proficiency in operating DCGS-A and other modernization capabilities is one of several baseline tenets to optimize resources of the intelligence enterprise. A key enabler to the Army's expeditionary readiness is the HQDA G2 Foundry program that provides critical intelligence training and professional education that ranges established and multi-disciplined skill sets, regionally-focused open-source intelligence awareness, and theater enterprise integration.

Another key enabler to intelligence readiness is the G2 OEE. This enterprise builds, validates, creates, maintains and delivers OE context and complexity for leader development, training and professional education, experience, and concept and capabilities development. The G2 OEE consists of subject matter experts and stakeholders in the operational and institutional domains, internal and external capability providers, and OEE management leaders that shape and govern enterprise activity.

OEE stakeholders focus enterprise activity by defining their needs within the context of institutional or operational missions, and/or other organizational requirements. The TRADOC G2 OEE studies and estimates probable and possible OE futures; describes and validates the conditions and variables of operational environments; delivers OE context and complexity to live, virtual, constructive, and gaming (LVCG) venues; and assesses, evaluates, and accredits the Army's training and education programs.

The OEE architecture-supported enablers are expanding in resource capabilities and accessibility on line for the ALM for the soldier, leader, and Department of the Army civilian. The enterprise capability providers develop and deliver products, services, and other support to meet OEE validated requirements.[26] Examples of OEE significant contributions toward Army readiness include but are not limited to the following:

- Serves as the Army lead for identifying, analyzing, documenting, and integrating OE and threats in support of all Army leader development, training, and experience (LD).

- Leads the development and validation of all capabilities development (CD) scenarios, and certifies all OEs, threats, and associated threat capabilities used throughout TRADOC in Army CD developmental studies, analyses, and experimentation.
- Conducts operational environment laboratory (OEL) prototype development within the modeling and simulation (M&S) community that incorporates OE-related behaviors associated with operational variables and the human, social, cultural, and behavioral (HSCB) aspects of an OE.
- Conducts research on military and security topics derived from unclassified foreign media.
- Educates leaders with tools to improve critical thinking with multiple and alternative perspectives, cultural perspectives, and worldviews.
- Provides OE and threat representation in Army and Joint experiments, wargame events, concept development venues, and test and evaluation events.
- Conducts social science-based human domain research, analysis, and training capability which fosters Army culture interoperability.
- Replicates the complexities of OEs by leveraging real-world data, information, and knowledge for focused application in training, education, and leader development venues.
- Incorporates lessons learned (LL) as a deliberate and systematic process of collecting and analyzing field data and disseminating, integrating, and archiving lessons and best practices collected from unified land operations and training events.
- Participates as a governance member of TRADOC Quality Assurance Office (QAO) accreditations for Army Centers of Excellence (CoE) and schools, training at the Combat Training Centers (CTCs), US Army Reserve training divisions, and Army National Guard collective training program(s) and other training organizations or programs using an OE for training purposes.

The S2-Intelligence Leader

As a leader, the intelligence staff officer must hone critical thinking and decision-making in intelligence analysis and resultant recommendations. Critical thinking must be disciplined and self-reflective and when conducted effectively, provide holistic, logical, and unbiased analysis for conclusions, refined intelligence, and advice. The nature of changing threats and OEs requires astute understanding of operational environment variables.

Through the IKN and observations, insights, and lessons learned (OIL), the brigade S2 actively feeds and retrieves experiences from the field, provides recommendations for areas where feedback is necessary, evaluates feedback provided, and incorporates working concepts and best practices into current and future intelligence and operations training. The brigade S2 participates in the intelligence architecture network as a forum for intelligence professionals to give and receive information, best practices, and procedures.[27]

Building trust between the commander and BCT S2 enables a common understanding critical to the intelligence warfighting function (IWfF) ability to support the commander's requirements and decision making. Army and joint doctrine is this common language. For the brigade combat team (BCT) intelligence office, Army Field Manual (FM) 2-19.4, *Brigade Combat Team Intelligence Operations*, is the foundational reference document of how the brigade intelligence officer and staff organize, train, and support current and future operations.[28]

As the Army and Joint forces pursue advanced cyber technologies, strategies, and procedures, the brigade S2 must be proficient in fielded cyber capabilities, and understand expanding capabilities among hardware and software systems that encompass emerging Army, Joint, and national information architecture infrastructure.[29]

Commanders, the intelligence officer, and other staff members collaborate: they actively share and question information, challenge assumptions, verify facts as relevant, and compare and contrast perceptions and ideas in order to best appreciate situations and dynamic OE conditions. The intelligence staff officer, using the intelligence enterprise and Army mission command philosophy, integrates timely, accurate, and relevant intelligence to enable a commander to balance the art of command and the science of control in order to conduct operations and achieve missions.[30]

Notes

[1] Headquarters, Department of the Army, Army Doctrine Publication 1. (17 September 2012). The Army. para. 1-20.
[2] Perkins, D. G. (October 2014). Army Operating Concept: Delivering the Future. Army. *64*(10), 66.
[3] Headquarters, Department of the Army, Army Doctrine Reference Publication 2-0. (31 August 2012). *Intelligence.* v, para 1.
[4] Headquarters, Department of the Army. (12 June 2013). U.S. Army Mission Command Strategy FY 13-19. 6.
[5] Headquarters, Department of the Army, Army Doctrine Publication 1. (17 September 2012). The Army. Foreword, para 4.
[6] Odierno, R. T. (October 2014). The U.S. Army: Trusted Professionals for the Nation. Army. *64*(10), 23-24.
[7] Operational Environment. (8 November 2010, as amended through 15 November 2014). In U.S. Department of Defense. Joint Publication 1-02, DOD Dictionary of Military and Associated Terms**.**
[8] Flynn, M.T., Pottinger, M., and Bachelor, P. D. (January 2010). Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan. Center for New American Security, 8.
[9] Broadwater, J. (2014). Synchronizing BCT Enablers to Shape the Subordinate Units' Fights. In C.W. Fisher (Ed.). Training for Decisive Action: Stories of Mission Command. (pp. 7-10). Ft Leavenworth, KS: Combat Studies Institute.
[10] Adams, S. (2014). Integrating Enablers into the Battalion Scheme of Maneuver. In C.W. Fisher (Ed.). Training for Decisive Action: Stories of Mission Command. (pp. 33-35). Ft Leavenworth, KS: Combat Studies Institute.
[11] Legere, M. A. (October 2014). Intelligence Supports Globally Engaged, Regionally Aligned Army. Army. *64*(10), 142.
[12] Headquarters, Department of the Army, U.S. Army Mission Command Strategy FY 13-19. June 2013, p 6.
[13] Moilanen, J. H. (April 2014). Operational Environment and Army Learning. TRADOC G2 OEE Red Diamond. 5.
[14] Headquarters, Department of the Army, Army Doctrine Reference Publication 2-0. (31 August 2012). *Intelligence.* v.
[15] Headquarters, Department of the Army, Army Doctrine Reference Publication 2-0. (31 August 2012). *Intelligence.* para. 2-37.
[16] Headquarters, Department of the Army, Army Doctrine Reference Publication 2-0. (31 August 2012). *Intelligence.* para. 2-38.
[17] US Army Training and Doctrine Command, TRADOC Pamphlet 525-3-1. (31 October 2014). The U.S. Army Operating Concept: Win in a Complex World, Preface, para. 1.
[18] US Army Training and Doctrine Command, TRADOC Pamphlet 525-3-1. (31 October 2014). The U.S. Army Operating Concept: Win in a Complex World, Preface, para. 2.
[19] Odierno, R. T. (October 2014). The U.S. Army: Trusted Professionals for the Nation. Army. *64*(10), 23.
[20] Headquarters, Department of the Army, Training Circular 7-102. (26 November 2014). Operational Environment and Army Learning.
[21] Headquarters, Department of the Army, Training Circular 7-101. (26 November 2010). Exercise Design. vii.
[22] Moilanen, J. H. (April 2014). Operational Environment and Army Learning. TRADOC G2 OEE Red Diamond. 6.
[23] Headquarters, Department of the Army, Army Doctrine Reference Publication 2-0. (31 August 2012). *Intelligence.* 3-39.
[24] Headquarters, Department of the Army, Army Doctrine Publication 1. (17 September 2012). The Army. para. 4-2.
[25] Headquarters, Department of the Army, Army Doctrine Publication 1. (17 September 2012). The Army. Foreword.
[26] Headquarters, Department of the Army, Training Circular 7-102. (26 November 2014). Operational Environment and Army Learning. 3-1.
[27] U.S. Army Intelligence Center of Excellence and Fort Huachuca. (n.d.). *Strategic Plan 2014-2019.* http://huachuca-www.army.mil/Files/Strat_Plan_Coffee_Table_27Mar.pdf
[28] Headquarters, Department of the Army. (25 November 2008). *FM 2-19.4 Brigade Combat Team Intelligence Operations*, para 2-5.
[29] U.S. Army Intelligence Center of Excellence and Fort Huachuca. (n.d.). *Strategic Plan 2014-2019.* http://huachuca-www.army.mil/Files/Strat_Plan_Coffee_Table_27Mar.pdf
[30] Headquarters, Department of the Army. (13 June 2013). U.S. Army Mission Command Strategy FY 13-19. 1.

WHERE IS THE READY RESOURCE OF THREATS/OPPOSING FORCE/OE PRODUCTS?

by TRADOC G2 ACE-Threats Integration, Operations

The TRADOC G2 ACE-Threats Integration Directorate is the US Army's lead to study, design, document, validate, and apply hybrid threat and operational environment (OE) conditions that support all US Army and joint training and leader development programs.

Products describe threat actors, threat tactics and techniques, and operational environment (OE) variables of political, military, economic, social, information, infrastructure, physical considerations, and time (PMESII-PT) for training and preparation for contingency missions and/or deployments. The Army Training Network (ATN) is your easy two-click access to these products.

THE ROCKET PROPELLED GRENADE (RPG)-28 KLYUKVA (CRANBERRY)

by Mike Spight, TRADOC G2 ACE-Threats Integration (CGI Ctr)

This is the last in a series about the latest developments in Soviet/Russian modern RPGs, with previous articles addressing the RPG-30 and RPG-32. This weapon is currently the largest RPG (125mm tandem warhead rocket) fired from a disposable, non-extending launcher that is known to have been developed. Operated by a single soldier, the RPG-28 is capable of inflicting a mobility kill or a catastrophic kill on any main battle tank (MBT) known to be in current service with any nation.

The 125mm rocket is capable of penetrating up to 1,000mm of rolled homogeneous armor (RHA), and that is after blasting through any explosive reactive armor (ERA) that is present on the outer hull of an MBT or infantry fighting vehicle (IFV). Additionally, it is extremely effective for engaging troops who are inside bunkers or buildings in built-up areas as it can penetrate 3,000mm of brick, over 1,500mm of re-enforced concrete, or 3,700mm of logs and dirt (bunker). Maximum effective range is 300 meters.

The RPG-28 in figure 1 is in its normal carry position and the 125mm rocket with fins deployed. Note that the RPG-28 launch tube does not have to be extended to fire. The soldier merely raises the organic iron sights to ready the weapon to fire. Note that the rubber end caps are not removed and blown off the launcher when it is fired. Like other unguided RPGs, the rocket propellant charge is totally expended in the launch tube. If, for whatever reason, a decision is made not to fire the weapon, the soldier can lower the iron sight back to the down position, which safes, or "uncocks," the launcher.

Figure 1. RPG-28 with optical sight and its 125mm rocket

The RPG-28, as noted, is a very large RPG. It is 1,200mm in length (firing and carry positions), and the loaded launcher weighs 13.5kg. The rocket alone weights 12kg, or approximately 24 pounds. Figure 2 depicts a fully assembled RPG-28 on the shoulder of a soldier, and the size of this weapon is quite clear. There is a shoulder pad present on the tube, and a short handled, folding mono-grip at the front of the tube that is used to stabilize the weapon once it is mounted on the shoulder. Back blast with this RPG is extreme, and the back blast area must be totally clear of personnel or any equipment that would certainly be damaged or destroyed if not clear when the RPG is fired. Obviously, this weapon cannot be fired from an enclosed space.

Figure 2. RPG-28 iron sight option

The RPG's sights are of a simple, iron "peep" configuration, although the optical PGO-7 sight is optional, and can be attached to the launcher if desired. The standard iron sight is graduated into ranges of 50, 100, 150, 200, and 300 meters. Figure 1, above, provides an excellent view of the attached PGO-7 optical sight, attached to the launch tube. In Figure 2, the iron sight is clearly in the raised or "firing" position.

The RPG-28 is a powerful and capable anti-armor/anti-structure weapons system. It is easy to use and to train Soldiers to use effectively, and it poses a significant threat to any MBT currently in the field. An effective hit with the RPG-28 is likely to result in a catastrophic kill or, at a minimum, a mobility kill on an MBT or IFV.

The TRADOC G2 *Worldwide Equipment Guide* update for 2015 is transitioning to an improved information sheet display. (See figure 3.) Data and an illustration are positioned in standardized locations for easy viewing and efficient electronic retrieval for other databases. A free text section for notes provides supplemental data and information

The WEG is published annually by TRASDOC G2 ACE-Threats Integration with the next formal update scheduled for December 2015. For more information, contact WEG POC John Cantin at john.m.cantin.ctr@mail.mil or 913-684-7952.

Russian RPG-28 Klyukva (Cranberry)

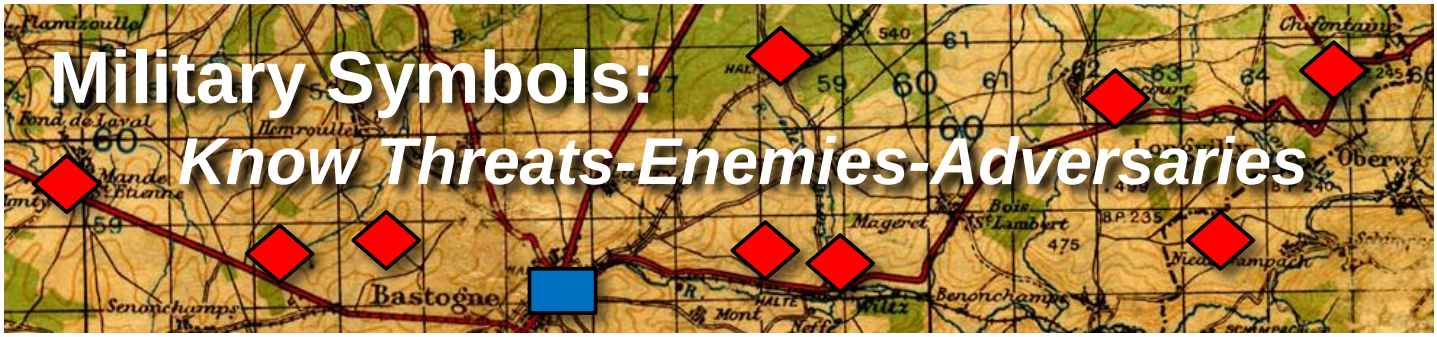
SYSTEM	SPECIFICATIONS	AMMUNITION	SPECIFICATIONS
Alternative designations:	None	High Explosive, Anti-Tank (HEAT) RPG	125mm, tandem warhead. Capable of penetrating ERA and up to 1000mm of RHA; up to 3000mm of brick/cinder block; 1500+mm of reinforced concrete; 3700mm of logs and dirt (bunker).
Date of introduction:	Adopted by Russian MOD in 2011		
Proliferation:	Russian Federation		
Weight (kg):	13.5 (loaded launcher) 12kg (rocket alone)		
Length (mm):	1200mm (carry and firing)		
Rate of fire (rd/min):	1 (single shot, disposable launch tube)		
Operation:	Manually cocked, then aimed and fired.		
Magazine:	N/A		
Magazine capacity:	N/A	VARIANTS	SPECIFICATIONS
Fire mode:	N/A	N/A	
SIGHTS	SPECIFICATIONS		
Name: PGO-7 or Iron			
Type: Optical or iron peep sight.	Iron sights are graduated 15, 100, 150, 200, and 300 meters		
Sighting range:	300m max effective range.		
Night sights available:	Unknown.		

NOTES

This weapon is currently the largest RPG (125mm tandem warhead rocket) fired from a disposable, non-extending launcher known to be in current service. Operated by a single Soldier, the RPG-28 is capable of inflicting a mobility kill or a catastrophic kill on any main battle tank (MBT) known to be in service with any nation.

1 | UNCLASSIFIED

Figure 3. WEG data sheet RPG-28



Part 2: Threats/OPFOR Symbology

by Jon H. Moilanen, ACE-Threats Integration (BMA Ctr) Part 2 of 2 Parts

This part 2 of a two-part article series provides additional discussion and illustrations of symbols for threats and/or opposing forces (OPFOR) to complement the rationale and symbols in the March 2015 *Red Diamond* article, "Military Symbols: Know Threats-Enemies-Adversaries."[1] To provide selected standardized threat/OPFOR symbols and graphics in support of US Army doctrine terms and military symbols, the TRADOC G2 Analytical and Control Element-Threats Integration Directorate (ACE-Threats Integration) identifies and updates Threats/OPFOR symbols and graphics in the HQDA Training Circular (TC) 7-100 series and associated TRADOC G2 training literature.

The TRADOC G2 ACE-Threats Integration directorate "serves as Army lead for designing, documenting, and integrating threat (or OPFOR) and OE [operational environment] conditions in support of all Army training, education, and leader development programs."[2] This directorate also reviews, analyzes, and provides recommendations for the integration of an OE and its critical variables into training, education, and leader development events.

Threat

Any combination of actors, entities, or forces that have the capability and intent to harm United States forces, United States national interests, or the homeland.

ADRP 3-0, *Unified Land Operations*

Enemy

A party identified as hostile against which the use of force is authorized.

ADRP 3-0, *Unified land Operations*

Adversary

A party acknowledged as potentially hostile to a friendly party and against which the use of force may be envisaged.

JP 3-0, *Joint Operations*

Examples in this month's article include how selected equipment and weapons systems are displayed as threat/OPFOR symbols and/or use amplifying terms when required for clarity. Other threat/OPFOR examples include activities and installations, and how threat/OPFOR units, cells, organizations, and an individual or individuals are identified with modified military symbols and icons as a complement to symbols in part 1 of this article.

Know the Threat—Know the Enemy

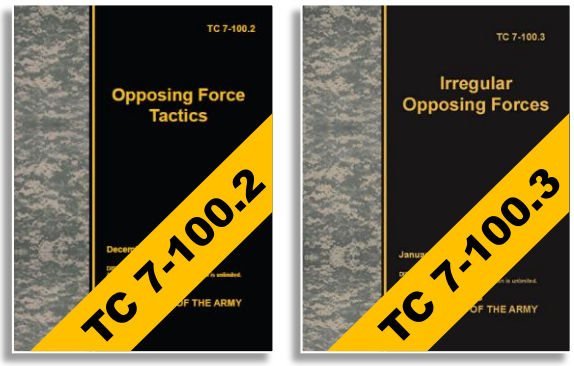
Representing threats and enemies effectively in visual presentations requires standardized symbology and graphics to provide for a common and cogent understanding of a threat, adversary, or enemy in OEs. The HQDA Training Circular 7-100 series and TRADOC G2 training literature provide common symbology and graphics measures from a threats/OPFOR perspective.[3] A fundamental recognition is that threat actors of current persistent conflicts in various regions of the world do not necessarily think, act, or appear as do US military forces in the conduct of military operations. Correspondingly, the threat/OPFOR in training, professional education, leader development, and other learning venues must represent these characteristics differently from US military forces.

Current US Army Doctrine for Symbols-Control Measures

The US Army updated Army Doctrine Reference Publication (ADRP) 1-02, *Military Terms and Symbols*, in February 2015. This publication constitutes approved Army doctrinal terms and symbols for use in Army training, education, and operations.[4] The TRADOC G2 ACE-Threats Integration directorate constructs treats/OPFOR symbols and graphics within the guidance and flexibility allowed by ADRP 1-02.[5]

Two threat/OPFOR symbols not included in ADRP 1-02 are the guerrilla unit and the insurgent organization. Most mission tasks for threat/OPFOR use symbols consistent with ADRP 1-02; however, several symbols appear different and/or have a different definition. Similarly, some threat/OPFOR control measures appear different for some types of movement and maneuver, fires, and defensive positions. An underlying reason for these differences is that the threat/OPFOR is a composite analysis of threats, enemies, and/or adversaries that may not operate within law of war, international conventions, and/or other regulations as do US military forces.

US Army Training Circular, TC 7-100.2, *Opposing Force Tactics*, describes the use of symbol, amplifiers, and modifiers for organizational echelon or task-organized status of threat/OPFOR units and organizations. For threat/OPFOR echelon designation, the echelon amplifier is centered above the symbol frame and does *not* touch the symbol frame. Symbol norms such as a threat/OPFOR guerrilla unit or insurgent organization are presented in US Army Training Circular, TC 7-100.3, *Irregular Opposing Forces*.



Threats/OPFOR Symbols for Training and Readiness

A military symbol is a graphic representation of a unit, equipment, installation, activity, control measure, or tactical task relevant to military operations that is used for planning or to represent a commonly understood operational picture on a map, display, or overlay.[6] Military symbols include unit, equipment, installation, and activity symbols, and control measure and tactical symbols. The icon, as the innermost part of a symbol, and the use of color are discussed in the part 1 article.[7]

Threat/OPFOR Units and Organizations

The threat/OPFOR identify two main groupings of military forces: regular forces and irregular forces. A unit or organization symbol is often not enough information to visualize organizational capability. In such cases, threat/OPFOR symbols use the free text area primarily to the right of a frame; however, free text is allowable to the left, right, or below in order to adequately communicate a unit, equipment, activity, or installation capability. Threat/OPFOR regular force unit and irregular force unit and organization symbols are introduced in part 1 of this article. For more information, see the folders on the Army Training Network (ATN) front page within the "Training for Operations" button, and its subordinate folder "ACE-Threats Integration Operational Environment Page." Click Threat Doctrine and Force Structure.

TC 7-100.3 describes three main categories of irregular forces: guerrilla units, insurgent organizations, and criminal organizations. This training circular also addresses a relevant population such as noncombatants who may be an active or passive supporter of regular and/or irregular forces. The threat or OPFOR does not describe itself as a terrorist force, group, or element. Acts of terrorism are addressed as a tactic applied with diverse techniques. See figure 1 for a sample of threat/OPFOR symbols.

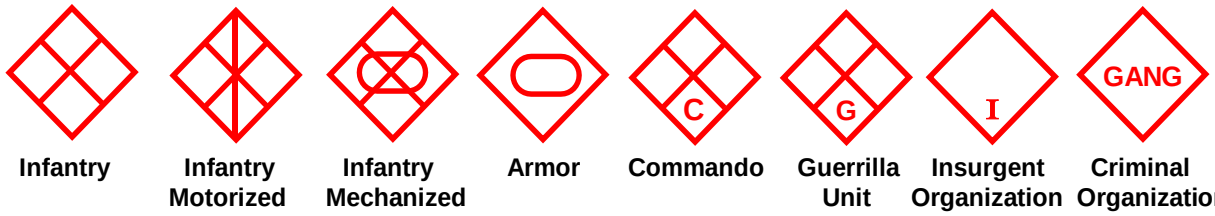


Figure 1. Threat/OPFOR regular and irregular unit, cell, and organization symbols (examples)

The guerrilla unit uses the basic infantry icon and adds the letter "G" in the lower sector of the symbol frame to identify this type of irregular paramilitary element or force. A hunter-killer (HK) unit task organization configures guerrillas into multiple small groups, sections, and teams to optimize dispersed tactical operations.

An insurgent organization places the capital letter "I" in the lower sector of the organization or cell symbol, and usually does not have other icons within the symbol frame. However, when clarity requires an icon and/or modifier, they are placed inside or next to the symbol frame. Neither an insurgent organization nor a criminal organization uses an echelon amplifier above the symbol.

Selected Equipment

Icons commonly used in threat/OPFOR tactical action sketches or other presentations for equipment may have the same or similar visual characteristics as US pieces or systems, but may differ in capability or how a weapon is categorized. The threat/OPFOR uses the term unmanned aerial vehicle (UAV) rather than the US Army term unmanned aerial system, even though the same type of system may be employed.[8] The UAV uses the DOD chevron-like equipment icon within a symbol frame.

The typical progression of capability in weapon systems is light, medium, and heavy. The following examples in figure 2 display a sample of selected threat/OPFOR weapon symbols for machineguns and mortars. The threat/OPFOR considers the 120-mm mortar as a medium mortar.

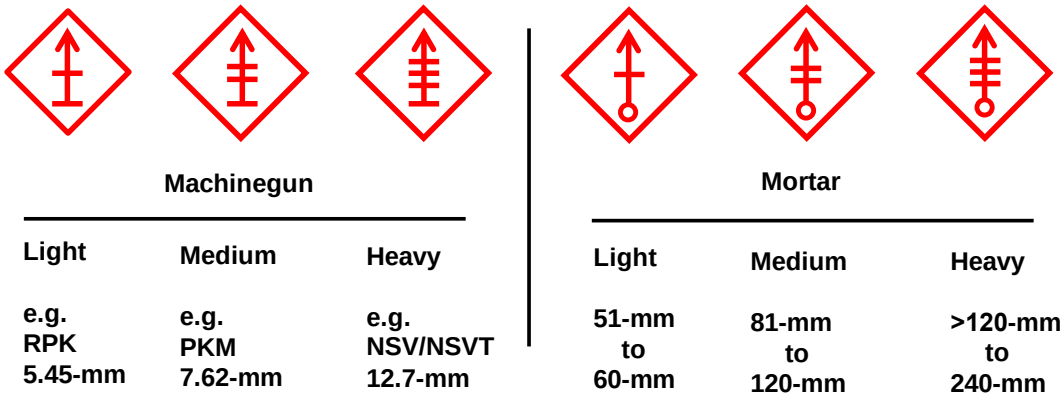


Figure 2. Sample of threat/OPFOR weapon categories and symbols

A category sequence exists for rifles. For a rifle, the capability is a single-shot rifle, semiautomatic rifle, or an automatic rifle. Examples include the bolt-action Mosin-Nagant 7.62-mm sniper rifle, SKS 7.62-mm semiautomatic rifle, and AK-47/AKM 7.62-mm rifle in a semiautomatic or automatic mode. Additional information is in TRADOC G2 *Worldwide Equipment Guide*.

Selected Activities and Installations

Activity symbols are associated with types of action conducted by an individual and/or individuals. The term *installation* applies to permanent, semi-permanent, and/or temporary structures. Examples in figure 3 include a mass demonstration inspired by the threat/OPFOR. This support may or may not be known to civilian or military forces supporting the established governance with which the threat/OPFOR may be in conflict. A similar situation can exist in a riot comprised of primarily of local citizens in a rural or urban environment. Other activity examples include a smuggling operation and/or illicit drug commerce. These activities may be solely criminal organizations, or may be affiliated or associated with paramilitary threat/OPFOR, or be sponsored by state actors to foment civil unrest.

Examples of locations include a safe house, a training facility within a tented camp, or a trafficking transfer facility that could be an intermodal transportation point as simple as a wheeled vehicle exchange point or a major transfer facility for commerce containers from rail to ships. A weapons cache can be several weapons in a house or a major holding area for multiple types of munitions. These examples are typical of activities, facilities, and/or installations encountered in offensive, defensive, and stability military operations.

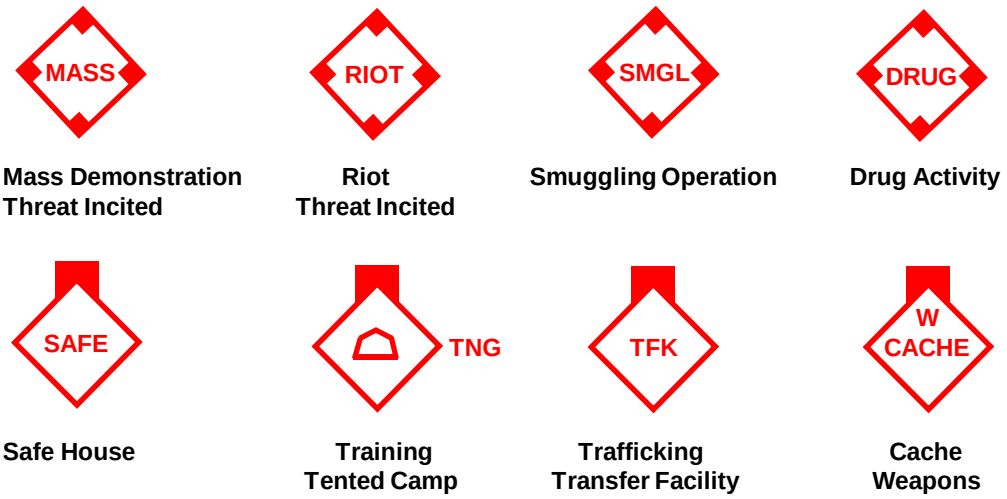


Figure 3. Sample of threat/OPFOR activity and facility-installation symbols

Selected Relevant Population and Activities

Individual icons commonly used in tactical action sketches or other presentations may have only a central icon within the symbol frame, or may include modifiers to clearly identify an activity or capability. Figure 4 displays a sample of modified symbols for a threat/OPFOR individual or individuals that designate the activity and/or action. These symbols are different from the types of killings or criminal activity victim symbols presented in ADRP 1-02.

From a threat/OPFOR perspective, the term *terrorist* is not used in self-description, and is not presented on threat/OPFOR symbols. In contrast, ADRP 1-02 presents terrorism symbols in the context of an adversary or enemy function affecting an OE and/or US Army forces.

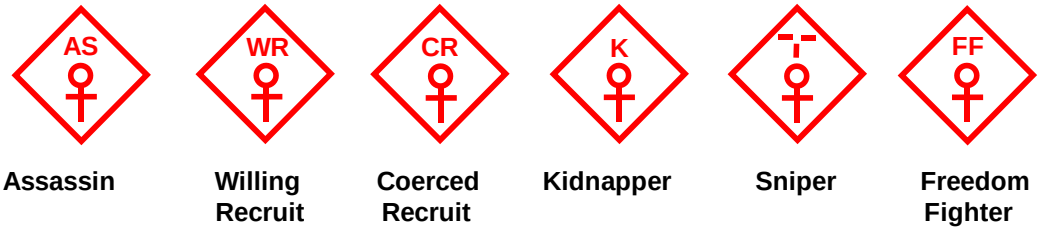


Figure 4. Sample of threat/OPFOR actors in a relevant population and activity symbols

Tactical conditions may include additional symbol frames and colors in a tactical diagram to indicate neutral, unknown, and/or civilian actors. Actions can include known, suspect, planned, or other assumptions. For example, the threat/OPFOR employs insider threat as a norm in covert activities. In US Army force operations, suspected insider threats may require a free-text modifier or a narrative description and date-time group status in a tactical diagram.

Mission Tasks and Control Measures

A tactical *mission task* symbol is the graphic representations of a tactical task. Most mission tasks for threats/OPFOR use symbols consistent with ADRP 1-02; however, several threats/OPFOR symbols appear different and/or have different definition. From a threat/OPFOR perspective, a tactical mission task can represent either an action by a friendly threat/OPFOR force, or the results or effects on an enemy force.[9] Threat/OPFOR mission tasks are typically illustrated with the color red, but can use black when this best displays the task in relation to other symbols and/or control measures. Figure 5 displays a sample of typical mission task symbols.

A *control measure* symbol graphically portrays operational information and functional expectation within a task or operation. Control measure symbols can be displayed as points, lines, and/or areas.[10] No standardized amplifier location exists for all types of control measures, so placement of a control measure and any amplifiers depends on effective positioning within an overall graphic representation such as an operations overlay or course of action sketch.

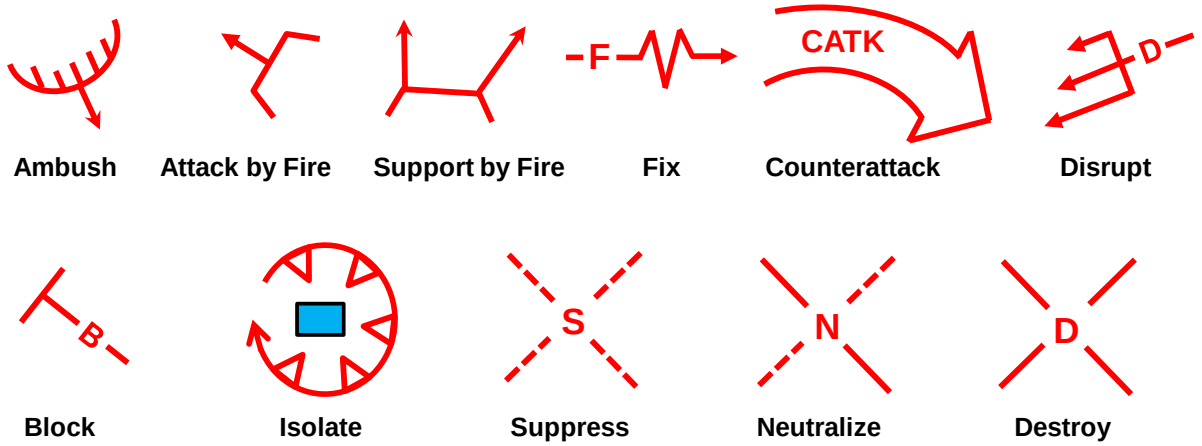


Figure 5. Sample of mission tasks and control measures

Movement and Maneuver. Actual movement-maneuver uses a solid line. The symbol for a planned threat/OPFOR movement is a dashed-line with an arrowhead pointed in the direction of movement. The symbol for threat/OPFOR infiltration or exfiltration is a serpentine line with an arrowhead pointed in the direction of movement. The word "infiltration" or the acronym "INFL" is placed near the control measure to clarify purpose. In a similar manner, the word "exfiltration" or the acronym "EXFL" is placed near the control measure. An axis of advance, as in US Army doctrine, is the general trace in which the majority of unit or organization combat power must move and maneuver. Threat/OPFOR emphasizes exploitation with a special control measure. See figure 6.

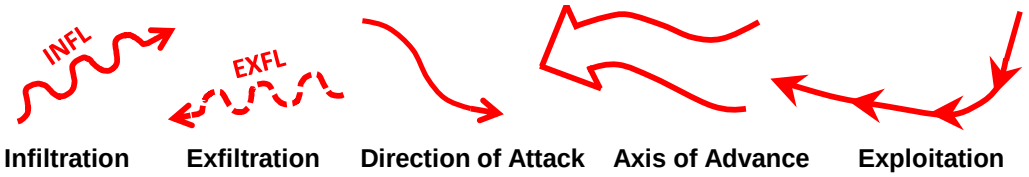


Figure 6. Sample of movement and maneuver control measures

Fires. The threat/OPFOR control measure for planned direct fires and/or principal direction of fire is a straight solid line with an arrowhead toward a primary assigned target or targets, expected direction of an enemy, or a kill zone. In a planning diagram, the threat/OPFOR control measure for indirect fire is a solid curved line with an arrowhead to the assigned target. A *kill zone* is a designated area on the battlefield where the threat/OPFOR plans to destroy a key enemy target.[11] Target reference points and targets orient fires inside and outside of a kill zone. See figure 7.

In a diagram that visualizes direct and/or indirect fire actions in progress, the direct and indirect fire control measure uses *dots* from the point of weapon origin to the target. Fires planning also uses measures such as a target reference point, indirect fires target, and principal direction of fire measures. These control measures typically use the color red, but can use black when this technique best displays the measure within a tactical diagram.

Figure 7. Sample of threat/OPFOR fires control measure symbols

Defensive Positions. In defensive operations, the threat/OPFOR use simple battle positions and/or complex battle positions. A *simple battle position* (SBP) is a defensive location oriented on the most likely enemy avenue of approach. In a detailed planning diagram, positions within a defensive position may appear in several variations. SBPs may or may not

be tied to restrictive terrain, but use camouflage, concealment, cover, and deception (C3D) measures in urban and rural areas, and employ as much engineer effort as possible to restrict enemy maneuver. SBP defenders conduct all actions to prevent enemy penetration of their position and defeat a penetration once it occurs.[12] Figure 8 presents several locations or positions that can be expected in a SBP and/or CBP.

Figure 8. Sample of threat/OPFOR position control measure symbols

A *complex battle position* (CBP) is a defensive location designed to employ a combination of complex urban or rural terrain, C3D, and engineer effort to protect the unit(s) within the CBP from detection and attack and deny its seizure and occupation by the enemy. Simple battle positions are integral to this defense and will also employ combat security outposts (CSOPs) for early warning of enemy approaches.

Characteristics that distinguish a CBP from SBPs in a disruption zone, battle zone, or support zone include CBP location away from expected enemy avenues of approach. In either urban or rural terrain, a CBP is located to avoid contact with the enemy; however, a CBP provides sanctuary from which to launch local attacks. Detailed planning of defensive positions may use several different control measures to identify individual or grouped positions. See figure 9 for the control measure that identifies the general location and orientation of a SBP and CBP.

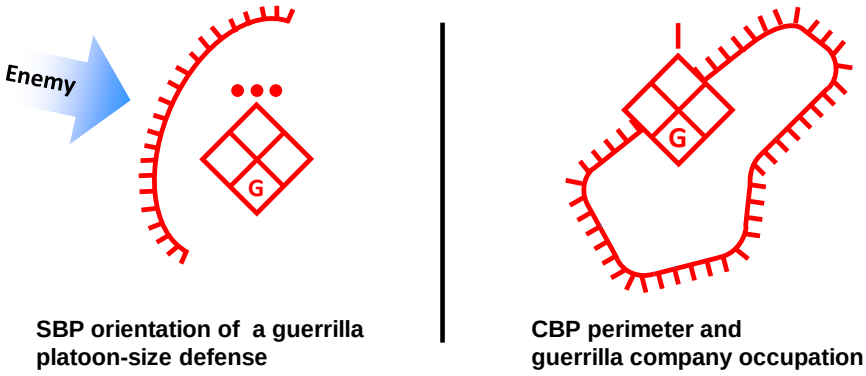


Figure 9. Simple battle position-complex battle position control measures (example)

CBPs are designed to deny their seizure and occupation by the enemy. Commanders occupying CBPs intend to preserve their combat power until conditions permit offensive action. In the case of an attack, CBP defenders will engage only as long as they perceive an ability to defeat aggressors. Should the defending commander feel that his forces are decisively overmatched, he will attempt a withdrawal in order to preserve combat power.[13] By TC 7-100.2 definition, a CBP does not serve the same purpose as a US Army strongpoint, even though the control measure graphically appears to be the same.

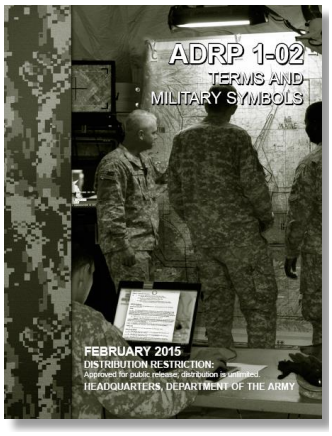
Implications for Army Training and Readiness

Knowing the threats, adversaries, and/or enemies is critical to the situational understanding of conditions in an operational environment. Intelligence preparation of the battlefield collects, analyzes, and refines information and inferences continually to determine facts and assumptions that support critical information, staff estimates and recommendations, and commander decisions. Training and readiness for missions and tasks can be evaluated in the context of at least two distinct conditions:

- When a specific threat force is not identified or known for mission readiness, a robust, realistic, and relevant OPFOR provides a composite of varying capabilities of actual worldwide forces in doctrine, tactics, organization, and equipment.[14]

- When an Army unit is preparing for a specified mission or contingency operation deployment in an OE with known threats, adversaries, and/or enemies, training replicates those actual OE and force capabilities and limitations to the optimum extent possible.[15]

In both training and operational preparations, conditions are identified and created to provide a challenging environment for the US Army commander to evaluate and confirm mission essential tasks or specified tasks to an Army standard. A common language and visual presentation of missions and tasks are fundamental to creating situational understanding of a mission or task and the conditions of an OE in order to plan for and achieve mission success.



ADRP 1-02 is the US Army doctrinal source for terms and military symbols. The *Army Dictionary online* augments this ADRP due to terminology changes that occur more frequently than traditional US Army publication media can be updated. See https://www.milsuite.mil/book/docs/DOC-40298. This terminology and symbology database, known as the *Army Dictionary*, is updated monthly to reflect the latest editions of Army publications. (Use a common access card (CAC) to access the Army dictionary database at https://jdeis.js.mil/jdeis/index.jsp?pindex=207.) This database is an official Department of Defense (DOD) website, maintained by the Combined Arms Doctrine Directorate (CADD) at the US Army Combined Arms Center (USACAC) and in collaboration with the US Joint Staff.[16]

The HQDA TC 7-100 series is the US Army source for tailoring a realistic, robust, and relevant array of threats and OEs to challenge designated training tasks, and is a key complement to understanding known threats, enemies, and adversaries. The TRADOC G2 functions as the Army Program proponent and Army staff focal point for all Army and Joint opposing force actions in accordance with the *Opposing Force (OPFOR) Program* (AR 350-2) across the Army.[17] The resources of the TRADOC G2 Operational Environment Enterprise (G2 OEE) support the comprehensive readiness mission of focused training, recurring professional military education, and US Army leader development.

Notes

[1] United States Army Training and Doctrine Command G2 OEE, ACE-Threats Integration, *Red Diamond* newsletter. "Military symbols: Know the threats-enemies-adversaries." March 2015. pp. 11-16.

[2] Headquarters, United States Army Training and Doctrine Command. TRADOC Regulation 10-5-1. 20 July 2010. para. 18-8, 1c(a). *Note*. TR 10-5-1 is in revision with TRADOC publication expected in 2015.

[3] This HQDA training circular (TC) 7-100 series is in final transition in 2015 from Army field manuals to training circulars. The currently published TC 7-100 series is on the Army Publishing Directorate (APD).

[4] Headquarters, Department of the Army. Army Doctrine Reference Publication 1-02. *Terms and Military Symbols*. 2 February 2015. p. v. *Note*. Department of Defense (DOD) Military Standard (MIL-STD) 2525C, *Common Warfighting Symbology*. 17 November 2008 remains in effect. *Note*. This DOD standard is in revision with a probable publication update in late 2015.

[5] Headquarters, Department of the Army. ADRP 1-02. *Terms and Military Symbols*. 2 February 2015. para. 3-15.

[6] Headquarters, Department of the Army. ADRP 1-02. *Terms and Military Symbols*. 2 February 2015. para. 3-1.

[7] Headquarters, Department of the Army. ADRP 1-02. *Terms and Military Symbols*. 2 February 2015. para. 3-14.

[8] US Department of Defense. Military Standard (MIL-STD-2525C). *Common Warfighting Symbology*. 17 November 2008. p. 425. *Note*. Threat/OPFOR uses the DOD unmanned aerial system (UAS) symbol with a "UAV" amplifier for a threat/OPFOR unmanned aerial vehicle.

[9] Headquarters, Department of the Army. ADRP 1-02. *Terms and Military Symbols*. 2 February 2015. para. 3-4.

[10] Headquarters, Department of the Army. ADRP 1-02. *Terms and Military Symbols*. 2 February 2015. para. 3-17.

[11] Headquarters, Department of the Army. Training Circular 7-100.2, *Opposing Force Tactics*. TRADOC G-2 Intelligence Support Activity (TRISA)-Threats, Complex Operational Environment and Threat Integration Directorate (CTID). 9 December 2011. para. 2-48.

[12] Headquarters, Department of the Army. Training Circular 7-100.2, *Opposing Force Tactics*. TRADOC G-2 Intelligence Support Activity (TRISA)-Threats, Complex Operational Environment and Threat Integration Directorate (CTID). 9 December 2011. para. 4-107 and 4-109.

[13] Headquarters, Department of the Army. Training Circular 7-100.2, *Opposing Force Tactics*. TRADOC G-2 Intelligence Support Activity (TRISA)-Threats, Complex Operational Environment and Threat Integration Directorate (CTID). 9 December 2011. para. 4-108 and 4-145.

[14] Headquarters, Department of the Army. Army Regulation 350-2. *Opposing Force (OPFOR) Program*. 9 April 2004. para 1-5a.

[15] Headquarters, Department of the Army. Army Regulation 350-2. *Opposing Force (OPFOR) Program*. 9 April 2004. para. 1-5f.

[16] Headquarters, Department of the Army. ADRP 1-02. *Terms and Military Symbols*. 2 February 2015. p. vii, para. 2.

[17] Headquarters, Department of the Army. Army Regulation 350-2. *Opposing Force (OPFOR) Program*. 9 April 2004. para 1-8.

COMING SOON—THREAT TACTICS REPORT-NORTH KOREA

by H. David Pendleton ACE-Threats Integration(CGI Ctr)

The TRADOC G-2 ACE-Threats Integration will release a Threat Tactics Report (TTR) on North Korea in the near future. ACE-Threats Integration will announce when this report is posted to our files on the Army Training Network (ATN) website.

The TTR explains how a threat actor—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 TTR actors are present in the Decisive Action Training Environment (DATE) and other US Army training materials for easy access and use across the Army Learning Model (ALM) venues. This TTR describes the Democratic People's Republic of Korea (DPRK) strategy and goals, key political and military leadership, major alliances, and the organizational size and structure of the Korean People's Army (KPA) and its subordinate organizations of the Korean People's Air Force and the Korean People's Navy. The TTR examines the KPA's strengths and weaknesses, their current unit dispositions, tactics and techniques, and defensive and offensive military strategies.

The US Army training community can use the North Korea TTR to gain insight into KPA 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.

Despite renewed efforts at diplomatic outreach, Kim continues to challenge the international community with provocative and threatening behavior in pursuit of his goals….He has codified this approach via his dual-track policy of economic development and advancement of nuclear weapons…. North Korea is another state actor that uses its cyber capabilities for political objectives.
***Worldwide Threat Assessment of the US Intelligence Community* (2015)**

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 Cleaves	
jon.s.cleaves.civ@mail.mil		913.684.7975	
Dep Director	DSN:552	Penny Mellies	
penny.l.mellies.civ@mail.mil		684.7920	
Operations–Analyst		Dr Jon Moilanen	
jon.h.moilanen.ctr@mail.mil	BMA	684.7928	
Product Integration-Analyst		Angela Wilkins	
angela.m.wilkins7.ctr@mail.mil	BMA	684.7929	
Intelligence Specialist		DAC Walt Williams	
walter.l.williams112.civ@mail.mil		684.7923	
Intelligence Specialist		DAC Jennifer Dunn	
jennifer.v.dunn.civ@mail.mil		684.7962	
Intelligence Specialist		DAC Jerry England	
jerry.j.england.civ@mail.mil		684.7934	
Intel Specialist-NTC LNO		DAC Kris Lechowicz	
kristin.d.lechowicz.civ@mail.mil		684.7922	
Senior Threats Officer		LTC Shane Lee	
shane.e.lee.mil@mail.mil		684.7907	
Threat Tactics & CoEs LNO		CPT Ari Fisher	
ari.d.fisher.mil@mail.mil		684.7939	
(UK) LNO	Warrant Officer	Matt Tucker	
matthew.j.tucker28.fm@mail.mil		684-7994	
Military Analyst		Rick Burns	
richard.b.burns4.ctr@mail.mil	BMA	684.7897	
Worldwide Equipment Guide		John Cantin	
john.m.cantin.ctr@mail.mil	BMA	684.7952	
Military Analyst		Laura Deatrick	
laura.m.deatrick.ctr@mail.mil	CGI	684.7925	
LNO to MCTP-Analyst		BMA Pat Madden	
patrick.m.madden16.ctr@mail.mil		684.7997	
Military Analyst		H. David Pendleton	
henry.d.pendleton.ctr@mail.mil	CGI	684.7946	
JMRC & JRTC LNO-Analyst		Mike Spight	
michael.g.spight.ctr@mail.mil	CGI	684.7974	
Intel Specialist-Analyst		(TBD)	
Intel Specialist-Analyst		(TBD)	
Intel Specialist-Analyst		(TBD)	