Red Diamond
Threats Newsletter

TRADOC G-2 Operational Environment Enterprise
Analysis & Control Element Threats Integration

Fort Leavenworth, KS | **Volume 8, Issue 09** | **September 2017**

INSIDE THIS ISSUE

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

For e-subscription, contact:
Nicole Bier (DAC), Intel OPS Coordinator, G-2 ACE-TI

Topic inquiries:
Jon H. Moilanen (DAC), G-2 ACE-TI
or
Angela Williams (DAC), Deputy Director, G-2 ACE-TI

Copy Editor:
Laura Deatrick (CGI CTR), G-2 ACE-TI

by Jon H. Moilanen, TRADOC G-2 ACE Threats Integration (DAC)

The All Partners Access Network (APAN) is an unclassified information sharing and collaboration enterprise of the US Department of Defense (DoD) and other partners as an unclassified means for timely and effective collaboration. APAN resources are available over the open Internet so individuals and organizations who do not have access to traditional US DoD systems and networks can participate and contribute in sharing information and expertise as members of learning organizations.

TRADOC G-2 ACE Threats Integration (ACE-TI) is preparing to offer access to most of its threat and opposing force (OPFOR) products on APAN in the near future. Other opportunities will include expanding coordination with multinational partners such as the United Kingdom, Australia, and Canada on initiatives for the US Army's Decisive Action Training Environment (DATE) and several regional DATE products being developed by 2018. Other capabilities include use by ACE-TI mobile training teams to access the Threat Tactics Course when training or exercising at remote sites. APAN provides community spaces and collaborative tools to leverage unclassified information for effective US Army, joint, and multinational training, professional education, and leader development venues. TRADOC G-2 ACE-TI will use the Red Diamond newsletter to announce when its products are available on a Sharepoint platform on APAN.

Additional elements of the TRADOC G-2 OEE with APAN sites include the Global Cultural Knowledge Network (GCKN), the Foreign Military Studies Office (FMSO), and Mad Scientist.

RED DIAMOND TOPICS OF INTEREST

by TRADOC G-2 ACE Threats Integration

This issue of *Red Diamond* opens with an article on an ambitious military transformation program being conducted by China to professionalize its military forces. Transformation at the tactical level is wide-ranging. The Chinese army has moved away from combat divisions to combat brigades organized in three primary variations: heavy, medium, and light. This article reviews these basic brigade types and their associated weapons platforms.

The Decisive Action Training Environment (DATE) ground forces, air forces, and associated insurgent groups' orders of battle (OBs) are now available on the Joint Training Data Service (JTDS) and Exercise Design Tool (EDT). While the OBs in DATE reach down to the brigade level, those on JTDS and EDT reach down to the entity level (individual soldier, system, weapon, or vehicle). A brief article discusses the advantages of using these OBs and how to potential users can gain access.

Camps and settlements for refugees have become a more common condition in crisis zones as conflicts increase in scope. The increasing size of camp populations is creating an environment in which threat actors seek opportunities to militarize these vulnerable populations. While refugee camps are often waved away as only a humanitarian issue, their intentional militarization by a range of threat actors could boil over and require a larger commitment of forces. An article discusses the similarities between these camps and traditional megacities, as well as potential methods of militarizing camp populations.

The next article is the second segment of a two-part series examining opposing force (OPFOR) tactical tasks with the technique of using antitank guided missiles, as seen through the lens of an irregular force videotape of an ambush. Generally, this tactic uses the terrain to the attacker's advantage and employs obstacles to halt the enemy, with the goal of keeping him in the kill zone throughout the action. This tactical vignette focuses on the OPFOR tactical task of ambush, with functions and subtasks compared to a real-world incident in the ongoing conflict between Yemeni rebels and Saudi Arabian forces.

Russian military doctrine has long centered on its artillery. As early as the 14th century, the Russians began placing a greater emphasis on larger artillery formations in proportion to their infantry in order to repel Mongol invaders. The first installment of a two-part series reviews Russian thought regarding use of artillery, changes in the country's military over recent decades, and the military's extensive use of deception.

A dispersed attack is a threat tactic that adapts to an operational environment and an enemy that is typically superior in relative combat power comparison to threat forces. The primary actions of a dispersed attack create conditions to mass selective threat combat power on key systems of an enemy force and combat system. The final Red Diamond article this month examines this tactics in detail, including types of forces used and associated tasks, and provides an example vignette.

by Marc Williams, TRADOC G-2 ACE Threats Integration (ThreatTec CTR)

> "They studied our doctrine, our tactics, our equipment, our organization, our training, our leadership. And, in turn, they revised their own doctrines, and they are rapidly modernizing their military today to avoid our strengths in hopes of defeating us at some point in the future."
>
> —General Mark Milley, Chief of Staff of the Army
> 2016 Association of the US Army Conference

The People's Republic of China (PRC) is conducting an ambitious military transformation program to professionalize the People's Liberation Army (PLA) and reach its goals. The PLA is a higher headquarters for the Army (PLAA), Navy (PLAN), Marines (PLANM), and Air Force (PLAAF). At the strategic level for the land forces, this transformation includes activation of a PLAA headquarters staff, renaming the Second Artillery Force to the PLA Rocket Force (PLARF), and activation of Strategic Support Forces (SSF).

Transformation of land forces at the tactical level is wide-ranging. The PLAA has followed the US lead and moved away from combat divisions to combat brigades. Most common in the PLAA are combined arms brigades in three variations: heavy, medium, and light. The PLAAF, not the PLAA, includes the PRC airborne forces, whose units are expanding in number. The PLANM is also growing into three full brigades.

Figure 1. PLA Emblem

PLA Size

The latest transformation of the PLA has reduced the PLAA while building the other services. Despite this, the PLAA is a sizeable modernized force. Future transformation of the PLA includes continued downsizing the PLAA by half and augmenting the other services (especially the PLAN) with more personnel and equipment by 2020. This will be the first time the PLAA active force will drop below one million. The strategic goal is a stronger PLA that can conduct overseas missions.[1] The 2016 force levels are shown below.

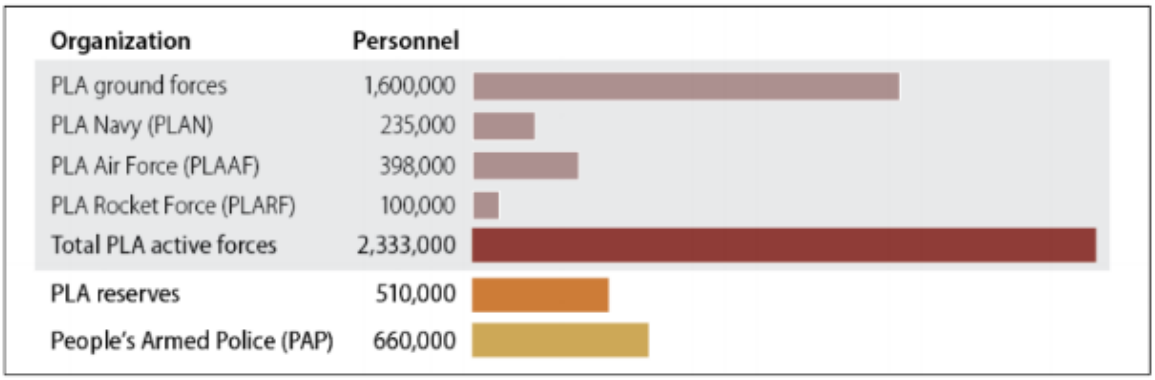


Figure 2. PLA military and security personnel

As PLAA transformation continues, the three most common brigade types are the heavy combined arms brigade, the medium combined arms brigade, and the light combined arms brigade.

PLAA Heavy Combined Arms Brigade[2]

Heavy combined arms brigades are mechanized with ZBD04A/ZTZ 99- or ZTZ 96-based units, which are sometimes called heavy tracked units.[3] The combined arms battalions of this type of brigade are equipped with main battle tanks (MBTs), infantry fighting vehicles (IFVs), and armored fighting vehicles (AFVs). Among these, the ZTZ 99 and ZTZ 96 MBTs are the most capable. The Type 59 MBT is the most common.[4]

Figure 3. ZTZ 99 MBT, ZTZ 96 MBT, and Type 59 MBT[5]

Among the assigned IFVs and armored personnel carriers, the ZBD 04A is the most modern. The Type 89 AFV is very common as a transport, and there is a command vehicle variant. The most modern units possess the PLZ 10 120-mm mortar/howitzer for organic indirect fire support to the battalion. This is sometimes referred to as a "combo-gun."

Figure 4. ZBD 04A IFV, Type 89 AFV, and PLZ 10 combo-gun

The air defense battalion is armed with medium-range/altitude surface-to-air missiles (SAMs) like the CSA 15. It is also armed with man-portable air defense systems (MANPADS) and self-propelled (SP) anti-aircraft artillery. The artillery battalion is equipped with PLZ 07 122-mm SP howitzers and 122-mm multiple rocket launchers (MRLs).

Figure 5. CSA 15 SAM, PLZ 07 SP howitzer, and 122-mm MRL

PLAA Medium Combined Arms Brigade[6]

PLAA medium combined arms brigades are mechanized with 6x6 or 8x8 wheeled armored vehicles. These are sometimes called medium high-mobility units. The combined arms battalions of this type of brigade are equipped with assault guns or "wheeled tanks" in the MBT role and possess ground-launched antitank guided missile capability.

Figure 6. 8X8 assault gun and 6X6 assault gun

The ZBL 09 and WZ 551 are the main 8x8 and 6x6 wheeled armored vehicles.[7] The most modern units also have PLL 05 120-mm mortar/howitzer support organic to the combined arms battalion.

Figure 7. ZBL 09 armored vehicle, WZ 551 armored vehicle, and PLL 05 combo-gun

The artillery battalion is equipped with the PLL 09 122-mm SP howitzer and new wheeled 122-mm MRL. The air defense battalion has the CSA 4B SAM and MANPADS.

Figure 8. PLL 09 SP howitzer, 122-mm MRL, and CSA 4B SAM

PLAA Light Combined Arms Brigade[8]

Light combined arms brigades are wheeled Mengshi-based units, sometimes called light high-mobility units. They use a variety of vehicles built on the Mengshi 4x4 chassis. The 4x4 are the basic HUMVEE types, and the 6x6 variants are the extended armored version.

Figure 9. Mengshi 4x4, Mengshi 4x4 with heavy machinegun, and Mengshi 6x6 armored variant

For artillery, the PLC 09 122-mm SP howitzers and the new wheeled 122-mm MRLs are the most commonly fielded indirect fire systems. There are also Mengshi-based mortar and anti-aircraft (AA) platforms.

Figure 10. 122-mm MRL, PLC 09 122-mm SP, and AA vehicle

Conclusion

The PLA transformation is far more comprehensive across the domains of land, maritime, air, space, and cyber than what is summarized in this article. China's defense industry production order of priority for modernization is (1) missile systems, (2) space systems, (3) maritime assets, (4) aircraft, and (5) ground systems. However, according to the US Secretary of Defense, "China's production capacity continues to advance in almost every area of PLA Army systems, including new tanks, armored personnel carriers, air defense artillery systems, and artillery pieces. China is capable of producing ground weapon systems at or near world-class standards."[9] Improvements have been made in training and exercises, and units have taken delivery of "advanced command, control, communication, computers, and intelligence (C4I) equipment that provides real-time data-sharing at the division and brigade level."[10] American brigade combat teams would do well to research these formations and develop an understanding of the capabilities of their combat systems.

Figure 11. PLAA tank platoon training in Shenyang

Notes

[1] Defense World. "China To Downsize Army By Half, Boost Navy Numbers." 12 July 2017.
[2] Information provided by the US Army Intelligence and Security Command National Ground Intelligence Center (NGIC).
[3] US Army, TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. Worldwide Equipment Guide – Volume 1: Ground Systems. December 2016. Pgs 25 and 28.
[4] US Army, TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. Worldwide Equipment Guide – Volume 1: Ground Systems. December 2016. Pg 31.
[5] Figures 3–10 provided by the US Army Intelligence and Security Command National Ground Intelligence Center (NGIC).
[6] Information provided by the US Army Intelligence and Security Command National Ground Intelligence Center (NGIC).
[7] US Army, TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. Worldwide Equipment Guide – Volume 1: Ground Systems. December 2016. Pg 43.
[8] Information provided by the US Army Intelligence and Security Command National Ground Intelligence Center (NGIC).
[9] Office of the Secretary of Defense. Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2016. Pg 80.
[10] Office of the Secretary of Defense. Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2016. Pg 33.

DATE 3.0 ORDER OF BATTLE IN JTDS AND EDT

by Lisa Leech (CGI Contractor) and LTC Ed Lerz, TRADOC G-2 OE Training Support Center (OE TSC), Data Science, Models, Simulations Directorate (DSMS)

The Decisive Action Training Environment (DATE) Version 3.0 ground forces, air forces, and associated insurgent groups' orders of battle (OBs) are now available down to the entity level (individual soldier, system, weapon, or vehicle granularity required for simulations) on the Joint Training Data Service (JTDS) and Exercise Design Tool (EDT). The DATE 3.0 document exists in PDF format and describes each DATE country to include an OB at the brigade level. Up to this point, home-station units were required to perform a crosswalk between the DATE, the *Worldwide Equipment Guide* (WEG), and TC 7-100.4, *Hybrid Threat Force Structure and Organization Guide*, to build out the necessary opposing and allied forces that comprise their desired exercise operational environment (OE) in constructive simulations. The lack of available planning time to conduct a proper crosswalk of publications caused home-station units to use their existing, now dated, counterinsurgency-based OB, which is not grounded in today's intelligence. Without an authoritative source to reference, there were inconsistent interpretations across the force that have resulted in disparities between home-station training scenarios and combat training center (CTC) scenarios.

TRADOC G-27, in conjunction with TRADOC G-2 ACE Threats Integration and Joint Staff J-7, collaborated to create DATE 3.0 OBs down to the entity level to provide training audiences with an authoritative source for creating training scenarios based on the DATE, and in a machine-readable format for use in the Army's current constructive simulations. The work involved the creation of over four million data nodes requiring unit composition and platform choices previously left to the interpretation of the exercise designer. The DATE 3.0 OB available on JTDS and EDT enables units to create exercise scenarios using the same authoritative source shared by the CTCs. Building partner and opposing forces is as simple as logging in and pulling the desired units into the exercise scenario. Exercise designers can make adjustments to suit specific training objectives without having to recreate an entire force. With CTCs using the same OE, force, and platform structure, pre-deployment certification exercises should increase effectiveness with more time spent on refining technique rather than making adjustments to the opposing force. DATE 3.0 ground forces, air forces, and insurgent groups are currently available, with naval/coast guard force OBs coming online in the near future.

Common access card holders can apply for JTDS access at https://jtds.jten.mil/jtds/ and EDT access at https://tbr.army.mil. Any questions or inquiries on how to access the DATE 3.0 data, use of the EDT, or other G-2 capabilities may be directed to LTC Ed Lerz at edward.b.lerz.mil@mail.mil or (757) 878-9747.

———————

by James (Jay) Hunt, TRADOC G-2 ACE Threats Integration (CGI CTR)

This article is the first in a series to introduce unique conditions that may be incorporated into training events to enhance realism and add complexity in a training context.

Camps and settlements for refugees and internally displaced persons (IDPs) have become a more common condition in crisis zones as conflicts increase in scope, with more noncombatants in harm's way. Managing large concentrations of civilian noncombatants has often been difficult for the international community and the hosting nation. The inherent difficulties are made worse by the instability caused by external and internal threat actors. Instability beyond the host country's capabilities could result in security assistance requests from US or coalition forces. While security of refugees is not a standard task for assisting forces, the regional security impact can be immense.

When considering refugees of any kind, unit commanders and the training community have generally focused on tasks that only involve force escalation and security at the small-unit level. The increasing size of camp populations is creating an environment in which threat actors seek opportunities to militarize these vulnerable populations. The threat conditions in and around the camps create a vicious cycle of destabilization that pushes the camps to collapse, creating a greater crisis. While refugee camps are often waved away as only a humanitarian issue, their intentional militarization by a range of threat actors could boil over and require a larger commitment of forces.

Large Refugee Settlement as Megacity Microcosm

The challenge of military operations within and around megacities has been difficult for the training community to implement for a number of reasons. Conditions that typify megacities, such as complex and multidimensional terrain, difficulty distinguishing combatants, extreme population density, and difficult outsider access, are often shared by large refugee settlements. For example, population density is one of the defining factors of a dense urban environment. The densities per square mile in the larger camps in Africa are comparable to densities of the top designated megacities.

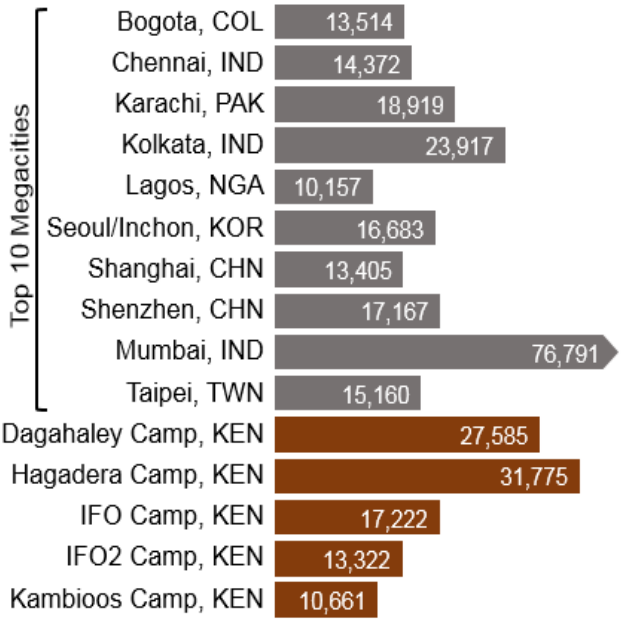


Figure 1. Population density per square mile

There are, of course, many differences that break the comparison. Most of these conditions are simply not feasible for constructive training solutions. Relegating dense urban environments to simulations does an immense disservice to the soldiers and commanders that may be called upon to operate under these conditions.

Large camps in recent history have generally developed as noncombatants and defeated combatants flee violence. They are often within a two-day walk from the border of the country experiencing conflict and established at or near junctions of existing lines of communication (LOCs). They may be self-organized or planned. The most common refugee settlements have populations between 10–20 thousand, while the most populous may exceed 90,000. The average population density often exceeds 20,000 per square mile. In comparison, the densities of the most populous megacities averages just over 22,000 per square mile.

Condition	Mega-Camps	Megacities
Rules of Engagement	Complex dynamics and concerns about noncombatants and collateral damage may reduce command flexibility	
Collateral damage risk	Damage to structures, infrastructure, no-fire targets highly likely and will be used for information warfare	
Complex terrain	Multiple concealed attack angles; in-depth knowledge of terrain	
Strategic INFOWAR	Pervasive cameras send selective images to worldwide and regional audience	
Tactical INFOWAR	Easy instant messaging and improvised signaling allow rapid situational awareness and on-demand massing of both combatants and noncombatants	
Dispersed threat actor(s)	Threat actors can rapidly disperse to make identification difficult and obfuscate force centers of gravity	
Difficulty discerning combatants	Threat actors may appear as civilians; noncombatants may also carry weapons and be highly agitated	
3-Dimensional attack risk	Attacks possible from 360°; limited height of structures prevents high-angle attacks	Attacks possible from concealed positions in multi-story buildings and even subterranean locations
Scope of improvised attack methods	Large explosive or fire attacks not as likely	Full range of improvised devices and car/tire fires

Table 1. Mega-Camp to megacity condition comparison chart

While obviously not an exact analogue, the conditions of large refugee settlements and camps present enough similar challenges to be relevant for training.

How do Refugee Camps Militarize?

Even well-managed camps can become militarized very quickly. Unchecked threats can develop with minimal visible signatures and threaten camp occupants and the camp's overall viability, as well as the host nation's economic and security situation. The complex and challenging living conditions within large refugee camps are not the primary threat of concern that military forces might face, but rather the danger of intentional militarization.

While a level of conflict within large camps is to be expected, aggressive militarization of camp residents can destabilize the camps to the point of collapse. This might in turn create an exodus of refugees either returning to the danger areas they fled or streaming into the host nation's towns and cities. Military or police forces may need to be deployed from their normal responsibilities to support or restore security in the region. Preventing the orchestrated implosion of these camps is in the best interest of peacekeeping forces and the host nation.

The path to growing a militarized population within a refugee camp often progresses as follows:

1. Punitive Attacks from Crisis Area

Military and/or paramilitary forces that prevailed in the crisis country follow their defeated adversaries across the border to a refugee camp to prevent re-arming and a possible return as a future threat. Attacks may be brutal, with violent raids against former soldiers and noncombatants alike. Violence against noncombatants may be in retaliation for supporting their "enemies" or to rob, rape, or enslave them. The attacking forces may be company- to battalion-sized army or guerrilla elements with mostly small arms and military or technical vehicles. Small formations of militants may also attack vulnerable refugees in transit.

Security around the camps and on the LOCs between the camps and the affected border region are likely missions for intervening forces. Tasks will vary greatly, from securing and managing various-sized groups of noncombatants to open combat with up to battalion-sized forces.

2. Exploitation of Vulnerable Camp Populations

Refugee populations within camps often either self-segregate or are grouped by language, ethnicity, tribe, area of origin, or other demographic characteristic. Threat actors will exploit fears of real or perceived external threats or "others." Populations of former combatants can create "refugee warrior communities" that leverage the sanctuary status of the camp to be free from outside attacks while recruiting and training from vulnerable populations.

Former soldiers in camps may initially recruit and train receptive refugees to "defend" themselves against internal and external threats. Insurgent groups may also be present alongside the guerrillas, seeking to add strength and numbers to their ideologically-focused plans. Threat actors will manage their activity levels of organization and militancy to prevent detection and interference by camp security elements. Non-uniformed guerrillas and insurgents may have up to 2–4 battalion-sized elements of former soldiers and camp recruits available. These forces will operate as small cells and reaction units to minimize action by camp security. Limited shows of force and tests of mobilizing larger groups of agitated civilians may occur in areas under their control.

Host-nation and other agreements that affect rules of engagement will dictate to what extent security forces can operate within the camps. In a training context, the ambiguity and rapidly shifting security situations possible are a signature condition of these dense communities.

3a. Seizing Control of Camp Resources and Infrastructure

The inherent volatility of dense, unsettled populations and the aggressive recruitment and militarization by threat actors within the camp may lead to uprisings and disturbances directed against aid workers, camp leadership, or security forces. Camp occupants may perceive violence as more widespread than is actually is. Multiple communication channels may amplify incidents, leading to disproportionate responses, both by camp security personnel and residents. If the security situation is perceived as untenable, camp residents may flee en masse to wherever or whomever they identify as a potential safe haven. This could clog roads and create havoc throughout the region.

Threat forces may manifest in groups ranging from dozens to hundreds. A force of non-uniformed guerrillas and insurgents may have up to 2–4 battalions of former soldiers and camp recruits available. These forces may have a variety of small arms and improvised weapons. Informal communication networks and capabilities allow the forces' ranks to rapidly swell and dissipate.

This is one of the most dangerous environments and the most similar to megacity conditions. Multiple attacks from easily disguised actors from numerous directions can quickly overwhelm local security forces and require surge capabilities to maintain the semblance of order. Local security elements and low-cost private security companies may not have the training or fortitude to withstand such assaults without breaking ranks or resorting to undesirable techniques.

3b. Using Camp as Sanctuary for Launching Attacks

Alternatively, threat actors and their militarized ranks may use the camp as a protected haven from which to launch attacks, rather than displaying open aggression within the camp. These attacks are usually directed against their former enemies, although more immediate targets may help satisfy grievances of their new constituents and solidify control. Particularly large camps and those with porous perimeters may be more prone to nefarious activities that allow large groups to come and go with little attention from beleaguered security elements. Attacks may range from securing unfettered access in the surrounding areas to large-scale raids against potential competitors or former adversaries.

Threat forces may manifest in groups ranging from dozens to hundreds. A force of non-uniformed guerrillas and insurgents may have up to 4–5 battalions of former soldiers and camp recruits available or combine with forces outside of the camp to create sizeable forces for specific operations. The forces from the camp may have a variety of small arms and improvised weapons, but may have larger weapons in external caches or in the hands of compatriots.

Conclusion and Implications for Training

While large refugee camps may not be the focus of a training event, they can be a primary driver of conflict. Threat dynamics associated with destabilized camps can result in a number of conditions that could be integrated into training events. Examples of these are:

- Ambushes or raids on lines of communications near the camps,
- Supply raids against aid organizations or kidnapping of personnel, or
- Attacks by armed groups either from the camp or from across a nearby border.

A degraded security environment in the region around the camp may also divert security forces from the desired training event.

Commanders have a range of tasks that could be trained by incorporating the real-world conditions associated with large refugee camps. These conditions could add realism and complexity to tasks such as force protection, area security, information operations, unit movement, and combating irregular forces.

References

Abubakar, Aminu and Philippe Rater. "Nigerian forces in 'unauthorised search' of UN camp." TerraDaily. 11 August, 2017.

Allen, Stephen. "Harboring or Protecting? Militarized Refugees, State Responsibility, and the Evolution of Self-Defense." The Fletcher Journal of Human Security. 2010.

Anderson, William G. "Megacities and the US Army." Parameters. Spring 2015.

Esri and Marina Koren. "Where Are the 50 Most Populous Refugee Camps?" Smithsonian Magazine. 29 June 2013.

Headquarters, Department of the Army. Training Circular 7-100.3, Irregular Opposing Forces. TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. 17 January 2014.

Headquarters, Department of the Army. Training Circular 7-100.4, Hybrid Threat Force Structure Organization Guide. TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. 4 June 2015.

Headquarters, Department of the Army. Training Circular 7-100.2, Opposing Force Tactics. TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. 9 December 2011.

Mungai, Christine. "Larger than 11 African capital cities: 10 dramatic facts about Dadaab, world's biggest refugee camp." Mail and Guardian Africa. 28 Jan 2016.

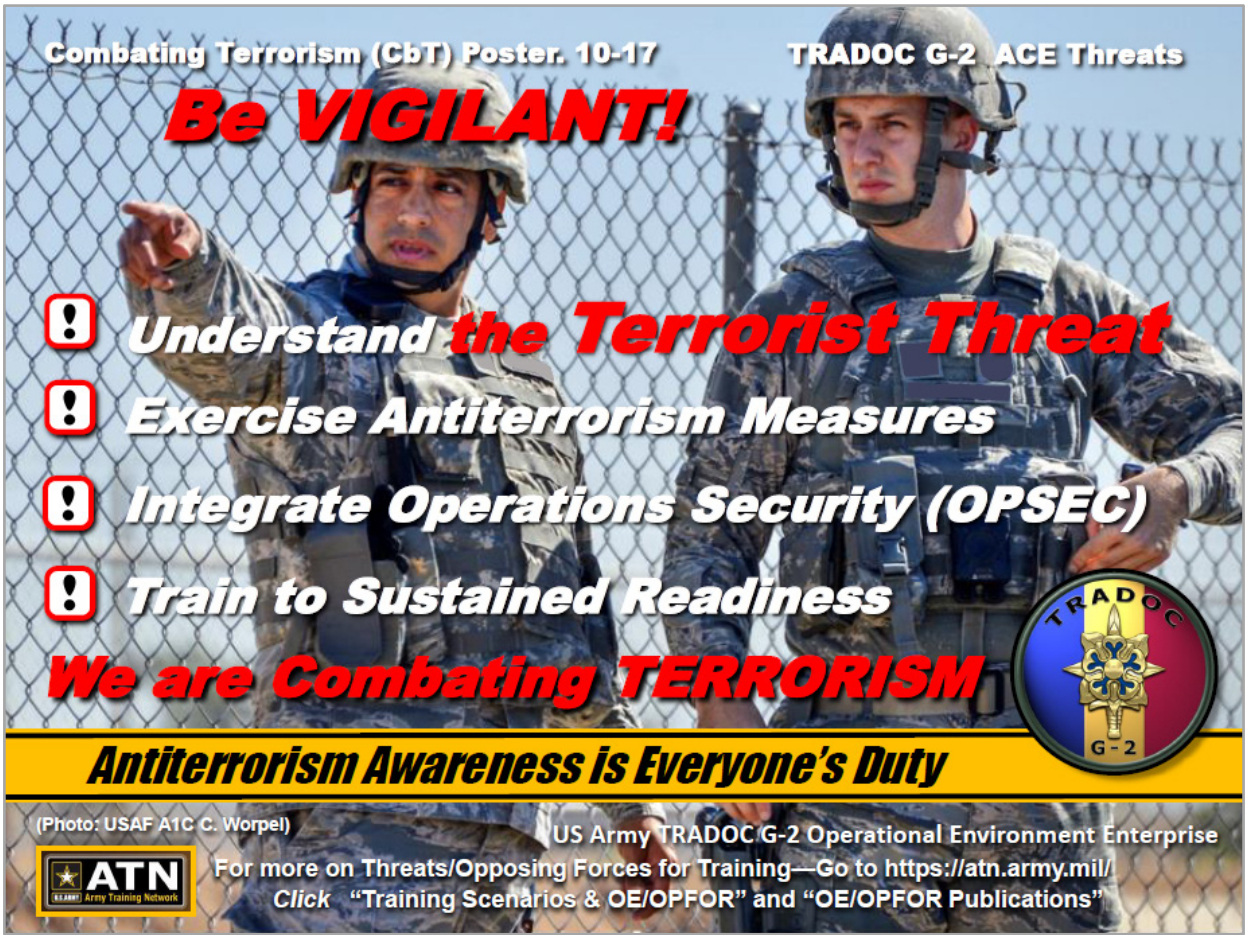
Schneider, Eric. "Militarization of Refugee Camps." Philologia Volume VII.

UN High Commissioner for Refugees, "Dagahaley Camp Profile." ReliefWeb. August 2015.

UN High Commissioner for Refugees, "IFO Camp Profile." ReliefWeb. August 2015.

UN High Commissioner for Refugees, "IFO2 Camp Profile." ReliefWeb. August 2015.

UN High Commissioner for Refugees, "Kambioos Camp Profile." ReliefWeb. August 2015.



by Kristin Lechowicz, TRADOC G-2 ACE Threats Integration (DAC), and MAJ Ric Tearle, S02 Foreign Material Exploitation/ British Exchange Officer (US Army), Defense Intelligence Agency's Missile Space Intelligence Center

This article is the second segment of a two-part series that examines opposing force (OPFOR) tactical tasks with the technique of using antitank guided missiles (ATGMs), as seen through the lens of an irregular force videotape of an ambush in US Central Command's area of operation. This tactical vignette focuses on the OPFOR tactical task of ambush, with ambush functions and subtasks compared to a real-world incident in the ongoing conflict between Yemeni rebels and Saudi Arabia forces. This video captures the tactical action of an ambush on a quick reaction force (QRF), which was likely responding to a raid on an isolated Saudi Arabian outpost near the two countries' borders in the vicinity of Najran province.[1] The video appears to have been taken over a number of different time periods with a number of rough edits.

The video begins with an ATGM raid by Yemeni rebels that engages stationary targets on an outpost, with a follow-on ambush on two targets that are likely the QRF responding in support of the bombarded outpost.[2] The video first shows the rebels monitoring two vehicles on routes, likely after the first attack on the outpost, which could have been part of the reconnaissance process to find a good ambush site. This article compares current threat doctrine with the tactical actions captured in the rebel video, focusing on the ambush of the QRF. This article is the fourth collaborative effort between the TRADOC G-2 ACE Threats Integration Directorate and the Defense Intelligence Agency's Missile Space Intelligence Center (MSIC). MSIC provided the ATGM video along with a basic analysis. ACE-TI provided further tactical analysis with the diagrams and comparison to threat doctrine for replication within the US OPFOR training community.

This series of articles compares OPFOR doctrine from the OPFOR Tactical Task List in Appendix B of Training Circular (TC) 7-101, *Exercise Design*, and TC 7-100.2, *Opposing Forces Tactics*, with real-world attack videos for training implications. This video footage has the ATGM system(s) as the primary action element engaging two vehicles in the QRF ambush.

Video Background[3]

- Date: Sometime between July–August 2016.
- Location: Najran, Yemen.
- Rebel group: Houthi Rebels (ATGM offensive tactical actions)
- Weapon system: ATGM (unknown)
- Weapon systems location: Slightly elevated
- Target(s): Two temporarily halted vehicles (ambush)
- Missile firing time to target: Unknown
- Endstate: Two burning vehicles

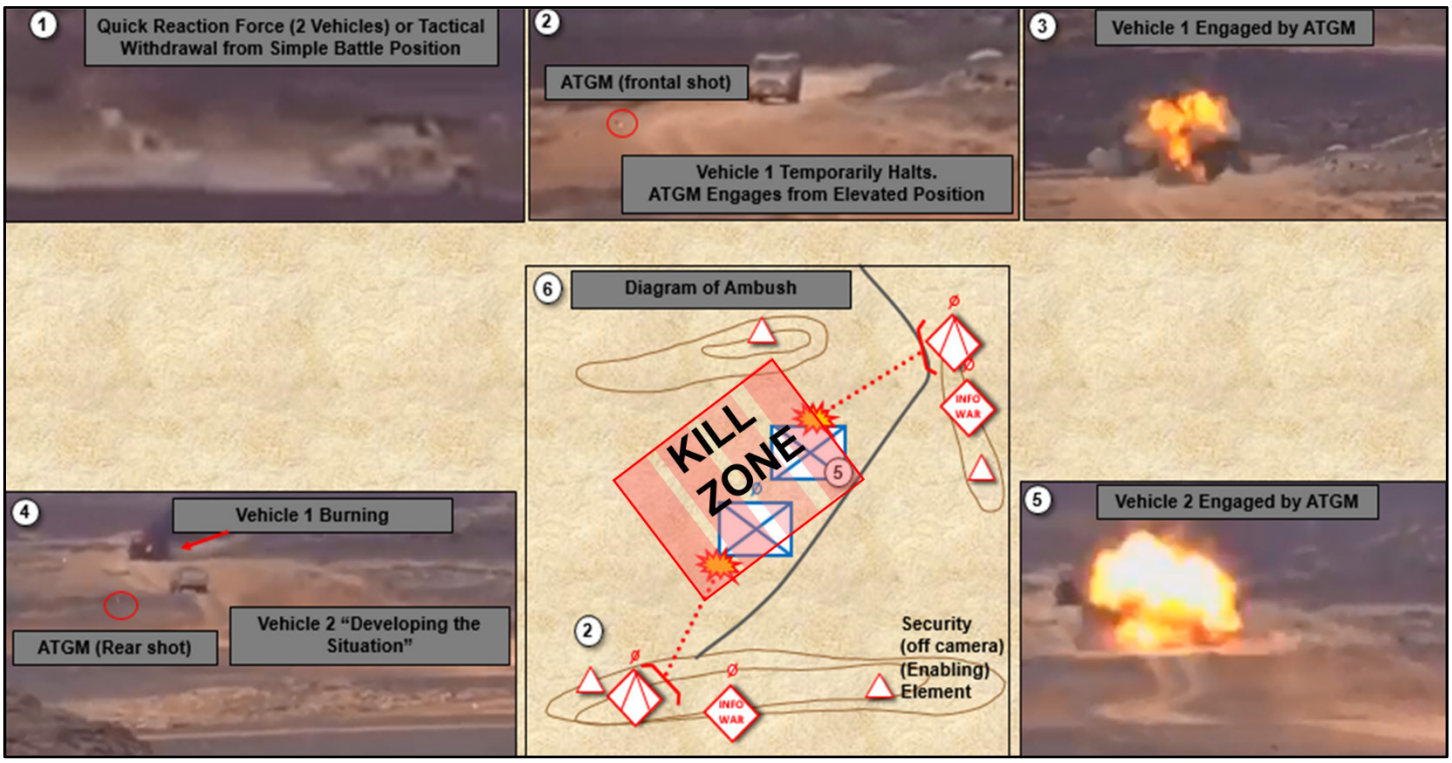


Figure 1. ATGM ambush diagram and video graphic

After the raid on the outpost, the video shows two vehicles responding to the tactical action. The video is edited and shows a different pair of vehicles that are ambushed in the kill zone. The Yemeni rebels likely moved undetected into the ambush site. The first vehicle is engaged with a frontal ATGM strike. The second vehicle is struck from the rear by another ATGM. The rebels had likely studied the QRF's routes and set up the ambush site based on those observations. It is likely that the ambush element had enabling elements isolating the battlefield**,** even though the threat elements were not in view on the video. This video illustrates a good example of a real-world threat that can be replicated by the training community. Replication by an OPFOR could also use a number of smaller hunter-killer teams in different positions around the base perimeter.[4]

OPFOR Implications and Training Support

The OPFOR Tactical Task List in Appendix B of TC 7-101, *Exercise Design*, consisted of 24 OPFOR-specific tactical tasks comparable in style to the US Army's Universal Task List.[5] A recent review by ACE-TI of the OPFOR tactical tasks in the US Army's Combined Arms Training Strategies (CATS) revised 17 OPFOR tasks, subtasks, and performance measures. Those revised tasks are in TRADOC G-2 Handbook 1.09, *Opposing Force Tasks: Collective Company/Subordinate Units*, available on the Army Training Network (ATN). These and other OPFOR tasks are currently being incorporated by ACE-TI into an updated version of TC 7-100.2, *Opposing Forces Tactics*. These tasks provide challenging OPFOR conditions for training to a US Army standard.

Tactical Task: Ambush

An *ambush* is a surprise attack from a concealed position, used against moving or temporarily halted targets. The purpose of an ambush is to destroy the enemy force. Per TC 7-100.2, "The OPFOR also uses ambush as a primary psychological warfare tool. The psychological effect is magnified by the OPFOR use of multi-tiered ambushes. A common tactic is to spring an ambush and set other ambushes along the relief or reaction force's likely avenues of approach."[6] These are violent attacks designed to ensure the enemy's return fire, if any, is ineffective. Generally, this type of ambush uses the terrain to the attacker's advantage and employs mines and other obstacles to halt the enemy in the kill zone. The goal of the obstacles is to keep the enemy in the kill zone throughout the action. The subtasks and measures for an OPFOR ambush, as listed in CATS, are as follows:

Plan

- Identify enemy element/force[1] capabilities and limitations to be ambushed;
- Conduct analysis to determine the type of ambush(es) [point or area] to be conducted;
- Identify ambush kill zone(s);
- Analyze action and enabling functions that must be performed to achieve mission success and consider tasks to deceive, disrupt, suppress, fix, contain, defeat and/or destroy;
- Determine the functional tactics to be applied by action and enabling elements;
- Identify situational understanding requirements for collection and analysis;
- Task-organize elements for the ambush task by function in accordance with TC 7-100.2/TC 7-100.3; and
- Determine how and when functional elements act or enable the ambush and/or transition to other tasks/subtasks.

Prepare

- Conduct continuous reconnaissance and surveillance to provide situational understanding of enemy and operational environment required for OPFOR success;
- Conduct continuous counterreconnaissance to prevent the enemy from obtaining situational understanding of OPFOR intentions;
- Conduct mission and task rehearsals; and
- Execute information warfare (INFOWAR).

Infiltrate

- Conduct undetected and sequenced movement by security elements through and/or into an area occupied by enemy elements to occupy a position(s) in order to fix enemy security or response elements;
- Conduct undetected and sequenced movement by support elements through and/or into an area occupied by enemy elements to occupy a position(s) in order to isolate the kill zone(s);
- Conduct undetected and sequenced movement by support elements through and/or into an area occupied by enemy elements to occupy an indirect fire position(s) in order to suppress, disrupt, or contain enemy at the kill zone(s);
- Conduct undetected movement by ambush element(s) through and/or into an area occupied by enemy elements to occupy a position(s) in order to ambush enemy and/or enemy materiel in the kill zone(s); and
- Determine if current tactical conditions require an adjustment to the ambush.

Isolate

- Conduct security tasks to provide early warning and/or protect the action, support, and security elements (other tactical tasks may include but are not limited to: block, canalize, contain, delay, destroy, disrupt, fix, interdict, suppress, or neutralize);
- Position support elements;
- Deliver and adjust lethal and/or nonlethal suppression effects on enemy elements to be isolated that prevent contact with other enemy elements;
- Degrade designated enemy elements to temporarily prevent those elements from assisting the isolated enemy element; and
- Maneuver security elements to a position(s) in order to deny the enemy freedom of movement along designated ground or air avenues of approach that can reinforce enemy elements in the intended kill zone or otherwise interfere with the tasks of the ambush action and other enabling elements.

Contain

- Use surprise, limited visibility, complex terrain, emplaced obstacles, camouflage, concealment, cover, deception, and fires to restrict and channel the enemy into the kill zone(s); and

[1] Hereafter referred to as "element."

- Stop, hold, or surround enemy elements in the kill zone or cause enemy elements to center their activity to a given front and prevent them from withdrawing any part of the element for use elsewhere.

Ambush

- Ambush with massed direct and/or indirect fires into the kill zone(s) to destroy the enemy;
- Assault to seize the objective in the kill zone, when designated in the mission task and intent;
- Support the ambush with appropriate enabling functions that may include but are not limited to: deception, breach, fix, disrupt, and/or employment of reserve elements;
- Exploit the objective site for enemy prisoners and enemy equipment and materiel, when designated in the mission task and intent;
- Consolidate the objective or kill zone area for its temporary occupation and defense while the site is being exploited by OPFOR elements; and
- Reorganize OPFOR elements to minimize the impacts of combat losses and functional capabilities.

Exfiltrate

- Distribute the reorganized OPFOR elements quickly into small elements for exfiltration along designated exfiltration lanes;
- Conduct undetected movement from the kill zone and/or objective area by stealth and deception to a designated rally point; and
- Continue the mission.

OPFOR AMBUSH Performance Measures (US Army CATS Task 71-CO-8502)		
No.	**Action Assessment/Evaluation**	**Criteria**
01	**Unit moves to and occupies ambush site without detection**	**YES/NO**
02	**Unit isolates kill zone from assistance**	**YES/NO**
03	**To execute ambush**	**Time**
04	**Enemy in kill zone during projected time window**	**YES/NO**
05	**Enemy contained in kill zone**	**YES/NO**
06	**Friendly forces available to continue mission**	**Percent**
07	**Combat effectiveness of enemy force**	**Percent**

Table 1. OPFOR ambush performance measures

OPFOR Replications and Training Support

This type of ATGM tactical action creates a formidable challenge for training units and can be used in combat training centers (CTCs) by the OPFOR elements. CTCs, scenario developers, and home-station trainers can find additional information on ATGM units, organization, or weapons systems in TC 7-100.4, its associated Threat Force Structure, and the Worldwide Equipment Guide (WEG). These types of real-world examples are key for the training community to include into scenario development and training.

References

Headquarters, Department of the Army. Training Circular 7-100.2, Opposing Force Tactics. TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. 9 December 2011.

Headquarters, Department of the Army. Training Circular 7-100.3, Irregular Opposing Forces. TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. January 2014.

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

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

Notes

[1] See "Anti-tank Guided Missile Raid" in the May 2017 edition of the *Red Diamond*.

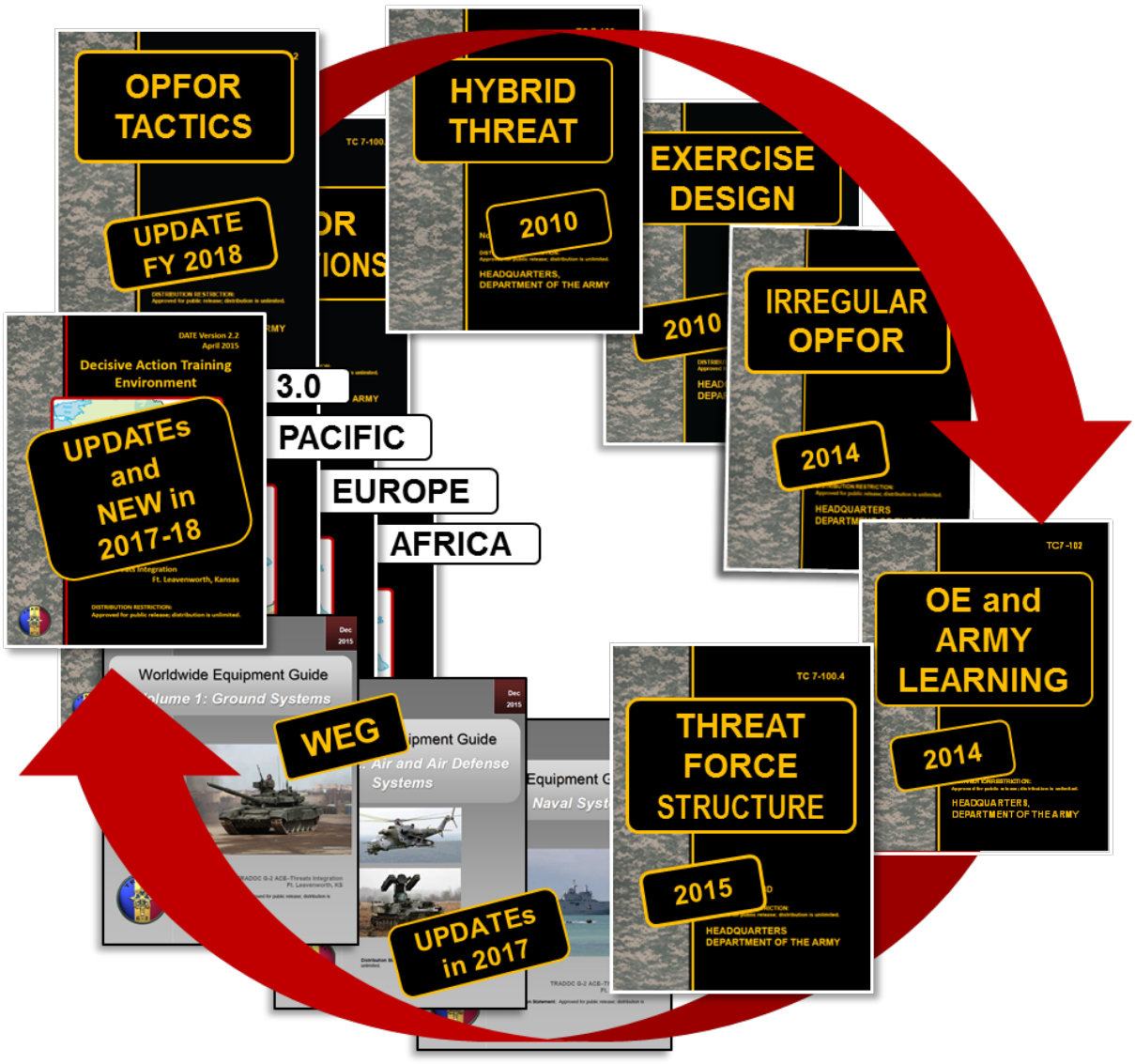
[2] YouTube. "Military Operations to the Heroes of the Yemeni Army and People's Committees breached in the Najran (translated)." Posted 14 August 2016.

[3] Missile and Space Intelligence Center (Antitank Guided Missile Systems). "ATGM Firings in the Syrian Conflict as of 16 August 2016." 16 August 2016.

[4] For additional information on hunter-killer teams, see TC 7-100.4 and its associated Threat Force Structure. TC 7-100.2 discusses the tactics of hunter-killer teams that can be implemented by the training community.

[5] Headquarters, Department of the Army. Training Circular 7-101, Exercise Design Guide. TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. November 2010. Pg B-3.

[6] Headquarters, Department of the Army. Training Circular 7-100.2, Opposing Force Tactics. TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. 9 December 2011. Para 3-134.



Opposing Force Resources to the Training Community

by MAJ James Andersen, TRADOC G-2 ACE Threats Integration

> *The Russian Army is an artillery army with a lot of combat vehicles. While Western Armies have gravitated to precision fires delivered by fewer systems, the Russians maintain a large artillery park and employ mass fires to destroy hectares of enemy-occupied territory.*[1]
>
> —Lester Grau and Charles Bartles

Russian military doctrine has long centered on its artillery. As early as the 14th century, the Russians began placing a greater emphasis on larger artillery formations in proportion to their infantry to repel Mongol invaders.[2] In the 15th century, Ivan the Terrible placed a large impetus on using improved artillery in large numbers to secure victory at Tartar City of Kazan and during the Livonian War.[3] Later, following an analysis of the Napoleonic Wars, Russian Lieutenant General Nikolay Okunev concluded that "artillery was not a supporting arm of military forces and could achieve decisive results by itself."[4] Okunev was a proponent of large massed artillery batteries of 80–100 guns.[5] Okunev's theories may have influenced the Soviet Union as to the importance of achieving fire superiority.[6]

After the First World War, which was thoroughly studied by the Soviet Union, it was determined that any penetration of enemy defensive lines would require massed fires in a ratio of 2:1 artillery to infantry.[7] Furthermore, according to Vladimir Triandfafillov—a prominent figure in Soviet military art— "artillery must follow the infantry, not just with fires, but with wheels."[8] Triandfafillov's judgments on mass and mobility again influenced Soviet military thinkers. This is likely the reason for the massive buildup of artillery during the interim war years between WWI and WWII.[9]

Despite the advent of both tactical and strategic nuclear weapon strategies in the 1960s, the Soviet Union did not allow its rocket and artillery forces to wilt away. On the contrary, Soviet brigade and battalion commanders maintained a quantitative advantage over NATO forces of organic artillery at their level, with decentralized control from higher echelons.[10] At higher echelons, such as division, a more centralized approach for rocket and artillery forces was adopted to support overall strategic objectives.[11] The high quantities of fires available to brigade and battalion commanders freed, in theory, Soviet division and corps assets from frequent fire-support requests from lower echelons. Moreover, the Soviets demonstrated a willingness to use artillery very aggressively, much closer to the front than other armies, and even direct fire when needed.[12] This often befuddled Western military thinkers, as it seemed to place artillery and antitank weapons at unnecessary risk.[13] As Chris Bellamy notes, this is because "Soviet gunners were not afraid and never have been afraid to lose a gun or rocket launcher if it rips the arm of an enemy off."[14]

The Fall of the Soviet Union

In December 1991, the Soviet Union collapsed and transitioned into the weakened Russian Federation. Dissolution of the Union of Soviet Socialist Republics (USSR) had a catastrophic effect on the once-mighty Soviet military.[15] Forces that did return from former Soviet Republics did so in a piecemeal fashion, to districts and bases unprepared for their return.[16] During its peak, the Soviet Union had maintained 210 divisions but, by 1999 under the Russian Federation, only approximately 50 brigades remained.[17] Russia's armed forces were underfunded, unable to man their smaller military,

and incapable of sustaining or upgrading their aging equipment.[18] Faced with such a crisis, Russia prioritized its spending, reforming its military while preserving and modernizing its nuclear forces to maintain a strategic deterrence.[19]

The Rise of the Russian Federation and Military Reform

From 1992–2008, a series of military reforms were attempted to fix problems that plagued the armed forces. Of those reforms, two had a major impact on how the Russian Army organizes itself today. The first reform envisioned the creation of smaller, fully manned units that could respond to a regional crisis until larger forces could be mobilized.[20] The second reform, beginning in 2004, was the creation of a more professional force through more contracted soldiers and fewer conscripts. Furthermore, this reform also restructured regional district commands, reducing bureaucracy. The military districts were consolidated from 16, under the Soviet Union, to four under the Russian Federation at present.[21] The realigned military districts also inform the West on where Russia perceives threats from its potential adversaries.[22] These reforms allowed Russia to respond relatively quickly in Chechnya in 1994 and 1999 and may have been the reason for the creation of their brigade tactical groups.[23] Since 2008, reforms have been aimed at correcting deficiencies noted in the Georgian War involving communications, electronic warfare, and targeting.[24] Lastly, these reforms helped Russia form a coherent policy "clearly formulated on post-Soviet Russian national defense."[25]

Figure 1. Russian regional military command after reforms[26]

The recent resurgence of Russian global influence may be an attempt by the Kremlin to counter US and NATO members' continued encroachment into previously held territories of the former Soviet Union. From the Russian perspective, this expansion is an aggressive attempt by NATO to encircle and mute Russian global influence.[27] Of particular concern for the Russians is the placement of ballistic missile defenses in eastern Europe, blunting their strategic nuclear deterrents.[28] Furthermore, the Russians view the expansion of NATO as a direct threat to their ability to project power regionally as well as defend themselves.[29] The inclusion of Poland and the Baltic states—Estonia, Lithuania, and Latvia—into NATO brought military elements against Russia's eastern border, approximately 500 miles from Moscow in the case of some Baltic states. Given this perception, it is not surprising that Russia would attempt to prevent Ukraine from potentially adopting a pro-Western government that could one day join NATO. Ukraine, as a member of NATO, could deny Russia's Black Sea fleet access to the port of Sevastopol. This is Russia's only warm-water port and its only convenient access to the Mediterranean Sea.[30]

New Tools, Same Paradigm

Despite the organizational shift to a smaller army less dependent on conscripts, the Russian Army, like its predecessor, remains a fires-focused army. The Russian Army retains both a quantitative 3:1 ratio in terms of the number of artillery pieces at the brigade echelon as compared to the US Army and a qualitative edge—namely range overmatch—to its near peers.[31] Furthermore, there has been an increased emphasis on improving the precision of its fires and creating additional target acquisition platforms to support fires. However, the Russian Federation understands that to successfully employ its fires against near-peer adversaries such as NATO and the US, tactics, strategies, and equipment have to be developed to overcome near-peer strengths.

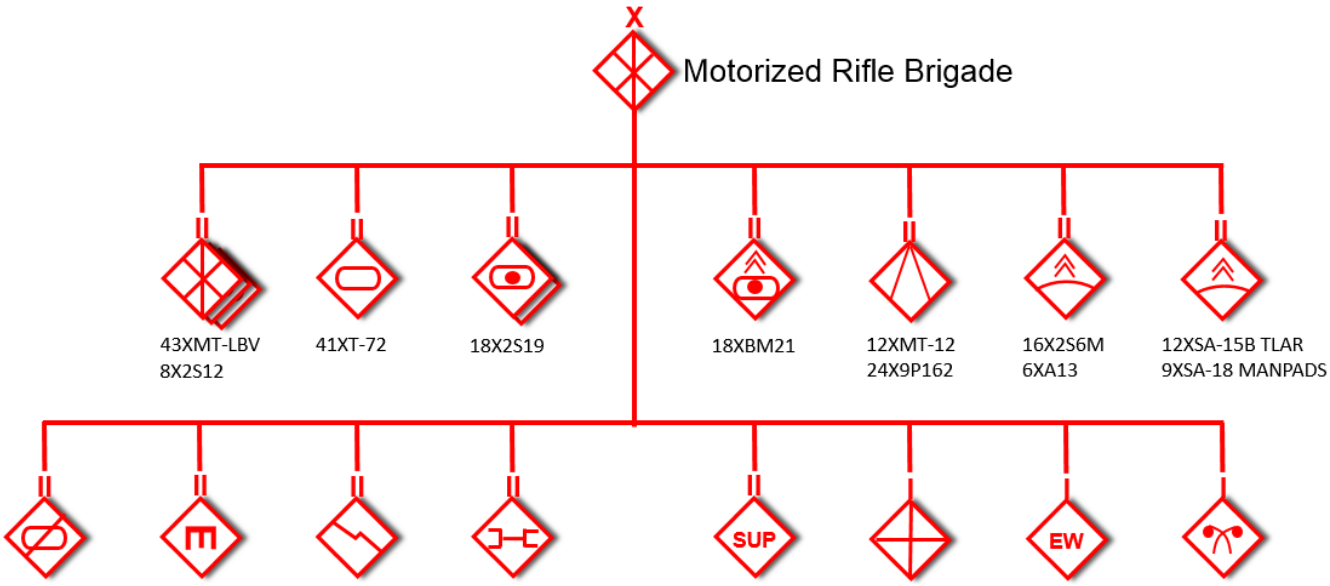


Figure 2. New Russian motorized rifle brigade[32]

The Soviet Union watched the success of the US-led coalition in the First Gulf War and noted the effective use of target acquisition and precision fires in attacking not only front line units, but command and control nodes, logistical hubs, and support areas, effectively paralyzing the enemy.[33] More importantly, the Gulf War served as proof of concept for the Russian "deep battle" doctrine developed in the 1930s, which was later revised in the 1980s to adopt new technology and non-nuclear precision fires.[34] Deep battle could, theoretically, "exercise a direct and decisive outcome of a future war…deep battle was a strategic concept that focused on terminating, overwhelming, or dislocating enemy forces not only at the line of contact, but throughout the depth of the battlefield."[35]

In addition to confirming Russian military theory, the First Gulf War confirmed the need to protect front line, artillery, and rear units from detection by improved US intelligence, surveillance, and reconnaissance (ISR) assets and destruction by air, land, and naval precision fires. During its modernization, the Russian Army focused on updating its considerable air defense capabilities and refining its existing artillery overmatch with increased precision, target acquisition, and electronic warfare capability. Russia understood that it was overmatched in the air and invested heavily in air defense.

Based on Russian reorganization and procurement of equipment, it is assessed that Russia views US and NATO strengths as follows:

- Ground, air, and naval fires precision fires aided by global positioning systems (GPS);
- Well-trained and -equipped armor and infantry units with professional, non-conscript soldiers;
- Effective technical means of intelligence collection via geospatial and aerial platforms;
- Command and control aided by GPS navigation systems and secure, reliable communications; and
- NATO and US overmatch in air power.

Russian Deception: Maskirovka

In order to counter its adversary's advantages and successfully employ fires, the Russian Federation has developed a multi-pronged approach. The first method is protecting the fires assets themselves. To do this, deception, or

maskirovka, is employed. Translated directly, maskirovka means "a little masquerade," which does not accurately convey the depth of the deceptions employed by the Russians.[36] Maskirovka under the Soviet Union could be defined as "the processes designed to mislead, confuse, and interfere with accurate collection regarding all Soviet plans, objectives, strengths, and weaknesses."[37]Maskirovka, in its different forms, is employed by the military at all levels, as well as politically at various levels of the state.

In a broader context, "[m]askirovka is in fact war that is short of war, a purposeful strategy of deception that may combine the use of force with disinformation and destabilization to create ambiguity in the minds of national leaders about how best to respond."[38] Creating such uncertainty amongst NATO members could allow the Russians to gain and maintain the initiative before and during a conflict, should one occur. An example of this is the deception employed in Ukraine, namely the denial of the presence of Russian soldiers, which had several effects. First, it caused the Western world to hesitate to act while it attempted to confirm conflicting reports. Second, it made it very difficult for the Ukrainian government to develop a strategy, as it was unsure of the composition of the adversary it faced.[39] Additionally, deception allowed the Russians to move personnel and materials and to mass forces against Ukraine, which included indirect fire systems, while the Western world debated courses of action.

Maskirovka is a fundamental component to both strategic and tactical military operations with three goals in mind: achieving "surprise, interference with the enemy's decision making, and preservation of combat power."[40] Surprise serves as a combat multiplier and may help seize the initiative.[41] Interference "ensures the enemy takes inappropriate action" or is paralyzed with indecisiveness, and "the final objective is to preserve combat forces."[42] Preservation of forces protects artillery, rocket, and missile forces, and is particularly important as the Russian Army doctrinally employs indirect fires systems to produce a majority of its casualties. According to Richard Wallwark, "analysis of many of the actions in Second World War attributed the destruction of 80 to 90 percent of the targets in the tactical zone to artillery; hence the name God of War."[43]

Russian deception planners first examine the truth and whether the intent is to hide the truth or create a false or half-truth.[44] Next, the resources available to conduct the deception are examined.[45] Finally, the adversary's reaction to the deception is anticipated and its ISR capabilities assessed.[46] There are five ways maskirovka is typically employed: concealment, imitation, simulation, demonstration, and disinformation.

Concealment decreases the chances of detection, hiding friendly information from an enemy.[47] It is the simplest form of deception and usually requires the least amount of coordination.[48] During WWII, the Soviet Union employed concealment using camouflage, night movement, and radio discipline, catching the Japanese completely unaware in 1939.[49] While concealment is typically associated with decisive action, in the case of Ukraine it was used to hide Russian troops among Ukrainian separatists and civilians.[50] It has been alleged that former Spetsnaz and Federal Security Service members were among those that infiltrated to support the fight against the Kiev-backed Ukrainian government.[51] The infiltration of non-uniformed personnel is not a new technique. The Soviet Union employed such methods in 1968 against Czechoslovakia and used non-uniformed *Narodnyĭ Kommissariat Vnutrennikh Del* "People's Commissariat of Internal Affairs" elements in Poland in 1945 to seize objectives before its adversary knew what was happening.[52] The arrival of uniformed men in the night without insignia, seizing key Ukrainian government facilities, caused confusion even among pro-Russian separatists. These soldiers, later identified as Russian, would be given the moniker "little green men."[53]

Imitation "involves the creation of false objects that appear to be real."[54] This may include decoy military equipment, false runways, and fake bridges. The desired effect is to cause confusion, conceal true intent, and make an adversary waste time and munitions attacking false targets. Simulation aids imitation by emulating the behavior of military equipment, such as adding heat signatures to decoys, creating false radio signatures or traffic, or falsifying tank tread markings in an effort to fool advanced sensors and intelligence assets and confirm the status of imitated items.

A demonstration is the use of real troops to create a feint or perform extensive reconnaissance to deceive an enemy about the nature or location of the main effort.[55] It was not uncommon in the Soviet-era military for members of the feint to be unaware of being part of a deception in order to increase operational security in case of capture.[56] More recently, Russia used military drills in its Western and Central Districts to move and mass units along the Ukrainian border.[57] Once massed, Russian units fixed Ukrainian forces along the eastern Ukrainian border, preventing them from "any military countermeasures in Crimea."[58] The massing of heavy units and artillery forced Ukraine to move

considerable combat power to the lightly defended eastern border, effectively fixing four Ukrainian brigades in place and preventing Russian forces in Crimea from being overwhelmed by Ukrainian forces.[59] Another demonstration was the very public use of humanitarian convoys, widely suspected of being used to resupply Russian forces, to draw the attention of Western intelligence collections assets while conventional forces slipped across the eastern Ukrainian border.[60]

Disinformation is the use of false information or half-truths and may include staged activities, fake products, or false news stories, and may be used against an adversary or against a country's own population or military.[61] Although the topic of disinformation has received a great deal of attention with the Russian incursion into Ukraine, Russian disinformation is not a new phenomenon. Russia has employed disinformation for much of its history; it was particularly important for the Soviet Union and received renewed emphasis during the late 1980s.[62] Today, "Moscow has established a new level of ambition, strategic Maskirovka, by which disinformation is applied against all levels of NATO's command chain and wider public opinion to keep the West politically and militarily off balance."[63] The little green men's allegiance to Russia was vehemently denied by both Russian military and state officials, to include Russian President Vladimir Putin.[64] Russia claimed that the little green men were local Ukrainian separatists, not Russian soldiers.[65] In addition to providing plausible deniability, disinformation provided Russia with justification for the incursion into Ukraine to protect ethnic Russians. It is believed that Russia manufactured stories about atrocities committed against ethnic Russians by Ukrainian forces to bolster separatist ranks and provide justification for Russian involvement.[66] The Russians used disinformation to create confusion and delay action. Disinformation was also used during the battle of Debaltseve, Ukraine, as well. Ukrainian soldiers received text messages during the battle falsely claiming that they were surrounded and that their commanders had abandoned them, sowing confusion and fear among their number.[67] The Russians believe that the "fog of war isn't something that just happens, they believe it can be manufactured."[68]

Training Implications

Currently, there is very little military deception taught to US Army officers, warrant officers, and noncommissioned officers (NCOs) in professional military education or specialty courses. Military deception, like many decisive action skills, has atrophied during the past 16 years. NCO and officer academies may consider including blocks of instructions on the subject, to include the history of military deception and both historical and modern case studies of threat deception. Additionally, tactical deception can be employed by the opposing force (OPFOR) during maneuver training center rotations. Such tactical deception includes employment of concealment to hide OPFOR units from blue force (BLUEFOR) sensors, imitation using decoys, and false electronic signatures. Furthermore, the use of feints and demonstrations to force the premature commitment of BLUFOR's main element may be employed. A permanent deception training course could established for both ISR collection managers and those assigned to the unofficial position of "Chief of Reconnaissance." This course, in addition to understanding deception, could train collection managers how to efficiently use cross-cueing and redundant ISR tasking to prevent enemy deceptions from being successful in an ISR-degraded environment.

This article is the first installment of a two-part series. Thus far the history of Russian artillery has been discussed, as well as reforms made by the country since the collapse of the Soviet Union and the Russian approach to deception. A future *Red Diamond* article will delve into Russian thinking on air defense, electronic warfare, and artillery employment, along with a review of selected Russian artillery platforms.

Notes

[1] Lester Grau and Charles Bartles. The Russian Way of War: Force Structure, and Modernization of Russian Ground Forces. Foreign Military Studies Office. Pg 155.
[2] Christopher Bellamy. Red God of War: Soviet Artillery and Rocket Forces. Brassey's Defense Publishers. 1986. Pg 11.
[3] Christopher Bellamy. Red God of War: Soviet Artillery and Rocket Forces. Brassey's Defense Publishers. 1986. Pg 11.
[4] Christopher Bellamy. Red God of War: Soviet Artillery and Rocket Forces. Brassey's Defense Publishers. 1986. Pg 21.
[5] Christopher Bellamy. Red God of War: Soviet Artillery and Rocket Forces. Brassey's Defense Publishers. 1986. Pg 21.
[6] Christopher Bellamy. Red God of War: Soviet Artillery and Rocket Forces. Brassey's Defense Publishers. 1986. Pg 21.
[7] Christopher Bellamy. Red God of War: Soviet Artillery and Rocket Forces. Brassey's Defense Publishers. 1986. Pg 46.
[8] Christopher Bellamy. Red God of War: Soviet Artillery and Rocket Forces. Brassey's Defense Publishers. 1986. Pg 46.
[9] Christopher Bellamy. Red God of War: Soviet Artillery and Rocket Forces. Brassey's Defense Publishers. 1986. Pg 47.
[10] Christopher Bellamy. Red God of War: Soviet Artillery and Rocket Forces. Brassey's Defense Publishers. 1986. Pg 215.

[11] Christopher Bellamy. Red God of War: Soviet Artillery and Rocket Forces. Brassey's Defense Publishers. 1986. Pg 215.
[12] Christopher Bellamy. Red God of War: Soviet Artillery and Rocket Forces. Brassey's Defense Publishers. 1986. Pg 215.
[13] Christopher Bellamy. Red God of War: Soviet Artillery and Rocket Forces. Brassey's Defense Publishers. 1986. Pg 215.
[14] Christopher Bellamy. Red God of War: Soviet Artillery and Rocket Forces. Brassey's Defense Publishers. 1986. Pg 215
[15] Karber Phillip. "Dr. Phillip Karber Explains Russian Operations in Ukraine." YouTube. 13 April 2017.
[16] Defense Intelligence Agency. Russia Military Power: Building a Military to Support Great Power Aspirations. 27 June 2017. Pg 10.
[17] Karber Phillip. "Dr. Phillip Karber Explains Russian Operations in Ukraine." YouTube. 13 April 2017.
[18] Defense Intelligence Agency. Russia Military Power: Building a Military to Support Great Power Aspirations. 27 June 2017. Pg 10.
[19] Defense Intelligence Agency. Russia Military Power: Building a Military to Support Great Power Aspirations. 27 June 2017. Pg 11.
[20] Defense Intelligence Agency. Russia Military Power: Building a Military to Support Great Power Aspirations. 27 June 2017. Pgs 11–13;
[21] David Isby. Weapons and Tactics of the Soviet Army. Jane's Publishing. 1989. Pg 31; Defense Intelligence Agency. Russia Military Power: Building a Military to Support Great Power Aspirations. 27 June 2017. Pg 14.
[22] Defense Intelligence Agency. Russia Military Power: Building a Military to Support Great Power Aspirations. 27 June 2017. Pg 14.
[23] Defense Intelligence Agency. Russia Military Power: Building a Military to Support Great Power Aspirations. 27 June 2017. Pg 12.
[24] Defense Intelligence Agency. Russia Military Power: Building a Military to Support Great Power Aspirations. 27 June 2017. Pg 12.
[25] Colby Howard and Ruslan Pukhov. Brothers Armed: Military Aspects of the Crisis in Ukraine. East View Press. 2015. Pg 75.
[26] Lester Grau and Charles Bartles. The Russian Way of War: Force Structure, and Modernization of Russian Ground Forces. Foreign Military Studies Office. Pg 28.
[27] Defense Intelligence Agency. Russia Military Power: Building a Military to Support Great Power Aspirations. 27 June 2017. Pg 15.
[28] Defense Intelligence Agency. Russia Military Power: Building a Military to Support Great Power Aspirations. 27 June 2017. Pg 15.
[29] Defense Intelligence Agency. Russia Military Power: Building a Military to Support Great Power Aspirations. 27 June 2017. Pg 15.
[30] Jim Sciutto. "Why Ukraine Matters to the U.S. & Russia." YouTube. 3 March 2014.
[31] Defense Intelligence Agency. Russia Military Power: Building a Military Power to Support Great Power Aspirations. 27 June 2017. Pg 15; Philip Karber and Joshua Thibeault. "Russia's New-Generation Warfare." Association of the United States Army. 20 May 2016.
[32] Data source: Defense Intelligence Agency. Russia Military Power: Building a Military Power to Support Great Power Aspirations. 27 June 2017. Pg 53.
[33] Defense Intelligence Agency. Russia Military Power: Building a Military Power to Support Great Power Aspirations. 27 June 2017. Pgs 33–34.
[34] Defense Intelligence Agency. Russia Military Power: Building a Military Power to Support Great Power Aspirations. 27 June 2017. Pg 34.
[35] Defense Intelligence Agency. Russia Military Power: Building a Military Power to Support Great Power Aspirations. 27 June 2017. Pg 34.
[36] Morgan Maier. Little Masquerade: Russia's Evolving Employment of Maskirovka. US School of Advanced Military Studies. 2016. Pg iii.
[37] Charles Smith. "Soviet Maskirovka." Airpower Journal. Spring 1988. Pgs 28–39.
[38] Julian Lindley-French. NATO: Countering Strategic Maskirovka. Canadian Defence & Foreign Affairs Institute. May 2015.
[39] Colby Howard and Ruslan Pukhov. Brothers Armed: Military Aspects of the Crisis in Ukraine. East View Press. 2015. Pg 204.
[40] Joseph Bridges. "[Military Weapons] What Is Maskirovka? Russian Military Deception #Military 101." YouTube. 22 May 2017.
[41] Joseph Bridges. "[Military Weapons] What Is Maskirovka? Russian Military Deception #Military 101." YouTube. 22 May 2017.
[42] Joseph Bridges. "[Military Weapons] What Is Maskirovka? Russian Military Deception #Military 101." YouTube. 22 May 2017.
[43] Richard Wallwork. Artillery in Urban Operations: Reflections on Experiences in Chechnya. US Army Command and General Staff College. 2004. Pg 31.
[44] Joseph Bridges. "[Military Weapons] What Is Maskirovka? Russian Military Deception #Military 101." YouTube. 22 May 2017.
[45] Joseph Bridges. "[Military Weapons] What Is Maskirovka? Russian Military Deception #Military 101." YouTube. 22 May 2017.
[46] Joseph Bridges. "[Military Weapons] What Is Maskirovka? Russian Military Deception #Military 101." YouTube. 22 May 2017.
[47] Joseph Bridges. "[Military Weapons] What Is Maskirovka? Russian Military Deception #Military 101." YouTube. 22 May 2017.
[48] Joseph Bridges. "[Military Weapons] What Is Maskirovka? Russian Military Deception #Military 101." YouTube. 22 May 2017.
[49] Richard Armstrong. "Soviet Operational Deception: The Red Cloak." US Army Command and General Staff College. 1989. Pg 4.
[50] Colby Howard and Ruslan Pukhov. Brothers Armed: Military Aspects of the Crisis in Ukraine. East View Press. 2015. Pg 204.
[51] Colby Howard and Ruslan Pukhov. Brothers Armed: Military Aspects of the Crisis in Ukraine. East View Press. 2015. Pg 204.
[52] Colby Howard and Ruslan Pukhov. Brothers Armed: Military Aspects of the Crisis in Ukraine. East View Press. 2015. Pg 204.
[53] Lucy Ash and Katy Hickman. "Maskirovka: Deception Russian-Style." BBC Radio 4. 1 February 2015.
[54] Charles Smith. "Soviet Maskirovka." Airpower Journal. 1988. Pgs 28–39.
[55] Joseph Bridges. "[Military Weapons] What Is Maskirovka? Russian Military Deception #Military 101." YouTube. 22 May 2017.
[56] Joseph Bridges. "[Military Weapons] What Is Maskirovka? Russian Military Deception #Military 101." YouTube. 22 May 2017.
[57] Colby Howard and Ruslan Pukhov. Brothers Armed: Military Aspects of the Crisis in Ukraine. East View Press. 2015. Pg 192.
[58] Colby Howard and Ruslan Pukhov. Brothers Armed: Military Aspects of the Crisis in Ukraine. East View Press. 2015. Pg 192.
[59] Colby Howard and Ruslan Pukhov. Brothers Armed: Military Aspects of the Crisis in Ukraine. East View Press. 2015. Pg 192.
[60] Lucy Ash and Katy Hickman. "Maskirovka: Deception Russian-Style." BBC Radio 4. 1 February 2015.
[61] Joseph Bridges. "[Military Weapons] What Is Maskirovka? Russian Military Deception #Military 101."
[62] Charles Smith. "Soviet Maskirovka." Airpower Journal. Spring 1988. Pgs 28–39.
[63] Julian Lindley-French. NATO: Countering Strategic Maskirovka. Canadian Defence & Foreign Affairs Institute. May 2015.
[64] Lucy Ash and Katy Hickman. "Maskirovka: Deception Russian-Style." BBC Radio 4. 1 February 2015.
[65] Lucy Ash and Katy Hickman. "Maskirovka: Deception Russian-Style." BBC Radio 4. 1 February 2015.
[66] Lucy Ash and Katy Hickman. "Maskirovka: Deception Russian-Style." BBC Radio 4. 1 February 2015.
[67] The Potomac Foundation. "Battle of Debaltseve: A Turning Point in the Russian War in Ukraine The Potomac Foundation." 2 March 2016.
[68] Lucy Ash and Katy Hickman. "Maskirovka: Deception Russian-Style." BBC Radio 4. 1 February 2015.

by Jon H. Moilanen, TRADOC G-2 ACE Threats Integration (DAC)

Dispersed attack is a threat tactic that adapts to an operational environment and an enemy that is typically superior in relative combat power as compared to threat forces. However, a dispersed attack can be executed against peer-level forces when the threat commander or leader analyzes conditions and determines an acceptable risk for mission success. The primary actions of a dispersed attack tactic create conditions to mass selective threat combat power on key systems of an enemy force combat system.

To achieve successful mission results, dispersed attacks recur at times and locations selected by the threat to continually disrupt and degrade the enemy. The intention of recurring offensive actions is to defeat the enemy's will and resolve to continue operations in the threat's area of responsibility (AOR).[1] Dispersed attacks rely on significant information warfare (INFOWAR) capabilities while using dispersion of threat forces to improve survivability and permit tactical offensive actions, even if overmatched by enemy precision standoff weapons and acquisition systems.

Dispersed Attack

The dispersed attack is typically a coordinated group of cell or unit actions conducted from multiple directions. The threat applies various capabilities through timed sequential, parallel, and/or simultaneous actions. The integrated actions of a dispersed attack are typically accomplished with threat combat power equivalent to a brigade tactical group or higher echelon headquarters task organization.[2] The attacks often target multiple objectives simultaneously, and threat actors adapt to tactical opportunities in time and locations to attack throughout the threat AOR. Dispersed attacks are conducted in order to—

- Focus on incremental defeat and/or destruction of enemy combat power by destroying or degrading key components of enemy combat systems, such as command and control (C2), logistics, and/or critical single-point-of-failure nodes in systems;
- Use deception and other elements of INFOWAR to degrade the enemy's situational understanding and ability to target threat formations;
- Fix and/or isolate selective enemy combat power;
- Employ small decentralized or independent subordinate forces;
- Concentrate capabilities with rapid movement, infiltration, and/or maneuver from dispersed locations;
- Mass combat power at a coordinated time and location;
- Conduct continuous sequential, parallel, and/or simultaneous attacks in time and at multiple locations; and
- Disperse threat combat power quickly after tactical engagements to preserve threat capabilities.

The offensive concept in this tactical vignette is to employ insurgent cells and affiliated units or organizations as enabling forces in several disruption zones. Actions include reconnaissance, intelligence, surveillance, and target acquisition (RISTA) in support of the mission order. Other actions disrupt the operations of enemy units, degrade effects of enemy combat support and combat service support systems, and target and neutralize or destroy critical systems in the enemy formations and defensive positions. The threat conducts RISTA at the tactical echelon and integrates RISTA from a higher headquarters in its AOR and zone of reconnaissance responsibility.[3] An exploitation force conducts the decisive action.

Selecting the appropriate components of the enemy's combat system to destroy or degrade is one of several initial decisions in planning the dispersed attack. For example, a high value target (HVT) would be an enemy force dependent on one geographical point for all or most of its logistics support and reinforcement.[4] Disrupting this activity at a critical time can support tactical decisions at other points in the AOR or may create opportunities to continue attacks on the enemy. In another example, an enemy force conducting stability operations could be disrupted with only threat indirect fires. A normal consideration is targeting enemy personnel in order to cause mass casualties that can delay or halt an enemy operation and potentially degrade enemy morale.

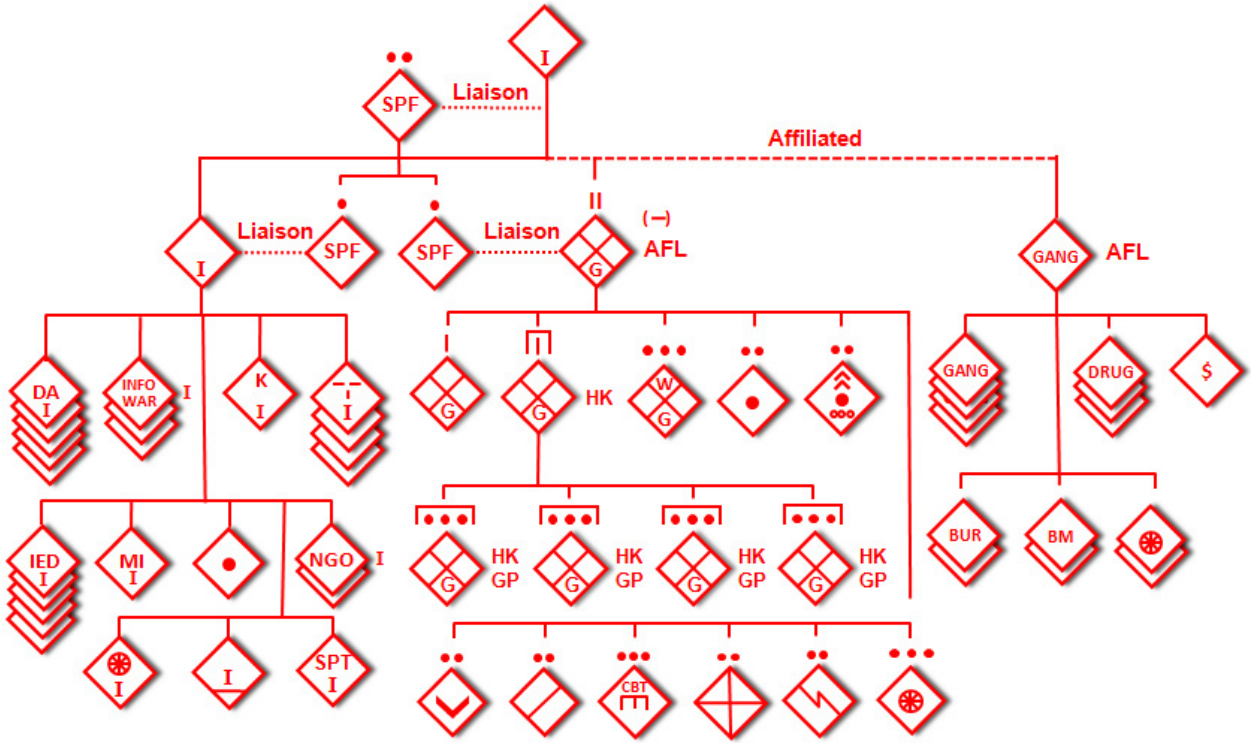


Figure 1. Task-organized insurgent organization with affiliations

Tactical Vignette Overview

The insurgent leader of the higher insurgent organization in this vignette has full use of multifunctional direct action and other functional cells within his local insurgent organization, and has affiliated actions with the dominant criminal organization that operates along the major motor transportation routes.[5] He has coordinated limited support with the regional guerrilla battalion, but recognizes that its support is conditional on mutual benefit to guerrilla actions in the region and the surrounding mountainous terrain.

The insurgent leader identifies critical tasks of his current mission:

- Destroy the recent enemy occupation of agrarian areas along the fertile river complex;
- Destroy enemy forces near the urban-center forward operating base to prevent interdiction of threat logistics and proxy support to his AOR from across the international boundary;
- Destroy enemy battalion command and control, and
- Defeat enemy stability actions with the local populace and civilian governmental activities.[6]

Recent fighting reduced enemy units—local activated reservists and mobilized militia—into a primarily defensive posture with local combat patrols in the city. However, enemy patrolling in the farming areas along the river and manning of combat outposts at key intersections along the main motor routes. Enemy mobility is by armored wheeled vehicles, with few other wheeled vehicle systems remaining operational. Cargo vehicles are often used to move enemy units.

Enemy forces in the city are committed to sustaining the regime. Actions along the river trace and farmlands are usually small-unit close-quarter firefights of short duration. Fighting in the urban areas continues to be house to house, with

extensive use of fortified buildings, complex battle positions, and tunnel systems. Improvised explosive devices, armed demolitions, and other military-grade mines are a norm throughout the fields and urban neighborhoods. Combat has been bitter, and reports indicate that the enemy has been summarily killing any insurgents who attempt to surrender. Threat use of mortars has been effective in the rural farming areas, supplemented by limited artillery, rocket launcher, and heavy-mortar fires from guerrilla systems positioned in the surrounding high ground outside of the city.

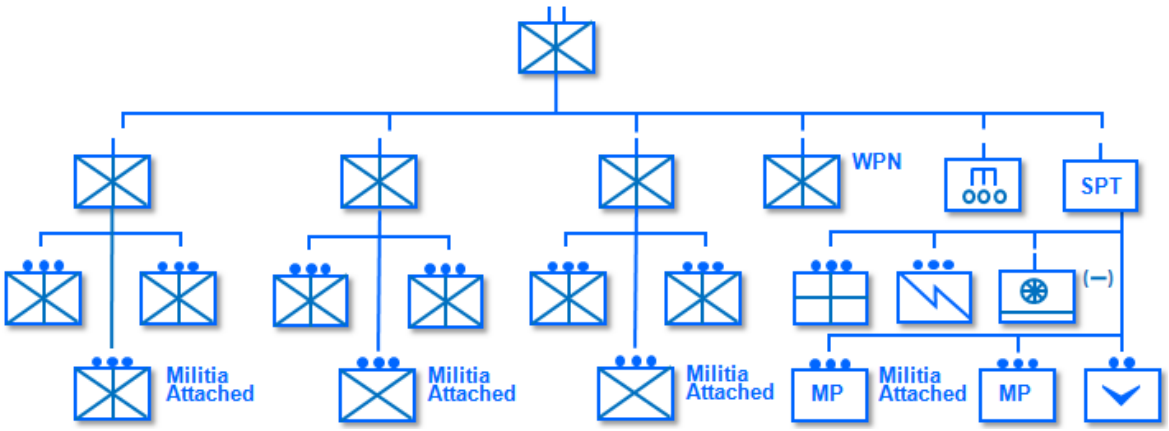


Figure 2. Insurgent estimate of enemy task organization

Enemy rules of engagement restrict its use of indirect fires or air support in urban areas for any reason but exceptional situations. INFOWAR is a key complement to the insurgents' tactical fight and promotes an effective message of insurgency righteousness to a local, regional, and global media community. A segment of the civilian population appears to be aligning more with the enemy forces than with the insurgency based on the continuous fighting and area mayhem; however, willing or coerced civilians remain a source for reporting enemy movements to insurgent cells and criminal teams inside and outside of the city.

The enemy battalion command post (CP) and support area are located in the urban center along the main north-south route. Two platoons near the city center may be the quick reaction force or a reserve. The main roadways of the north-south axes on each side of the river are under nominal government control, but insurgent ambushes have isolated the city from any significant enemy support via ground movement or maneuver. Enemy aerial logistics support is minimal based on aircraft losses due to insurgent integrated air defenses and effective all-arms air defenses by cells and units.

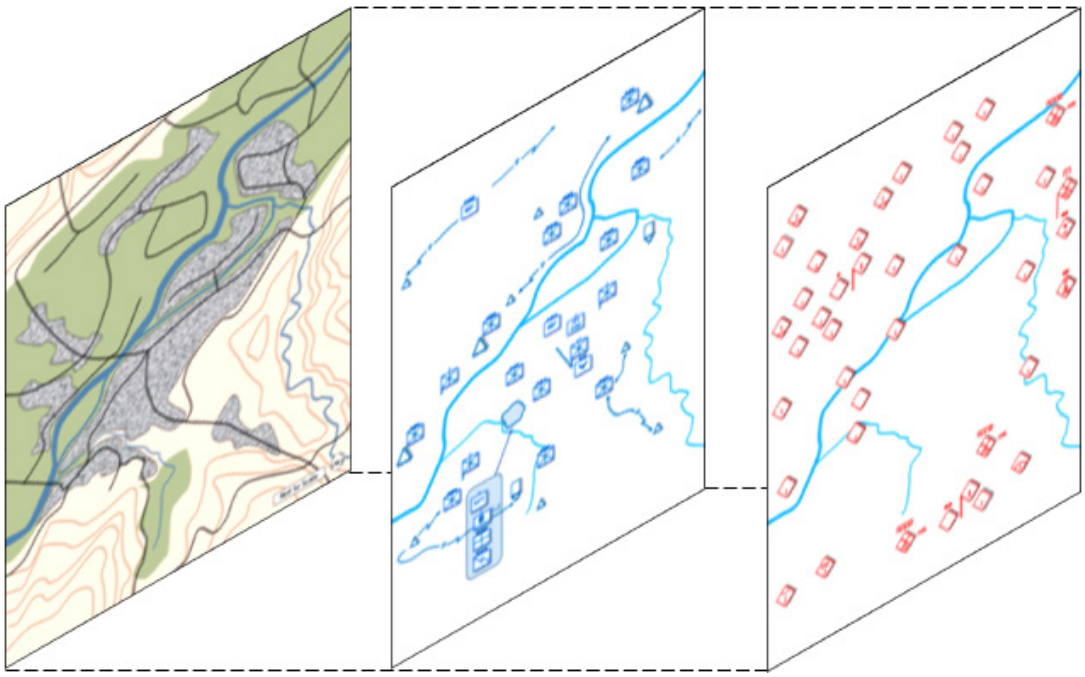


Figure 3. Terrain appreciation, enemy dispositions, and initial array of insurgent organization with affiliations

The river is a significant east-west movement restriction, and also limits some movements in north-south axes. Two enemy combat outposts west of the river are under the C2 of one company and cannot mutually support each other. Militia military police conduct mounted patrolling on the northern highway. East of the river, two companies are deployed by platoons to secure the main motor routes to the north, east, and south, and cannot mutually support each other.

The insurgent leader assesses his current dispositions and how to use the rural and urban terrain to his best tactical advantage. Given the insurgent organization sustains its dispersed attacks, the insurgent leader is confident in the ultimate destruction of enemy forces in his AOR and renewed support of the local population.

The insurgent leader at the higher insurgent organization emplaces and supports several disruptions zones in the AOR to focus his local insurgent organization mission, and coordinates actions of the affiliated criminal network in the urban areas and guerrilla capabilities in the eastern mountainous area. The threat continues its point-attacks throughout the AOR with direct fires, indirect fires, and improvised explosive devices. Each disruption zone has enemy forces and locations identified for decentralized disruptive threat actions that support the insurgent leader's mission intent.

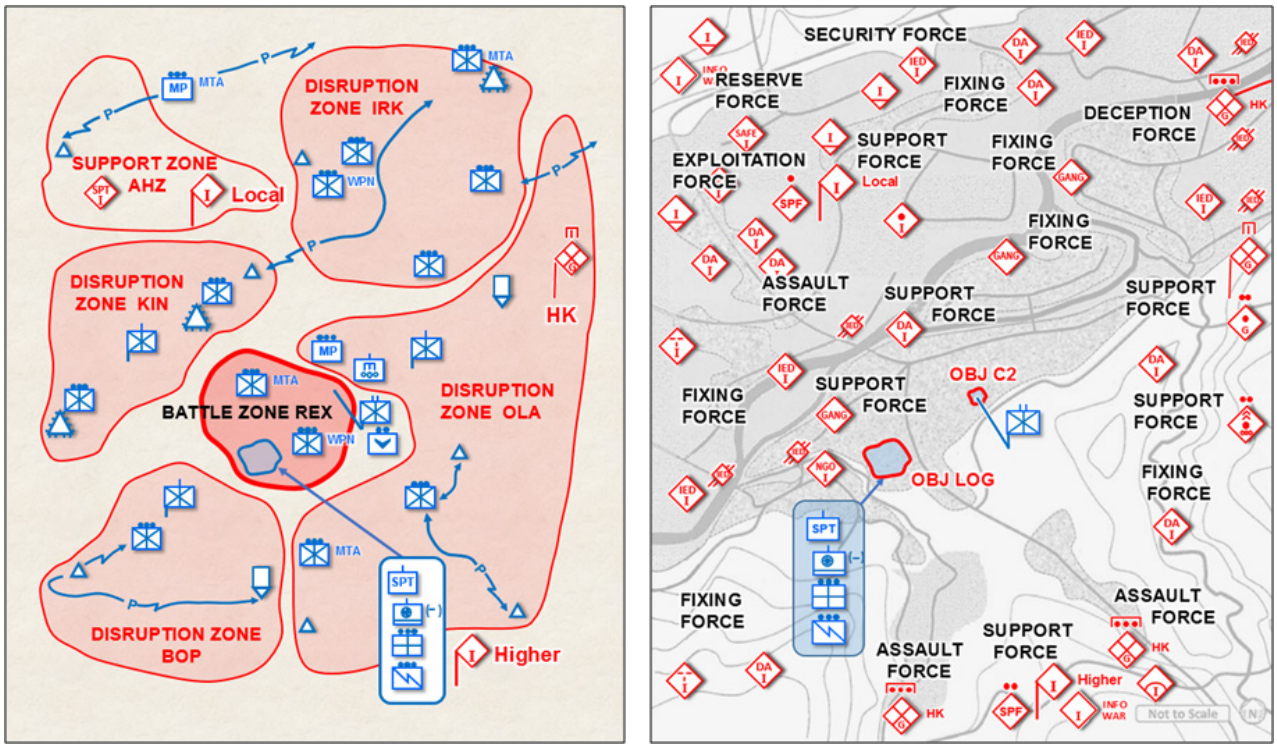


Figure 4. Insurgent zones planning sketch and initial insurgent forces array

The insurgent organization comprises insurgent cells with varied capabilities in its current task organization. Guerrilla units and criminal organizations affiliated with the insurgent organization provide additional capabilities particularly useful in the surrounding countryside and urban areas. The criminal organization operates in primarily the urban neighborhoods and center of the city, and reports any observations of enemy activities, particularly any changes within the support area, routines of the motorized platoon near the center of the city, and actions of the nearby weapons platoon. The hunter/killer guerrilla company from the guerrilla battalion is ready in its mountainous area sanctuaries to the east of the city, and has reconnaissance elements along its axes of attack observing enemy dismounted and mounted patrols.

The progressive success of insurgent disruption activities to disrupt, fix, and/or isolate designated enemy forces will set conditions for more aggressive combat action. Once tactical conditions indicate that decisive actions can be achieved in the battle zone, the insurgent leader will order a transition to exploitation. In this mission, the exploitation force is primarily insurgent cells of the local insurgent organization with urban support from the criminal network. The guerrillas will support from outside the city in a series of assaults and establish a group of blocking positions. The visible presence of insurgents in victory is the coordinated expectation for INFOWAR perception management effects.

A dispersed attack uses control measures such as objectives, attack zones, and boundaries, and may use additional measures when necessary to coordinate insurgency actions. Areas identified for insurgent missions may be oriented at point targets, and are often noncontiguous to other insurgent mission task areas. The insurgent leader remains watchful for tactical opportunities that might emerge unexpectedly, and encourages subordinate leaders to use initiative in order to achieve mission objectives.

Conditions favorable to execute dispersed attacks can be created by the threat or may appear as opportune factors in the AOR. The threat can influence creating favorable conditions with actions such as:

- Destroying enemy ground reconnaissance and counterreconnaissance;
- Deceiving enemy imagery and signals sensors;
- Creating enemy uncertainty of threat air defense environment;
- Controlling or coercing relevant civilian population to prevent support to the enemy;
- Optimizing use of complex terrain and relevant population for shielding and/or sanctuary;
- Denying enemy situational awareness and understanding of threat tactical capabilities and intentions; and
- Promoting insurgency actions and successes via INFOWAR and social media.

Functional Organization for a Dispersed Attack

A dispersed attack employs various types of functional forces. The insurgent leader assigns subordinate cells, units, and organizations with functional designations that correspond to their assigned roles and tasks. The two general functional types of forces with the insurgent organization are enabling forces and action forces.

Enabling Forces

Various types of *enabling forces* are charged with creating the conditions that allow the action force the ability to operate.[7] See figure 5 to visualize several of the continuous, sequential, and/or simultaneous enabling actions in this dispersed attack. These enabling actions precede additional enablers of fixing and/or isolation actions to set the conditions for exploitation forces to attack and destroy the enemy and seize objectives.

In order to create conditions for the action force to succeed, the enabling force may be required to operate at a high degree of risk and may sustain substantial casualties. However, an enabling force may not even make contact with the enemy, but instead conduct actions such as a demonstration to distract or disrupt. Functional titles for disruption forces can include:

- Disruption force;
- Security force;
- Deception force;
- Fixing force;
- Assault force;
- Support force; and/or
- Reserve force.

In this tactical vignette, multiple enabling actions disrupt the enemy forces throughout the AOR in the assigned disruption zones. Primary enabling actions are to provide security and support to the threat mission, and to deceive, fix, assault, defeat, or destroy designated enemy forces and capabilities.

Exploitation Forces

Exploitation Force. The most common type of action force in a dispersed attack is the *exploitation force*. Such a force must be able, through its capabilities or positioning relative to the enemy, of destroying the target of the attack. In some situations, the exploitation force could accomplish the ultimate objective with only fires. Support by special-purpose forces (SPF) liaison teams provides the RISTA, communications, and fires support for long-range or precision fires when HVTs are identified for attack. Dispersed attacks can use multiple exploitation forces separated in time and location.

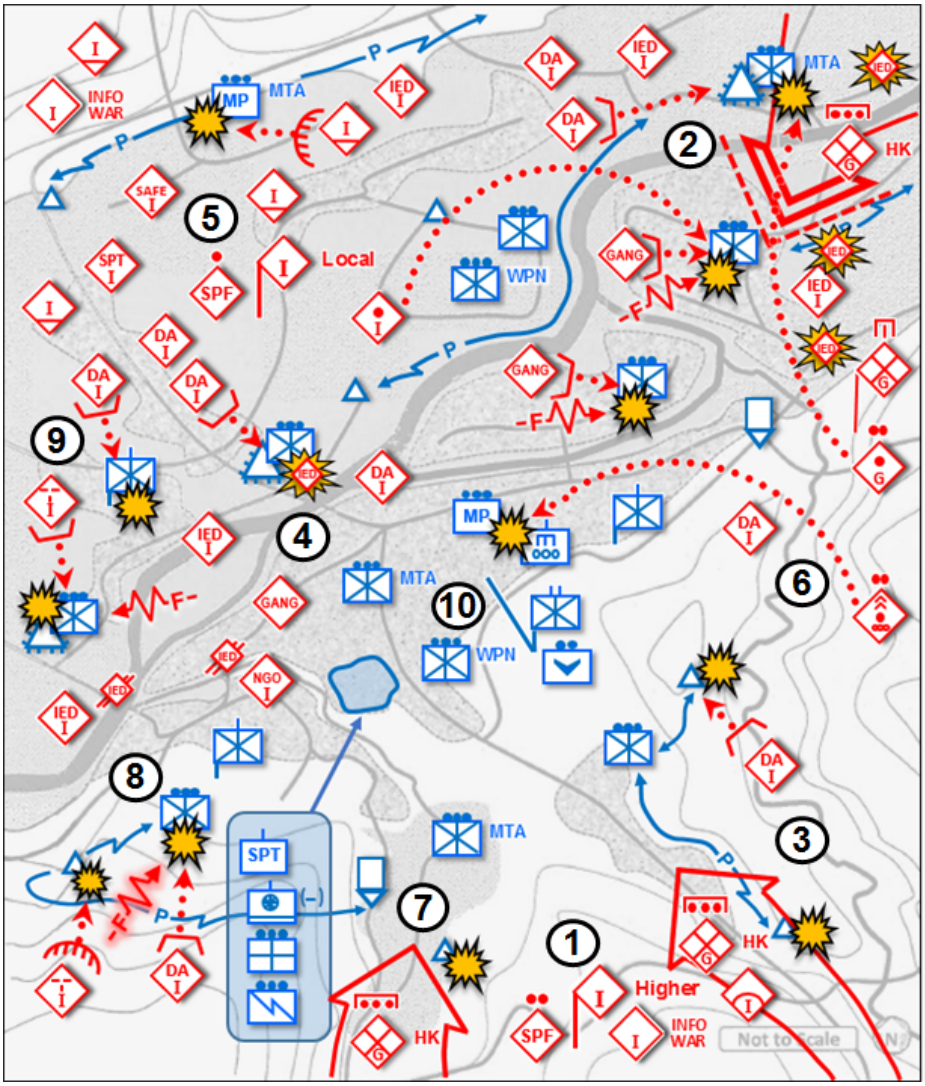
In this tactical vignette, the exploitation force is comprised of insurgent direct action cells supported by criminal teams in the urban area and guerrilla units in blocking positions. The insurgent leader employs multiple enabling forces prior to

and during the exploitation force attack. See figures 5–7 for a tactical vignette series of progressive enabling actions followed by an order for the exploitation force to attack. Figure 7 illustrates the insurgent exploitation force attack.

Disruption Forces (Enabling Forces) in a Dispersed Attack

Reconnaissance and counterreconnaissance actions are continuous throughout the threat AOR provide situational understanding on the current disposition and composition of enemy forces and any shift in targets and/or critical systems in the enemy dispositions. Initial disruption forces coordinate with fixing forces and assault forces for battle handover and sustained contact with enemy forces.

Threat security forces provide early warning and protection prior to and during the attack. Affiliated units provide timely information and intelligence, and conduct actions against enemy security forces. Threat initial priorities of effort in fires, maneuver, and deception efforts convince the enemy to focus its main effort in the north—an area other than the planned threat main attack by the exploitation force.



1. **SUPPORT FORCE** — INFOWAR by higher insurgent organization expands effective perception management campaign
2. **DECEPTION FORCE** — Assaults, IEDs, and indirect fires indicate main effort from the north
3. **ASSAULT FORCE** — Assaults disrupt enemy ground maneuver ISR from south
4. **SUPPORT FORCE** — Criminal affiliates report status of enemy COP at bridge and probable reserve southeast of bridge
5. **SECURITY FORCE** — Discrete attacks/ambushes remain limited in number in northwest as part of the deception story
6. **SUPPORT FORCE** — MRL fires disrupt enemy CS
7. **ASSAULT FORCE** — Assaults continue disruption actions from south
8. **FIXING FORCE** — Assaults/ambushes fix enemy
9. **FIXING FORCE** — Attacks by fire and sniping disrupt/fix enemy
10. **SUPPORT FORCE** — Insurgent actors (NGO) report on actions in enemy support area

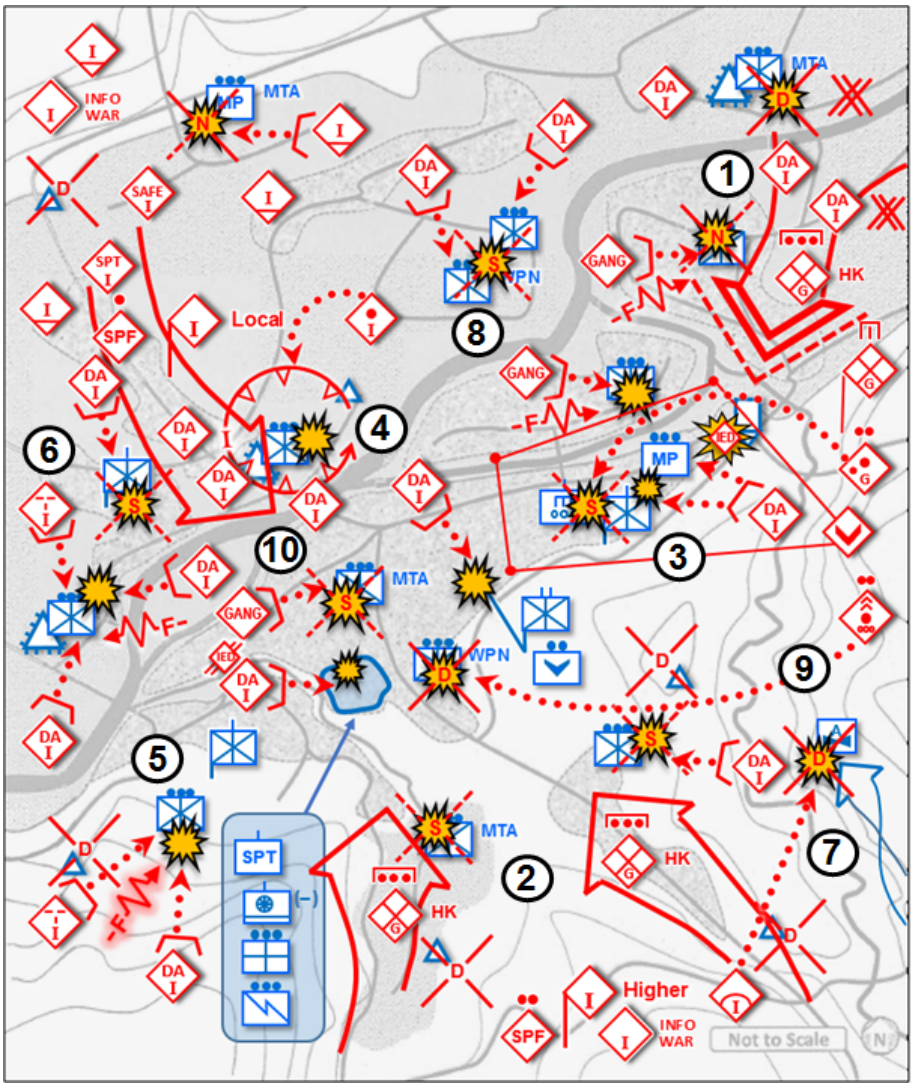
Figure 5. Enabling forces and disruption actions in a dispersed attack (1 of 3)

SPF units conduct direct action support and coordination with irregular forces. Guerrilla units and/or insurgent cells ambush or attack enemy positions or capabilities with direct and indirect fires. Criminal organizations attack enemy facilities and seize commodities for profiteering on local black markets. Other SPF direct actions disrupt, suppress, or neutralize enemy forces in the depth of the AOR. RISTA disruption forces continue surveillance and report on HVTs, disrupt enemy force logistics and movements, and prepare to report damage assessment on HVTs after an attack. Additional significant actions by enabling forces can include actions to:

- Destroy, neutralize, or suppress enemy force reconnaissance and counterreconnaissance;
- Identify and report enemy forces disposition and composition;
- Disrupt enemy forces movement with integrated fires and integrated air defense systems, maneuver, countermobility, and information warfare measures;
- Report information and intelligence updates on enemy forces in the AOR;
- Acquire, target, and attack HVTs at designated times and locations;
- Fix and/or isolate designated enemy forces;
- Ambush to disrupt or destroy critical enemy combat support and combat service support; and
- Attack to suppress or neutralize enemy forces C2 and sustainment with direct and indirect actions, and long-range and precision fires.

Fixing and Assault Forces (Enabling Forces) in a Dispersed Attack

Successful fixing and assault forces set the conditions for the decisive action as the enabling actions continue their assigned functions. Once these enabling forces have accomplished their mission tasks, the primary action shifts to an exploitation force that penetrates or infiltrates through the enemy defenses and attacks to destroy enemy forces and seize objectives.



1 DECEPTION FORCE
Deception of main effort in north causes enemy to shift forces to northeast urban area

2 ASSAULT FORCE
Guerrilla forces attack north toward urban center

3 SUPPORT FORCE
UAV tracks enemy reinforcements for direct/indirect fires and monitors enemy CP actions

4 ISOLATION FORCE
Assaults/indirect fires isolate enemy COP; insurgents secure bridge and attack objectives

5 FIXING FORCE
Attacks fix enemy in south

6 FIXING FORCE
Attacks fix enemy north of river

7 SUPPORT FORCE
Integrated air defense identifies in-bound aviation for destruction

8 ASSAULT FORCE
Direct action forces and criminals fix/suppress enemy in positions

9 SUPPORT FORCE
MRL fires destroy heavy weapons in urban defensive position

10 EXPLOITATION FORCE
Insurgents mass combat power to assault enemy C2/support area

Figure 6. Enabling forces and continued disruption actions in a dispersed attack (2 of 3)

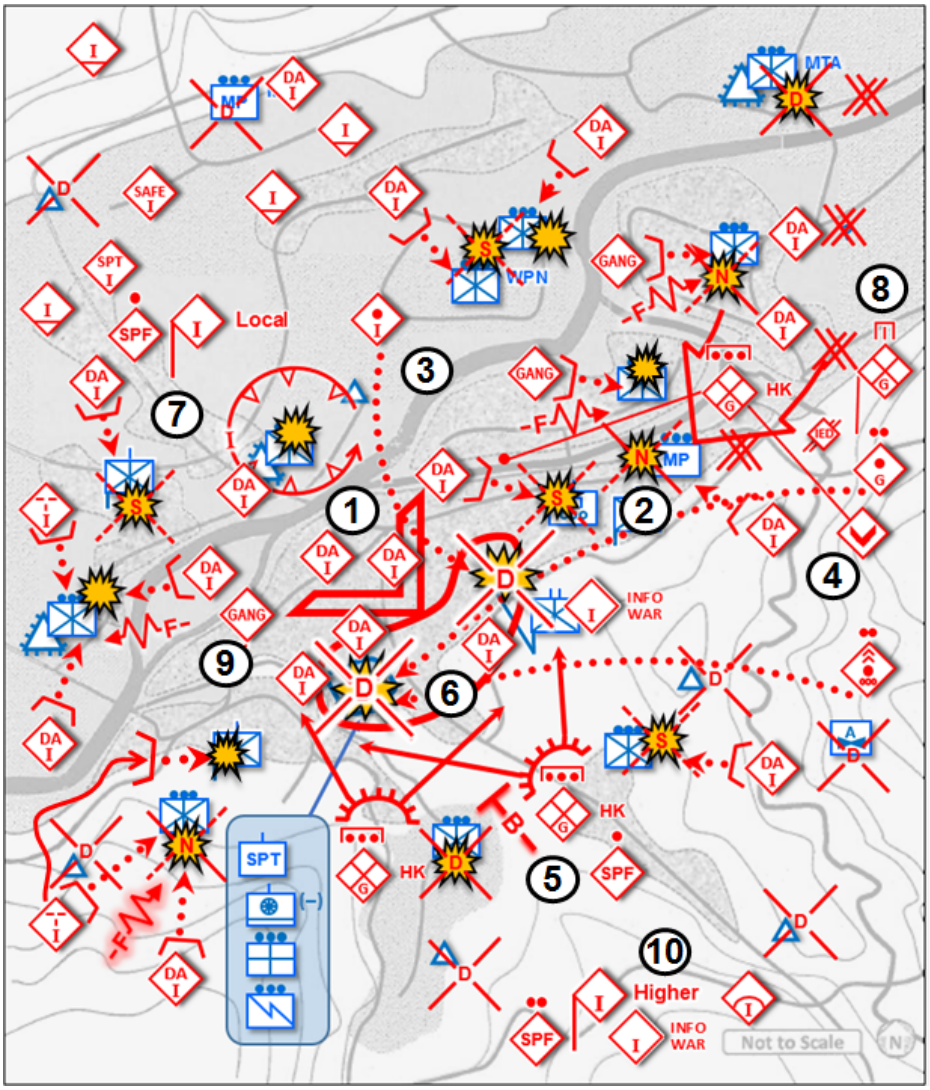
Fixing forces attack to prevent enemy forces from moving from a specific location for a designated time. These actions support other forces as they fix enemy forces in their respective zones and improve the local tactical situations and combat power for assault forces to attack in their zone. Fixing forces are also directed to isolate designated enemy

forces to further degrade enemy combat power. Fixing forces, in conjunction with SPF and RISTA capabilities in the disruption zones, orient and direct long-range area and/or precision fires to prevent enemy forces or reserves from effectively interdicting the main effort of the dispersed attack.

Assault forces in the battle zone may be directed to initially fix or isolate a specific enemy force in order for other threat forces to bypass or envelop designated enemy forces and sustain offensive momentum to mission follow-on objectives. Security forces continue mission tasks in the assault formations to provide early warning and protection.

Enabling tasks include but are not limited to:

- Disrupt enemy C2 communications;
- Defeat enemy aerial attacks and unmanned aircraft systems with integrated air defenses;
- Conduct INFOWAR actions to demoralize enemy forces;
- Seize assigned initial objectives;
- Facilitate passage and forward momentum of exploitation forces t; and
- Defeat enemy forces in assigned objectives; on order, continue attack; and
- Destroy or neutralize designated enemy forces and critical systems.



1 EXPLOITATION FORCE
Local insurgent cells assault toward enemy CP and support area

2 SUPPORT FORCE
Guerrilla artillery and MRL attack support area with observed fires by insurgents and SPF coordination

3 SUPPORT FORCE
Insurgent indirect fires attack BN CP with observed fires

4 SUPPORT FORCE
Local insurgent organization UAV continues to track enemy attempt to break contact in city

5 FIXING FORCE
Guerrilla forces occupy blocking positions to destroy any enemy attempting to withdraw east

6 EXPLOITATION FORCE
Insurgents assault objective/seize enemy support area/CP area

7 SUPPORT/RESERVE FORCES
Local insurgent organization secures OBJ, reorganizes/consolidates with affiliate 8 guerrilla unit and local criminal organization 9

10 SUPPORT FORCE
Higher insurgent organization uses INFOWAR to exploit tactical success and affiliation with guerrilla BN and regional criminal network

Figure 7. Exploitation and decisive actions in a dispersed attack (3 of 3)

The dispersed attack main effort—the exploitation force—may require assault forces to seize specified areas in order to support the exploitation attack. For example, in breaching or infiltrating enemy defenses at designated points, assault forces secure designated points or areas, continue forward momentum, and facilitate passage of the exploitation force

to objectives. Securing an area may require assault forces to block or fix enemy forces attempting to disrupt the sustained momentum of the dispersed attack.

Exploitation Forces (Action Forces) in a Dispersed Attack

Objectives for the exploitation force are destruction of the sustainment ability to the enemy force and destruction of enemy force C2. Other threat forces continue to interrupt and limit enemy response to the exploitation force and continue to disrupt remaining enemy forces in the AOR. Significant actions of exploitation forces include but are not limited to:

- Penetrate through enemy defenses and seize initial objectives;
- Exploit to destroy the enemy at intermediate objectives;
- Destroy enemy forces in zone and seize objectives;
- Continue attack to defeat and/or destroy other enemy capabilities in the AOR.

In this tactical vignette, exploitation forces penetrated enemy defenses and attacked to destroy the sustainment area and C2 of the enemy battalion. The insurgent leader accomplished his mission to destroy enemy occupation of the rural river valley, destroy enemy forces in the city, and regain control of the relevant population and regional resources for the insurgency.

Training Implications

This tactical vignette illustrates and describes key actions in a series and group of successful dispersed attacks. The insurgent leader used affiliated irregular forces and SPF liaison support in disruption zones to disorient the enemy commander with multiple actions and to counter enemy stability initiatives. The insurgent leader set tactical conditions favorable to threat success. He recognized that expert knowledge of the terrain, relevant population, tactical experiences of the irregular forces, and SPF familiarity with the population and culture were significant combat multipliers in shaping the many actions and options for future offensive operations. Timing of execution—sequential, parallel, and simultaneous—was critical to effectively employing threat combat power throughout the disruption zones and battle zone. Support cells and caches concealed throughout the urban and rural terrain in a general support zone provisioned continuous and responsive logistics actions.

Using multiple deception techniques and other INFOWAR capabilities, the insurgent organization masked the strengths of its offensive preparations and convinced the enemy commander that the threat main effort would occur in what was actually a supporting effort and deception. This deception complemented the ability to mass combat power in both time and location to surprise the enemy commander when and where the threat main effort would occur. Dispersed attacks allowed for rapid exploitation and destruction of the enemy.

The insurgent leader accomplished his ongoing mission as part of the insurgency. He forecasted the destruction of the enemy and reestablishment of insurgent control of the population and province. He conducted offensive fires and maneuver by directing where and when key actions would occur to create and exploit vulnerabilities in the enemy defenses. Dispersed attacks disrupted the enemy's combat systems, with particular attention against designated systems critical to enemy command and control. Targeting enemy combat support and combat service support was similarly critical to degrading enemy capabilities. Without the sustainment and support of these systems, enemy forces in direct contact with insurgent forces became vulnerable to defeat or destruction.

The higher insurgent organization used its combined-arms task organization and affiliations—and support from its higher headquarters and liaison support from SPF—to optimize the combat systems of its cells, units, and subordinate organizations. Tactical actions for fires, with augmentation from higher headquarters and SPF liaison, provided an integrated approach for massed fires and effective maneuver of insurgent ground forces. Task-organized capabilities with the insurgent forces included but were not limited to:

- Designated mortars placed in hide positions throughout the AOR near pre-registered firing positions;
- Designated cannon, rocket artillery, and heavy mortars dispersed in depth in the surrounding countryside and mountainous area;
- Air defense systems integrated in urban and rural areas for coverage throughout the AOR;
- Mobility and countermobility capabilities for engineer-like support throughout the AOR;

- Selective use of guerrilla hunter-killer teams for direct action assaults and ambushes;
- Coordination for decentralized conduct of criminal activities to disrupt enemy stability activities;
- Unmanned aerial vehicles for reconnaissance and surveillance in conjunction with C2 and fires coordination by ground and aerial maneuver forces;
- Liaison support from SPF for RISTA, C2, and fires;
- Electronic warfare and other INFOWAR capabilities support for deception, target acquisition and tracking, electronic attack, satellite-link jamming or disruption, and spoofing of enemy unmanned aircraft and global positioning systems; and
- Cooperative relationships with the indigenous civilian population and key civilian leaders.

The US Army commander, trainer, or educator responsible for training, professional education, and leader development venues must sustain expert understanding of real-world threat capabilities witnessed in recent or ongoing persistent conflicts. An opposing force (OPFOR)—as one of many conditions in Army learning events—provides the complexity of real-world threat capabilities to stress the unit commander in demonstrating US Soldier, leader, and unit proficiency.[8] An opposing force uses traditional and adaptive threat tactics and techniques to create or take advantage of potential vulnerabilities of US armed forces and supporting organizations in operational missions. The ability to represent or replicate many of these actual threat capabilities as an OPFOR in current US Army training—live, constructive, virtual, and in conjunction with gaming simulations—provides the required demanding operational environments and threats as realistic, robust, and relevant challenges in order to achieve US Army standards for sustained readiness.

Notes

[1] Headquarters, Department of the Army. Training Circular 7-100.2, Opposing Force Tactics. TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. 9 December 2011. Paras 3-74–3-76.

[2] Headquarters, Department of the Army. Training Circular 7-100.2, Opposing Force Tactics. TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. 9 December 2011. Paras 2-19 and 2-20. See also, Headquarters, Department of the Army. Training Circular 7-100.3, Irregular Opposing Forces. TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. January 2014. Paras 2-46 and 2-51.

[3] Headquarters, Department of the Army. Training Circular 7-100.2, Opposing Force Tactics. TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. 9 December 2011. Paras 8-38–3-39.

[4] Headquarters, Department of the Army. Training Circular 7-100.2, Opposing Force Tactics. TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. 9 December 2011. Paras 7-18 and 9-96.

[5] Headquarters, Department of the Army. Training Circular 7-100.3, Irregular Opposing Forces. TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. January 2014. Chs 2, 3, and 4.

[6] Headquarters, Department of the Army. Training Circular 7-100.2, Opposing Force Tactics. TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. 9 December 2011. Paras 2-32–2-35.

[7] Headquarters, Department of the Army. Training Circular 7-100.2, Opposing Force Tactics. TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. 9 December 2011. Paras 2-54–2-55.

[8] Headquarters, Department of the Army. Army Regulation 350-2, Operational Environment and Opposing Force Program. 19 June 2015. Para 1-5b. (See also: US Army, TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. Decisive Action Training Environment. Version 3.0. July 2017.

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 DIR & DATE	DAC Angela Williams	angela.m.williams298.civ@mail.mil -7929
Intel OPS Coordinator	DAC Nicole Bier	nicole.n.bier.civ@mail.mil DSN:552 -7907
UK LO to ACE-TI	WO2 Danny Evans	daniel.j.evans92.fm@mail.mil -7994
Threats Officer	LTC Bryce Frederickson	bryce.e.frederickson.mil@mail.mil -7930
Threats Officer	MAJ James Andersen	james.r.andersen20.mil@mail.mil -7952
Threats Officer	MAJ EJ Kesselring	emil.j.kesselring.mil@mail.mil -7898
Threats Officer	CPT Frank Reyes	francisco.j.reyes6.mil@mail.mil -7991
Threat Models	DAC Jerry England	jerry.j.england.civ@mail.mil -7934
Threat Tactics Course	DAC Kris Lechowicz	kristin.d.lechowicz.civ@mail.mil -7922
Threat Doctrine	DAC Dr. Jon H. Moilanen	jon.h.moilanen.civ@mail.mil -7928
Training-Edu-Ldr Dev	DAC Walt Williams	walter.l.williams112.civ@mail.mil -7923
Threat Analysis	CGI Brian Allen	brian.d.allen44.ctr@mail.mil -7948
Threat Analysis	IDSI Dr. Jim Bird	james.r.bird.ctr@mail.mil -7919
Threat Analysis	BMA Rick Burns	richard.b.burns4.ctr@mail.mil -7987
Worldwide Eqmt Guide	BMA John Cantin	john.m.cantin.ctr@mail.mil -7899
Thr Analysis & Editing	CGI Laura Deatrick	laura.m.deatrick.ctr@mail.mil -7925
Threat Analysis	CGI Jay Hunt	james.d.hunt50.ctr@mail.mil -7960
ACE-TI LO to MCTP	BMA Pat Madden	patrick.m.madden16.ctr@mail.mil -7997
Threat Analysis	CGI Mike Marsh	michael.g.marsh3.ctr@mail.mil -7897
Threat Analysis	CGI Brad Marvel	bradley.a.marvel.ctr@mail.mil -5963
Threat Analysis	CGI Dave Pendleton	henry.d.pendleton.ctr@mail.mil -7946
ACE-TI LO to JRTC/JMRC	CGI Mike Spight	michael.g.spight.ctr@mail.mil -7974
Threat Analysis	CGI Jamie Stevenson	james.e.stevenson3.ctr@mail.mil -7995
Threat Analysis	CGI Wayne Sylvester	vernon.w.sylvester.ctr@mail.mil -7939
ACE-TI LO to NTC	ThreatTec Marc Williams	james.m.williams257.ctr@mail.mil -7943