Red Diamond
Threats Newsletter

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

Fort Leavenworth, KS **Volume 8, Issue 08** **August 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 LTC Bryce Frederickson, TRADOC G-2 ACE Threats Integration

TRADOC G-2 ACE Threats Integration has been actively teaching functional analysis as a method for planning and developing opposing force (OPFOR) courses of action. The core concept is that, while every battle is unique, certain functions continue to be performed by the enemy to reach mission accomplishment. Functional analysis determines threat objectives, the battlefield functions required, and the capabilities available for performing each function. There are four main functions the OPFOR will use to complete its goals and objectives: action, enabling, fixing, and security.

There are several advantages to using this methodology: 1) it forces the staff to learn and understand tactics, 2) it reduces the ability of the enemy to deceive analysts, and 3) it works across the range of military operations.

Functional analysis and functional tactics are currently discussed in depth in ATP 2-01.3, *Intelligence Preparation of the Battlefield*, Appendix B. However, in the current update to ATP 2-01.3, there is a potential that functional analysis will move from an appendix to the main body. This analysis methodology also continues to be taught during the Threat Tactics Course, in both the resident and mobile training team courses. Additionally, functional analysis was taught to the recent graduates of the Command and General Staff College during the Brigade S2 course in June 2017. Intelligence professionals that have studied functional analysis in order to understand battlefield tactics will then be able to make more accurate tactical predictions to their commanders.

RED DIAMOND TOPICS OF INTEREST

by TRADOC G-2 ACE Threats Integration

This issue of *Red Diamond* opens with part two of an article series on the Russian Snow Dome. Starting in the days of the Tsarist Empire, Russian Ground Forces were built around their artillery. This doctrine extended throughout the Cold War, explaining the consistent investment the Red Army made in its artillery corps. This article reviews several Russian artillery systems and how they are typically used by the Russian military.

Integrated attack is a tactic that applies massed effects and rapid actions of threat forces to achieve of a mission objective. Aspects of threat brigade-echelon capabilities observed in recent and current tactical real-world operations include substantial integrated air defense, indirect fires, electronic warfare, and other combat power enablers in conjunction with ground and aerial maneuver. These types of capabilities are typically present in the brigade tactical group (BTG) task organization. An article and associated vignette describe significant actions of an integrated attack conducted by an opposing force (OPFOR) in US Army learning events.

In the days leading up to Ramadan, Philippine President Rodrigo Duterte and selected members of his cabinet traveled to Russia on a diplomatic mission. Only days later, a storm of violence erupted in Marawi City, on President Duterte's home island of Mindanao. There, on 23 May 2017, elements of the Armed Forces of the Philippines and Philippine National Police raided a safe house to arrest an Islamist extremist and take him into federal custody. The authorities got more than they bargained for: a firefight erupted that ended in a standoff by nightfall, leaving three members of the government security force dead and eleven others wounded. The first article in a two-part series discusses the operational environment during this time, what led up to the raid, and the events that happened immediately afterward.

The purpose of the Decisive Action Training Environment (DATE) is to provide the US Army training community with a detailed description of the operational environments of five fictitious countries in the Caucasus region: Ariana, Atropia, Donovia, Gorgas, and Limaria. The DATE applies to all US Army units that participate in an Army or joint training exercise. This past July, the latest update to this document—DATE 3.0—was published, and includes many revisions, both substantial and minor. The final article in this issue of the *Red Diamond* highlights major changes made to this newest edition of the DATE.

by Brad Marvel, TRADOC G-2 ACE Threats Integration (CGI Federal CTR)

Russia's proxy war in the Crimea set alarm bells ringing throughout NATO and the US Department of Defense. Observers, analysts, and military professionals alike were shocked at how prevalent, and how decisive, Russian artillery was throughout the region.[1] At the time, the US Army was just beginning the process of divesting its stockpiles of dual-purpose improved cluster munition (DPICM) artillery munitions, apparently having forgotten the dramatic effects that simple overwhelming firepower can have in a peer or near-peer conflict.[2] Seeing the results of well-targeted DPICM and thermobaric rocket artillery on both hard and soft targets was a serious wake-up call that the US Army's capabilities had shifted, perhaps excessively, away from protection and firepower.[3] To observers whose perspective was shaped largely by many years of counter-insurgency operations, it appeared that the Russian-backed separatists had uncovered some sort of revolutionary way to employ their big cannons and rockets. To Cold War scholars, or to Cold Warriors themselves, however, there was more than a hint of familiarity to what they saw in the Crimea. What the Russian-backed separatists did there was a simple evolution of Russian and Soviet artillery doctrine predating the First World War.

Artillery the Russian (and Soviet) Way

Starting in the days of the Tsarist Empire, Russian Ground Forces were built around their artillery.[4] Artillery regiments of the Imperial Russian Army were given the best and brightest officers, along with first choice of equipment. The famed "Deep Battle" operational-level doctrine that helped the Red Army win the Great Patriotic War was, at its core, built around the "artillery offensive."[5] This doctrine extended throughout the Cold War, explaining the consistent investment the Red Army made in its artillery corps.[6] The Red Army envisioned land combat in World War III as a clash between large maneuver formations in Central Europe; its force structure supported this vision. Soviet forces were to move rapidly to positions of advantage; massed artillery, supported by effective targeting and mathematical analysis, would harass, disrupt, or destroy NATO armored formations long before they could close with Soviet maneuver units. Upon transitioning to the offensive, artillery was to become their decisive battlefield capability, shooting deep and moving quickly to support maneuver units as they attacked rear areas and utilizing a mixture of sensors and shooters referred to as the recon-fires complex.[7] Counterfire—and counter-counterfire—was heavily emphasized as the most critical component of the Soviet battle plan.[8]

Figure 1. Red Army 76.2mm field guns on the Eastern Front in the spring of 1945

This doctrine differed from Western (chiefly American and German) armies in a fundamental way. Instead of viewing artillery as fire support for fast-moving maneuver formations, maneuver formations became the exploitation force for openings created by massed artillery fire.[9] In other words, Russia viewed artillery, and not maneuver, as the decisive capability of the army.[10] This difference in perspective between East and West continued right through the end of the Cold War into present day. While the US Army heavily divested its artillery capabilities over the last 15 years, Russian Ground

Forces developed a number of new artillery systems, then fielded them in high densities throughout their force structure. The American battle plan of the future envisions semi-independent maneuver brigades closing with and destroying the enemy.[11] Conversely, Russian formations appear built to standoff, attrite, and defeat the enemy through massed artillery fire. This strategy was demonstrated repeatedly in the Crimea and Eastern Ukraine.

Field Artillery as a Component of the "Snow Dome"

Surface-to-surface fires are a key component of the tactical and operational area-denial suite of capabilities this series of articles refers to as the "Snow Dome." Artillery provides this capability, while surface-to-air fires interdict or deter threat airpower, and electronic warfare and cyber warfare elements interfere with threat sensors and networks. The Snow Dome concept essentially seeks to bring enemy maneuver forces into an artillery battle, where the superior weight of Russian artillery can decisively engage before the enemy can close with and engage Russian forces in close combat.

Contemporary Russian Artillery: An Overview

Russian Ground Forces utilize a variety of systems, with varying ranges, yields, and precision, to create something of a combined arms effect with their artillery. For example, Russian commanders prefer to use self-propelled, armored artillery in direct support of maneuver forces where the counterfire threat is highest, while preferring to use unarmored towed systems as reinforcing fires. The most destructive or powerful systems are paired with the best sensors to facilitate rapid targeting. Lightweight, mobile systems operate dispersed, allowing delivery of massed fires from unexpected directions—a key enabler of effective counterfire. Russian forces also commonly use their guns, particularly the heavy self-propelled guns, in direct fire roles.[12]

Figure 2. The 9A52-2 MRL is nearly twice the size of the American M270 MRLS[i]

One key difference between Russian and American systems is their weight and size. Russian systems do not need the same expeditionary capabilities of their American counterparts. Thus, practically all Russian systems in a given class are both heavier and bulkier than the equivalent American system. For artillery, this generally translates to greater range and better rate of fire due to due to larger munitions, longer barrels, and heavier gun breeches. However, it also increases sustainment requirements and, in some cases, reduces tactical mobility.[13]

The other key difference between Russian and American artillery systems is their density. For any given echelon, Russian units typically have three times the number of a given class of system. For example, a Russian motorized rifle brigade has two self-propelled howitzer battalions and a rocket battalion, as compared to an American brigade combat team's single howitzer battalion, which may or may not be self-propelled. The large number of available systems, coupled with the logistical support necessary to sustain these systems, enables many of the artillery tactics and techniques used by Russian commanders.

Towed Howitzers

Towed howitzers have been the backbone of field artillery throughout the industrial age. In recent years, however, Russia's towed systems have taken something of a backseat to self-propelled and rocket systems. This is due to two primary factors: first, the Russians' fear of counterfire led them to value the protection and mobility offered by self-propelled systems; second, the widespread mechanization/motorization of Russian Ground Forces made towed guns less well-suited to brigade-level formations. Nonetheless, Russia operates hundreds of towed systems, predominantly in its airborne units and as corps- or army-level reinforcing fires through artillery brigades.

---

[i] The generic Russian term for rocket artillery systems is "multiple-launch rocket (MRL)," while the US refers to its M270 rocket artillery system as a "multiple launch rocket system (MLRS)." This article uses "MRL" to refer to Russian rocket artillery systems and MLRS to refer to the American M270.

D-30/2A18 howitzer is a 122mm light howitzer. An old Soviet design, it is widely proliferated around the world. It currently equips Russian airborne artillery battalions and is used as a quick, lightweight reinforcing fire option for heavier units. Russian units regularly train to use the D-30 in a direct fire antitank role.

Figure 3. D-30 122mm light towed howitzer

2A36 and ***2A65 howitzers*** are both 152mm guns. Both date from the Soviet era; the 2A65 is somewhat newer. They are large and heavy; long-ranged and rapid-firing compared to their NATO counterparts. They can fire a variety of ammunition types, to include precision-guided munitions (PGMs). These heavy guns comprise the bulk of Russian firepower at echelons above division.[14]

Self-Propelled Guns and Mortars

Self-propelled guns (SPGs) are the mainstay of the contemporary Russian field artillery capability. They are used in every artillery role and are present in significant numbers in practically every formation.[15] Their most significant roles, however, are direct support to maneuver units and counter-battery. Brigade-level commanders typically have two battalions of SPGs, giving them the flexibility to employ one battalion in a direct support role and the other in a reinforcing or counter-battery role. Field artillery brigades also feature large numbers of SPGs that provide a fast-moving artillery capability, allowing the brigade to mass fire at decisive points on the battlefield.

Figure 4. The 2S1 SPG is the world's most widely proliferated self-propelled howitzer

2S1 self-propelled howitzer is the self-propelled version of the 2A18 122mm gun. It is fielded in large numbers all over the world, to include Russian Ground Forces. Despite a relative lack of firepower, Russian forces value the 2S1's excellent speed, mobility, and smaller logistical footprint.[16] Thanks to its mobility, it is often employed when the counterfire threat is high: in support of raids or other actions that require close contact with threat fires systems.[17] The 2S1 is currently being developed into an evolved system called the 2S34.

2S3/5/19 self-propelled howitzers are all 152mm SPGs. They are the heavy-hitters of the Russian mechanized force. They are roughly similar in appearance and function: the 2S3 dates from the late 1960s and the 2S19 from the late 1980s, with an equivalent increase in capability. These guns comprise most of the artillery battalions within mechanized and armored brigades as well as providing operational fires at the army level, and are used in every artillery role.[18] They employ a variety of 152mm munitions, from simple unguided high-explosive and cluster munitions, to PGMs, to non-lethal rounds such as smoke or electromagnetic jamming rounds.[19] The 2S19 produces a greater volume of fire and outranges the American M109A6, thanks largely to its longer barrel and heavier breech.[20] A new SPG, called the 2S35, is currently in the early stages of fielding.[21]

Figure 5. 2S19 SPG

Russian Ground Forces utilize a variety of self-propelled mortars (SPMs). Most Russian SPMs are considered to be in the "heavy" class of mortars by Western standards (e.g., a caliber around 120mm), exemplified by the widely proliferated **2S9 "Nona,"** and the recently fielded **2S31 "Vena."** Due to their short range, high angle-of-fire, high rate-of-fire, and highly destructive ammunition, they are best suited to providing direct support to maneuver units, in very close proximity to threat maneuver forces. While somewhat limited in ballistic performance, their role within the Russian artillery complex is very important: if the long guns and rockets are tied up firing deep, in the counterfire fight, or are otherwise unavailable, maneuver units can still count on effective, if somewhat less responsive, fire support from lightweight and mobile SPMs.

Multiple-Rocket Launchers (MRLs)

Russian rocket artillery received more attention than any other single type of system during the conflict in Crimea. Rocket systems are employed in concert with enhanced target acquisition (notably by drones and irregular forces) to devastating effect against a variety of target types. The Crimea was one of the few times that massed rocket fires were employed since WWII; each time, it seems, the military community is re-awakened to their destructive power.[22] Russia routinely employs rocket artillery at lower tactical levels, largely unconstrained by complex and time-consuming clearance-of-fire procedures or concern for collateral damage.[23] They are used as reinforcing fires, counterfire, and as the decisive component of artillery offensive action against exposed maneuver forces, as seen prominently in the Crimea and eastern Ukraine.[24]

Figure 6. BM-21 MRL

BM-21 is the most widely proliferated MRL in the world. It employs a lightweight 122mm rocket with a variety of different munition types (High Explosive, DPICM, radio frequency jamming). It is relatively light and tactically mobile, allowing it to keep pace with mechanized forces or move to positions of advantage quickly.

9P140 *and 9A52-2* are Russia's heavy MRLs, and the most powerful artillery pieces employed by Russian Ground Forces. They are similar in appearance and use the same munitions (227mm and 300mm rockets); the 9A52-2, however, is roughly twice the size of the 9P140 and thus has a much larger basic ammunition load. These systems are large, relatively slow, less tactically mobile, and have a large logistical footprint. However, the effect of their massed fires can be decisive, especially when targeted rapidly and accurately. They employ a variety of munition types to include uniquely destructive thermobaric rounds, satellite-guided fragmentary rounds, and antipersonnel or antitank mines. Both of these systems are scheduled for replacement by the **9A52-4 Tornado**, a lighter, more mobile system that employs the same rocket munitions.

Figure 7. 9P140 MRL

Surveillance and Targeting

While much attention—and rightly so—has been given to Russian Ground Forces' use of UAVs as targeting platforms for their artillery, UAVs are only one component of a network of sensors in the reconnaissance fires complex. Forward observers (FOs), usually operating in artillery reconnaissance sections, remain a critical enabler for Russian artillery at all echelons.[25] FOs can be assigned to virtually any unit and can be employed in a centralized manner (e.g., reporting to a fire direction cell) or decentralized (e.g., tied directly to a specific shooter). FOs direct both cannon and rocket fires. Some—particularly mounted FOs—employ digital data links to shooters, but many still utilize voice communications and analog (e.g., paper map) technology. Untrained observers in irregular forces can be tied into the sensor network, reporting through trained FOs, or can use commercial communications networks and technologies to call for fire.

Figure 8. The Orlan series of UAVs is widely proliferated and very capable

Russian unmanned aircraft targeting capabilities are expansive and growing.[26] Russian Ground Forces utilize some 20 different UAV types, with a variety of sizes and capabilities. UAVs are employed in much the same way as FOs: they are operated at relatively low tactical echelons (brigade/battalion) and are typically tied directly to a specific shooter, most often a rocket battalion. This enables rapid targeting, as the UAV operator can pass target data directly to the shooters, who can then fire with minimal clearance and authorization. Russian forces also make use of electronic and signal surveillance, satellite imagery, and cyber surveillance, passing targeting data down to shooters or retaining data to inform more centralized operations.

Russian Artillery Employment at the Brigade Level

The Russian brigade commander has three organic artillery battalions at his disposal. While their composition varies, a typical allocation is one light SPG (2S1) battalion, one heavy SPG (2S19) battalion, and one heavy rocket (9P140) battalion. In addition, the brigade commander can expect reinforcing fires from one of the field army's artillery brigades, likely a battery of towed heavy (2A65) howitzers. Russian techniques in the attack and defense center largely on how and when artillery is employed.

In the following example, a Russian brigade tactical group attacks an entrenched infantry brigade. The brigade commander establishes battalion-level detachments, called battalion tactical groups (BTGs), each consisting of a maneuver battalion, a field artillery battery, an air defense battery, and other task-organized forces. Each BTG is allocated a battery of SPGs in direct support; BTG commanders utilize them to suppress or destroy targets in support of the BTG. The brigade retains its rocket battalion, an SPG battery, and the reinforcing heavy towed howitzer battery, which are centrally controlled by the brigade commander.

This attack leverages artillery as the decisive battlefield capability. A combination of surveillance assets and maneuver forces detect, locate, and fix the elements of the enemy infantry brigade; artillery then harasses, neutralizes, or annihilates targets in accordance with the commander's priorities. Through a mix of massed and precision fires designed specifically to preclude close contact between maneuver forces, artillery enables maneuver units to penetrate into deep areas, then targets key assets to disrupt or degrade the enemy's response to the attack.

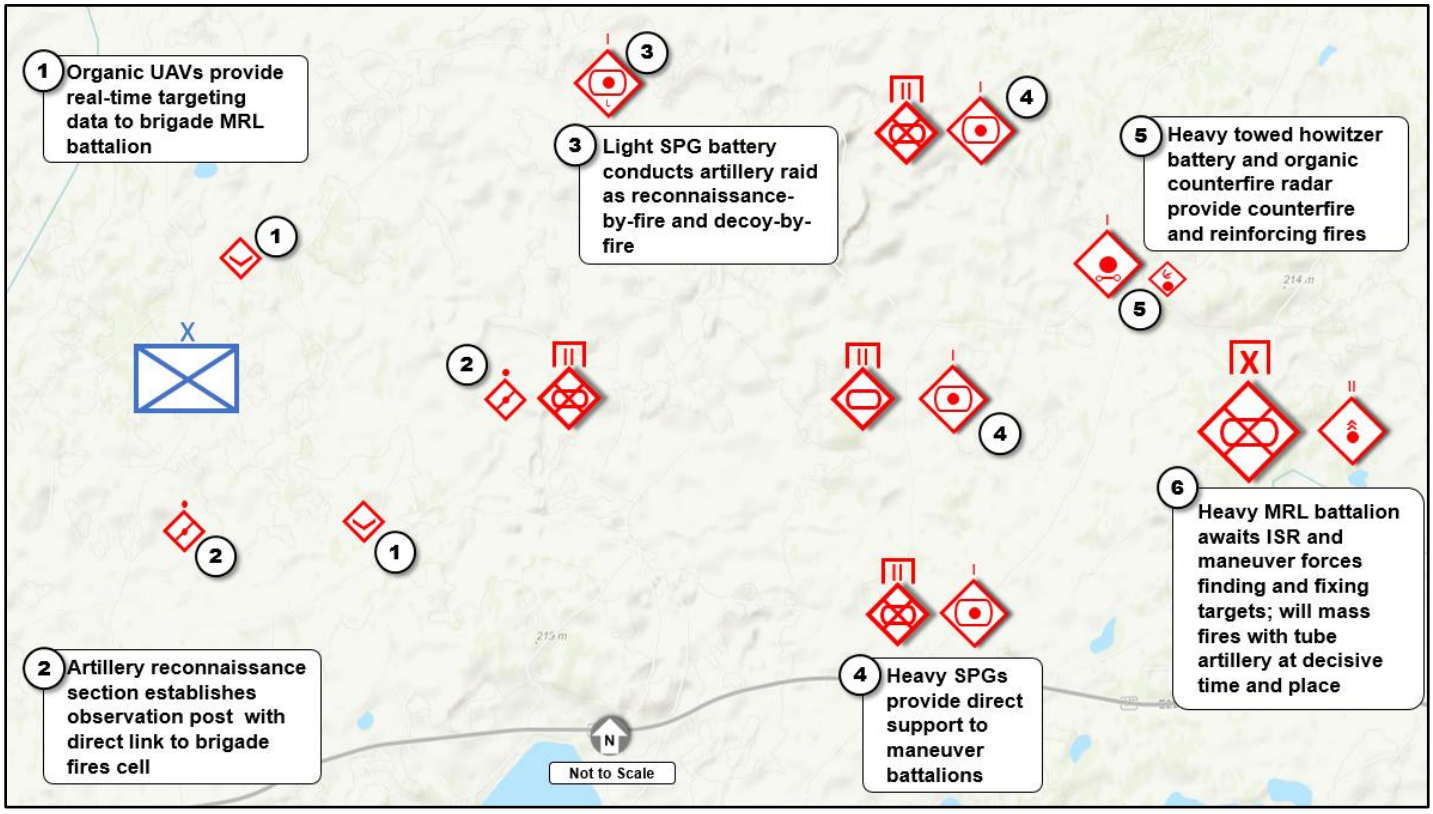


Figure 9. A Russian motorized rifle brigade in attack

FO teams infiltrate forward of the brigade's main body with the mission of locating high-value targets. This includes C2 nodes, supply areas, assembly areas, and lines of communication. The FOs have a direct digital link to the brigade fire direction center and can rapidly request a variety of different effects on detected targets. The primary mission of these artillery reconnaissance sections is to get into position to engage targets, not coordinate and synchronize artillery fires with maneuver. Concerns over establishing priority of fires to support the brigade's scheme of maneuver and clearing fires are less important to the BTG commander than getting artillery fires on the right targets quickly.

A light (2S1) SPG battery infiltrates forward of the brigade's main body on an artillery raid. This raid has two purposes: first, to harass enemy rear areas, and second, to provoke a counterfire response. This requires the enemy to reveal the

location of some of its fire support assets, forcing its fire-finder radars to emit and weapons systems to go into action. This creates a targetable footprint for the SPGs, MRLs, and heavy towed howitzers that are centralized at the brigade to engage enemy fire support systems.

Three SPG batteries (1x2S1, 2x2S19) are assigned as direct support to maneuver battalions as a part of BTGs. These units provide their supported battalions with heavy indirect, and possibly direct, fire support. They move along with mechanized forces, ideally around 3–6 kilometers behind the forward line of troops. These guns engage points of resistance and high-value targets that the BTG encounters during its advance.

A heavy towed howitzer (2A65) battery represents one part of the brigade's artillery reserve. This battery's primary mission is counterfire. It is paired directly with a counterfire radar plus the counterfire section of the brigade's fire direction center. As enemy artillery systems fire, this battery engages their positions with a mix of high-explosive fragmentation and cluster munitions, designed to destroy, neutralize or suppress enemy artillery systems. This battery may also contribute to massed fires on a critical target at the brigade commander's discretion.

A heavy MRL (9P140) battalion represents the other part of the brigade's artillery reserve. This unit contains the largest portion of the brigade's firepower and is reserved for the most critical targets at the most crucial times. This unit has direct digital communications with the brigade's UAVs; as the UAVs identify and locate targets, the 9P140s rapidly deliver a variety of rocket munitions. Direct links to designated FOs are also established as either a redundant or primarily means of target acquisition for 9P140 rocket fires. Radar acquisitions also play a large role in directing MRL counterfire. The long range of the 9P140 allows them to remain relatively stationary, making resupply relatively simple, though this does make them susceptible to counterbattery fire. To cover this vulnerability, the 9P140rely on counter-counterfire from artillery units organized and controlled at echelons above the brigade, an example of the combined-arms focus for the recon-fires complex.

Training Implications

The prevalence and efficiency of Russian artillery has significant training implications for units training against an opposing force emulating Russian Ground Forces. Dispersion, deception, concealment, hardening, and constant movement are all essential to survival against an artillery-heavy opponent. Unfortunately, many of these skills have atrophied in the recent counterinsurgency era, where threat indirect fire was sporadic and largely ineffective. Gunners and commanders alike should reinvigorate counterfire and counter-battery training, with an emphasis on using a wide spectrum of potential capabilities—not just indirect fire—to effectively neutralize threat artillery and enable friendly freedom of maneuver. Finally, the joint force needs to prioritize joint-level counterfire operations training, with the objective of neutralizing threat artillery systems before they can lock horns with friendly ground forces.

Notes

[1] R. Beckhusen. "Russia Unleashes Artillery in Eastern Ukraine." War is Boring. 31 January 2017.

[2] M. Jacobson. "Cluster Munitions No More: What This Means for the U.S. Military." eArmor. October 2014.

[3] S. Woodford. "The Russian Artillery Strike That Spooked The U.S. Army." The Dupuy Institute. 29 March 2017.

[4] L. Grau. "Soviet Artillery Planning in the Tactical Defense." Soviet Army Studies Office. 1990.

[5] J.T. Stacks. "Field Artillery in the Deep Battle." US Army War College. 1978.

[6] Even on a per-unit basis, Soviet artillery consistently outnumbered equivalent NATO systems at roughly a 3:1 ratio. In addition, the Red Army used several systems, particularly heavy rocket artillery, which had no NATO equivalent.

[7] J.T. Stacks. "Field Artillery in the Deep Battle." US Army War College. 1978.

[8] "Counter-counterfire" is measures taken to reduce the effectiveness of the opponent's counterfire efforts. It can be either active (engaging the opponent's counterfire guns and sensors) or passive (camouflage and movement).

[9] United States Army. Russian New Generation Warfare Handbook. 2017.

[10] United States Army. Russian New Generation Warfare Handbook. 2017.

[11] United States Army. Functional Concept for Movement and Maneuver. 2017.

[12] A.C. Rossow. "Making Sense of Russian of Russian Hybrid Warfare." Association of the United States Army. 2017.

[13] An interesting sidenote to the Russian heavy MRLs: Russian Ground Forces appear to have deliberately chosen to make these systems wheeled, instead of tracked. This was likely done to reduce fuel consumption, but significantly reduces cross-country mobility. The implication is either that cross-country mobility is not highly prioritized or, alternatively, that these systems are not intended to be used extensively away from improved roads.

[14] K. Kane. "Adapting Towed Artillery Today to Meet a Near Peer Competitor Tomorrow." Small Wars Journal. 6 February 2017.

[15] F. Bjorn. "The BTG of the 35th Motorized Rifle Brigade of the Russian Invasion Force." Inform Napalm. 21 December 2014.

[16] Federation of American Scientists. "2S1 M-1974 122-mm Self-Propelled Howitzer." 1999.

[17] L. Grau. "Artillery and Counterinsurgency: The Soviet Experience in Afghanistan." Field Artillery Journal. 1997.

[18] US Army, TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. Worldwide Equipment Guide – Volume 1: Ground Systems. December 2016. Pgs 447–448.

[19] Army Technology. "MSTA-S 2S19 152mm Self-Propelled Howitzer."

[20] Q.E. Hodgson. "Deciding to Buy: Civil-military Relations and Major Weapons Programs." Strategic Studies Institute. 2010.

[21] Though Western knowledge of the 2S35 is incomplete, the system may represent a significant leap forward in SPG capability. Onboard fire direction—a unified C2 system—does both technical and tactical fire direction. It also features an autoloader, an 8 rounds-per-minute sustained fire capability, three person crew, and a chassis common with other systems.

[22] Since the end of WWII, rocket artillery was used somewhat sparingly in Korea, very little in Vietnam or other such proxy wars. The M270 saw extensive use in Desert Storm, India employed extensively in the late 1990s conflicts with Pakistan, and Russia used them in the Chechnya and Georgia conflicts. Only in Desert Storm, and now in the Ukraine, have we seen massed fires from modern rocket systems.

[23] S. Woodford. "The Russian Artillery Strike That Spooked The U.S. Army." The Dupuy Institute. 29 March 2017.

[24] S. Woodford. "The Russian Artillery Strike That Spooked The U.S. Army." The Dupuy Institute. 29 March 2017.

[25] R. Beckhusen. "Russia Unleashes Artillery in Eastern Ukraine." War is Boring. 31 January 2017.

[26] P. Tucker. "How the Pentagon is Preparing for a Tank War With Russia." Defense One. 19 May 2016.

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

Integrated attack is a tactic that applies massed effects and rapid actions of threat forces to achieve of a mission objective. This vignette describes significant actions of an integrated attack conducted by an opposing force (OPFOR)[ii] in US Army learning events and as presented in US Army Training Circular 7-100.2, *Opposing Force Tactics*.[1] Aspects of threat brigade-echelon capabilities observed in recent and current tactical real-world operations include substantial integrated air defense, indirect fires, electronic warfare, and other combat power enablers in conjunction with ground and aerial maneuver. These types of capabilities are typically present in the brigade tactical group (BTG) task organization.

Tactical Overview

A BTG conducts an integrated attack to defeat an enemy in a zone occupied by a US Army armor brigade combat team (ABCT). Affiliated insurgent organizations and guerrilla units, supported by special-purpose forces (SPF), augment BTG combat power and impact significantly on situational awareness of enemy coalition actions throughout the depth of the BTG disruption zone and battle zone. Indigenous criminal organizations are loosely associated with the threat military forces and provide additional information and intelligence collection, as well as disruption actions against the US forces. In this article's example, the BTG is a supporting effort to a higher headquarters tactical mission employing multiple brigade-size tactical groups.

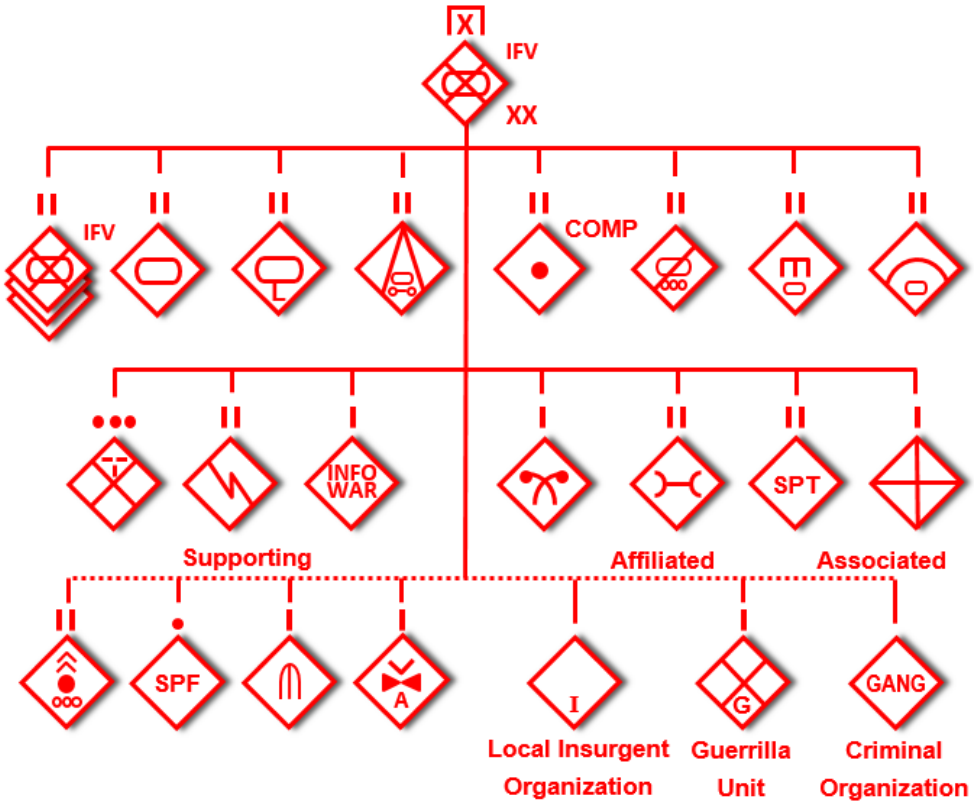


Figure 1. Task-organized brigade tactical group (example)

[ii] For the purpose of this article, the term "threat" will be used synonymous to "opposing force" (OPFOR).

The offensive concept is to employ affiliated and associated units and organizations in a BTG disruption zone to conduct reconnaissance, intelligence, surveillance, and target acquisition (RISTA) actions and, on order, to disrupt the tempo of ABCT lead 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 BTG conducts RISTA at the tactical echelon and integrates RISTA from a higher headquarters in the BTG area of responsibility (AOR) and its zone of reconnaissance responsibility (ZORR).[2] The ZORR is a combination of a unit's AOR and the area outside of that AOR that can be observed or monitored by the unit's technical sensors.[3] These types of sensor systems can include the information and intelligence provided from affiliated and associated units.

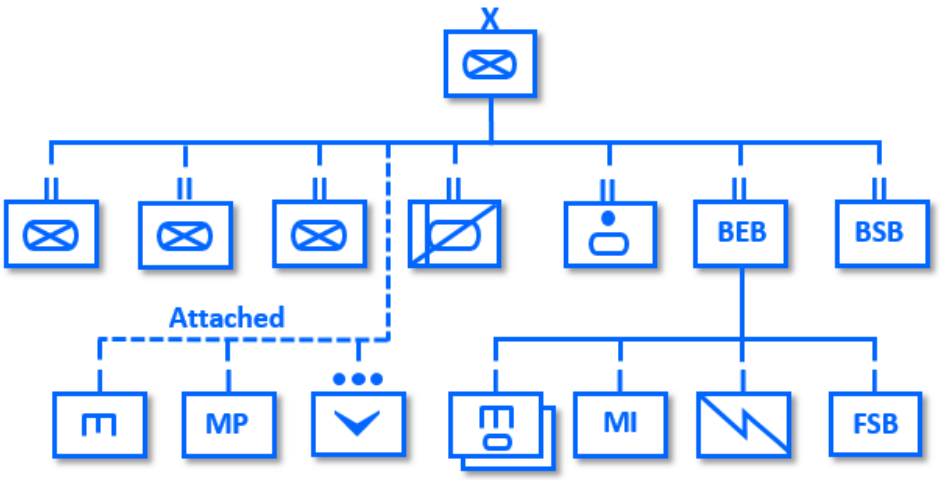


Figure 2. Armor brigade combat team (example)

Ground and aerial maneuver and support forces advance across designated terrain in an integrated attack using control measures such as objectives, attack zones, boundaries, limit of responsibility (LOR) lines, battle lines, and support lines to orient the BTG use of fires and maneuver and its command and control. The BTG commander remains attuned to tactical opportunities that might emerge unexpectedly, and is willing to use initiative and deviate from a published order in order to achieve his assigned mission objective.

The threat defines an AOR as a geographical area and associated airspace within which a commander has the authority to plan and conduct combat operations. An AOR is bounded by a LOR beyond which the organization may not operate or fire without coordination through the next-higher headquarters. AORs typically consist of three basic zones: *disruption* zone, *battle* zone, and *support* zone. An AOR may also contain one or more *attack* zones. An attack zone is assigned by a unit commander to a subordinate unit commander with an offensive mission that specifies clearly where that unit commander will conduct offensive operations.[4] Attack zones are often used to control offensive action by a subordinate unit inside a larger battle or operation.

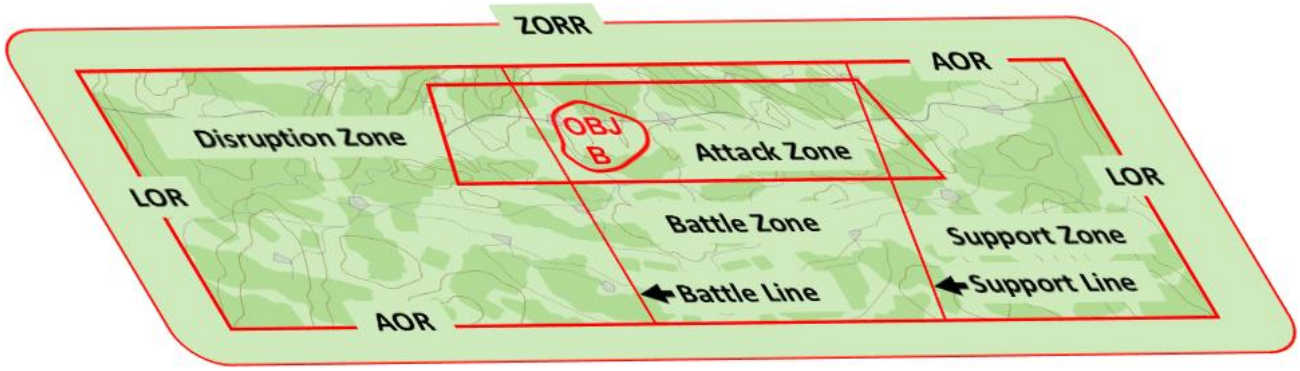


Figure 3. Terrain orientation for BTG tactical actions

Integrated Attack

The *integrated attack* is an offensive action that seeks military success by destroying the enemy's will or ability to continue fighting through the application of threat combined arms effects. A mission task of integrated attack may also be employed

against a more sophisticated and capable opponent if an appropriate window of opportunity is created or otherwise available.[5] The primary objective of an integrated attack is destroying the enemy's will and ability to fight.[6] The threat recognizes that modern militaries cannot continue operations effectively without adequate logistics support and command and control. The threat identifies vulnerabilities in enemy systems and optimizes actions to cripple sustainment functions and to deceive or defeat enemy situational understanding of conditions and actions in an operational environment.

Several fundamentals tasks of an integrated attack are coordinated throughout the three tactical zones of a unit's AOR. Offensive tactical actions taken by threat units and activities in an integrated attack can typically include tasks of assault, ambush, raid, and/or reconnaissance attack.[7] Major characteristics and intentions of an integrated attack include but are not limited to:

- Deceive the enemy of planned threat operations and offensive main effort;
- Disrupt enemy logistics and command and control (C2);
- Fix key elements of the enemy's force in place with the minimum threat force necessary to sustain the task;
- Isolate designated enemy capabilities from the enemy's main combat power;
- Optimize complex environmental factors that force the enemy to fight at a tactical disadvantage;
- Apply additional deception and other components of information warfare (INFOWAR) to degrade the enemy's situational awareness and understanding of the integrated attack;
- Employ maneuver such as flank attack or envelopment once an enemy force has been fixed in position;
- Conduct deliberate breaching operations, as necessary, to penetrate enemy main defenses;
- Defeat enemy C2 and logistics;
- Penetrate into the enemy rear area to achieve integrated attack mission objectives; and
- Destroy enemy combined arms combat power.

Conditions that the threat considers in ordering an integrated attack include but are not limited to:

- Combat power overmatch compared to enemy forces;
- Air parity or superior airpower for selective time periods over critical portions of the disruption, battle, support zones; and
- Protection from enemy stand-off RISTA systems in order to operate effectively without high levels of risk.

Planning an integrated attack requires focus on the mission objective, higher-headquarters mission intent, and the ability to identify decisive points for success of the attack. An attack is an offensive operation that can have objectives to destroy or defeat an enemy force, seize and secure terrain, or a combination of both. These actions seek to achieve tactical decision through primarily military means by defeating the enemy's military power. This defeat and eventual destruction are achieved through the disruption, dislocation, and subsequent paralysis of an enemy that occurs when combat forces are rendered irrelevant by the loss of capability or will to continue the fight.[8]

Plan

Subtasks to consider in planning an integrated attack course of action include:

- Determine decisive points for threat mission success;
- Plan backwards from achieving the mission objective and defeat or destruction of critical enemy combat, combat support, and combat service support systems;
- Employ disruption force to conduct RISTA of the enemy;
- Employ integrated fires and supporting systems to disrupt or defeat enemy RISTA and fires;
- Employ counterreconnaissance forces to defeat or destroy enemy ground and aerial reconnaissance forces;
- Consider use of a deception force;
- Employ fixing forces against designated enemy forces;
- Employ isolation forces, as needed, against designated enemy forces;
- Maneuver assault forces to enable an exploitation force;
- Maneuver exploitation force to seize or occupy the mission objective;
- Consider capabilities required for a reserve force;
- Destroy designated enemy forces;

- Plan forward from initiation of the integrated attack to mission success, and adjust or confirm actions analyzed in backward planning; and
- Conduct rehearsals.

Prepare

Subtasks to consider in preparing for an integrated attack include:

- Create task organization and C2 of disruption force, fixing forces, isolation force, assault force, exploitation force, reserve force, and deception force;
- Conduct detailed rehearsals; and
- Execute deception and disruption operations and other INFOWAR concurrent to the preparation phase.

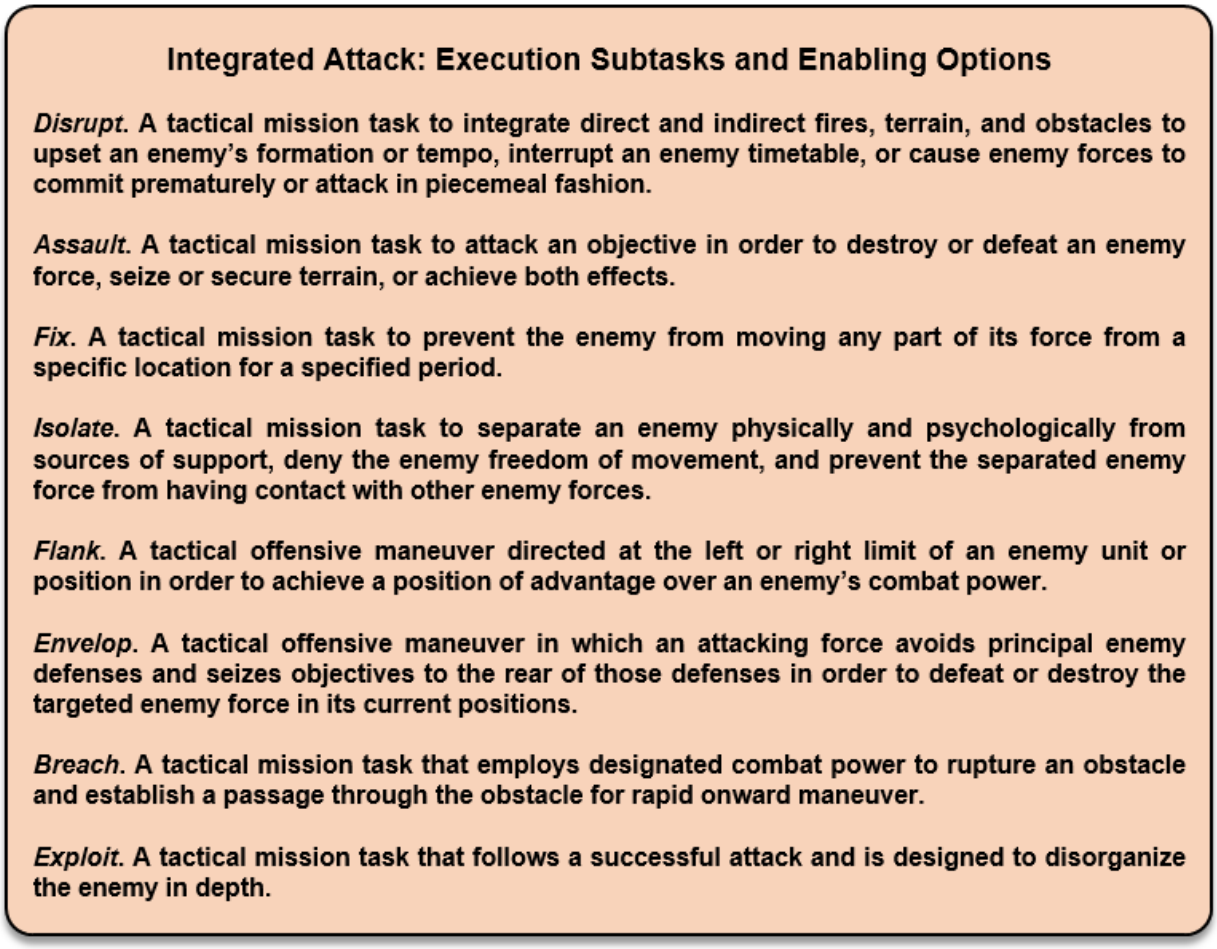


Figure 4. Mission task considerations in an integrated attack

Execute

- Use a disruption force to disrupt enemy dispositions and ability to move or maneuver;
- Use threat counterreconnaissance forces to defeat or destroy enemy reconnaissance or security forces;
- Maneuver and deploy threat security forces to ensure additional enemy forces do not join the battle unexpectedly. (Security forces may transition to become fixing forces);
- Fix critical enemy maneuver and fire capabilities, and sustain situational understanding of enemy actions;
- Isolate designated enemy forces possessing the ability to maneuver and fire or otherwise affect decisive threat actions;
- Conduct deception actions to prevent detection of the threat exploitation force location and intentions;
- Conduct deception actions to prevent detection of the threat reserve force location and intentions;
- Assault enemy forces and capabilities to set conditions for exploitation force success; and

- Conduct exploitation force actions to destroy designated enemy forces, logistics support, and C2 capabilities, or to seize assigned objective(s).

Functional Organization of an Integrated Attack

An integrated attack employs various types of functional forces. The tactical group commander assigns functional designations to subordinate units that correspond to their intended roles in the attack. Task organization and combined arms are norms in the attack array. An integrated attack often employs disruption, fix, assault, exploitation, and support forces. A disruption force can be designated when tactical conditions indicate this type of offensive action supports fixing or isolation forces and subsequent actions by assault forces and exploitation forces.

Action Force

An *action* force is responsible for performing the primary function or mission task that accomplishes the overall mission or assigned objective. The higher-unit commander will typically state a more specific designation to identify the function or task the action force is to accomplish.[9]

The fundamental action force of an integrated attack is typically an *exploitation* force. This force must be capable of penetrating or avoiding enemy defensive forces in order to attack and destroy designated enemy support infrastructure and disrupt command and control, thus causing defeat or destruction of the enemy forces. An exploitation force is task-organized for a combination of mobility, protection, and firepower. A higher-echelon commander may provide other capabilities if conditions are practical to continue the attack deep into the enemy rear areas after success of the assigned objective. An exploitation task can be reassigned during a tactical mission based on emergent operational conditions.

Enabling Forces

Given the action force is the principle force to achieve mission success, all other forces and capabilities of the threat organization provide *enabling* functions.[10] Each of these forces has a title to clearly identify the specific function or task it performs. For example, a force that fixes enemy forces is titled a *fixing forces*. Types of enabling forces titled by their specific function can include but are not limited to:

Assault force. One or more assault forces can be employed by the threat commander. The assault force in an integrated attack has a mission task to destroy a particular part of the enemy force or seize key position(s). The mission task of an assault force can be intended to create a window of opportunity for an exploitation force to continue an attack and penetrate through enemy defenses. An assault force may also employ infiltration techniques to preselected points in the support or battle zone to support a penetration of enemy forces and continued attack by an exploitation force.

Disruption force. Disruption forces operate in a disruption zone can conduct varied mission tasks:

- Maintain observation and reporting for facilitating long-range fires on priority targets;
- Confirm intelligence on movement and maneuver of front-line and rearward enemy echelons; and
- Continue actions to disaggregate enemy forces as the threat continues its offensive actions through enemy security forces and into the enemy main defenses.

Other threat and higher-headquarters forces can be coordinated to position and maneuver in the disruption, battle, or support zones in order to provide required support to BTG maneuver forces in the disruption and battle zone tasks of the integrated attack.

Fixing forces. Fixing forces prevent a designated part of the enemy force from moving from a location for a specific period of time so it cannot interfere with the primary threat action. The fixing forces in an integrated attack prevents enemy defending forces, reserves, and quick-response forces from interfering with the actions of assault and exploitation forces.

Security force. Security forces provide security for the force and higher-echelon headquarters. Reconnaissance and counterreconnaissance actions are often complements to security tasks.

Deception force. Deception forces conduct actions that convince an enemy to act in ways or set other conditions that favor the success of the threat mission. Threat arrays use extensive methods of camouflage, cover, concealment, and deception (C3D) actions.

Support force. Support forces provide fires and other combat support or combat service support to an action force or other enabling forces, and sustains C2 functions for conducting the threat mission.

Reserve force. The threat commander retains a *reserve* as an uncommitted force. This ensures the threat commander has the ability to apply uncommitted combat power to tactical opportunities or unexpected circumstances during the mission. If and when this reserve force is subsequently assigned a specific function and mission, the force is titled with an appropriate functional designation.[11] For example, a reserve force could be designated a counterattack force, or could be ordered to be an exploitation force in order to sustain the momentum of previous threat exploitation success.

The Integrated Attack

The threat concept is to conduct an integrated attack throughout the AOR to defeat enemy forces and defenses in zone. The tactical example in this article is a supporting attack as part of a higher-headquarters mission. The threat objective is typically to destroy the sustainment ability of enemy forces and defenses, defeat its command and control, and defeat or destroy designated ground maneuver forces.

Irregular forces. Affiliated irregular forces—such as insurgent organizations, guerrilla units, and criminal organizations—supported by special-purpose forces (SPF),augment threat combat power throughout the disruption zone and battle zone. Aspects of C3D mislead enemy forces on the actual disposition and intention of threat forces. Threat actions combine to disaggregate enemy force capabilities at selected times to create or enhance vulnerabilities in the enemy force defenses.

Regular forces. Threat regular forces are typically combined arms task-organized for combat based on assigned mission tasks, and complement an overarching systems-warfare approach to threat operations. Affiliation and/or association with irregular forces is a norm in threat operations.

Integrated fires command. The threat configures its attack forces in successive maneuver-oriented arrays, complemented with multiple fires of artillery, rockets, ballistic missiles, and other support. The integrated fires command (IFC) and integrated air defense systems (IADS) provide sophisticated overlapping protection to threat forces in their formations throughout the depth and breadth of assigned terrain and responsible airspace. The IFC provides reconnaissance fires, interdiction fires, counterfire, and close support fires integral to an integrated attack. The significant long-distance radar and emission acquisitions of enemy movement and maneuver are shared within the IFC and IADS for action. Selected fires and air defense systems will not emit until notified of approaching targets and will engage specified targets with minimal signature warning to enemy forces.

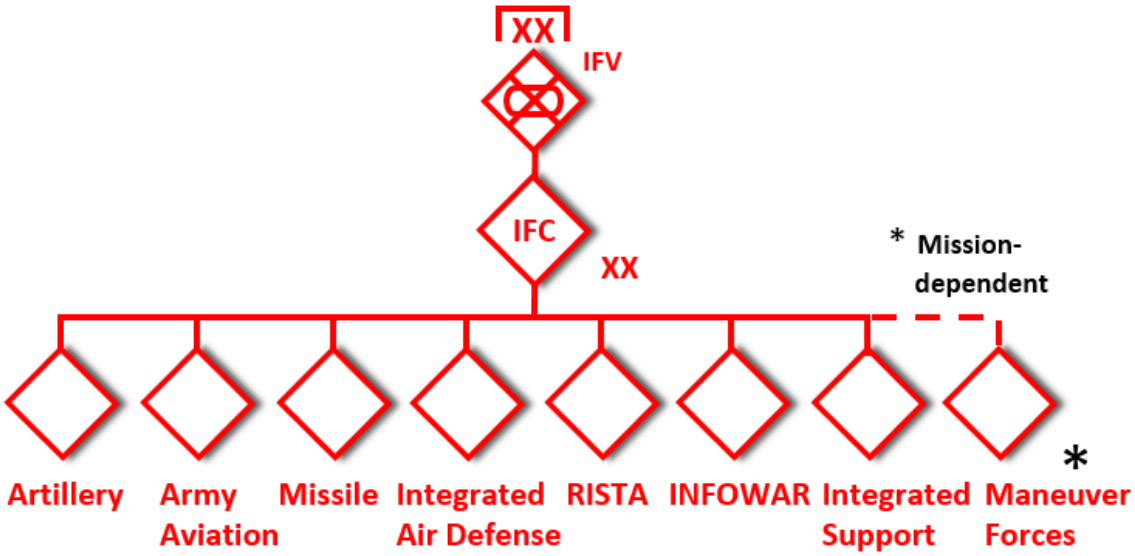


Figure 5. Integrated fires command possible components for task organization

The IFC is a combination of a standing C2 structure and task-organizing of constituent and dedicated fires units. All division-level and higher-echelon headquarters possess an IFC C2 structure. BTGs have task-organized fires but do not have an IFC.[12] Integrated fire support to a BTG mission is provided by a higher-headquarters IFC. The composition of an IFC is dependent on the mission and assets assigned from within a division and/or higher headquarters.

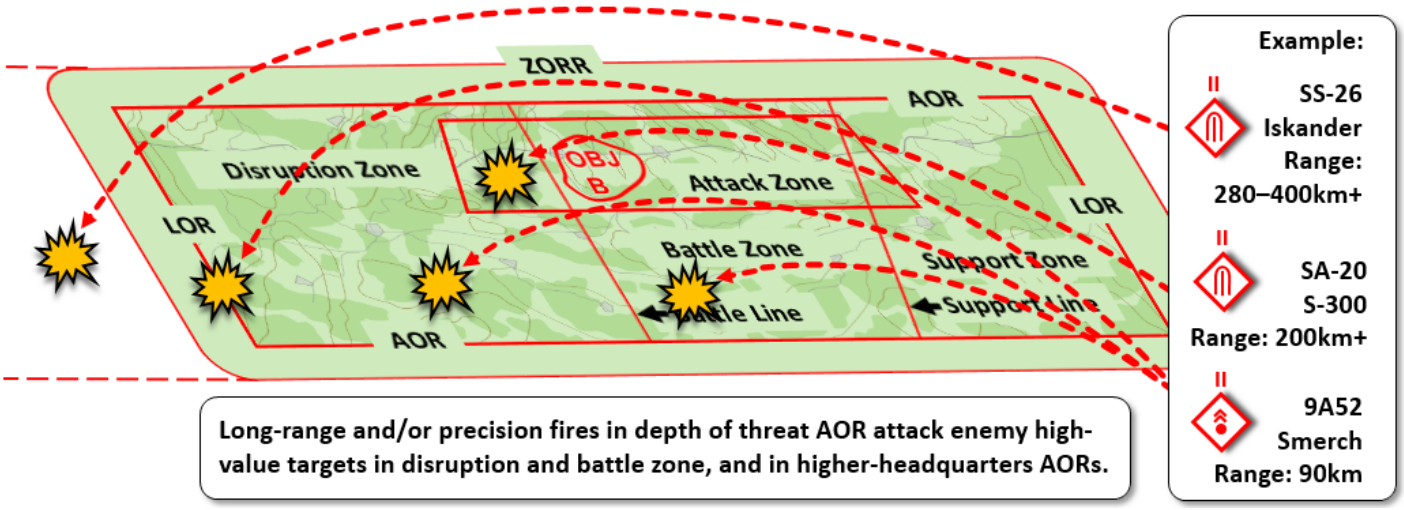


Figure 6. Integrated fires command possible capabilities for long-range or precision fires

RISTA. Threat reconnaissance, intelligence, surveillance, and target acquisition assets maintain situational awareness and understanding of enemy dispositions and actions. Unmanned aerial vehicles and other aerial platforms at each threat unit echelon provide a multi-tiered intelligence, surveillance, a reconnaissance capability throughout the AOR and ZORR to complement other target-acquisition capabilities. Signals intelligence, as one of several capabilities, is normally active to identify and track enemy movement, maneuver, and concentrations. Long-range reconnaissance assets, irregular forces, or SPF embedded throughout the zones of an AOR augment confirmation of enemy actions and probable intentions.

Information warfare. INFOWAR forces make significant use of deception methods to include decoy radar emitters, decoy signals emitters, and other physical or electronic decoy measures. Electronic warfare, computer warfare, and information attack disrupt enemy command and control communications or jam designated networks at specified time periods and deceive enemy situational understanding of the current operational environment. Forces employ perception management techniques to distribute believable misinformation, influence the relevant population against enemy forces, and further disrupt enemy decisionmaking and C2.

Other Support Forces. Threat engineer support is task-organized in the assault force echelons for engineer reconnaissance, mobility, and breaching or bridging to sustain attack momentum and exploitation. Once breaches are secured, engineer capabilities allocate specified assets to countermobility efforts in support of the attack. Threat army aviation and air forces are coordinated for direct air support, air interdiction, and suppression of enemy air defense actions. IADS deploy overlapping short-, medium-, and long-range air defenses to defeat enemy rotary-wing and fixed-wing aviation. Other forces providing technical or functional capabilities are task-organized as needed to support the mission.

Threat combined arms capabilities include ground and aerial maneuver, integrated long-range and precision fires, integrated air defense systems, long-range antiarmor systems, mobility and countermobility means, and electronic warfare or other signals deception in INFOWAR. Weapons of mass destruction use at the tactical echelon, with particular options for chemical weapons, is a threat planning consideration. Chemical weapon use, when authorized, may include toxic industrial chemicals and toxic industrial materials in combination with INFOWAR perception management techniques against the enemy.

Disruption Forces in an Integrated Attack

The offensive concept is to maintain reconnaissance and counterreconnaissance actions throughout the threat AOR in order to identify the disposition and composition of enemy forces and to target and destroy critical systems in the enemy force defensive array. Disruption forces coordinate with fixing forces and assault forces for battle handover and sustained contact with enemy forces. The boundary of the disruption zone moves forward into the depth of the AOR with the shifting control measures of the battle zone and following support zone as the integrated attack progresses.

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 counterreconnaissance forces fix,

isolate, or destroy designated enemy security forces with direct and indirect fires, and set favorable conditions for continuation of the integrated attack and exploitation actions.

Threat initial priorities of effort in fires, maneuver, and deception efforts convince the enemy to focus its main effort in an area other than the actual threat main attack. In the vignette example, deceptive preparatory actions convince the enemy that the threat main effort is to be in the north.

SPF units conduct direct action tasks and coordination in support of 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. Other RISTA disruption forces continue surveillance and report on high-value targets (HVTs), disrupt enemy force logistics and movements, and prepare to report damage assessment on HVTs after an attack.

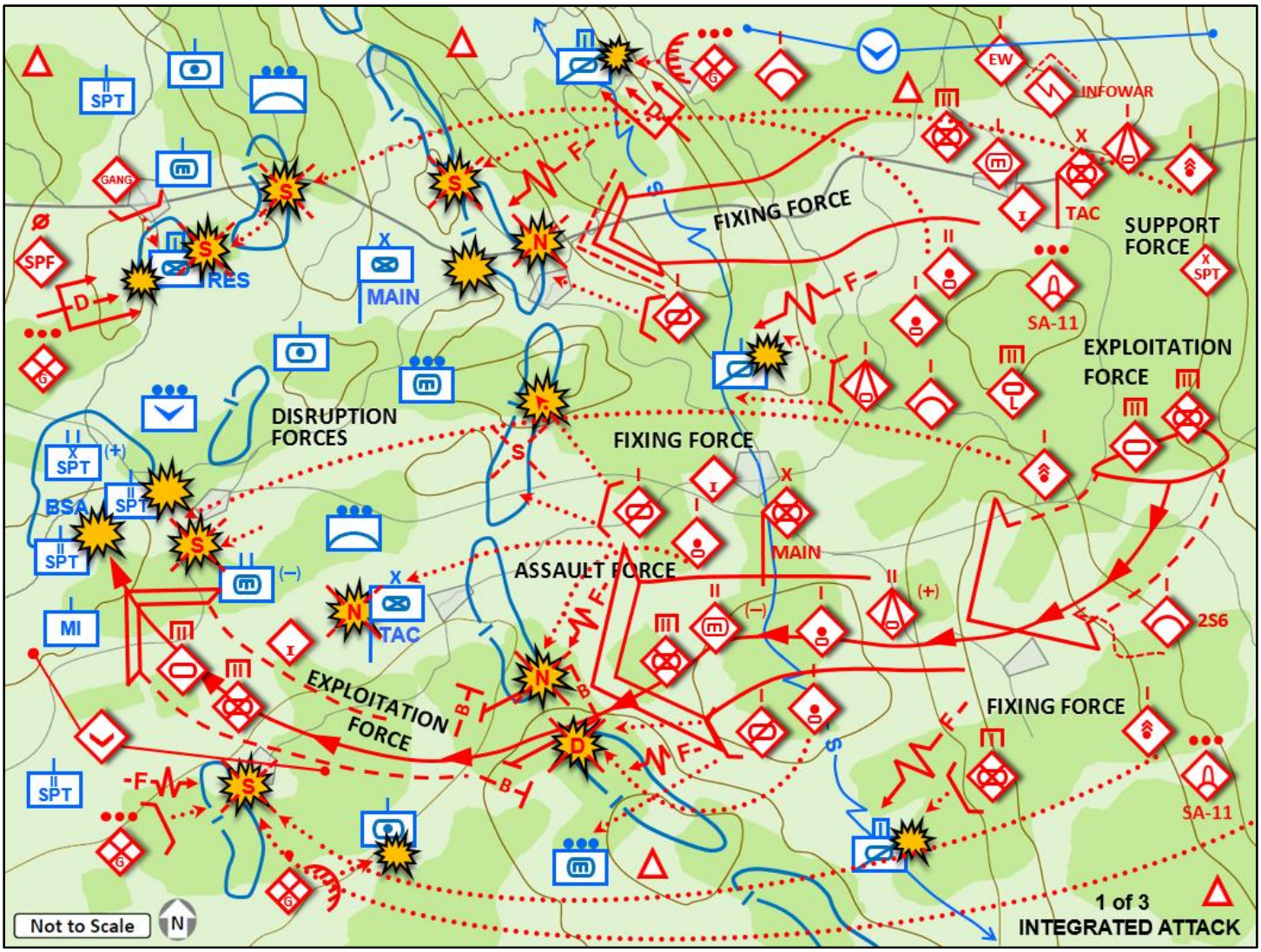


Figure 7. Disruption force action in an integrated attack (1 of 3)

Additional significant actions portrayed in Figure 7 by disruption forces include affiliated irregular organizations working in coordination with regular units and detachments, supported by SPF, 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, and maneuver; countermobility, and information warfare measures;

- Report information and intelligence updates on follow-on enemy forces in depth of AOR;
- Acquire, target, and attack HVTs at designated times and locations;
- Fix 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 actions and long-range and precision fires.

Fixing and Assault Forces in an Integrated Attack

The decisive action of an integrated attack is enabled by disruption forces, fixing forces, assault forces, and support forces. Once these forces have accomplished their mission tasks, the primary action of an integrated attack shifts to an exploitation force that penetrates through the enemy force main defenses and attacks into the depth of the enemy defensive area. Objectives can include destruction of the sustainment ability to enemy force main defenses, defeat of enemy force command and control, defeat of designated ground maneuver forces, or to accomplishment of other assigned or contingency mission tasks.

Fixing forces in the battle zone 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 situation and combat power for assault forces to attack in their zone. Fixing forces may also be directed to isolate designated enemy forces to prevent influence on the combat power of assault forces in their attack zone. Fixing forces, in conjunction with SPF and RISTA capabilities in the disruption zone, can orient and direct long-range and/or precision fires to prevent enemy forces or reserves from effectively interdicting the main effort of the integrated 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. The integrated attack main effort may require assault forces to seize specified areas in order to breach the enemy's main defenses. Breaching enemy defenses at designated points, assault forces secure the breaching area, continue forward momentum, and facilitate passage of an exploitation force through the breach lanes. Securing the breach area may require assault forces to block or fix enemy forces attempting to disrupt the sustained momentum of the integrated attack.

In this integrated attack vignette, the threat task-organizes northern fixing forces with fires, maneuver, and INFOWAR capabilities and convinces the enemy commander that the threat main effort is in the north. As other threat forces fix enemy forces along the main defensive array, the actual main effort with effective C3D of key support systems is in the south, and transitions from fixing forces to an assault force in order to breach enemy defenses. The success of multiple breach points allows exploitation forces to become the main effort. The exploitation force passes and clears through the breach lanes, penetrate rapidly, and maneuvers toward objectives in the depth of the enemy forces.

Significant actions by fixing forces portrayed in Figure 8 fix enemy forces with assault forces and conduct deliberate breaching tasks of the enemy main defenses to facilitate penetration by an exploitation force, which include:

- Accept battle handover from threat disruption forces and continue coordinated fires and maneuver on enemy forces;
- Fix designated enemy forces;
- Isolate designated enemy forces, if necessary, to support threat offensive main effort and supporting efforts;
- Coordinate irregular organizations and units in actions to support defeat of enemy forces in disruption and battle zones;
- Disrupt, defeat, or destroy enemy force command and control with electronic warfare, signals INFOWAR capabilities, and long-range and/or precision fires;
- Conduct INFOWAR perception management activities to convince the enemy commander that he cannot move from particular locations, or otherwise influence his decision to remain in a static defensive posture;
- Suppress or neutralize enemy forces or command and control with massed fires, and conduct immediate dispersal/reposition of firing units;
- Defeat enemy aerial attacks and unmanned aerial systems with integrated air defenses;

- Suppress, neutralize, or interdict enemy capabilities in depth and along the axis of attack for the exploitation force;
- Coordinate for rotary-wing and fixed-wing support in conjunction with higher-headquarters objectives;
- Seize assigned initial objectives and continue actions to accomplish follow-on objectives;
- Conduct breach at designated points and secure breach area;
- Destroy or neutralize designated enemy forces and critical systems;
- Facilitate passage and forward momentum of exploitation forces through the breach area; and
- Defeat enemy forces in main defenses; on order, continue offensive momentum; and be prepared to continue attack.

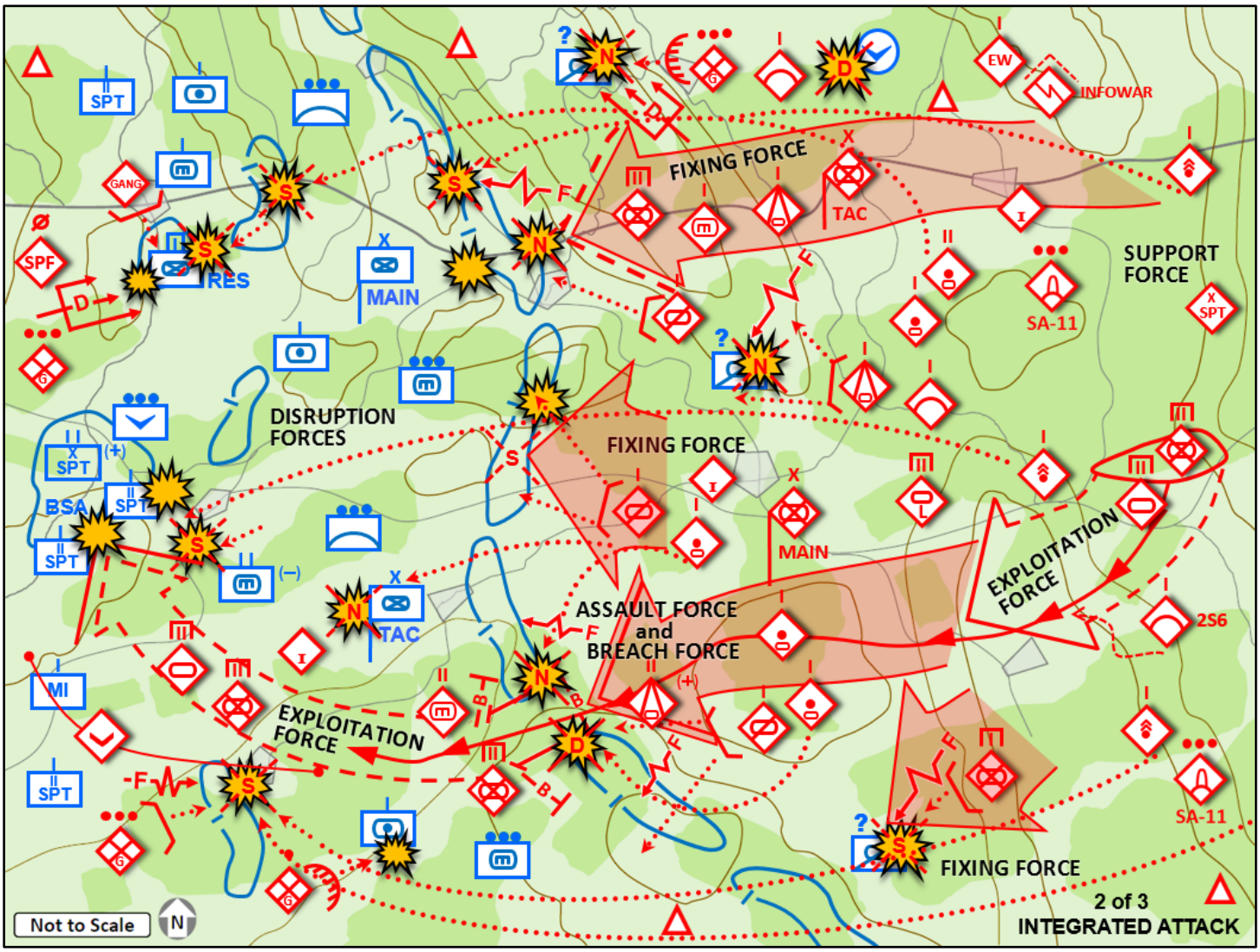


Figure 8. Fixing and assault force actions to breach enemy defenses and secure passage lanes (2 of 3)

Exploitation Forces in an Integrated Attack

Exploitation forces, task-organized as self-contained combined arms units, penetrate through the secure breach and attack on an axis toward their primary objective of destroying the sustainment area of the enemy main defenses. The attack of an exploitation force dislocates enemy forces; destroys critical enemy systems; disrupts, defeats, or destroys enemy command and control; and destroys the sustainment ability to the enemy defense in zone. Given the exploitation force achieves its initial mission objective and force combat power is capable, subsequent objectives may be ordered to continue the exploitation momentum.

Disruption forces continue actions to interrupt and limit enemy response to the exploitation force, and continue to act in a shifting disruption zone to maintain contact with and disrupt enemy forces in the AOR. Fixing forces along the main enemy defenses continue to fix, isolate, or contain enemy forces in support of the exploitation. Uncommitted threat forces continue to approach toward threat forces in contact with the enemy, and are ready to assist threat supporting efforts and/or continue in zone to support the main effort and reinforce threat exploitation forces in contact. These threat forces can be directed to support the exploitation force or to assume continuation of the integrated attack into the depth of the enemy defenses.

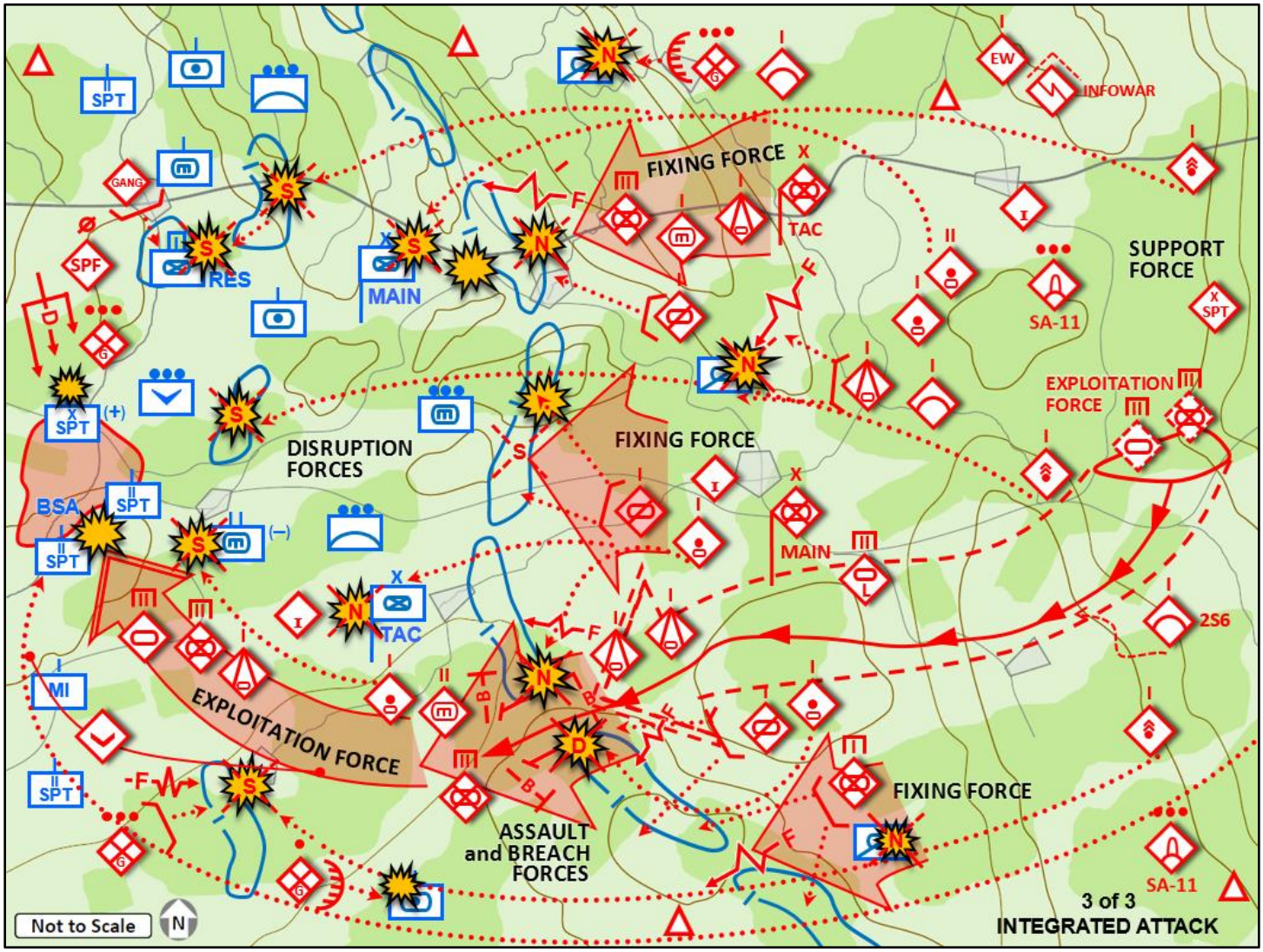


Figure 9. Exploitation forces attack to destroy enemy forces and seize assigned objectives (3 of 3)

Significant actions of exploitation forces portrayed in Figure 9 include:

- Penetrate through the secure breach and seize initial objectives;
- Exploit to destroy assigned follow-on objectives in the enemy force sustainment area;
- Continue to coordinate integrated fires and maneuver on enemy forces in zone to disrupt enemy freedom of movement and maneuver on ground and aerial avenues of approach;
- Maintain contact with enemy forces;
- Fix and defeat enemy combat formations in kill zones;
- Continue guerrilla unit, insurgent cell, other irregular forces, and SPF direct actions throughout the depth of the enemy defenses and AOR;
- Reinforce threat forces in contact to fix or isolate enemy forces for defeat or destruction;
- Position reserve forces for rapid commitment, as appropriate, to support the integrated attack;

- Inform uncommitted threat follow-on forces on current situational understanding of exploitation success and possible or probable contingencies for continued offensive mission tasks;
- Defeat enemy forces in zone; on order, continue to attack in zone; and
- Be prepared to continue integrated attack to destroy enemy capabilities in the enemy support zone and further in depth of AOR.

Training Implications

This tactical vignette illustrates and describes key actions of a successful BTG integrated attack. The BTG commander used primarily affiliated irregular forces and SPF in the disruption zone in order to disorient the enemy commander and set tactical conditions for decisive defeat of the enemy force in the offensive battle zone. Expert knowledge of the terrain, relevant population, and tactical experience of regular and irregular forces were significant combat multipliers in shaping the battle and enhancing options for future offensive operations. Timing of execution—sequential, parallel, and simultaneous—was critical to effectively employing threat combat power throughout the shifting geographic areas and boundaries of the disruption zone and battle zone, and performing actions for continuous support of a responsive support zone in the attack.

Using multiple deception techniques and ample measures for camouflage, cover, and concealment, the BTG masked the strengths of its offensive logistic preparations and staging or assembly arrays, and convinced the enemy commander that the threat main effort would occur in what was actually a supporting effort and deception. This BGT deception complemented the BGT commander's ability to mass combat power in both time and location to succeed in breaching and securing a penetration of enemy main defenses, allowing rapid exploitation into the enemy rear areas for defeat of the enemy deliberate defense and destruction of significant enemy forces in zone.

The BTG commander accomplished his mission. He conducted offensive fires and maneuver by directing where and when key actions would occur to create and exploit vulnerabilities in the enemy defense. Once combat actions were initiated, a continuous attack disrupted the enemy's combat system, with particular attention against designated systems critical to enemy command and control. Targeting enemy combat support and combat service support was similarly critical to degradation of enemy capabilities. Without the sustainment and support of these systems, enemy forces in direct contact with the BTG attack quickly became vulnerable to defeat or destruction.

The BTG used its combined arms task organization—and support from higher headquarters—to optimize the combat systems of its mechanized infantry, tank, and antitank maneuver and fires forces. Tactical actions for fires in depth, along with augmentations from higher headquarters, provided an integrated approach to massed fires and effective maneuver of ground and aerial forces. Task-organized capabilities with the maneuver forces included but were not limited to:

- Designated cannon and howitzer artillery and mortars placed well forward in zone;
- Designated cannon and rocket artillery dispersed in depth and integrated for survivability and rapid repositioning after fire missions.
- Air defense systems well forward, with maneuver forces to provide integrated area coverage throughout the zone;
- Engineers task-organized with designated maneuver forces for support of mobility and countermobility tasks;
- Unmanned aerial vehicles for reconnaissance and surveillance in conjunction with C2 and fires coordination by ground and aerial maneuver forces;
- Electronic warfare (EW) and other INFOWAR capabilities support for deception, target acquisition and tracking, electronic attack, satellite link jamming or disruption, and spoofing of unmanned aircraft and global positioning systems;
- Force support from SPF, with particular value in coordinating actions with affiliated irregular forces and RISTA assets; and
- Force affiliation with insurgent cells, guerrilla units, criminal organizations, and supportive civilian members in the relevant population of the AOR.

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—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. 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.

Opposing Forces

An OPFOR is a plausible, flexible, and free-thinking mixture of regular forces, irregular forces, and/or criminal elements representing a composite of varying capabilities of actual worldwide forces and capabilities (doctrine, tactics, organization, and equipment). The OPFOR is used in lieu of a specific threat force for training and developing US forces. The OPFOR is tailored to replicate highly capable conventional and unconventional threats that, when combined, can replicate hybrid threats and their strategies as further described in the US Army Training Circular (TC) 7–100 series.

Army Regulation 350-2, *Operational Environment and Opposing Force Program*

Figure 10. Opposing forces for training, professional education, and leader development

The ability to represent or replicate many of these actual threat capabilities 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] Training Circular 7-100.2, Opposing Force Tactics is in review at TRADOC G-2 ACE Threats Integration Directorate for update and revision in fiscal year 2018. Periodic information updates will be presented in future issues of the *Red Diamond* newsletter.

[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 2-33–2-35 and 8-38–3-39.

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

[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 2-33, 2-36, and 2-47.

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

[6] Headquarters, Department of the Army. Training Circular 7-101, Exercise Design Guide. TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. November 2010. Appendix B. See also TRADOC G-2 Handbook 1.09, April 2017.

[7] US Army, TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. TRADOC G-2 Handbook 1.09, Opposing Force Tasks: Collective Company/Subordinate Tasks. April 2017.

[8] 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. Chapter 3.

[9] Headquarters, Department of the Army. Training Circular 7-100.2, Opposing Force Tactics. TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. 9 December 2011. Para 2-52.

[10] 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.

[11] 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 2-56–2-57.

[12] 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 9-20–9-21, 9-27, 9-39, 9-80, and 9-105.

by Jim Bird, TRADOC G-2 ACE Threats Integration (IDSI Ctr)

Pray for Manchester, Pray for Marawi

In the days leading up to Ramadan, Philippine President Rodrigo Duterte and selected members of his cabinet traveled to Russia on a diplomatic mission. No sooner had they reached their destination than world media attention fixated on Manchester, England, where on 22 May 2017 a Muslim militant detonated a homemade bomb following an Ariana Grande concert. Despite the 23 deaths and scores of injuries resulting from the terrorist attack, few would argue that a single deranged perpetrator and perhaps his handlers seriously endangered the national existence of the United Kingdom.[1] The same could not be said for the storm of violence that erupted approximately 7,000 miles away in Marawi City, on President Duterte's home island of Mindanao. There, on 23 May 2017, elements of the Armed Forces of the Philippines (AFP) and Philippine National Police (PNP) raided a safe house to arrest an Islamist extremist and take him into federal custody. The authorities got more than they bargained for: a firefight erupted that ended by nightfall in a standoff, leaving three members of the government security force dead and eleven others wounded. Government forces backed off overnight, throwing a cordon around the city of 200,000 while they waited for daylight and the arrival of reinforcements.[2]

Figure 1. Peacetime view of Marawi City, overlooking Lake Lanao

This article is the first of a two-part series. The initial component provides an overview of the siege—including an information warfare (INFOWAR) dimension—that confronted national security forces (NSF) in the days following the initial firefight; discusses some unique strategic and tactical considerations in play within the operational environment; and describes some of the major threat actors involved. A follow-on article, to be published at a later date, will discuss the tactical evolution of the siege between 23 May, when President Duterte imposed martial law, and 18 July, when he formally asked the Philippine congress to extend the period of martial law until the end of calendar year 2017.[3]

As Philippine authorities tried to draw what was going on in Marawi into sharper focus, it was at least clear that events transpiring on Mindanao amounted to a national emergency. By 2200 local time in the Philippines, President Duterte had cut short his diplomatic visit to Moscow and invoked martial law in Mindanao, based on authority codified in the country's national charter. After meeting briefly with Russian President Vladimir Putin, Duterte departed Moscow almost immediately. As a presidential spokesperson put it, "The presence of the President, the physical presence, is needed in the Philippines. This is the President's assessment; and his priority is always the protection of each and every Filipino."[4]

Figure 2. Philippine National Police escort noncombatants out of Marawi

Little time passed before Filipinos started making comparisons between the Manchester suicide bombing and the terrorist assault on Marawi. The BBC reported that "in the wake of the…attack at Manchester Arena, people around the world rallied to support the victims, using [social media] hashtags like 'Pray for Manchester' and

'we stand together.'"[5] In similar fashion, albeit on the other side of the world, "More than 1.3 million tweets used the hashtag 'Pray for Marawi,'" as locals streamed out of the stricken city and towards evacuation centers being established throughout Mindanao.[6] In its entirety, the island group that bears the name of Mindanao is the most culturally diverse region of the Philippines, and incidentally includes the largest concentration of citizens who subscribe to the teachings of Islam.[7]

Despite the wide divergence of geographical, demographic, and tactical aspects of each respective attack, both the Manchester bombing and the terrorist assault on Marawi share one important characteristic in common: the Islamic State of Iraq and Syria (ISIS) as a source of inspiration and focus of allegiance. Indeed, ISIS claimed responsibility for both attacks. A 23 May 2017 statement broadcast on ISIS media channels hailed the Manchester bombing perpetrator as "one of the soldiers of the caliphate," and suggested that the attack was retribution for "transgressions against the lands of the Muslims."[8] On the same day, Philippine presidential spokesperson Ernesto Abella confirmed that reports of outrages committed in Marawi were being streamed from ISIS' website in the Middle East.[9]

Although these attacks brought tragedy to both the United Kingdom and the Philippines, the terrorist siege of Marawi clearly jeopardized the ability of the Asian country to govern over one-third of its territory and 22 million people—roughly the same proportion of its population.[10]

Figure 3. Republic of the Philippines

The Lay of the Land

Figure 3 shows the island group that comprises the Republic of the Philippines, as well as the relative positions of Manila (the national capitol) and Marawi City, the capitol of Lanao del Sur Province, where the firefight broke out on 23 May.

As mentioned above, the protracted Marawi fight directly impacts a region that contains the Philippines' highest concentration of Muslim citizens. This island group, officially designated the Autonomous Region in Muslim Mindanao (ARMM), is highlighted in red in Figure 4.

Figure 4. Autonomous Region in Muslim Mindanao

Lanao del Sur is one of five provinces encompassed by the ARMM, and Marawi City is its capitol. Figure 5 shows Lanao del Sur and neighboring provinces. Marawi City is highlighted in red.

Intelligence Failure with a Positive Outcome

It was not supposed to be a firefight. In short, a bid by Philippine security forces to capture Isnilon Hapilon—a fugitive leader of the Abu Sayyaf terrorist group and long sought by the AFP and PNP—first went awry, then spiraled out of control. When national security forces attempted to serve arrest warrants, they were met with fierce resistance and an unexpectedly high concentration of small-arms fire. Almost immediately, beleaguered Abu Sayyaf fighters appealed to their local Maute group allies for assistance. As these militant reinforcements arrived overnight, they fanned out to occupy several establishments throughout Marawi City. Their targets included the city hall, a nearby medical center, and the Marawi police office and city jail. They set fire to the jail, releasing over 100 prisoners in the process. After firing on the Camp Ranao military base in the northern part of town, in the southern part they

Figure 5. Lanao del Sur Province and Marawi City

torched a cathedral, seized hostages (including the local priest), and destroyed religious paraphernalia and icons. Showing an equal contempt for Presbyterians, the militants burned several buildings on the Dansalah College campus. They also tried to block approaches to Marawi by occupying key bridges leading into the city.[11]

In the night of 23 May 2017, Marawi city was under blackout conditions. Abu Sayyaf and Maute fighters infiltrated strategic positions that offered clear fields of fire, while trapped civilians hunkered down and sheltered in place to avoid drawing fire from either the militants or the NSF. Meanwhile, government authorities took to the airwaves to advise the local populace to keep a low profile, trying to minimize the risk of noncombatant casualties being inflicted by forces on both sides. They were also told to stand by for further instructions, which would include provision for an impending noncombatant evacuation.[12]

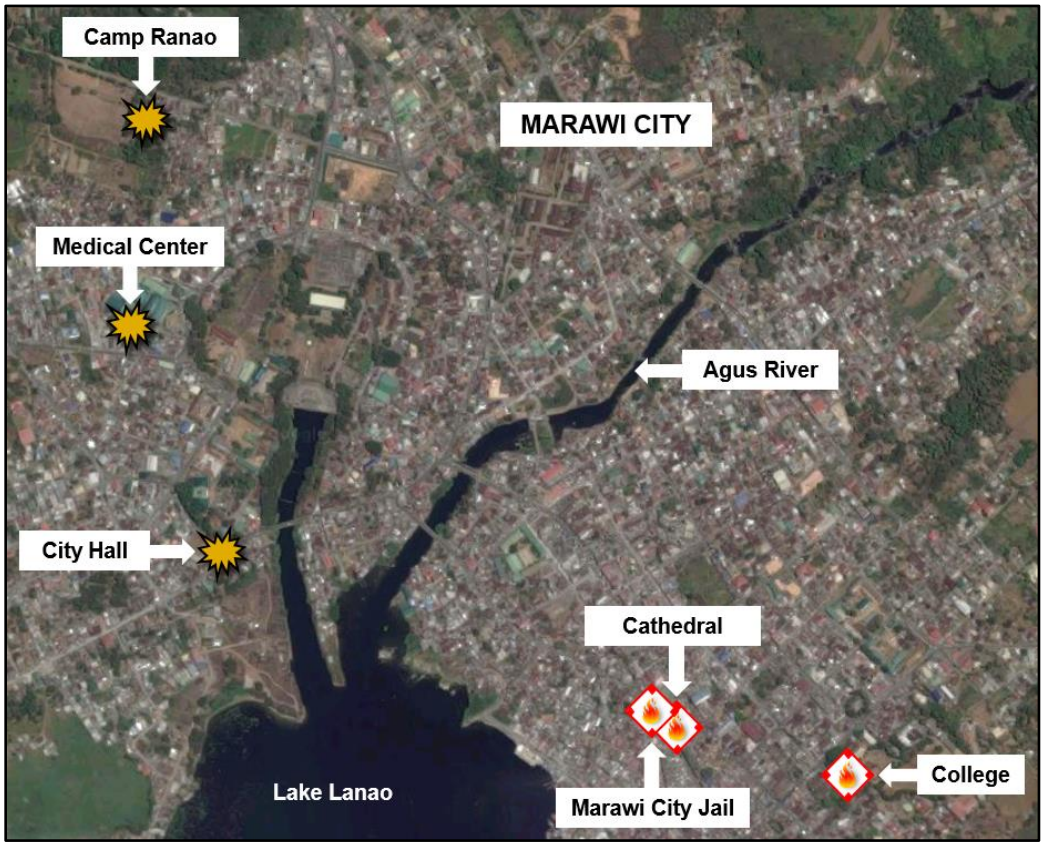


Figure 6. Positions attacked by militants, 23–24 May (Google Maps/ACE-TI)

Local civil authorities apparently had little, if any, foreknowledge of a planned raid by security forces to capture an infamous terrorist leader. A government official noted during a press conference that the Abu Sayyaf group and the Maute group were thought to be in disarray earlier in the year, but that it was becoming apparent that they enjoyed considerable support in the vicinity of Marawi City, which enabled them to infiltrate the local area undetected.[13] He also indicated that Isnilon Hapilon's presence was the primary reason for conducting the raid and, had he not been discovered seeking medical attention in Marawi, no raid would have occurred.[14] Hapilon was thought to be seeking medical attention because of wounds he sustained from a military airstrike in January.

From a public relations point of view, the fight in Marawi embarrassed the Philippine intelligence community, at least initially. In the early phases of the battle, enemy strength estimates ranged from as few as fifteen militants to as high as several hundred. Armed Forces Chief General Eduardo Año initially indicated that about 50 gunmen had entered the city, while Marawi City Mayor Majul Usman Gandamra placed the figure at anywhere between 100–200. Over time, both of these estimates would be revised drastically upward. Gandamra later admitted that the attack caught local officials off-guard, and indicated that they knew something was about to happen but underestimated "the number of Maute militants who entered the city."[15] When asked whether Marawi had fallen victim to an intelligence shortfall, Defense Secretary Dilfin Lorenzano denied that any intelligence failure had occurred, and suggested that the real problem pertained to how the intelligence was interpreted.[16]

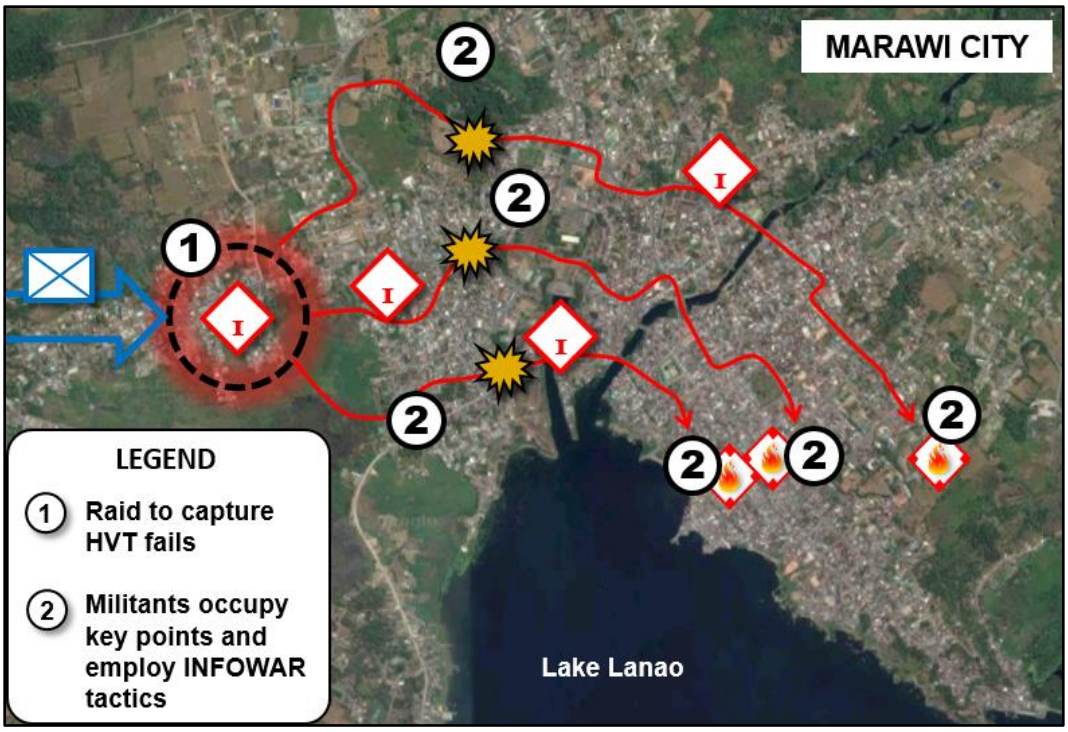


Figure 7. Events of 23–24 May (Google Maps/ACE-TI)

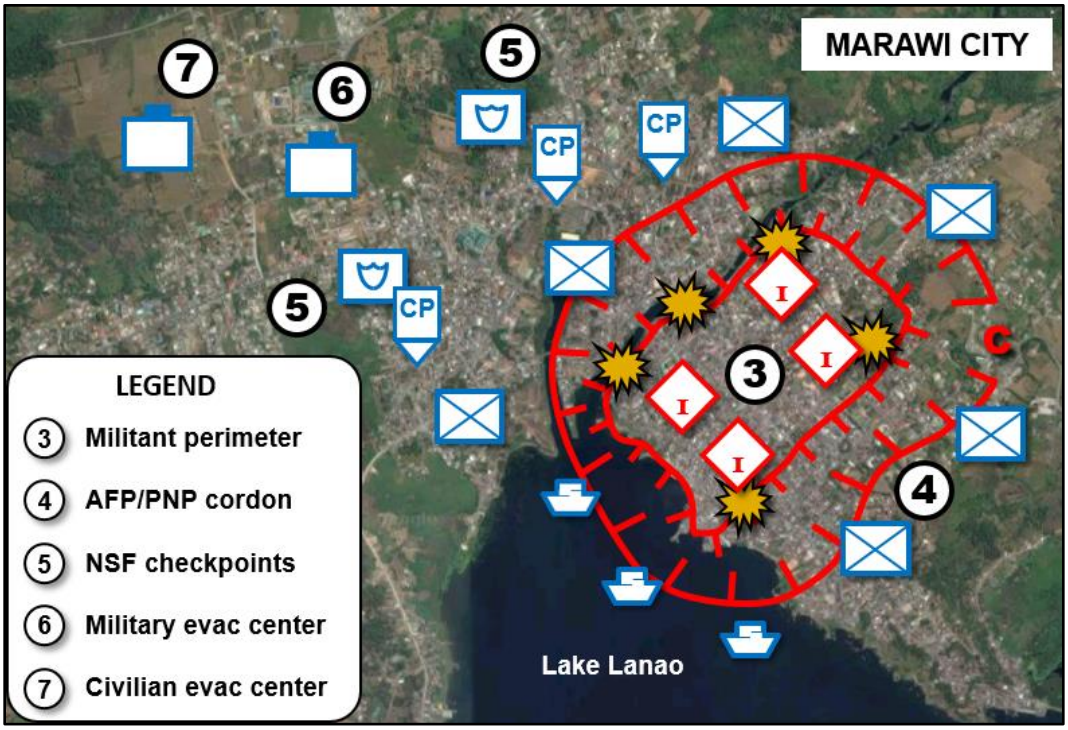


Figure 8. Situation prevalent after 25 May 2017 (Google Maps/ACE-TI)

Conservative estimates of enemy strength, logistical support, and tenacity initially led to government overconfidence concerning expectations of when the AFP and PNP would be able to bring the terrorists to bay and definitively win the battle. On 24 May, military sources indicated that friendly reinforcements were being blocked by rebel forces and that "Maute snipers and booby traps were hampering operations which the army said could last three more days."[17] Once in position around Marawi, the AFP and PNP soon began to gain the upper hand, at least to the extent of shrinking the militant perimeter inside the city (Figure 8). That said, all did not go well. After the initial contact with the enemy on 23 May, the NSF began a series of adjustments to its timetable for neutralizing the rebellion.

Figure 9. AFP soldiers deploying to Marawi

By 29 May—a week into the fighting—the official death toll stood at 19 civilians, 17 soldiers, 3 PNP personnel, and 65 militants. The death toll was expected to climb much higher as security forces encountered improvised explosive devices and employed helicopter gunships to penetrate the city's public market area, which—based on the pungent smell that pervaded the area—was thought to be full of decomposing corpses.[18] Despite incessant pressure from the Philippine military, an undetermined number of militants remained dug-in at various pockets around the city, where an estimated 2,000 residents were still believed to be trapped. At that point in the fighting, Marawi City Police Chief Parson Asadil said of the terrorists, "These guys know how to fight. It looks like they have had some training."[19] Eventually the estimated time required to quash the rebellion would grow from three days to more than two months. At length, the Philippine president would request an extension of the 60-day martial law period through the end of the year, based on a growing realization that "the existing rebellion in Mindanao…will not be quelled completely by 22 July 2017."[20]

In the face of all the negative news about trapped civilians, intelligence lapses, and mounting casualties, the Philippine army could at least find solace in one positive outcome: its aborted raid had caught the enemy midstream in plotting an elaborate takeover of Marawi. According to Major General Rolando Bautista, the commander who ordered the raid on Hapilon's safe house, the military had gotten wind of an impending terrorist strike against Marawi "two or three weeks before May 23."[21] Tipped off by local residents, authorities observed a gathering of suspicious personalities. These locals helped police distinguish individuals who were residents of the barangay (i.e. neighborhood) from those who were not.[22] The AFP and PNP were hoping to locate Abdullah Maute and Omarkhayam Romato Maute, brothers and ringleaders of a family-led organization that recently swore allegiance to ISIS. Instead, they learned—much to their surprise—that Isnilon Hapilon was present in Marawi. Though not their original quarry, Hapilon emerged as a classic target of opportunity. "If we did not act," said General Bautista, "then he [could] go away. We've been looking for Hapilon for so many months."[23] Accordingly, based on what General Bautista believed to be credible information on a high-value target (HVT), he authorized the raid.

Figure 10. Isnilon Hapilon (yellow headscarf) and Abdullah Maute (long hair, standing), at planning table

Although the raid against Hapilon's lair unexpectedly mushroomed into a much larger firefight, Bautista insisted that it prematurely exposed a clandestine terrorist operation that would have produced far worse results for the Philippines had it not been sprung early by the NSF.[24] A report generated by the Solicitor General of the Philippines (OSG) corroborated General Bautista's interpretation of events. It called the 23 May siege of Marawi City "a pivotal event in a grander scheme to dismember Mindanao from the rest of the Philippine territory and pledge its allegiance to the Islamic State of Iraq and Syria."[25] Quoting the 45-page OSG document, ABS-CBN News reported that videos and other items gathered during the raid on Hapilon's safe house "revealed the terrorists intended 'to raze the entire city of Marawi on the day of Ramadan…26 May 2017' so that the siege of Marawi would serve as a 'precursor for other terrorist groups to stage their own uprising across Mindanao.'"[26] The intent behind these simultaneous uprisings was "to establish an ISIS wilayah (administrative division or region) in Mindanao, with the Marawi siege 'setting the stage for this purpose.'"[27]

The 12 June 2017 OSG document also explained why the terrorists were able to efficiently fan out and occupy key terrain and establishments throughout Marawi so rapidly once the fighting started: It was essentially what they intended to do based on their original plan, although the government raid effectively preempted it and forced them to execute it prematurely. Armed ISIS militants drove through town and quickly occupied key positions in dense urban terrain. Snipers

stationed atop high-rise buildings awaited the advance of government troops and, when they came within range, brought them under fire.[28] According to ABS-CBN, the OSG report confirmed rebel possession of a "large arsenal of military hardware, including RPGs [rocket propelled grenades] that can destroy tanks and [an] inexhaustible amount of ammunition for high-powered assault rifles."[29] By the time the OSG report was published, the estimated number or terrorists had grown to 500.

Foreign Fighters: Strategic Dimension of a Tactical Fight

The ground combat that ensued throughout the waning days of May and the two months that followed was a close-quarters fight that played out street-by-street, house-to-house, and sometimes room-to-room.[30] Meanwhile, only a few days passed before AFP spokesperson Brigadier General Restituto Padilla confirmed publicly that of 12 terrorists killed during a recent firefight, "half of them are foreigners."[31] They included Malaysians, Indonesians, and Singaporeans. According to an al Jazeera journalist, such an announcement in a public forum was "a rare admission" by Philippine authorities "that outsiders were collaborating with domestic groups…But for years, the Philippine military denied even the existence of Maute and its links with ISIL [ISIS]."[32] That the rebellion caused President Duterte to curtail his Russian visit, impose martial law, and return home immediately spoke for itself regarding the importance Philippine authorities attached to the militant threat. Now, the recent turn of events inspired Solicitor General Jose Calida to explain how the discovery of foreign fighters on Philippine soil was a game-changer: "What is happening in Mindanao is no longer a rebellion of Filipino citizens. It has transmogrified into an invasion by foreign fighters. They want to make Mindanao part of the caliphate."[33]

International concern that ISIS might expand its geographical reach dates to November 2014 when, according to analysts at the Washington Institute for Near East Policy, it "announced the addition of new provinces outside its core territory in Syria and Iraq."[34] ISIS provinces in the Arab world include Libya, Yemen, the Sinai, and the Hejaz (a region west of present-day Saudi Arabia); those outside the Arab sphere include the Caucasus, Afghanistan/Pakistan, and Nigeria. The Washington Institute also indicated that "other groups, such as those in the Philippines…remain unrecognized by [the] IS [ISIS] core as official provinces despite having pledged an oath of allegiance to the Islamic State. IS has issued criteria for prospective affiliates and appears to be savvy to maintaining the value of its brand by not…'compromising its standards' or expanding 'too quickly.'"[35]

Figure 11. Philippine cabinet members inspect firearms captured from militants

By 26 May 2017, different Philippine government agencies were sending out mixed messages. Even as the Solicitor General was declaring that the rebellion had morphed into an invasion, a military spokesperson denied the existence of any concrete evidence linking the rebellion to sources outside the Philippines.[36] Earlier, in the first hours of fighting, a member of President Duterte's cabinet described the rebels as "groups that have been auditioning for recognition [by] ISIS."[37] Predictably, the new discovery of foreign fighters fueled international speculation that downward-spiraling fortunes in Iraq and Syria made ISIS less concerned about maintaining the value of its brand and increased its eagerness to establish provinces beyond its core region in the Middle East. The OSG's aforementioned report supporting President Duterte's martial law declaration cited an "ISIS report in April 2016 which announced the appointment of ASG [Abu Sayyaf] leader Hapilon as the emir of all Islamic State forces in the Philippines."[38] A subsequent ISIS video released on 21 June the same year proclaimed Hapilon "the mujahid authorized to lead the soldiers of the Islamic State in the Philippines."[39] A year later, it was dawning on Philippine leaders that their indigenous terrorist groups' auditions for ISIS recognition had come to fruition, and posed a clear and present foreign danger to the sovereignty of their island nation.[40]

During the second week of the Marawi siege, alarm spread among the Philippines' neighbors regarding the potential establishment of an ISIS foothold in southeast Asia. In early June, Malaysia, the Philippines, and Indonesia agreed to pool resources in conducting joint naval patrols in the waters near Mindanao. The sea patrols began on 19 June, with joint air patrols scheduled for a later date. Speaking to delegates attending a Singapore conference on 3 June, Malaysian Defense

Minister Datuk Seri Hishammuddin Hussein declared, "If you talk about [the] Sulu Straits, [it] would involve Malaysia, Indonesia and the Philippines. So…we decided at least these three countries, to avoid being accused of doing nothing, the three of us took the initiative to have the joint patrols…in the Sulu Straits."[41] The Sulu Strait initiative was a proactive move to seal the porous maritime borders of these three nations from penetration by threat actors.

The ISIS threat to the Philippines also affects the defense interests of the United States. Although the US military presence in the Philippines has diminished in recent years, the Associated Press reported that US officials feared that "ungoverned areas in the mostly Muslim region around Marawi could make the area a terror hub."[42] In June, Defense Secretary James Mattis told a meeting of regional defense chiefs that "together we must act now to prevent this threat from growing," and stressed to the US Congress the importance of sharing intelligence as an alternative to deploying US soldiers.[43] Republican Senator Joni Ernst of Iowa, who chairs a US Senate panel on emerging threats, could not substantiate ISIS direct involvement in Marawi, but indicated that "they are certainly trying to get fighters into that region…We need to address the situation. It should not get out of control."[44]

Figure 12. Marawi City, taken on 15 June 2017

Meanwhile a small number of US Special Forces personnel remained on the ground in Mindanao, shoring up the situational awareness of the AFP. AFP spokesperson Brigadier General Restituto Padilla confirmed in mid-June that "there are some US personnel who are operating equipment to provide information on situation awareness to our troops."[45] General Padilla told reporters that "in a battle or a place of battle, the most important thing for a commander is to know what is happening in the entire area…The assistance that [the Americans] are giving is about that."[46]

The US was hardly the only major power to take an active interest in the Marawi siege. President Duterte told Russian President Vladimir Putin that he was "counting on Russia to supply weapons to the Philippines to fight terrorism."[47] According to the Russian state news agency Tass, Duterte also said, "of course our country needs modern weapons, we had orders in the United States, but now the situation there is not very smooth and in order to fight the Islamic State, with their units and factions, we need modern weapons."[48] Meanwhile, late in the initial 60-day martial law period, the Chinese seized an opportunity to send a shipment of small arms and ammunition to the Marawi operational environment. This marked the first occasion since President Duterte assumed office that the Chinese had sent a sizeable shipment of military aid to the Philippines, and Duterte hailed it as "the dawn of a new era in Philippine-Chinese relations."[49]

Threat Actors and Perpetrators

Filipinos traveled a rocky road to national sovereignty after gaining their independence following World War II. Between 1946 and 1965—when Ferdinand Marcos was elected President—relations between Muslims and Christians on Mindanao were considered strained but essentially peaceful. The situation deteriorated following Marcos' rise to power in 1966, and eventually culminated in a rebellion by the separatist Moro National Liberation Front (MNLF). At the time, the MNLF boasted two international backers: the regime of Libyan president Muammar Gaddafi, and the government of Malaysia. When Marcos refused MNLF demands for Mindanao's independence a civil war ensued, with Muslim factions arrayed on one side and the Philippine military and assorted Christian paramilitary forces on the other.[50]

The bloodshed abated in 1976 with the signing of the Tripoli Agreement, under which the Philippine government formally acknowledged Muslim aspirations for autonomy, in return for the MNLF renouncing its separatist agenda. The agreement caused some of the more radical MNLF factions to break away from the parent organization to form a splinter group—the Muslim Islamic Liberation Front (MILF)—which in its turn accepted a subsequent government promise of support for eventually creating a new Muslim autonomous region to be called *Bangsamoro*.[51] Over time, as the influence of militant

Islam spread throughout the Middle East, the Afghanistan/Pakistan region, and in some areas of southeast Asia, a corresponding set of disaffected militant groups proliferated in the Philippines.

One of the more notorious breakaway factions, the Abu Sayyaf group, split from the MLNF in 1991 to pursue a more militant approach to harassing and undermining the Philippine government. The English translation of Arabic Abu Sayyaf means "father of the swordsman."[52] According to the BBC, the group named itself "after a mujahedin fighter in Afghanistan in the 1980s, where a number of its members fought against the Soviet-backed regime."[53] Abu Sayyaf claimed responsibility for perpetrating the worst terrorist attack in Philippine history: the February 2004 Superferry 14 bombing—in which 116 people lost their lives.[54]

Figure 13. [Superferry 14 in its heyday (above) and on 27 February 2004 (below)]

Over time, the group's tactics have encompassed kidnapping and extortion. Its current commander, Isnilon Hapilon, is regarded as one of Asia's top militant leaders. In 2002, the US Department of Justice indicted Hapilon for his role in the kidnapping of 20 hostages from a Philippine resort. Three US citizens numbered among the victims, one of whom was subsequently beheaded. Now on the department's Most Wanted Terrorist List, Hapilon currently has a $5 million price on his head.[55]

The Philippine armed forces conducted an operation in February 2017 that resulted in the death of Muamar Askali, another Abu Sayyaf commander, and five of his compatriots. The success of that operation led the AFP to mistakenly conclude that Abu Sayyaf had been rocked back on its heels and no longer presented a viable threat beyond a few small island bases in the extreme southwest reaches of Mindanao. This year's Marawi siege effectively disabused Philippine authorities of the notion that the Abu Sayyaf threat had been neutralized. Hapilon's aptitude for forging alliances and unifying groups with disparate interests made him a prime candidate for leading the ISIS franchise in Southeast Asia.[56]

The Maute group is the largest band of four major local groups to bolster the militant ranks in Marawi. Virtually unknown three years ago, the Mautes started out as a wealthy family with political connections and grounded in matriarchy: the mother, Farhana, is the central figure. This clan, according to Reuters journalists, "were criminals who morphed into militancy."[57] When the Mautes became embroiled with a local official over awarding government contracts, the dispute blossomed into a clan feud in which the Mautes portrayed themselves as disciples of ISIS. Joseph Franco, a research fellow at Singapore's S. Rajaratnam School of International Studies, argues that the Maute group's "tactical use of imagery took on a life of its own. And now we have this Maute Group, who call themselves IS-Ranao," after a traditional name for a region in Mindanao that includes Marawi.[58] Mohammed Ampuan, a Marawi native who now resides in Manilla, observed that the Mautes "want a society faithful to Allah."[59]

Figure 14. [Omarkhayam Maute (left) and Abdullah Maute (right), from a PNP poster]

Within this Maute family, the parents play an important role, albeit mainly as figureheads, with the matriarch serving as the central symbolic figure. The parental offspring include seven sons, all said to occupy key leadership positions in the militant group that bears the family name. Among these siblings, Omar and Abdullah Maute are probably the most notorious and sought-after by Philippine authorities. The two men surfaced as ringleaders of the local ISIS-inspired paramilitary forces that answered

Abu Sayyaf's call for reinforcements during the 23 May AFP/PNP raid on Hapilon's safe house. Both brothers studied in the Middle East, where they became fluent in Arabic and, at some point, radicalized before returning to the Philippines. On his Facebook page, Omar Maute described himself as "a walking time bomb."[60] The Maute brothers were reportedly killed during the Marawi siege, but they have been presumed dead before. In July, The Manilla Inquirer reported an eyewitness confirmation that Abdullah remained alive and unhurt.[61]

The Bangsamoro Islamic Freedom Fighters (BIFF) and Ansar al Khilafah (AKP) are both breakaway factions, formerly aligned with the MILF, that threw their weight behind the uprising in Marawi. President Duterte's 19 July letter asking for the extension of martial law in Manilla blamed the BIFF for "at least thirteen (13) violent incidents since 23 May 2017, most of which involved harassments of AFP, PNP and paramilitary detachments and patrol bases."[62] Though less numerous than the Maute group or Abu Sayaff, these two organizations complicated the challenges authorities faced in imposing Duterte's 23 May declaration of martial law, and did their part to increase the AFP/PNP casualty figures.

A Threat Greater than the Sum of its Parts

From a both a strategic and tactical perspective, the various militant Islamist groups discussed above are less important individually than the consolidated organization they combined to form: the Dualah Islamya Wilayatul Mashriq (DIWM), the self-styled ISIS province in East Asia. Rappler reports that "the DIWM is the umbrella organization of all armed groups in the Philippines that have pledged allegiance to ISIS."[63] The Philippine Solicitor General's Office declared that "the four rebel groups find their roots and have solidified their membership base in different provinces and cities in Mindanao, and the success of establishing a wilayah in Mindanao demands a consolidation of their efforts; hence, the need to appoint one head…as the emir."[64] Isnilon Hapilon occupied the top position of the ISIS command and control structure in Mindanao, and was likely chosen for skill sets noted above. ABS-CBN News reported that the OSG told the Philippine Supreme Court that Hapilon's group performed a "symbolic ritual" on 31 December 2016, "for the purpose of uniting…the ISIS-inspired rebel groups in mainland Mindanao."[65] As of 18 July 2017, when President Duterte requested that the Philippine Congress extend martial law until the end of the calendar year, the ISIS leadership infrastructure remained intact despite the attrition inflicted on rebel forces by the AFP and PNP.

Figure 15. ISIS propaganda on Marawi social media

The INFOWAR Dimension

It became apparent early in the uprising that the ISIS-inspired militants knew a thing or two about leveraging the power of social media to make their Marawi exploits seem more impressive than they really were. So adept were the militants at spreading their propaganda message that, two days into the fight, Western Mindanao Command spokesperson Captain Jo-Ann Petinglay noted their skills at inflating their own strength levels: "They tried to paint the scenario that they have seized major areas in Marawi using videos and photos spread on social media."[66] According to Petinglay, as national security

Figure 16. PNP public advisory cautioning against spreading unverified information

forces first entered the city's residential area, locals became unwitting dupes of the Maute group by "reposting the visual materials showing the militants on the streets brandishing their guns and black flags," thus making an isolated local incident appear universal and widespread.[67] During the first day of fighting, the presence of civilians hampered AFP and PNP operations because of concern over causing collateral damage and casualties among noncombatants.

Meanwhile, by 24 May Philippine authorities were promoting a counter-narrative, insisting that the situation in Marawi was stabilizing and cautioning the public against inadvertently spreading enemy propaganda. "We are not toning down the issue," declared PNP spokesperson Dionardo Carlos; "What we are doing is not to allow propaganda."[68] Authorities enjoined citizens to think about their country's national interest and to be more discerning in posting and sharing photos on social media, in order to avoid spreading inaccuracies and lending credence to false information.

Threat Doctrine Manifestations and Training Implications

The siege of Marawi provides an apt case study of actions taken by opposing forces (OPFOR) to exploit the advantages of dense urban terrain in a multi-domain battle. This is especially the case from an INFOWAR perspective. Appendix A of Training Circular (TC) 7-100.3, *Irregular Opposing Forces*, defines information warfare as "specifically planned and integrated actions taken to achieve an information advantage at critical points and times."[69] Militant groups in Marawi definitely initiated such integrated actions to spread the ISIS propaganda message throughout the course of the siege. Perception management and information attack are two terms included among seven elements of INFOWAR listed in the appendix. Perception management pertains to "measures aimed at creating a perception of truth that best suits irregular OPFOR objectives," and an information attack is the "intentional disruption or distortion of information in a manner that supports accomplishment of the irregular OPFOR mission."[70] The Maute group, Abu Sayyaf, and their allies initially succeeded in creating a perception among the local populace that their forces were much larger and more successful than was actually the case. A sample of this perception leaching into the international news media was provided when a publication associated with the New York Daily News reported that "the Philippine Army withdrew from most of [Marawi] city on Tuesday morning, thereby making it the first city in Southeast Asia to come under Islamic State control."[71] In fact, this was being reported even as AFP and PNP reinforcements were deploying to Marawi for the purpose of neutralizing the insurgents. There is nothing to prevent training developers and scenario writers from using the Marawi case study as a point of departure for sharpening soldier skills in meeting the multi-dimensional challenges inherent in conducting operations in a dense urban terrain environment.

About five weeks into the Marawi siege, Admiral Harry Harris, Commander, US Pacific Command, delivered an address at the Australian Strategic Policy Institute at Brisbane, Australia. His remarks are instructive for Army units and leaders whose missions could encompass a potential deployment to the Asia-Pacific region: "Marawi is a wake-up call for every nation in the Indo-Asia-Pacific. Foreign fighters are passing their ideology, resources, and methods to local, home-grown next-generation radicals. So we must stop ISIS at the front end and not at the back end when the threat can become even more dangerous."[72] Although delivered in the context of emphasizing the need for international cooperation, Admiral Harris' comments also imply a heavy responsibility for tactical–level Army leaders. Depending on circumstances, their task could entail meeting a strategic challenge by conducting tactical operations to neutralize a deft and adaptive adversary.

Notes

[1] Pritha Paul. "Philippine President Rodrigo Duterte Invokes Martial Law in Marawi." Yahoo! News. 23 May 2017.

[2] Pritha Paul. "Philippine President Rodrigo Duterte Invokes Martial Law in Marawi." Yahoo! News. 23 May 2017; Romeo Ranoco. "Thousands Flee Philippine City After Rebel Rampage Claimed By Islamic State." Yahoo! News. 24 May 2017.

[3] ABS-CBN News. "READ: Duterte's Letter to Congress Asking for Mindanao Martial Law Extension." 19 July 2017.

[4] Pritha Paul. "Philippine President Rodrigo Duterte Invokes Martial Law in Marawi." Yahoo! News. 23 May 2017.

[5] BBC News. "How The Manchester Attack Echoed in the Philippines." 25 May 2017.

[6] BBC News. "How The Manchester Attack Echoed in the Philippines." 25 May 2017.
[7] Cecil Morella. "Fear, Confusion as Philippine Muslim City Burns." Yahoo! News. 29 May 2017.
[8] Kate Samuelson and Jared Malsin. "ISIS Claims Responsibility For Manchester Concert Terrorist Attack." Time. 23 May 2017.
[9] Pritha Paul. "Philippine President Rodrigo Duterte Invokes Martial Law in Marawi." Yahoo! News. 23 May 2017.
[10] Beaumont Enterprise. "Top Militant Hapilon Often Has Eluded Philippine Authorities." 24 May 2017; Al Jazeera. "'Foreigners Fighting' With ISIL-Linked Philippine Group." 26 May 2017.
[11] Mikas Matsuzawa, Roel Pareno, and John Unson. "Marawi Crisis: What We Know—And Don't Know—So Far." Philippine Star. 25 May 2017; Chris Inton, et al. "Battle For Marawi." Reuters. Accessed 19 August 2017.
[12] Pritha Paul. "Philippine President Rodrigo Duterte Invokes Martial Law in Marawi." Yahoo! News. 23 May 2017.
[13] Pritha Paul. "Philippine President Rodrigo Duterte Invokes Martial Law in Marawi." Yahoo! News. 23 May 2017.
[14] Pritha Paul. "Philippine President Rodrigo Duterte Invokes Martial Law in Marawi." Yahoo! News. 23 May 2017; Beaumont Enterprise. "Top Militant Hapilon Often Has Eluded Philippine Authorities." 24 May 2017.
[15] Mikas Matsuzawa, Roel Pareno, and John Unson. "Marawi Crisis: What We Know—And Don't Know—So Far." Philippine Star. 25 May 2017; ABS-CBN News. "READ: Duterte's Letter to Congress Asking for Mindanao Martial Law Extension." 19 July 2017.
[16] Mikas Matsuzawa, Roel Pareno, and John Unson. "Marawi Crisis: What We Know—And Don't Know—So Far." Philippine Star. 25 May 2017.
[17] Romeo Ranoco. "Thousands Flee Philippine City After Rebel Rampage Claimed By Islamic State." Yahoo! News. 24 May 2017.
[18] Cecil Morella. "Fear, Confusion as Philippine Muslim City Burns." Yahoo! News. 29 May 2017.
[19] Cecil Morella. "Fear, Confusion as Philippine Muslim City Burns." Yahoo! News. 29 May 2017.
[20] ABS-CBN News. "READ: Duterte's Letter to Congress Asking for Mindanao Martial Law Extension." 19 July 2017.
[21] Carmela Fanbuena. "How A Military Raid Triggered Marawi Attacks." Rappler. 29 May 2017.
[22] Carmela Fanbuena. "How A Military Raid Triggered Marawi Attacks." Rappler. 29 May 2017.
[23] Neil Jerome Morales and Tom Allard. "The Maute Brothers: Southeast Asia's Islamist 'Time Bomb.'" ABS-CBN News. 12 June 2017; Raju Gopalakrishnan and Manuel Mogato. "The Mautes of the Philippines: From Monied Family To Islamic State." Reuters. 23 June 2017; Carmela Fanbuena. "How A Military Raid Triggered Marawi Attacks." Rappler. 29 May 2017.
[24] Carmela Fanbuena. "How A Military Raid Triggered Marawi Attacks." Rappler. 29 May 2017.
[25] Ina Reformina. "SolGen Defends Martial Law: Marawi Siege 'A Pivotal Event.'" ABS-CBN News. 12 June 2017.
[26] Ina Reformina. "SolGen Defends Martial Law: Marawi Siege 'A Pivotal Event.'" ABS-CBN News. 12 June 2017.
[27] Ina Reformina. "SolGen Defends Martial Law: Marawi Siege 'A Pivotal Event.'" ABS-CBN News. 12 June 2017.
[28] Ina Reformina. "SolGen Defends Martial Law: Marawi Siege 'A Pivotal Event.'" ABS-CBN News. 12 June 2017.
[29] Ina Reformina. "SolGen Defends Martial Law: Marawi Siege 'A Pivotal Event.'" ABS-CBN News. 12 June 2017.
[30] Carmela Fonbuena. "Marawi Battle Zone: Urban Warfare Challenges PH Military." Rappler. 19 June 2017.
[31] Arlene Lim. "AFP: Foreign Terrorists Are Fighting Alongside Maute Group." Manila Standard. 26 May 2017.
[32] Al Jazeera. "'Foreigners Fighting' With ISIL-Linked Philippine Group." 26 May 2017.
[33] BBC News. "Philippines Violence: IS-Linked Fighters 'Among Militants In Marawi.'" 26 May 2017.
[34] Katherine Bauer, ed. "Beyond Syria and Iraq: Examining Islamic State Provinces." Washington Institute for Near East Policy. November 2016. Pg vii.
[35] Katherine Bauer, ed. "Beyond Syria and Iraq: Examining Islamic State Provinces." Washington Institute for Near East Policy. November 2016. Pg xviii.
[36] BBC News. "Philippines Violence: IS-Linked Fighters 'Among Militants In Marawi.'" 26 May 2017.
[37] Pritha Paul. "Philippine President Rodrigo Duterte Invokes Martial Law in Marawi." Yahoo! News. 23 May 2017.
[38] Ina Reformina. "SolGen Defends Martial Law: Marawi Siege 'A Pivotal Event.'" ABS-CBN News. 12 June 2017.
[39] Ina Reformina. "SolGen Defends Martial Law: Marawi Siege 'A Pivotal Event.'" ABS-CBN News. 12 June 2017.
[40] Neil Jerome Morales and Tom Allard. "The Maute Brothers: Southeast Asia's Islamist 'Time Bomb.'" ABS-CBN News. 12 June 2017.
[41] Agence France-Presse. "Malaysia, Philippines, Indonesia to Kick Off Joint Patrols Off Mindanao to Fight Militants." New Straits Times. 3 June 2017.
[42] Matthew Pennington. "Islamic State Poses A Growing Threat To Southeast Asia." Associated Press. 19 June 2017.
[43] Matthew Pennington. "Islamic State Poses A Growing Threat To Southeast Asia." Associated Press. 19 June 2017.
[44] Matthew Pennington. "Islamic State Poses A Growing Threat To Southeast Asia." Associated Press. 19 June 2017.
[45] Philip C. Tubeza. "Armed US Troops Support AFP Operations in Marawi." Philippine Daily Inquirer. 15 June 2017.
[46] Philip C. Tubeza. "Armed US Troops Support AFP Operations in Marawi." Philippine Daily Inquirer. 15 June 2017.
[47] Associated Press. "Islamic State-Linked Militants Besiege Philippine City." News Corp Australia. 25 May 2017.
[48] Associated Press. "Islamic State-Linked Militants Besiege Philippine City." News Corp Australia. 25 May 2017.
[49] Agence France Presse. "China Donates Arms to Philippines for Raging Islamist Fight." Yahoo! News. 28 June 2017.
[50] Annabelle Quince and Patrick Carey. "Marawi Battle Only Latest Chapter in Long, Fraught History of Islam in the Philippines." Australian Broadcasting Corporation. 29 June 2017.
[51] Chris Inton, et al. "Battle For Marawi." Reuters. Accessed 19 August 2017.
[52] BBC News. "Who Are the Abu Sayyaf?" 30 December 2000.
[53] BBC News. "Who Are the Abu Sayyaf?" 30 December 2000.
[54] ASKET Ltd. "Superferry 14 – Bombing by Abu Sayyaf 2004." 28 February 2017.
[55] Federal Bureau of Investigation. "Most Wanted Terrorists." Accessed 28 July 2017.
[56] Beaumont Enterprise. "Top Militant Hapilon Often Has Eluded Philippine Authorities." 24 May 2017; Jacob Zenn. "Cooperation With Civilians Leads to Killing of Abu Sayyaf Commander." OE Watch. June 2017. Pg 34; Federal Bureau of Investigation. "Most Wanted Terrorists." Accessed 28 July 2017.
[57] Raju Gopalakrishnan and Manuel Mogato. "The Mautes of the Philippines: From Monied Family To Islamic State." Reuters. 23 June 2017; Romeo Ranoco. "Who Are The ISIS-Linked Maute Group Militants Terrorizing the Philippines?" Newsweek. 23 June 2017.

[58] Raju Gopalakrishnan and Manuel Mogato. "The Mautes of the Philippines: From Monied Family To Islamic State." Reuters. 23 June 2017.
[59] Raju Gopalakrishnan and Manuel Mogato. "The Mautes of the Philippines: From Monied Family To Islamic State." Reuters. 23 June 2017.
[60] Neil Jerome Morales and Tom Allard. "The Maute Brothers: Southeast Asia's Islamist 'Time Bomb.'" ABS-CBN News. 12 June 2017.
[61] Jeoffrey Maitem. "Maute Group Leader Seen Alive, Unhurt July 17." Manilla Daily Inquirer. 23 July 2017.
[62] ABS-CBN News. "READ: Duterte's Letter to Congress Asking for Mindanao Martial Law Extension." 19 July 2017.
[63] Rommel C. Banlaoi. "The Maute Group and Rise of Family Terrorism." Rappler. 15 June 2017; Chris Inton, et al. "Battle For Marawi." Reuters. Accessed 19 August 2017; Ina Reformina. "SolGen Defends Martial Law: Marawi Siege 'A Pivotal Event.'" ABS-CBN News. 12 June 2017.
[64] Ina Reformina. "SolGen Defends Martial Law: Marawi Siege 'A Pivotal Event.'" ABS-CBN News. 12 June 2017.
[65] Ina Reformina. "SolGen Defends Martial Law: Marawi Siege 'A Pivotal Event.'" ABS-CBN News. 12 June 2017.
[66] Roel Pareno. "Westmincom: Maute Militants Isolated." Philippine Star. 25 May 2017.
[67] Roel Pareno. "Westmincom: Maute Militants Isolated." Philippine Star. 25 May 2017.
[68] Julianne Love De Jesus. "PNP Warns Against 'Propaganda' Exaggerating Marawi Attack." Manilla Daily Inquirer. 24 May 2017.
[69] 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. Pg A-1.
[70] 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. Pg A-2.
[71] Voice of People Today. "IS Claims Freeing Over 100 Prisoners, Killing 75 Soldiers in Marawi, Philippines—Amaq." 25 May 2017.
[72] Harry Harris. "Challenges, Opportunities, and Innovation in the Indo-Pacific." US Pacific Command. 28 June 2018.

DATE 3.0
Modifications and Additions to the Decisive Action Training Environment

by Laura Deatrick, TRADOC G-2 ACE Threats Integration (CGI Federal Ctr)

This past July, TRADOC G-2 ACE Threats Integration (ACE-TI) published the latest update to the Decisive Action Training Environment (DATE). DATE 3.0 includes many revisions—some minor, others substantial. The largest modifications involve the addition of new groups, changes in country borders, the removal of Kalaria, the addition of a new chapter focused on threat actors, and the minimization of real-world countries and ethnicities. In addition, orders of battle (OBs) for DATE threat actors have been moved to a new chapter, and the scope of Donovia's Physical Environment variable was expanded to include the entire country. This article highlights substantial changes made to this newest edition of the DATE, as outlined in the document's Strategic Setting. A comprehensive list of changes to the DATE OEs is available on the DATE page of ACE-TI's website on the Army Training Network (ATN).

General Revisions

Strategic Setting. Sections were added that address access to the Black Sea and the assignment of countries to US Combatant Commands (COCOMs) in the DATE world. Additional guidance on modifying DATE conditions for exercises was given, including examples of acceptable and unacceptable changes. Explanations of the concepts of "fixed" dates (e.g., January 1969) and "sliding" dates (e.g. six years ago) as used in the DATE were also incorporated.

Borders. Borders for Ariana, Gorgas, and Limaria have been restored to those used in DATE 2.1, as shown below. All maps in DATE 3.0 have been updated to reflect these changes. Related information, such as road miles and percentage of arable land, have also been revised in the affected countries.

Kalaria. All mentions of Kalaria, including its citizens, ethnicity, and language, have been removed from the DATE. Text discussing Limarian conflict with Kalaria has also been removed, resulting in Limaria's main focus being limited to one DATE country—Atropia.

Real-World Countries. All mention of named non-DATE border countries has been removed from the DATE. Most of these mentions have been removed in their entirety. In a few select instances, text referring to a specific country has been modified to refer to an "eastern neighbor" or "regional conflict." All maps were revised to eliminate defined borders for non-DATE countries. In addition, mention of other real-world countries not bordering the DATE OEs has been minimized, and all references to the Global War on Terror (GWOT), Operations Enduring Freedom (OEF), and Operation Iraqi Freedom (OIF) have been removed.

Figure 1. DATE border changes

Elections. The election cycle discussion for each country was augmented. Each one now includes length of term; term-limit information; sliding date(s) of the last election(s); and sliding date(s) of the next election(s). In addition, information is given on when each president was elected and how long he has been in office.

Tables and Timelines. Country-specific tables were added to each country's Physical Environment variables, and timelines of events were added to the Time variables.

Units of Measure. All units of measure, except for those associated with military weapon systems, have been converted from metric to English (Imperial) units.

New Groups. Multiple new threat groups have been added, to include two religious-based violent extremist organizations, One Right Path and The True Believers; a hacking/computer crimes group, Saints of Cognitio; and several country-specific criminal groups. In addition, several new fictional nongovernmental organizations (NGOs) were added.

Threat Actors Chapter. Force structures for OE threat groups—e.g., insurgents—were moved from the individual countries' OBs to the new Threat Actors chapter at the end of Section Two. This chapter also includes a summary table—shown below—listing each threat group by location (countries) and type, as well as a more detailed table. Force structures were added for the violent extremist organizations and the Lower Jangan Army.

Type	Ariana	Atropia	Donovia	Gorgas	Limaria
Criminal	• *Gentlemen's Purdah Society* • *Hacking for Ariana* • *Saints of Cognitio* • Drug and Weapons Organizations	• Al Iksir Cartel • *Amali Diners' Club* • Atropian Organized Crime • Bocyowicz Crime Family • *National Social Media Foundation* • *Pan-Muslim Relief Society* • *Saints of Cognitio*	• Al Iksir Cartel • Donovian Mafia • Jinat Crime Family • *National Inter-Business Cooperative* • *Pan-Caucasus Miner's League* • *Pan-Donovian Law Enforcement Brotherhood* • *Saints of Cognitio* • Criminal Actors	• *Gorgan Tourist Association* • *Hawala Assistance Brotherhood* • *Pan-Caucasus Petrol Distributers* • Criminal Actors	• Abgar Bozian's Bozian Gerdastan • Limarian National Labor Union • Limarian Socialist Democratic Party • *Pan-Caucasus Petrol Distributers* • Criminal Actors
Insurgent/ Guerrilla	• God's Helpers Brigade • Anti-Ariana Insurgent Groups	• Bilasuvar Freedom Brigade • Free Lower Janga Movement • Limarian Liberation Front • Provisional Army of Lezgin • Salasyl • South Atropian People's Army	• Bilasuvar Freedom Brigade • Anti-Donovia Insurgent Groups	• Falcon Brothers • *Jarie Separatists* • People's Liberal Republican Martyrs Group • South Ostremek Separatists • Zabzimek Irregular Forces • Zabzimek Separatists	• Free Lower Janga Movement • Limarian Liberation Front
Violent Extremist	• *One Right Path*	• *One Right Path* • *The True Believers*	• *One Right Path* • *The True Believers*	• *One Right Path*	• *One Right Path*
Unknown	• *NTAT Modeler's Club*				

Table 1. Threat groups in DATE 3.0 (*new groups shown in italics*)

Orders of Battle. The structure of some antitank brigades was modified significantly: all now consist of a brigade headquarters, four antitank battalions, a reconnaissance battalion, a man-portable air-defense system (MANPADS) company, a materiel support company, an engineer platoon, a signal platoon, and a medical company. All Arianian and Donovian motorized infantry divisions now have three motorized infantry brigades instead of two. Some units were added to the military disposition maps in the Military variables and other units changed locations, as reflected in the same maps.

Events Section. Section Three was updated, with many events rewritten in whole or in part. Mission-essential task list (METL) tasks for all events were also updated to conform to the most recent version of the Army Universal Task List (AUTL).

Country-Specific Revisions

Ariana. The province of Alani was broken into two provinces: Alani (new borders) and Karaj. Mentions of Persian ethnicity and culture were removed and replaced with Arianian ethnicity and culture. Likewise, the Persian/Farsi language was replace with Arianian. Three new country-specific threat groups were added: the Gentlemen's Purdah Society, Hacking for Ariana, and the NTAT Modeler's Club, as well as a new NGO. The 92nd Motorized Infantry Division was changed to a mechanized infantry division, and all motorized infantry divisions now have three motorized infantry brigades instead of two. Several subsections were added or rewritten, including Family Authority (Political); Army Doctrine and Tactics (Military); Internal Security Forces (Military); Foreign Military Presence (Military); Joint Capabilities (Military); and Special Considerations (Military).

Atropia. The country was changed from a dictatorship to an oligarchy, and was defined as consisting of provinces that are broken down into rayons and cities. Lower Janga, previously called a region, was clearly defined as a breakaway province of Atropia. Language in the Military variable was revised in places to make clear that the Atropian Army does not have any divisions. Ethnicities, religions, languages, and their relative percentages were modified. Three new country-specific threat groups were added: the National Social Media Foundation, the Pan-Muslim Relief Society, and the Amali Diners' Club. Information was added on techniques commonly used by Salasyl. Several subsections were added or rewritten, including Family Authority (Political); Army Doctrine and Tactics (Military); Internal Security Forces (Military); Reserves and Militia (Military); Foreign Military Presence (Military); Joint Capabilities (Military); and Relative Humidity (Physical Environment).

Donovia. The country's flag was added, as was the long form of its name (United Republics of Donovia). An explanation was added of the war in Gamrun Republic. Three new country-specific threat groups were added: the Pan-Donovian Law Enforcement Brotherhood, the National Inter-Business Cooperative, and the Pan-Caucasus Miner's League. Zabzimek and South Ostremek, previously referred to as regions or republics, were clearly defined as breakaway provinces of Gorgas. A breakdown of non-Donovian languages was added. The Physical Environment variable was extensively rewritten to expand it from the North Caucasus area to the entire country. In the OB, an Integrated Fires Command and an Integrated Support Command were added to the Donovian Ground Forces Command. The 720th Motorized Infantry Brigade (forward deployed to Limaria) was also added to the Southern Army, and organizational structures were added for eight commands and divisions. Several subsections were added or rewritten, including Family Authority (Political); National Security Strategy (Military); Foreign Military Presence (Military); Research & Development Goals (Military); and Special Considerations (Military).

Gorgas. The country's flag was added, as was the long form of its name (Democratic Republic of Gorgas). Gorgas was defined as consisting of provinces that are broken down into districts. Provincial borders were revised, with the addition of three new provinces (Rissi, Ornli, and Kura). Language in the Military variable was revised in places to make clear that the Gorgan Army does not have any divisions. Gorgas' militia battalion is now the National Guard, and the Critical Infrastructure Security Service was added to the OB under the Ministry of the

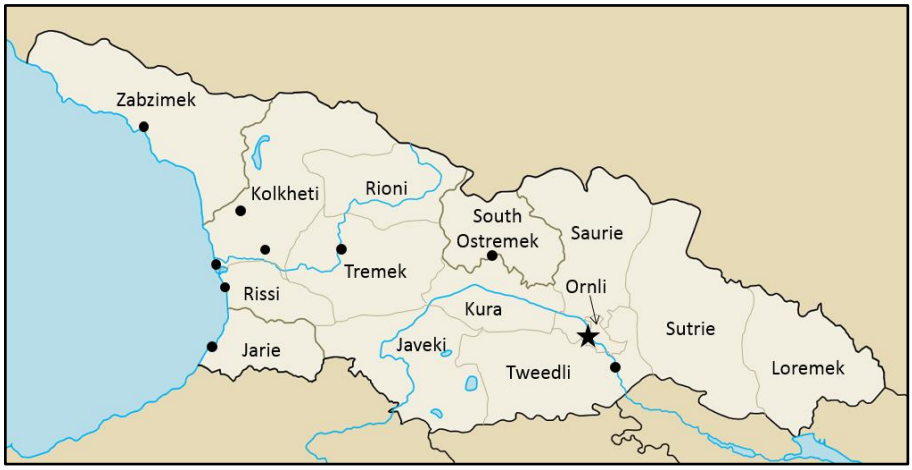


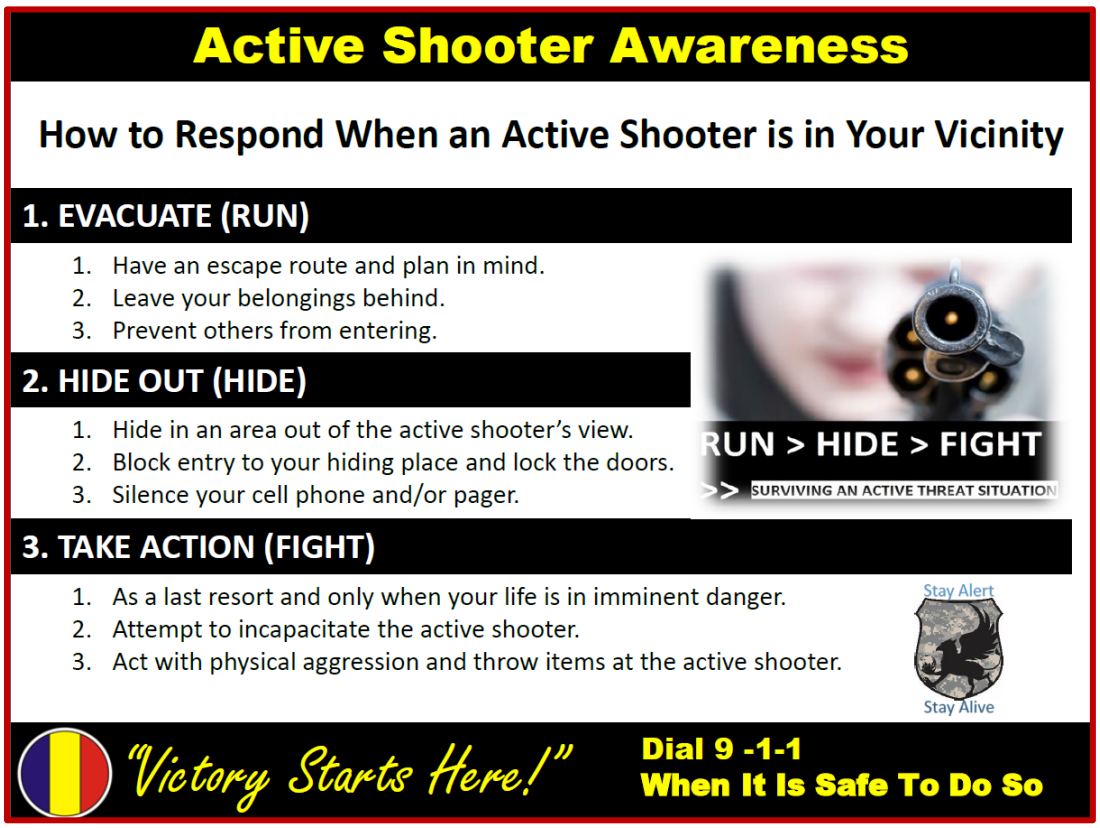
Figure 2. Gorgan provinces

Interior's State Security Directorate. Zabzimek and South Ostremek, previously referred to as regions or republics, were clearly defined as breakaway provinces of Gorgas. Three new country-specific threat groups were added: the Gorgan Tourist Association, the Hawala Assistance Brotherhood, and Pan-Caucasus Petrol Distributers. Many Zabzimeks now possess Limarian heritage, with ancestors having migrated there centuries ago. Due to border changes, the port city of Hopa was eliminated. Several subsections were added or rewritten, including Corruption (Political); Army Doctrine and Tactics (Military); Reserves and Militia (Military); Foreign Military Presence (Military); Joint Capabilities (Military); INFOWAR (Military); Chemical, Biological, Radiological, and Nuclear (Military); and Wind (Physical Environment).

Limaria. The long form name of Limaria was added (Democratic Republic of Limaria). Lower Janga, previously called a region, was clearly defined as a breakaway province of Atropia. The country's religion was defined as Limarian Apostolic. Language in the Military variable was revised in places to make clear that the Limarian Army does not have any divisions. Several subsections were added or rewritten, including Military Authority (Political); Army Doctrine and Tactics (Military); Reserves and Militia (Military); Joint Capabilities (Military); Command and Control (Military); INFOWAR (Military); Chemical, Biological, Radiological, and Nuclear (Military); and Wind (Physical Environment).

Training Implications

The purpose of the Decisive Action Training Environment (DATE) is to provide the US Army training community with a detailed description of the conditions of five operational environments (OEs) in the Caucasus region; specifically the fictional countries of Ariana, Atropia, Donovia, Gorgas, and Limaria. It presents trainers with a tool to assist in the construction of scenarios for specific training events but does not provide a complete scenario. The DATE offers discussions of OE conditions through the political, military, economic, social, information, infrastructure, physical environment, and time (PMESII-PT) variables. This DATE applies to all US Army units (Active Army, Army National Guard, and Army Reserve) that participate in an Army or joint training exercise. DATE 3.0 and a comprehensive list of changes to the five OEs are available on the DATE page of ACE-TI's webpage on the Army Training Network.



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