



Red Diamond Threats Newsletter



TRADOC G-2 Operational Environment Enterprise
ACE Threats Integration

Fort Leavenworth, KS

Volume 6, Issue 10

OCT 2015

INSIDE THIS ISSUE

N./S. Korea Standoff	4
Tactical Vignette	13
CbT Posters 2015	21
Cartel Warfare	22
Threat Actors: Pakistan.....	28
JRTC DATE Rotation.....	33
WEG: SpyLite	37
ACE-TI POCs	42

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

Send suggestions to:

ATTN: *Red Diamond*
Angela Wilkins
Chief Editor and
Product Integration
IDSI Contractor



TTR Compendium

by [Angela Wilkins](#), TRADOC G-2 ACE Threats Integration (IDSI Ctr)

TRADOC G-2 ACE Threats Integration (ACE-TI) will soon publish to ATN the Threat Tactics Report (TTR) Compendium, which is a compilation of the first four published TTRs: [ISIL, Russia, and North Korea, and China](#). This book combines these four TTRs into a single product, designed for printing.

TTRs study threats and operational environments with a focus on the military variable of the actors (regular forces and/or irregular forces), to include capabilities and limitations, training exercises, and recent actions. The TTR series is produced in accordance with *Intelligence Community Directive Number 203: Analytical Standards* (Effective: January 2015). ACE-TI coordinates each TTR with relevant SMEs at organizations such as the National Ground Intelligence Center (NGIC), Army Service Component Commands (ASCCs), Foreign Military Studies Office (FMSO), Asymmetric Warfare Group (AWG), HQDA G-2, and SMEs from TRADOC and FORSCOM.

Each TTR includes a comparison of an actor's real-world tactics to threat doctrinal concepts and terminology. A TTR will also identify where the conditions specific to the actor are present in [Decisive Action Training Environment \(DATE\)](#) and other training materials so that these conditions can easily be implemented across all training venues.



RED DIAMOND TOPICS OF INTEREST

by [Angela Wilkins](#), TRADOC G-2 ACE-Threats Integration, Editor, *Red Diamond* Newsletter (IDSI Ctr)

This issue of *Red Diamond* begins with an article that studies two incidents between North and South Korea occurring August 2015 and November 2010 to determine if any similarities can be found between the two events. The article will also probe the possible reasons behind both attacks and demonstrate that both events come directly out of the normal North Korean playbook—create an incident, deny responsibility, make threats to resume war, and then accept a compromise that gives North Korea what it wanted in the first place—assistance, often in the form of food.

The tactical vignette series continues this month with the fifth installment. Focusing on reconnaissance and counterreconnaissance as economy of force actions, the screen mission incorporates both tasks as integral to providing early warning and a degree of protection to the force main body. Other tactical tasks anticipated in a screen include actions to *delay* in order to accomplish the intent of the mission and not become decisively engaged by the enemy. See page 13.

Beginning on page 22 is an article describing the violent criminal activities of drug trafficking organizations (DTOs) in Mexico. DTOs are becoming increasingly militarized, potentially a result of the integration of ex-military defectors into their ranks. Their acquisition of military-grade weapons and equipment contributes to this capability. Implications on US forces, particularly US Army Military Police (MP) units, are that they that could potentially be used to provide security force assistance to Mexican security forces, and should factor battlefield survivability tasks into training exercises.

A forthcoming Threat Tactics Reports (TTR) on Pakistan delves into the multiple threat actors present in that operational environment (OE). The article on page 28 highlights the actors in a convenient chart, and touches on their motives and organization. This TTR is in progress and will likely be published by early 2016. Look for it on ATN.

ACE-TI analysts serve as members of accreditation teams for Combat Training Center (CTC) exercises. In August and September, a team observed a DATE-based rotation at the Joint Readiness Training Center (JRTC) at Fort Polk, LA. The analyst recounts his observations, noting that JRTC DATE Rotation 15-10 was an excellent example of how the OPFOR, even with inferior numbers and equipment, can still subject BLUFOR to a serious challenge.

Finally, this month's WEG article focuses on the SpyLite/SkyLite. Originally concentrated in Israel, this unmanned aerial vehicle (UAV) has now proliferated to other OEs in Africa and Chile.

Email your topic recommendations to:

Angela Wilkins, ACE Threats Integration

Product Integration, IDSI CTR
angela.m.wilkins7.ctr@mail.mil

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

Dr. Jon Moilanen, ACE Threats Integration

Operations, IDSI CTR
jon.h.moilanen.ctr@mail.mil

Red Diamond Disclaimer

The *Red Diamond* presents professional information but the views expressed herein are those of the authors, not the Department of Defense or its elements. The content does not necessarily reflect the official US Army position and does not change or supersede any information in other official US Army publications. Authors are responsible for the accuracy and source documentation of material that they reference. The *Red Diamond* staff reserves the right to edit material. Appearance of external hyperlinks does not constitute endorsement by the US Army for information contained therein.



Director's Corner

Thoughts for Training Readiness



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

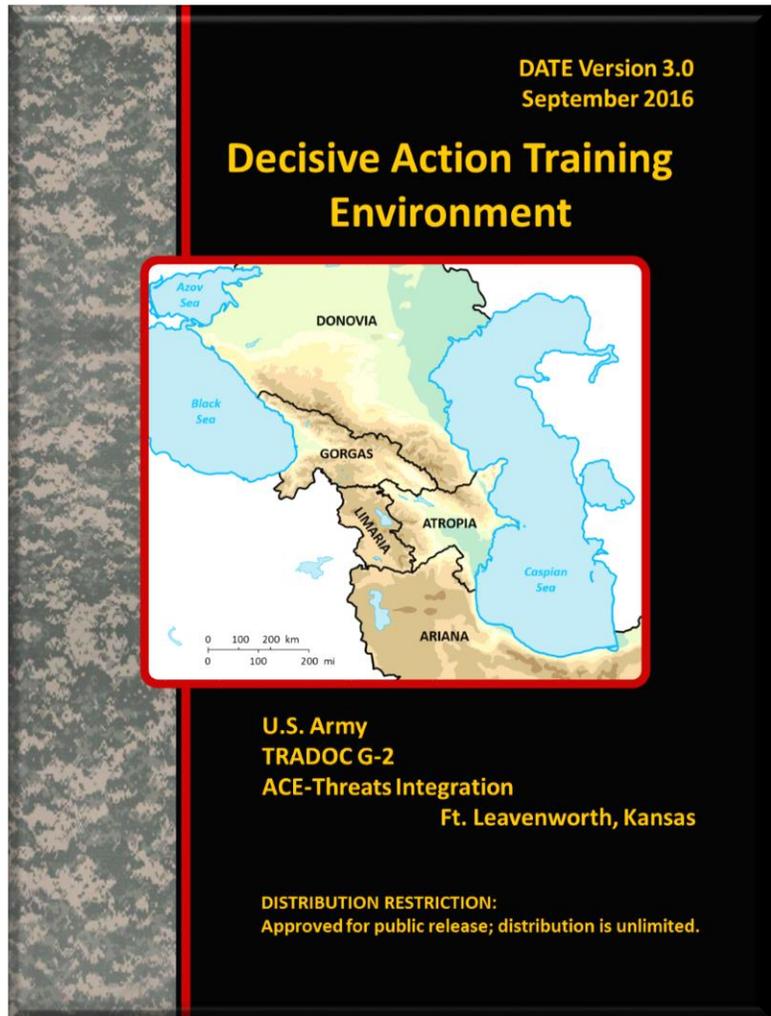
One of the most visible documents that my organization produces is the Decisive Action Training Environment ([DATE](#)), which is the foundation for all non-MRE/MRX training in the US Army. Last month we kicked off the production process for version 3.0 with a VTC explaining the vision for this edition. Several organizations participated in that VTC, all of which have my thanks.

A major part of the DATE 3.0 vision is participation by current and probable end users in sculpting the final product. While my team can make educated guesses as to how a proposed change may affect users, only you—the actual user of DATE—can speak to it definitively. My team has asked for known users, including the Combat Training Centers, international partners (e.g. the United Kingdom), and the US Army's sister services, to participate in this process. While some have responded to this request, others have not.

Subgroup leaders are already contacting their members and beginning work on their assigned tasks. Those who wish to provide input need to let my team know now. The working group will be meeting at Fort Leavenworth on 8–11 December. While I strongly encourage physical presence at this meeting, it is not a requirement for participating in either the main group or any of the affiliated subgroups. To learn more about the working group and its subgroups or to add your name/organization to the participants list, contact one of the following:

- Laura Deatrick
913-684-7925
laura.m.deatrick.ctr@mail.mil)
- CWO2 Matthew Tucker
913-684-7994
matthew.j.tucker28.fm@mail.mil)

JON





North and South Korea August 2015 Standoff: Yeonpyeong Island Déjà Vu?

by [H. David Pendleton](#), TRADOC G-2 ACE Threats Integration (CGI Ctr)

In early August 2015, two South Korean soldiers received substantial injuries to their lower extremities when three wooden box mines exploded as they patrolled the south barrier fence that separates the Demilitarized Zone (DMZ) from the rest of South Korea. The South Korean government blamed North Korea for setting the booby traps. The North Korean government, as usual, denied any responsibility for the incident. Over the next three weeks, tensions escalated to such a level that the two sides exchanged artillery fire.¹

This is not the first time that the North Korean government has manufactured incidents that have raised the defensive postures of both countries and brought the two countries to the brink of a resumption of hostilities. Technically, North and South Korea are still at war. The 1953 treaty was only an armistice (ceasefire) as the two sides negotiate peace terms. After 62 years, the two sides have yet to sign a final peace treaty to end the Korean War. One of the more intense incidents in the last decade between the two sides occurred on 23 November 2010, when an exchange of artillery fire occurred between North Korea's KPA (Korean People's Army) artillery at two locations and South Korean marine artillery on Yeonpyeong Island, located off South Korea's west coast.²

This article will examine both the August 2015 and the November 2010 incidents to determine if any similarities can be found between the two events. The article will also probe the possible reasons behind both attacks and demonstrate that both events come directly out of the normal North Korean playbook—create an incident, deny responsibility, make threats to resume war, and then accept a compromise that gives North Korea what it wanted in the first place—assistance, often in the form of food.

August 2015 Events

On 4 August 2015, a small South Korean unit on a routine foot patrol along the south barrier fence walked into an unmarked minefield and an explosion occurred. Two South Korean soldiers received severe wounds that required the amputation of a single leg from an NCO and both legs from a second sergeant. South Korea, along with officials from the United Nations Commission (UNC), Colombia, New Zealand, and the US, conducted an immediate investigation into the explosion. Their findings, released on 6 August, placed the responsibility for the blast on North Korea for three reasons. First, the mines detonated in terrain that made it impossible for rain or other weather conditions to have shifted them to that location. Second, the mines used the same type of paint typically fielded by the KPA. Last, Kim Yong Chol, a KPA hardliner, was soon seen wearing a fourth star again, signifying his return back to the rank of full general. Kim Yong Chol had been demoted to Lieutenant General, for unknown reasons, four months previous to this event. He is also believed by many analysts to be the North Korean officer most likely responsible for the 26 March 2010 sinking of the South Korean corvette, *Cheonan*, and the 23 November 2010 artillery attack of Yeonpyeong Island.³



Figure 1. [South Korean Soldiers on patrol](#)

In retaliation for this unprovoked KPA attack, the South Korean army on 10 August resumed loudspeaker propaganda broadcasts along the DMZ aimed at the North Korean citizenry. This was the first time that South Korea had used its loudspeaker system since the two sides agreed in 2004 to stop all broadcasts. In the intervening 11 years, the South Korean army developed a more sophisticated loudspeaker system with additional power so the sound can travel even farther into North Korea. On the same day, the UNC called for a meeting with the KPA over this blatant violation of paragraphs 6, 7, and 8 of the armistice agreement.⁴

Two days later, South Korea's defense committee unanimously adopted a resolution that condemned North Korea's action, urged North Korea to apologize for the incident, and encouraged the KPA to adopt steps so a similar incident would not occur in the future. On the same day, South Korea publically announced an increase in the quantity of its loudspeaker propaganda war. On 17 August 2015, North Korea retaliated and resumed its own propaganda broadcasts aimed at South Korea. By coincidence or not, 17 August 2015 was also the first day of the United States Forces-Korea (USFK) and South Korean military exercise, *Ulchi Freedom Guardian*, scheduled to run until 28 August 2015. This exercise ensured more US troops were in South Korea than during most other times of the year.⁵

On 20 August 2015, North Korea, without any notice, fired two to four artillery shells at one of South Korea's propaganda speakers. The artillery attack not only failed to hit the speakers or cause any casualties, but did little damage except to unoccupied ground in the vicinity of where the shells landed. A South Korean army artillery battery immediately fired 29 rounds of 155-mm counter-battery fire aimed at the KPA unit that fired the initial rounds. While highly unlikely, North Korea claimed that the South Korean artillery also caused no damage or casualties. That night, the North Korean Central Military Committee (CMC) met and endorsed an ultimatum to South Korea to stop its propaganda broadcasts.⁶

On the following day, North Korean leader Kim Jong Un placed the KPA into a quasi-state of war and issued the demand that South Korea cease the propaganda by 1700 hours local time on Saturday, 22 August 2015, or face the consequences. The CMC ultimatum basically declared that North Korea would go to war if the South Korean loudspeakers did not go silent. South Korea responded by preparing itself for war. South Korean government officials evacuated several villages in the Yecheon District, the area where the North Korean artillery had landed. The South Korean government also restricted its civilians' access to the Kaesong industrial zone, an area in North Korea where South Korean companies built manufacturing plants that hire workers from both sides of the border. This economic zone supplies North Korea with



Figure 2. South Korean [K-9 155-mm howitzers](#) firing

desperately-needed hard currency for the cash-strapped North Korean government. The South Korean President, Park Geu Hye, canceled her normal appointments and visited a military command post dressed in a South Korean army camouflage uniform. The USFK Commander also put the *Ulchi Freedom Guardian* exercise on hold pending resolution of the incident.⁷

On the morning of the day of the North Korean deadline, 22 August 2015, both sides agreed to meet at Panmunjom to discuss the issue along with the UNC. Hwang Pyong So, the KPA's political officer, and Kim Yang Gon, North Korea's senior official for South Korean affairs, represented North Korea. Some analysts consider Hwang Pyong So to be the second-most important person in North Korea after Kim Jong Un. Kim Kwan Jin, the Presidential National Security Director, and Hong Yong Pyo, the Unification Minister, represented South Korea in the negotiations. Despite the ongoing talks, the South Korean military raised its WatchCon alert level from 3 to 2, the second-highest alert level for its military forces.⁸

After little headway in the discussions on Saturday, the two sides took an 11-hour break and resumed negotiations the next day, 23 August 2015. On the same Sunday, however, the KPA sent 50 submarines—70% of its underwater fleet—to sea, while doubling the normal number of artillery units positioned along the DMZ. In response to this KPA activity, the South Korean military recalled six fighter jets from Alaska that were conducting a Red Flag exercise with the American Air Force.⁹

Fewer than 24 hours later, the KPA also moved ten air cushioned landing craft carrying special forces soldiers, useful for conducting amphibious landings, from their base in Cholsan to a forward base located only 60 km north of the Northern Limit Line (NLL), the dividing line between the two Koreas off the west coast of the peninsula. When questioned about the ongoing negotiations in the light of North Korean military activity, Park Geu Hye, the South Korean president, announced to the public that it was important that North Korea apologize for planting the landmines.¹⁰

After three days of intense discussions, North and South Korea came to an agreement on 25 August 2015. The major clause was that North Korea would pen a statement that expressed regret for the landmine explosion and that the South Korea would turn off its propaganda speakers. North Korea would back off from its semi-state of war declared the previous Friday. Both sides also agreed to resume the reunions of family members separated by the 1950–53 war with the expectation that the visits would take place around 27 September 2015, the Korean holiday of *Chuseok*. *Chuseok* is very similar to Thanksgiving in the US. While South Korea may claim they extracted an apology from the North Korea for the incident, some analysts believe the document fell far short of an actual apology. The KPA recalled its submarines, but this decision might have been more to do with the approach of Typhoon Goni or that its diesel boats can only stay underwater

for 72 hours before they must surface to recharge their batteries, making them more susceptible to detection. On the same day, the South Korean military lowered its WatchCon alert back to its early August level. Within a few days, both sides were back at the same defensive posture as before the landmine explosions on 4 August 2015. Despite signing the note of regret, a top North Korean official, Hwang Pyong So, told North Korean television viewers the North Korea was not responsible for the landmines and that South Korea learned its lesson for alleging phony charges against North Korea. This announcement may have been more to save face with North Korea's internal audience than a renunciation of the regret memo just signed.¹¹

Yeonpyeong Island Artillery Duel—23 November 2010



Figure 3. [Yeonpyeong Island](#) housing complex

Unlike the recent incident that took three weeks to conclude, the Yeonpyeong Island incident occurred in just a single day. On 23 November 2010, an artillery duel broke out between 76.2-mm artillery batteries and a 122-mm multiple rocket launcher (MRL) battalion, located on both the North Korean mainland and Mudo Island, and a 155-mm South Korean marine K-9 battery stationed on Yeonpyeong Island. The North Korean 122-mm MRL most likely used the BM-21 Grad to fire some of its artillery rounds. The batteries that fired were on opposite sides of the NLL, the *de facto* border that separates the North Korean and South Korean territorial waters.¹²

North Korea does not recognize the NLL as the border between the two Koreas while South Korea, the US, and most Western countries do observe the NLL as the dividing line between the two countries. In 1953, the United Nations Commission (UNC) unilaterally drew the line in the waters off the west coast of the Korean peninsula to serve as a continuation of the Military Demarcation Line (DML) that separated the military forces on land. Part of the conflict between the two Koreas stems from the North Korean claim of twelve nautical miles as its territorial waters compared to the internationally accepted three nautical mile territorial limit.¹³

The area around Yeonpyeong Island has seen its share of incidents between the naval forces of North and South Korea. In November 2009, naval vessels from the two sides exchanged fire, with the North Korean patrol boat suffering major damage. The South Korean ships forced the aged Korean People's Navy (KPN) ship to flee after it was set ablaze by cannon fire. Besides the ship's damage, the KPN suffered one sailor killed and three injured, while the South Korean ships suffered no casualties despite one of its vessels taking 15 direct hits from the KPN ship. Other naval incidents between the two sides in the vicinity of the island have occurred in 1991, 2002, 2010, 2011, and 2012. In March 2010, eight months before Yeonpyeong Island artillery strike, a North Korean submarine sank the South Korean ship, *Cheonan*, killing 46 South Korean sailors. North Korea, however, denied any responsibility for the ship sinking.¹⁴

The following is the timeline for the events that took place on 23 November 2010 (all times are local):¹⁵

- 0820: North Korea sent a message to South Korea directing it to halt the planned artillery training exercise on Yeonpyeong Island.
- 1000: South Korea started the artillery training exercise by firing shells into the ocean to the south and southwest of Yeonpyeong Island.
- 1430: The Korean People's Air Force (KPAF) scrambled five MiG-23ML fighters from the 60th Regiment at Pukchang and flew above North Korean airspace north of the NLL, but near Yeonpyeong Island.
- 1434: KPA artillery units fired approximately 150 shells from Mudo Island and the Kaemori area on the mainland at Yeonpyeong Island. Only about 60 of the 80 shells that hit Yeonpyeong Island exploded, while the remaining 70 shells dropped harmlessly into the sea.
- 1438: The Republic of Korea Air Force (ROKAF) sortied two KF-16 fighters to the vicinity of Yeonpyeong Island.
- 1440: The ROKAF sent four additional F-15K fighters to the airspace above Yeonpyeong Island.
- 1446: The ROKAF scrambled an additional two KF-16 fighters for a total of eight fighter jets in the vicinity of Yeonpyeong Island.
- 1447: The South Korean marine 155-mm K-9 battery on Yeonpyeong Island fired 50 artillery shells at previously-identified command and control elements and barracks located on Mudo Island, because the Marines' counter-battery radar was non-functional at the time.
- 1450: The South Korean military issued a "Jindogae Hana (Jindo Dog 1) alert, the highest level for local attacks.
- 1455: The KPA artillery units temporarily ceased firing.
- 1512: The KPA artillery units resumed firing with 20 additional rounds that all hit Yeonpyeong Island.
- 1525: With their AN/TPQ-37 radar back in operation, the South Korean Marines fired their K-9 howitzers in counter-battery mode at a multiple rocket launcher battery located on the mainland in the vicinity of Kaemori.
- 1530: A South Korean general contacted his North Korean counterpart and requested an immediate halt to the artillery shelling.
- 1540: The South Korean Joint Chiefs of Staff, General Han Min Gu and the United States Forces-Korea (USFK) Commander, Walter L. Sharp, held a video teleconference to discuss the incident.
- 1541: North Korea halted its artillery firing.
- 1630: South Korea reported its first military casualty.
- 1635: South Korean, Foreign, and National Security representatives began a meeting, which lasted three hours, about the incident.
- 1642: The South Korean Marine artillery battery fired its final round.

- 1840: The South Korean Joint Chief of Staff Director for Operations, Lee Hong Gi, held a press briefing to discuss the artillery attack by the KPA.
- 2035: General Han Min Gu briefed South Korean President Lee Myung Bak in person about the incident.

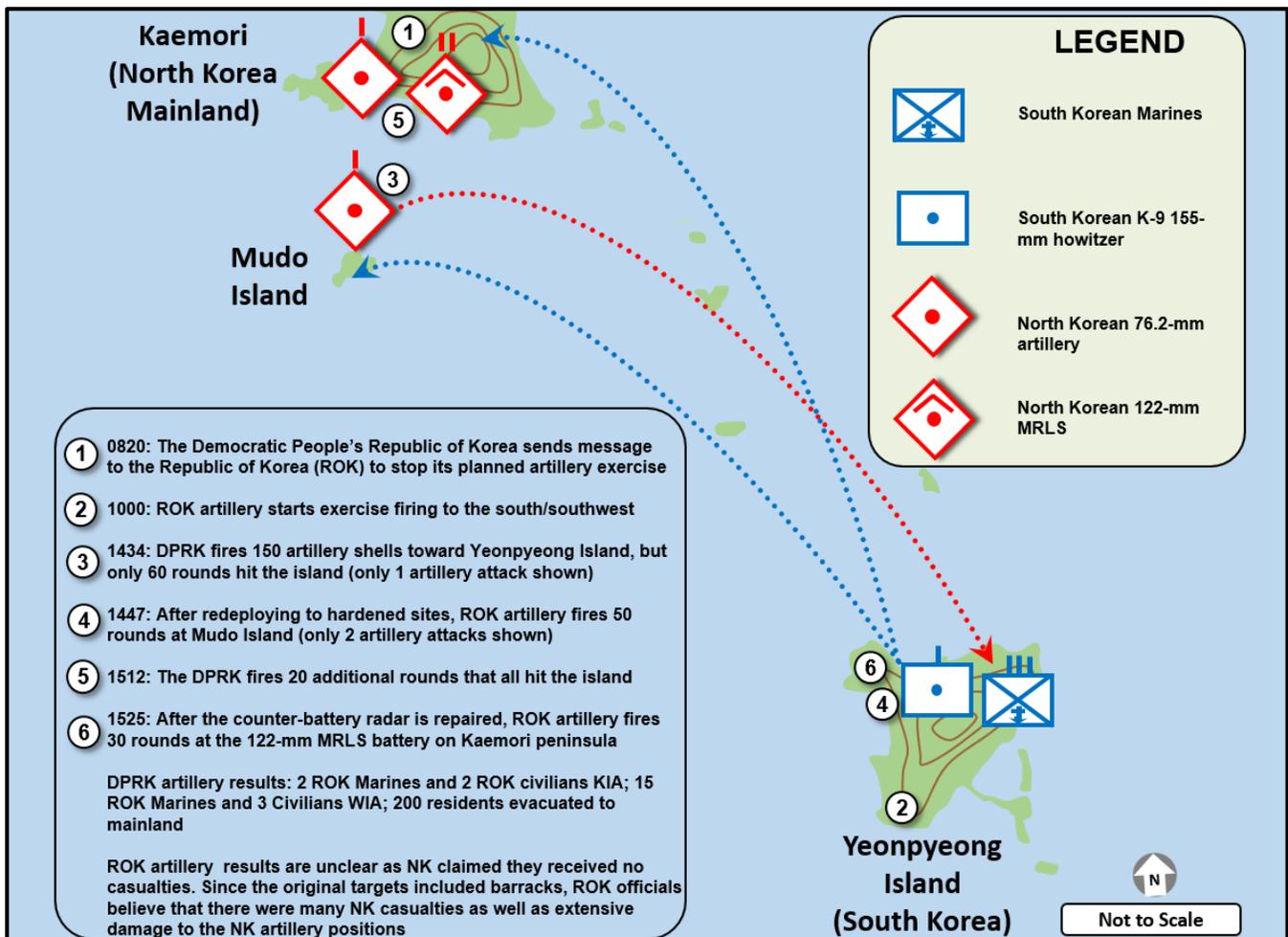


Figure 4. Yeonpyeong Island Duel, 23 November 2010. Graphics by ACE-Threats Integration, 8 October 2015

The results of what happened on Yeonpyeong Island are known, but what occurred in North Korea is open to speculation. What is known is that two South Korean marines and two civilians were killed by the KPA artillery, with an additional 15 marines and three civilians injured. The North Korean artillery hit a military base, a police station, and a maritime police guard post on Yeonpyeong Island. The North Korean artillery also damaged a South Korean K9 155-mm self-propelled howitzer inside a concrete bunker. Several civilian locations on the island were also hit including a health center, a township office, an inn, and a museum. After the Yeonpyeong Island civilians fled to one of the 20 shelters on the island, the South Korean government later evacuated approximately 200 civilians to the mainland. Many of the artillery rounds fired by the KPA units were incendiary rounds. It is unclear whether North Korea intended to start fires on the island or if those were the most easily accessible type of munitions available to the artillery units. The large number of complete misses of the island—70 of the initial 150 rounds—indicates that there may be some major issues with the artillery battalion's fire direction center or with the ability of the soldiers on the line to successfully place the proper data on their guns or MRLs. Of the 80 rounds that did hit the island, the North Koreans suffered a 25% dud rate—a very high frequency—indicating a possible lack of quality control in their ammunition manufacturing process.¹⁶

North Korea claimed its forces suffered no casualties, but that is probably just propaganda for internal North Korean consumption. Based upon the original targets—command and control facilities and a barracks—on Mudo Island and the

counter-battery fire once the South Korean radar became operational again, it is likely that there were several KPA casualties and significant damage to the KPA facilities. The South Korean Defense Minister, Kim Tae Yong, resigned after accusations that the South Korean government had responded weakly to the KPA artillery attack. Kim Tae Yong said in his defense that he did not order a retaliatory air strike on the KPA artillery units because he feared that such an act might cause the Korean War to go hot again. Calmer heads prevailed and neither side raised the stakes, which would have caused an escalation in events.¹⁷

Tumult around the Yeonpyeong Island continues in the present day. In late April 2015, the KPA began the construction of five artillery positions, a command post, barracks, and other related facilities on Gal-do Island, just 4.5 km from Yeonpyeong Island. Gal-do is a small island, only one-half kilometer in length, located about 2.5 km north of the NLL. In July 2015, the KPA deployed a 122-mm multiple rocket launcher battery on Gal-do Island. The 122-mm MRL can reach targets 20 km away and even 30 km with rocket-assisted rounds. The closer the target, the more accurate the 122-mm MRL rounds, making it easier for the KPA to hit its desired targets on Yeonpyeong Island if it decided to shell the island again.¹⁸

North Korean Provocations—Why?

Speculation abounds on why the KPA launched the artillery attack against Yeonpyeong Island when it did in 2010. One theory was that it was an opportunity for a young Kim Jong Un, being groomed to replace his father, to add gravitas to his military credentials. Just hours before the artillery strike, Kim Jong Un and his father, Kim Jong Il, visited the artillery base on Kaemori. It is reasonable to believe that the local artillery commander did not fire the artillery without permission from high up the KPA chain of command—maybe even from the very top. Incidents in the waters off the west coast of the Korean peninsula around the NLL continue to occur after Kim Jong Il's death. While North Korea regularly breaks the armistice agreement, South Korea usually mutes its responses to these violations. The prevention of open warfare between North and South Korea appears to still be a primary concern of the South Korean military and civilian leaders.¹⁹

The latest provocation in August 2015 may be a different matter. The actual audience for the incident might not have been South Korea, but the People's Republic of China (PRC) to its north. Many times when North Korea wants assistance from its northern neighbor, it creates a crisis with South Korea to give the appearance that a resumption of the Korean War is imminent. In response, the PRC caves in and gives additional support to North Korea, as China fears an economically powerful and democratic, unified Korea on its southern border. Observers note that immediately after previous provocations between North and South Korea, when normalcy returns, increased activity in the form of cross-border vehicle convoys from China to North Korea also often occur. In the past, the support included Chinese food, trucks, or heavy equipment—given essentially free to North Korea. It is yet to be determined what North Korea gained from the PRC in this August 2015 incident because North Korea received virtually nothing from South Korea except a return to the situational status quo before the South Korean soldiers lost their legs in the minefield explosion. It will be interesting to see what China promised North Korea, if anything, to ratchet down the rhetoric and sign the statement of regret. So far, it did not get North Korea's envoy to the Chinese



Figure 5. American General James D. Thurman, the UNC Commander, and South Korean General Jung Seung Jo, the ROK-US Combined Forces Deputy Commander, along with their staffs [visited Yeonpyeong Island](#) on 18 October 2011. This was General Thurman's first visit to the island after he took command in July 2011

ceremony commemorating the end of World War II a prominent seat near the PRC leader, and reports are that Kim Jong Un did not attend because he would not be seated anywhere near the Chinese leader either.²⁰

Training Implications

These two examples of unprovoked artillery attacks on South Korea exemplify the difficulty in predicting what North Korea will do next. All South Korean military personnel and American soldiers stationed in South Korea must be prepared for the unexpected. Anyone in the DMZ or the area just south of the DMZ or the NLL need to be alert. One never knows when a training exercise might turn into actual military action.

The Combat Training Centers (CTC) and home station Opposing Forces (OPFOR) could initiate a training exercise with a similar unprovoked and unorthodox event. The CTCs or other OPFOR could also throw in similar incidents during an exercise to test the ability of the US units to respond to such unplanned events.

Notes

- ¹BBC. "[South Korea blames North for DMZ mine blast.](#)" 10 August 2015; The Korea Observer. "[U.N. Command denounces N.K. mine blasts in DMZ as violations of armistice.](#)" 10 August 2015.
- ²BBC. "[South Korea blames North for DMZ mine blast.](#)" 10 August 2015.
- ³BBC. "[South Korea blames North for DMZ mine blast.](#)" 10 August 2015; The Korea Observer. "[U.N. Command denounces N.K. mine blasts in DMZ as violations of armistice.](#)" Yonhap News. 10 August 2015; Ju Min Park. "[South Korea condemns North over land mine blast, vows retaliation.](#)" Reuters. 10 August 2015; The Korea Observer. "[Top NK general may be blamed for landmine blast.](#)" Yonhap News. 11 August 2015.
- ⁴BBC. "[South Korea blames North for DMZ mine blast.](#)" 10 August 2015; The Korea Observer. "[U.N. Command denounces N.K. mine blasts in DMZ as violations of armistice.](#)" Yonhap News. 10 August 2015; Ju Min Park. "[South Korea condemns North over land mine blast, vows retaliation.](#)" Reuters. 10 August 2015; Shin Hon Hee. "[Seoul to expand border broadcasts across DMZ.](#)" Korea Herald. 12 August 2015; Ju Min Park and James Pearson. "[North Korea goes on war footing against South Korea as deadline looms.](#)" Reuters. 21 August 2015.
- ⁵Shin Hon Hee. "[Seoul to expand border broadcasts across DMZ.](#)" Korea Herald. 12 August 2015; Ju Min Park, Sohee Kim, James Pearson, and David Brunnstrom. "[North Korea retaliates against South with loudspeaker propaganda.](#)" Reuters. 17 August 2015; BBC. "[South Korea evacuation after shelling on western border.](#)" 20 August 2015; Ju Min Park and James Pearson. "[North Korea goes on war footing against South Korea as deadline looms.](#)" Reuters. 21 August 2015.
- ⁶BBC. "[South Korea evacuation after shelling on western border.](#)" 20 August 2015; Ian Williams. "North Korea Puts Army on 'Quasi State of War,' Sets Loudspeaker Deadline." NBC News. 21 August 2015; Ju Min Park and James Pearson. "[North Korea goes on war footing against South Korea as deadline looms.](#)" Reuters. 21 August 2015; Park Chan Kyong. "[N. Korea's Kim put troops on war footing with South.](#)" AFP. 21 August 2015; Park Chan Kyong. "[N. Korea's Kim put troops on war footing with South.](#)" AFP. 21 August 2015.
- ⁷Ju Min Park, Sohee Kim, James Pearson, and David Brunnstrom. "[North Korea retaliates against South with loudspeaker propaganda.](#)" Reuters. 17 August 2015; BBC. "[South Korea evacuation after shelling on western border.](#)" 20 August 2015; Ian Williams. "North Korea Puts Army on 'Quasi State of War,' Sets Loudspeaker Deadline." NBC News. 21 August 2015; Ju Min Park and James Pearson. "[North Korea goes on war footing against South Korea as deadline looms.](#)" Reuters. 21 August 2015; Park Chan Kyong. "[N. Korea's Kim put troops on war footing with South.](#)" AFP. 21 August 2015.
- ⁸The Korea Observer. "[U.N. Command denounces N.K. mine blasts in DMZ as violations of armistice.](#)" Yonhap News. 10 August 2015; Laura Connor. "[More than 50 North Korea submarines 'leave their bases' as war talks with South continue.](#)" Reuters/Getty via Mirror. 23 August 2015; Chad O'Carroll. "[As talks enter third day, N. Korea forward deploys landing crafts, special forces.](#)" NK News. 24 August 2015; Choe Sang Hun. "[Koreas Agree on Deal to Defuse Tensions.](#)" The New York Times. 24 August 2015.
- ⁹Laura Connor. "[More than 50 North Korea submarines 'leave their bases' as war talks with South continue.](#)" Reuters/Getty via Mirror. 23 August 2015; Chad O'Carroll. "[As talks enter third day, N. Korea forward deploys landing crafts, special forces.](#)" NK News. 24 August 2015.
- ¹⁰Jack Kim and Ju Min Park. "[South Korea's Park says important for North Korea to apologize.](#)" Reuters. 23 August 2015; Chad O'Carroll. "[As talks enter third day, N. Korea forward deploys landing crafts, special forces.](#)" NK News. 24 August 2015.
- ¹¹Reuters. "[North Korea expresses regret over landmines that wounded South soldiers: statement.](#)" 24 August 2015; Choe Sang Hun. "[Koreas Agree on Deal to Defuse Tensions.](#)" The New York Times. 24 August 2015; Choe Sang Hun. "[Koreas Agree on Deal to Defuse Tensions.](#)" The New York Times. 24 August 2015; The Korea Times. "[Deployed N. Korean submarines returning to bases after inter-Korean deal.](#)" 24 August 2015; BBC. "[South and North Korea agree deal to reduce tensions.](#)" 25 August 2015; Ju Min Park and Tony Munroe. "[North, South Korea reach agreement to ease tensions.](#)" Reuters. 25 August 2015; The Korea Times. "[S. Korean military relaxes top-level defense posture at border.](#)" 25 August 2015; Yonhap News. "[NK official: S. Korea will take lesson from latest stand-off.](#)" 25 August 2015; Jee Abbey Lee. "[North Korea's 'Apology' Over Land Mine Attack Criticized.](#)" Voice of America (VOA). 26 August 2015.
- ¹²STRATFOR. "Tactical Details of the Nov. 23 Korean Artillery Exchange." November 2010.
- ¹³Moo Bong Ryou. "The Korean Armistice and the Islands." Strategy Research Project. US Army War College. Carlisle Barracks PA 17013-5050. USAWC Class of 2009.

- ¹⁴ Blaine Harden. "[North Korea says naval skirmish was 'planned provocation' by South.](#)" Washington Post Foreign Service. 12 November 2009; Mark McDonald. "['Crisis Status' in South Korea After North Shells Island.](#)" The New York Times. 23 November 2010; Jack Kim and Lee Jae-Won. "[North Korea shells South in fiercest attack in decades.](#)" Reuters. 23 November 2010; Associated Press. "[S. Korean Troops on High Alert After Shelling.](#)" 24 November 2010; Phil Stewart and Andrew Quinn. "[U.S. vows unified response to N. Korea.](#)" Reuters. 23 November 2010; Jon Van Dyke. "[The Maritime Boundary between North & South Korea in the Yellow \(West\) Sea.](#)" 38 North. 29 July 2010; Jane's Sentinel Security Assessment. "Korea. North > Armed Forces." 2 July 2014; Military Periscope. "[Nations/Alliances/Geographic Regions: Asia – North Korea: Navy.](#)" September 2014; Jane's Sentinel Security Assessment. "Korea. North > Navy." 1 September 2014; CSIS. "The Aftermath of the Cheonan." 2010; John Sudworth. "[How South Korean ship was sunk.](#)" BBC. 20 February 2014.
- ¹⁵ Blaine Harden. "[North Korea says naval skirmish was 'planned provocation' by South.](#)" Washington Post Foreign Service. 12 November 2009; Mark McDonald. "['Crisis Status' in South Korea After North Shells Island.](#)" The New York Times. 23 November 2010; Jack Kim and Lee Jae-Won. "[North Korea shells South in fiercest attack in decades.](#)" Reuters. 23 November 2010; Associated Press. "[S. Korean Troops on High Alert After Shelling.](#)" 24 November 2010; Phil Stewart and Andrew Quinn. "[U.S. vows unified response to N. Korea.](#)" Reuters. 23 November 2010; Jon Van Dyke. "[The Maritime Boundary between North & South Korea in the Yellow \(West\) Sea.](#)" 38 North. 29 July 2010; Jane's World Armies. "World Armies > Korea. North." 3 April 2014; AP. "[Tensions high as North. South Korea trade shelling.](#)" 24 November 2014; STRATFOR. "Tactical Details of the Nov. 23 Korean Artillery Exchange." November 2010.
- ¹⁶ Mark McDonald. "['Crisis Status' in South Korea After North Shells Island.](#)" The New York Times. 23 November 2010; Jack Kim and Lee Jae-Won. "[North Korea shells South in fiercest attack in decades.](#)" Reuters. 23 November 2010; Associated Press. "[S. Korean Troops on High Alert After Shelling.](#)" 24 November 2010; Phil Stewart and Andrew Quinn. "[U.S. vows unified response to N. Korea.](#)" Reuters. 23 November 2010; Jon Van Dyke. "[The Maritime Boundary between North & South Korea in the Yellow \(West\) Sea.](#)" 38 North. 29 July 2010; Jane's World Armies. "World Armies > Korea. North." 3 April 2014; AP. "[Tensions high as North. South Korea trade shelling.](#)" 24 November 2014; STRATFOR. "Tactical Details of the Nov. 23 Korean Artillery Exchange." November 2010.
- ¹⁷ Mark McDonald. "['Crisis Status' in South Korea After North Shells Island.](#)" The New York Times. 23 November 2010; Jack Kim and Lee Jae-Won. "[North Korea shells South in fiercest attack in decades.](#)" Reuters. 23 November 2010; Associated Press. "[S. Korean Troops on High Alert After Shelling.](#)" 24 November 2010; Phil Stewart and Andrew Quinn. "[U.S. vows unified response to N. Korea.](#)" Reuters. 23 November 2010; Jon Van Dyke. "[The Maritime Boundary between North & South Korea in the Yellow \(West\) Sea.](#)" 38 North. 29 July 2010; Jane's World Armies. "World Armies > Korea. North." 3 April 2014; AP. "[Tensions high as North. South Korea trade shelling.](#)" 24 November 2014; STRATFOR. "Tactical Details of the Nov. 23 Korean Artillery Exchange." November 2010.
- ¹⁸ John G. Grisafi. "[North Korea stations artillery near Yeonpyeong-do.](#)" NK News. 23 July 2015.
- ¹⁹ Stephen McDonnell. "[North Korea attack linked to leadership succession.](#)" ABC News. 25 November 2010; STRATFOR. "[North Korea's Unpredictable Behavior.](#)" 27 August 2010.
- ²⁰ BBC. "[How potent are North Korea's threats?](#)" 21 August 2015; Park Chan Kyong. "[N. Korea's Kim put troops on war footing with South.](#)" AFP. 21 August 2015; Choe Sang Hun. "[Koreas Agree on Deal to Defuse Tensions.](#)" The New York Times. 24 August 2015; William Johnson. "[What the blow up between North and South Korea may really have been about.](#)" Reuters. 24 August 2015; Yonhap News. "[N. Korea: Kim Jong-un snubs China's invitation to military parade.](#)" 24 August 2015; Hwan Yong Kim. "[Kim Skipping WWII Ceremony Shows Troubled China-North Korea Ties.](#)" VOA. 27 August 2015; Jess McHugh. "[North Korea China Military Parade Snub: Kim Jong Un Refuses Chinese Invitation As Border Tensions With Seoul Heighten.](#)" 24 August 2015.

REPORT SUSPICIOUS ACTIVITY 1 (800) CALL SPY (225-5779)

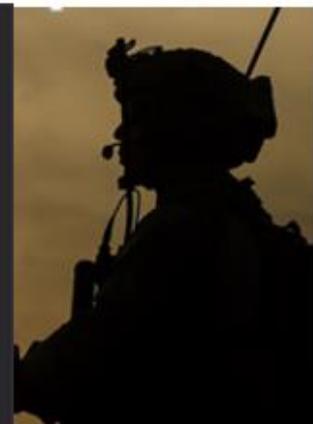


What to Report:

- Unauthorized attempts to access classified or sensitive data
- Person advocating support for a terrorist organization
- Contacts that may suggest extremist group recruitment
- Suspicious behavior possibly associated with terrorist activity

How to Report:

- Contact your local Counterintelligence (CI) office
- CONUS Hotline: 1 – 800 – CALL SPY (1-800-225-5779)
- iSALUTE – The CI reporting portal via AKO at:
<https://www.us.army.mil/suite/page/633775>





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

Part 5 in RZ-CRZ Series

The October 2015 *Red Diamond* newsletter article is the fifth article in this tactical vignette series. Focusing on reconnaissance and counterreconnaissance as economy of force actions, the screen mission incorporates both tasks as integral to providing early warning and a degree of protection to the force main body. Other tactical tasks anticipated in a screen include actions to *delay* in order to accomplish the intent of the mission and not become decisively engaged by the enemy.

Situation Update

From previous *Red Diamond* newsletter articles, the rapid advance of the encirclement operation continues deep into the enemy’s rear zone toward the KRONATZ river line. Mechanized and motorized forces organized as division tactical groups (DTGs) are maneuvering to linkup and close the encirclement. One divisional reconnaissance company with a flank screen mission has intermittent contact with its task-organized platoons across a wide zone. The platoon in this tactical vignette, task-organized as an *independent reconnaissance patrol (IRP)*, continues its tasks of reconnaissance and counterreconnaissance after contact with lead enemy dismounted elements.

An ambush by one of the scout squads stopped lead enemy elements south of Hill 21, but other enemy elements were attempting to maneuver to the eastern flank of the hill and unto the high ground. A raid disrupted the dismounted enemy maneuver, gained time to assess the current situation, and gathered tactical intelligence and one enemy prisoner from the raid site.

The platoon leader on the northern slope of Hill 21 in the east part of the zone is receiving reports from his senior sergeant on the western axis road and predicted enemy location (PEL) 23. No enemy have been sighted on this axis since the original assault into BEJUNIK when enemy soldiers destroyed the bridge and withdrew south.

Actions in PEL 23

The senior sergeant perks in the middle of his radio transmission and rises higher in his BTR cupola as the morning mist suddenly starts to clear. Visibility extends well south of the trail intersection and road in PEL 23. He senses something is not normal as he visually

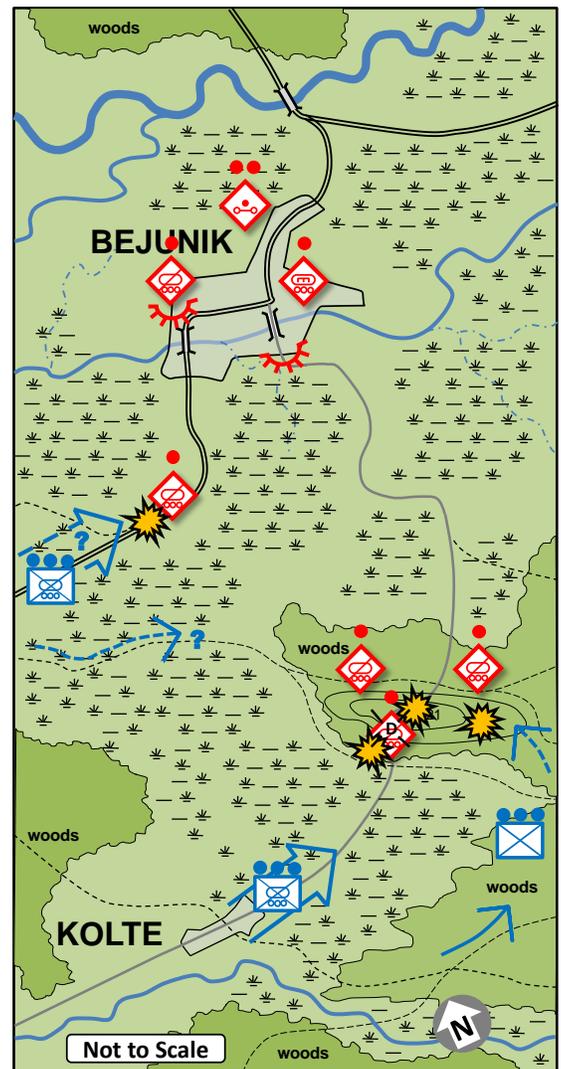


Figure 1. Current Tactical Situation

scans the road, marsh, and woodline south of the trail intersection. Scouts start to dismount from the BTR. Later, he would recall that he saw the flash at the woodline at the same moment the ground erupted just in front of his BTR.

“Contact!” was all he could yell before he engaged his smoke grenade launchers and ordered the BTR into reverse. An enemy antitank gun or cannon had shot short-line by mere meters, but the direction of fire was accurate and almost on target. The senior sergeant knew the marsh to each side of the road limited his maneuver options but he moved his BTR immediately down the far shoulder of the road bed to provide some level of protection. He oriented his gunner in the direction of enemy contact with a simple hand motion as he initiated a call for fire from the mortar section.

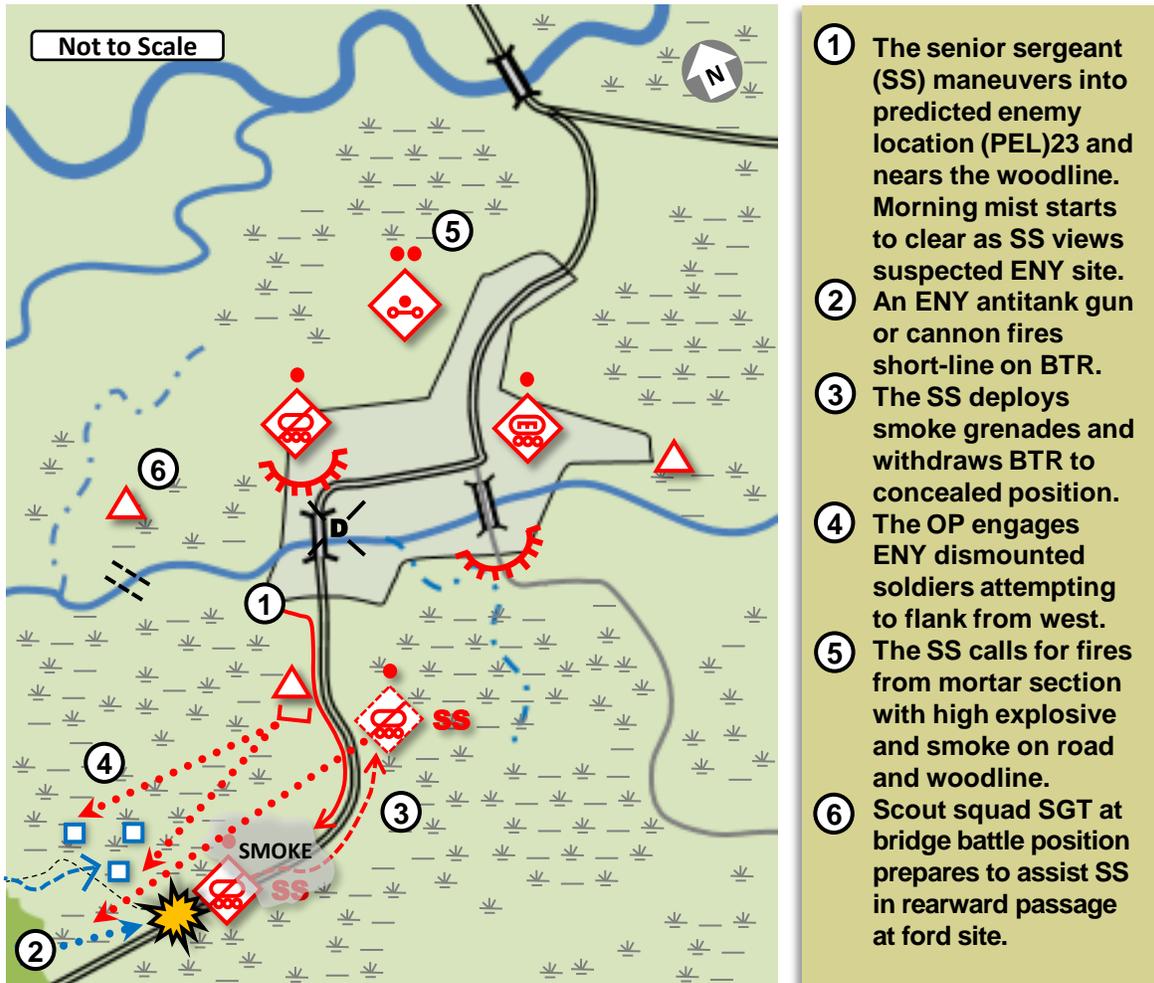


Figure 2. Contact in predicted enemy location 23

Enemy machinegun fire was beating clods of dirt into the air along the road and an occasional main gun or cannon round screamed through the smoke past the BTR to land somewhere to the north. Fortunately, the smoke screen was preventing any accurate siting of where the BTR had positioned, but even then, several machinegun rounds were ricocheting off the vehicle's front slope.

Hill 21 and Enemy Contact

In the east at Hill 21, enemy indirect fire continues to land sporadically along the road at the southern woodline, on the hillcrest, and is creeping over the northern slope. The platoon leader is quickly assessing current combat readiness and

risk, and what he knows—or believes he knows—is occurring in zone on the western axis and south of his current location at Hill 21. His mission includes not becoming decisively engaged by the enemy.

- Enemy elements are approaching BEJUNIK on both roads and probably have dismounted elements in the marshy terrain in between the roads and center in zone.
- A small number of enemy soldiers are maneuvering to the northeast of his current positions on Hill 21, even after the successful ambush and raid in the wood line. The captured enemy soldier states he is part of a reconnaissance platoon headed to link up with militia positioned in BEJUNIK.
- Three wheeled armored vehicles emerging north of KOLTE are moving parallel to the road toward Hill 21, and two other vehicles, one with a turreted main gun, is approaching along the main road. At least a reinforced enemy platoon is maneuvering to Hill 21 with enemy artillery fires preventing any clear visibility of their mounted progress.

Hill 21 is key terrain south of the MIN River and has a commanding view of the marshland and eastern road all the way to BEJUNIK. Maneuver, time, and distance factors for his elements are problematic to a delay given the open space and relatively flat terrain once he departs Hill 21. He is also much farther from BEJUNIK than his senior sergeant currently in contact with the enemy on the western road.

Delay—Disrupt—Fix

***Delay* is a tactical task to slow the time of arrival of enemy forces or capabilities or alter the ability of the enemy or adversary to project forces or capabilities.**

***Disrupt* is a tactical task to upset an enemy's formation or tempo, interrupt the enemy's timetable, cause the enemy to commit his forces prematurely, and/or cause him to attack in piecemeal fashion.**

***Fix* is a tactical task to prevent the enemy from moving any part of his force from a specific location for a period of time.**

Some enemy indirect fire starts to land in the marsh and on the road north of Hill 21 as other indirect fire hits the hill crest. As the platoon leader's other BTR emerges from the high scrub brush to link up, the platoon leader directs several concise orders over the platoon radio net.

- The separated sections of the platoon are to delay back to BEJUNIK and be prepared to temporarily defend.
- The senior scout sergeant in the west is to delay as long as he can forward in position, without becoming decisively engaged, to allow time for the platoon leader's section to egress back toward the bridge at BEJUNIK.
- The mortar section sergeant continues to support the senior sergeant call for fires, but on order, shifts to provide fires on Hill 21 and along the western road to obscure visibility from Hill 21.
- The engineers at the MIN River are to arm the demolitions at the bridge and several antitank and antipersonnel mines emplaced near and in both roads. Dismounted scouts remain on site to guide the senior sergeant's BTR and the platoon leader's BTRs through the mined obstacles.

The scout squad at the destroyed bridge site listens to the engagement south of the Min River and receives updates from the scout observation post (OP) south of the river. The sergeant has his PKM fire controlled bursts down the western flank of the road, knowing that the BTR is positioned to the eastern side of the roadbed.

Smoke still obscures any distinct visibility but the machinegun fire may slow any dismounted advance along that side of the road bed. He keeps the tripod-mounted Kornet-E antitank guided missile (ATGM) oriented on the road.¹ Where surprise provided a distinct advantage in the earlier engagements against dismounted soldiers, the tactical situation is now quite different with the enemy knowing the platoon's general locations with some elements in direct contact. The

Coordinating with the scout OP to his immediate rear near the riverbank, the senior sergeant masses his combat firepower on the most dangerous enemy direction of attack—along the main road. Indirect fires from the mortar section with high explosive rounds and smoke rounds are effective for now, but he knows that priority of fires will have to shift at some point to the platoon leader's maneuver rearward.

The 20-mm canon of the BTR will not stop any dedicated advance by armored vehicles, but can slow or temporarily stop armored wheeled vehicles if they approach up the road. No tanks have been reported yet in zone in what appears to be a motorized infantry unit based on initial interrogation of the enemy soldier captured in the platoon leader's earlier raid.

Using available cover and concealment with camouflage provides a degree of protection, as well as supporting the coordinated withdrawal actions using smoke.⁴ Time is a constant and actions must be prioritized to the time available. Even then, conditions change and time is often more constrained than originally planned. The Kornet-E gunner in the dug-in battle position of the OP is prepared and has the road as his primary direction of fire. The PKM gunner nearby in the OP fighting position orients to the west of the road. The BTR's 20-mm cannon, as well as its machinegun, orients on and to the east of the road. Vehicle and dismounted direct fire plans are intersecting sectors to at least disrupt or fix the enemy to the south.

The scout squad leader at the destroyed bridge continues to man a defensive position in BEJUNIK and conducts dismounted patrolling in conjunction with the engineer squad. He tells the senior sergeant that his patrols found and secured a ford west of BEJUNIK used by farm carts or small vehicles and provides the coordinates.

The mortar section sergeant updates the platoon leader and senior sergeant on his status. He prepositioned ammunition not only at the present site but farther northeast at the outskirts of BEJUNIK. When he displaces from his primary firing position, any gap in fires support will be minimal. He retains the combat load of on-board ammunition for any immediate fire mission hip-shoot while moving between positions.

Delay at PEL 23

No vehicles appear through the smoke at the road but dismounted enemy soldiers start to emerge from the white background on each side of the road. The senior sergeant fans BTR coax machine gun fire into each side of the road and soldiers either fall from wounds or drop to prone positions. He adjusts indirect high explosive (HE) fires closer to his BTR and calls for more smoke farther to the south.

The OP sergeant identifies several soldiers with his binoculars attempting to flank the position from the west. He directs the PKM gunner to suppress this area while remaining alert any movement on the road. Enemy actions subside for a short period, but soon afterward, enemy indirect fires start to fall along the road and near the BTR.

The senior sergeant is withdrawing from his roadside position in a slightly covered route along the berm of the road. He is almost abreast of the OP with his BTR when an enemy armored personnel carrier appears out of the smoke moving rapidly toward their position. Firing his 20-mm cannon at the carrier as he continues across the road, the whoosh and back-blast of the Kornet-E missile are comforting sounds as he moves into an expedient fighting position. The impact of the missile on the enemy carrier is a catastrophic explosion as the carrier turns abruptly in flames and blocks the narrow raised road.

The platoon leader listens to the ongoing combat actions and directs the senior sergeant to withdraw to BEJUNIK and continue to slow the enemy advance. Mines emplaced and covered in the road berm are rechecked as armed. Antipersonnel mines along the marsh woodline are also checked as armed with tripwires. Scouts throw several smoke grenades and upload into the BTR. A scout guides the senior sergeant to the ford site.

The senior sergeant reports to the platoon leader that he has reached the far river bank and is entering BEJUNIK. Indirect fires have shifted to the platoon leader's delay in the east. As the senior sergeant and scout squad sergeant update each other in the simple battle position near the river line, they hear an explosion south of the river. The nod at each other as the senior sergeant grins and says, "Antitank mine—one less vehicle." He notes that several scouts from his BTR occupy

a defensive position at the ford site and are already emplacing antitank mines near the northern bank waterline of the river.

The scout squad leader takes responsibility for these scouts as the senior sergeant moves in this BTR through BEJUNIK to coordinate with the engineer squad sergeant defending the bridge site. The platoon leader's delay and passage across the bridge is most likely to be a passage while in enemy contact.

The platoon leader is already delaying north along the roadway as enemy indirect fires explode intermittently near or on the road between his location and the bridge. Hill 21 appears to his rear more as a white cloud of smoke than a hill mass as his mortar section fires to obscure enemy observation from this high ground. Looking north to the bridge site ahead, he almost feels relieved when—suddenly— bullets start ricocheting off his vehicle from his left flank.

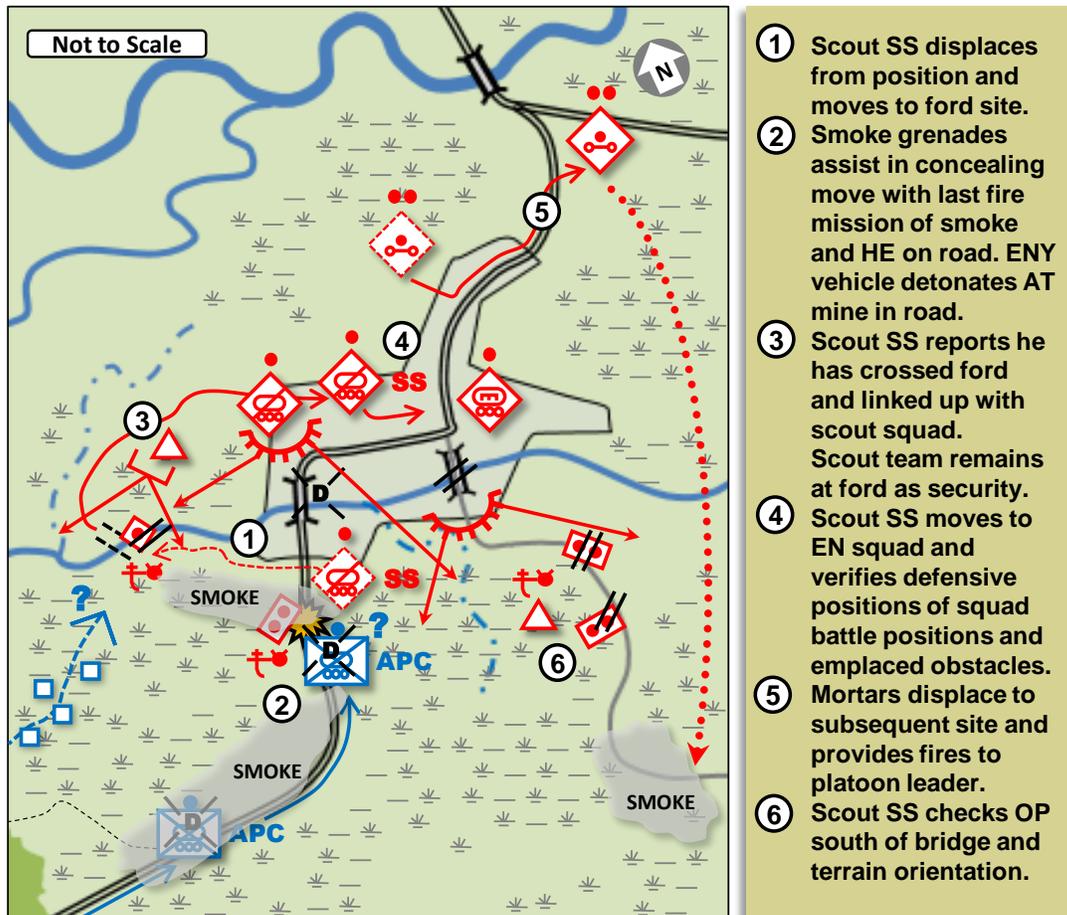


Figure 4. Delay and subsequent battle positions

What Next?

The next article in this vignette series will address additional tactical actions as the platoon leader and senior sergeant coordinate the linkup and passage across the MIN River, and continue the mission as an independent reconnaissance patrol in a larger offensive operation and encirclement of enemy forces.

Training Implications

This article illustrates the value of individual skills proficiency and effective execution of small unit drills and tactical tasks based on quality training, teamwork, and leadership. The orderly guidance described in doctrine may appear very different in execution of mission tasks when conditions change quickly, time is a constraint on what actions can be effectively

executed, and critical immediate decisions by tactical leaders require more than a clear understanding of mission and intent.

When conditions allow, a delay can be visualized typically into three elements: a *delay* [action] element, *security* element(s), and *support* element(s). The principle of security and dedicated elements to provide security can be problematic, especially in the small unit/element tactical vignette of this article. The OPFOR addresses delay-type actions in larger scale operations and defensive maneuver—normally described for tactical groups, divisions, and/or brigades—as a defensive array group of positions in which one or more subordinate units have orders to defend for a certain time within a higher headquarters’ area of responsibility (AOR). The OPFOR can accept large intervals between defensive positions in such an array, and may employ natural and/or manmade obstacles or deception defensive positions. In the spaces between such positional arrays, defenders typically execute disruption when conditions allow.⁵

In small-scale unit missions such as this independent reconnaissance platoon conducting a delay and to not become decisively engaged, the tactical actions may appear as a two-element maneuver complement to each other. Actions of security and disruption can blur a distinction between delay with main defense actions and what is a support action by function. Security elements are *enabling* elements and are primarily focused on disrupting or fixing enemy security and response forces.

In this vignette, the *delay* [action] element executes contact with the enemy and *disrupts* the enemy by defeating enemy lead elements; determining the location, disposition, and composition of other attacking elements; and may be able to target designated subsystems of the attacking enemy’s combat system. This OPFOR action element prepares to maneuver to its next alternate or subsequent simple battle position, and coordinates the transfer of delay task responsibility with other friendly elements already positioned and prepared to keep the enemy under continuous observation, fires, and attack.⁶

Smoke is typically employed to obscure enemy observation and reduce effectiveness of enemy actions in general. The deception aspect of using smoke can be integral to camouflage as *protective* smoke, and a larger principle of concealment.⁷ Cover, concealment, camouflage, and deception (C3D) by an opposing force is a fundamental principle in offensive and defensive actions. In addition to vehicle or weapon smoke grenade launchers, and direct and indirect fire smoke rounds, other capabilities include smoke hand grenades, smoke pots, smoke-dispensing systems, and expedients while operating in an operational environment. Some smoke products, expedient or militarized, might include carcinogens or toxic compounds.⁸

When the delay element is in contact with the enemy, this element provides the *main defense* action of a delay. When the delay element displaces from its simple battle position and has coordinated the transfer of main defensive actions to another element in contact with the enemy, the former delaying element becomes a *support* [enabling] element,

Opposing Force and Hybrid Threat in Training

When training is not focused on a particular real-world threat, Army activities use an opposing force as stated in Army Regulation 350-2. This regulation is a 2015 update on the operational environment (OE) and opposing force (OPFOR) program. As a *hybrid threat*, the OPFOR can represent or replicate diverse and dynamic combination of regular forces, irregular forces, terrorist forces, and/or criminal elements unified to achieve mutually benefitting effects. OPFOR tactical doctrine, tactics, and techniques are in Army Training Circular 7-100.2 and Army Training Circular 7-100.3.

TRADOC G-2 ACE Threats Integration Directorate

completes its maneuver, and occupies its *subsequent* simple battle position as in this vignette to assist the delay element in contact with the enemy. Another technique is to plan and conduct *alternate* battle positions in a delay.

The support element(s) assists the delay and other enabling elements of a delay. Types of OPFOR support include but are not limited to: combat service support (CSS), C2, supporting direct fires, supporting indirect fires, and supporting nonlethal actions such as smoke obscurants and other engineer support.⁹ Other forms of support not included in this tactical vignette include armor, aviation, air defense, and/or information warfare (INFOWAR).

The OPFOR can represent a particular threat, hybrid threat, and/or adversary that can morph in capabilities and influence within a relevant population and operational environment. Knowing the threat/OPFOR is essential to planning and combating the capabilities and limitations of an enemy or adversary in a training mission. When a specified threat exists in a deployment order, the actual threat force is represented or replicated in training and pre-deployment evaluations.

In 2015-2016, the Threats Integration Directorate (ACE-TI) is reviewing and revising the threat/OPFOR tasks found in TC 7-101. The updated list of tasks and subtasks, with conditions, standards, and performance measures for US Army training readiness, will address traditional offensive and defensive tasks, as well as tasks involving instability environments in an era of persistent conflict now and for the foreseeable future.

Notes

¹ US Army, TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. [Worldwide Equipment Guide – Volume 1: Ground Systems](#). August 2014. pp. 2-20 and 6-31.

² Headquarters, Department of the Army. [Training Circular 7-100.2, Opposing Force Tactics](#). TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. 9 December 2011. para. 8-83—8-86. Task-organized elements are best understood by knowing the unit and weapon system capabilities as presented in US Army [TC 7-100.4](#) and its TRADOC G-2 [Threat Force Structure e-folders](#) of units. Another source for equipment and weapon capabilities is the TRADOC G-2 [Worldwide Equipment Guide](#).

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. 4-67.

⁴ Headquarters, Department of the Army. [Training Circular 7-100.2, Opposing Force Tactics](#). TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. 9 December 2011. para. 4-6—4-7.

⁵ Headquarters, Department of the Army. [Training Circular 7-100.2, Opposing Force Tactics](#). TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. 9 December 2011. para. 4-67—4-68.

⁶ Headquarters, Department of the Army. [Training Circular 7-100.2, Opposing Force Tactics](#). TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. 9 December 2011. para. 4-111—4-112.

⁷ Headquarters, Department of the Army. [Training Circular 7-100.2, Opposing Force Tactics](#). TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. 9 December 2011. para. 13-134 and 13-139.

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. para. 13-123.

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. 4-116. A *reserve* element provides the OPFOR commander with tactical flexibility. During a delay action, a reserve may be directed to augment forces in a disruption zone to provide additional security to the delaying main defense element, and/or be positioned for tasks such as counterattack, counterpenetration, blocking or destroying enemy penetration, and/or anti-landing defense.

Combating Terrorism Posters

FY15 Review

TRADOC G-2 ACE Threats Integration



Complete Operational Environment and Threat Integration Handbook

PROTECT

US ARMY TRADOC TRISA

THE CYBER DOMAIN

We are at War and Combating Cyber Terrorism

Know the Threats-Know the Enemy

TRISA Learning Services (L3) Poster No. 05-02 U.S. Army TRADOC G-2 Operational Environment Enterprise TRADOC G-2 Intelligence Support Activity (ISIA)

We are at War and Combating TERRORISM

US ARMY TRADOC TRISA

THE CYBER DOMAIN

Know the Enemy

Be Cyber Threats Aware-Be Ready!

TRISA Learning Services (L3) Poster No. 05-02 U.S. Army TRADOC G-2 Operational Environment Enterprise TRADOC G-2 Intelligence Support Activity (ISIA)

Complete Operational Environment and Threat Integration Handbook

US ARMY TRADOC TRISA

We are at War and Combating TERRORISM

Know the Threats-Know the Enemy

TRISA Learning Services (L3) Poster No. 05-02 U.S. Army TRADOC G-2 Operational Environment Enterprise TRADOC G-2 Intelligence Support Activity (ISIA)

U.S. Army TRADOC G-2 Operational Environment Enterprise TRADOC G-2 Intelligence Support Activity (ISIA)

Know the Threats We are Combating TERRORISM

We will work with our allies and partners to prevent a terrorist regime from establishing, advancing and extending its global influence. And we will continue our counterterrorism mission against the remnants of al Qaeda to ensure that Afghanistan is never again used to stage attacks against innocent people.

Resolute and Ready

TRISA Learning Services (L3) Poster No. 05-02 U.S. Army TRADOC G-2 Operational Environment Enterprise TRADOC G-2 Intelligence Support Activity (ISIA)

U.S. Army TRADOC G-2 Operational Environment Enterprise TRADOC G-2 ACE-Threats Integration

Know the Threats We are Combating TERRORISM

Know the Enemy

Antiterrorism Awareness in Field Units

TRADOC G-2 Handbook 1.07 G-2 Hip-Pocket 5" x 7"

TRISA Learning Services (L3) Poster No. 05-02 U.S. Army TRADOC G-2 Operational Environment Enterprise TRADOC G-2 Intelligence Support Activity (ISIA)

U.S. Army TRADOC G-2 Operational Environment Enterprise TRADOC G-2 ACE-Threats

Know the Threats We are Combating TERRORISM

Know the Enemy

Training Antiterrorism Awareness in Units

TCY-100.2

TRISA Learning Services (L3) Poster No. 05-02 U.S. Army TRADOC G-2 Operational Environment Enterprise TRADOC G-2 Intelligence Support Activity (ISIA)

U.S. Army TRADOC G-2 Operational Environment Enterprise TRADOC G-2 ACE-Threats

Antiterrorism Awareness in an ABR

Know the Threats Know the Enemy

Know the Enemy

ATN

TRISA Learning Services (L3) Poster No. 05-02 U.S. Army TRADOC G-2 Operational Environment Enterprise TRADOC G-2 Intelligence Support Activity (ISIA)

U.S. Army TRADOC G-2 Operational Environment Enterprise TRADOC G-2 ACE-Threats

Know the Threats Know the Enemy We are Combating TERRORISM

Know the Enemy

Antiterrorism Awareness

Handbook 1.07 G-2

TRISA Learning Services (L3) Poster No. 05-02 U.S. Army TRADOC G-2 Operational Environment Enterprise TRADOC G-2 Intelligence Support Activity (ISIA)

U.S. Army TRADOC G-2 Operational Environment Enterprise TRADOC G-2 ACE-Threats

Multinational Antiterrorism Readiness-Training

Know the Threats Know the Enemy We are Combating TERRORISM

Know the Enemy

ATN

TRISA Learning Services (L3) Poster No. 05-02 U.S. Army TRADOC G-2 Operational Environment Enterprise TRADOC G-2 Intelligence Support Activity (ISIA)

U.S. Army TRADOC G-2 Operational Environment Enterprise TRADOC G-2 ACE-Threats

Antiterrorism Training: Alert and Ready

Know the Threats Know the Enemy We are Combating TERRORISM

Know the Enemy

ATN

TRISA Learning Services (L3) Poster No. 05-02 U.S. Army TRADOC G-2 Operational Environment Enterprise TRADOC G-2 Intelligence Support Activity (ISIA)

U.S. Army TRADOC G-2 Operational Environment Enterprise TRADOC G-2 ACE-Threats

Antiterrorism Awareness and Application

Know the Threats Know the Enemy We are Combating TERRORISM

Know the Enemy

ATN

TRISA Learning Services (L3) Poster No. 05-02 U.S. Army TRADOC G-2 Operational Environment Enterprise TRADOC G-2 Intelligence Support Activity (ISIA)

U.S. Army TRADOC G-2 Operational Environment Enterprise TRADOC G-2 ACE-Threats

Never Forget... 9/11 Attack on the Homeland

Know the Enemy We are Combating TERRORISM

Know the Enemy

ATN

TRISA Learning Services (L3) Poster No. 05-02 U.S. Army TRADOC G-2 Operational Environment Enterprise TRADOC G-2 Intelligence Support Activity (ISIA)

Know the Threats — Know the Enemy

We are Combating Terrorism

Cartel Warfare: Analyzing Mexican Drug Trafficking Organizations (DTOs)

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

Since December 2006, Mexico has been mired in a barbarous war with a quasi-omnipotent foe: Mexican drug trafficking organizations (DTOs). Characterized by extreme violence, intimidation, and unbounded profit and facilitated through widespread corruption, the Mexican War on Drugs has had a deleterious effect on the state's image, security environment, and quality of life for Mexican citizens. Homicide rates have increased dramatically—up nearly threefold from 8.1 per 100,000 in 2007 to 23.7 per 100,000 in 2010—ostensibly attributable to the rise in DTO activities.¹ The preponderance of Mexico's municipalities are at best influenced—if not fully infiltrated—by the diverse actors categorized under the organized crime umbrella.² Likely conservative estimates indicate that DTOs virtually control 30% of Mexico's territory.³



Figure 1: [2014 STRATFOR Estimate of Cartel Areas of Influence](#)

Unfortunately, there are no signs that the violence will abate anytime soon. The seemingly perpetual state of conflict engulfing Mexico serves as the impetus for this article, as it will strive to serve as a primer for analyzing DTO criminal activities, terrorist actions, functional tactics, and their potential impact on Unified Action partner training.

The Concept of a “Criminal Insurgency”

Joint Publication 3-24, *Counterinsurgency*, defines insurgency as “the organized use of subversion and violence to seize, nullify, or challenge political control of a region.”⁴ In the case of DTOs, nullification (or at least co-opting) of the state is the principle focus as they seek “to weaken the structures of governance and rule of law to secure maneuver room for their own operations and influence.”⁵ And although they do not seek the ends of a traditional insurgency—the overthrow of the existing state, self-rule, and/or a revolutionary transformation—DTOs have developed an ascertainable strategy.⁶

The criminal insurgency strategy of DTOs is a three-pronged attack: attrit or co-opt law enforcement officers through a campaign of terror; conduct information warfare (INFOWAR) to degrade public and state resolve, intimidate rivals, and martial support; and conduct high profile assassinations of state officials.⁷ The long-term goal of this strategy is to force the Mexican state to abandon its offensive against DTOs so they can maintain their criminal enclaves of impunity, increase power, and maximize profit.⁸ DTOs use a combination of several ways and means to achieve their aforementioned ends. In the context of “criminal insurgency”* the actions can be described as criminal activities, terrorist actions, functional tactics, and information warfare (INFOWAR).

Criminal Activities

Criminal activities can be defined as the varied use of tactics and techniques in violation of state statutes to make a fiscal profit and/or achieve influence.⁹ While DTO criminal activity has an ancillary effect of maintaining the coerced support of noncombatants through intimidation, its primary functions are to maintain control of the *plazas* (drug shipment corridors that serve as cartel support zones) and generate profit. Two of the most common criminal activities that DTOs engage in are extortion and trafficking, both of which greatly contribute to the real and perceived insecurity and instability of the nation.

Protection rackets requiring Mexican citizens to pay *derecho de piso* (protection money) to DTOs is an innocuous means of revenue generation relative to other DTO criminal activities. DTOs require local business proprietors to make recurring payments in exchange for the DTOs’ protection from street gangs, rivals, and/or corrupt Mexican authority figures. This revenue stream is directly linked to the DTOs’ ability to maintain and acquire “turf.” The more “turf” a DTO controls, the more protection money it generates. The importance of acquiring and maintaining terrain cannot be understated. DTOs derive their power from the *plazas* in that they provide them the ability to generate revenue via criminal activities, primarily trafficking. The widely accepted theme is that drugs and people move north while money and guns move south.

Although the profit generated by “shakedowns” in a protection racket is substantial, no criminal activity is as lucrative as the DTOs’ main effort—drug trafficking. All instances of criminal activity coalesce around the production, distribution, and sale of illegal psychotropic drugs, mainly heroin, methamphetamine, and cocaine. The US Department of Justice estimates that Colombian and Mexican DTOs generate between \$18 billion and \$39 billion annually solely from drug sales in the United States.¹⁰ Proceeds from narco-trafficking is the lifeblood of these organizations, enabling reinvestment into licit and illicit markets alike, ranging from real estate investment to the purchase of precursor chemicals necessary to manufacture drugs.¹¹

*Author’s interpretation of Sullivan and Elkus’s term “criminal insurgency” is that the “criminal” modifier serves to clarify the goals and motivations of the cartels while the “insurgency” subject illustrates the more kinetic methods they use to achieve them.

AREAS OF CARTEL INFLUENCE, WITH SMUGGLING ROUTES

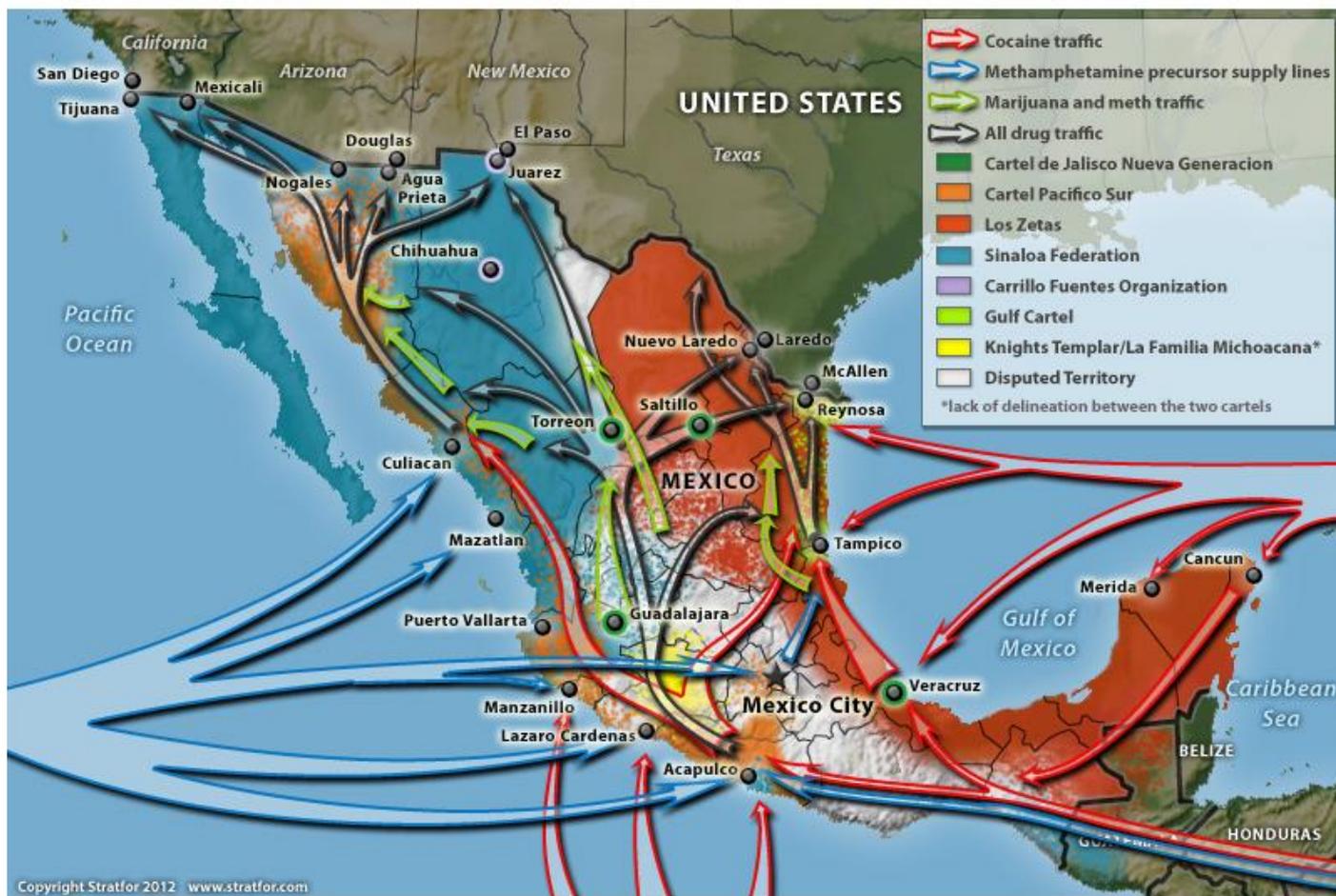


Figure 2: [2012 STRATFOR Estimate of Cartel Areas of Influence w/ Smuggling Routes](#)

Terrorist Actions

According to Training Circular (TC) 7-100.3, *Irregular Opposing Forces*, “Terrorism can be defined as the use of violence or the threat of violence to instill fear and coerce governments or societies.”¹² The key distinction between quintessential terrorist organizations (e.g. al-Qaeda and its affiliates) and DTOs is that the latter use terrorist actions as means to obtain profit and not in the furtherance of a religious or political ideology. Additionally, DTOs use terrorism to psychologically affect rivals, the state, and the citizenry with the goal of convincing or compelling them to act in a desired manner.¹³ Predominate motivations for DTO terror campaigns are diverse: disrupt their enemy’s ability to act, obtain active and/or passive support from the relevant population, deter continued enemy operations in a particular geographic area, dissuade enemy governmental influence over the relevant population, and develop acceptance and legitimacy of their criminal agenda.¹⁴

One of the more common terrorist actions perpetrated by DTOs is kidnapping. This action is often combined with the criminal activities of murder and maiming to enhance the message’s potency. Targets range from rival DTO *sicarios* (Spanish slang for hitman) and *halcones* (Spanish for falcons, a moniker given to cartel lookouts) to municipal police. Kidnapping victims often face macabre execution methods like decapitation by chainsaw, dismemberment, and dynamiting. The latter is a recent technique used by the Jalisco Cartel-New Generation (CJNG) in Jalisco state in which the

captured victims have sticks of dynamite taped to them (typically to their torso or neck) that are detonated while still alive.¹⁵

Although less frequent than commonplace terrorist actions like kidnapping, genocide-like mass executions can have a much more paralyzing effect on intended audiences. Countless *narcofosas* (mass graves) have been found throughout the country, the most memorable being a result of the 2011 San Fernando Massacre. Members from Los Zetas (defected Mexican Special Forces Soldiers previously employed by the Gulf Cartel as enforcers) intercepted several buses full of Central and South American migrants traveling north toward border towns.¹⁶ Suspecting that the migrants were recruits of the rival Gulf Cartel, Los Zetas murdered all 193 captives and buried them in several mass graves. The alleged sole survivor recounted to a Mexican media outlet that women were raped, men were forced to fight one another to the death in a gladiator-style blood sport, and that infants were thrown into vats of acid.¹⁷

Alternative assessments exist, however, and some analysts believe that the mass murder was a message to the Central American “coyotes” engaged in the lucrative human smuggling enterprise. The message: everyone must pay.¹⁸

Functional Tactics

The United States Armed Forces defines tactics as “the employment and ordered arrangement of forces in relation to each other.”¹⁹ Similarly, the Hybrid Threat (HT) employs functional tactics. The HT chooses which functional tactic to use (e.g. ambush, raid, or reconnaissance attack) based upon the functions (e.g. disrupt, fix, or destroy) that need to be performed as part of an action to bring about its success.²⁰ The following vignette illustrates the applicability of the term “criminal insurgency” to DTOs because criminals typically do not have the ability to execute functional tactics.²¹

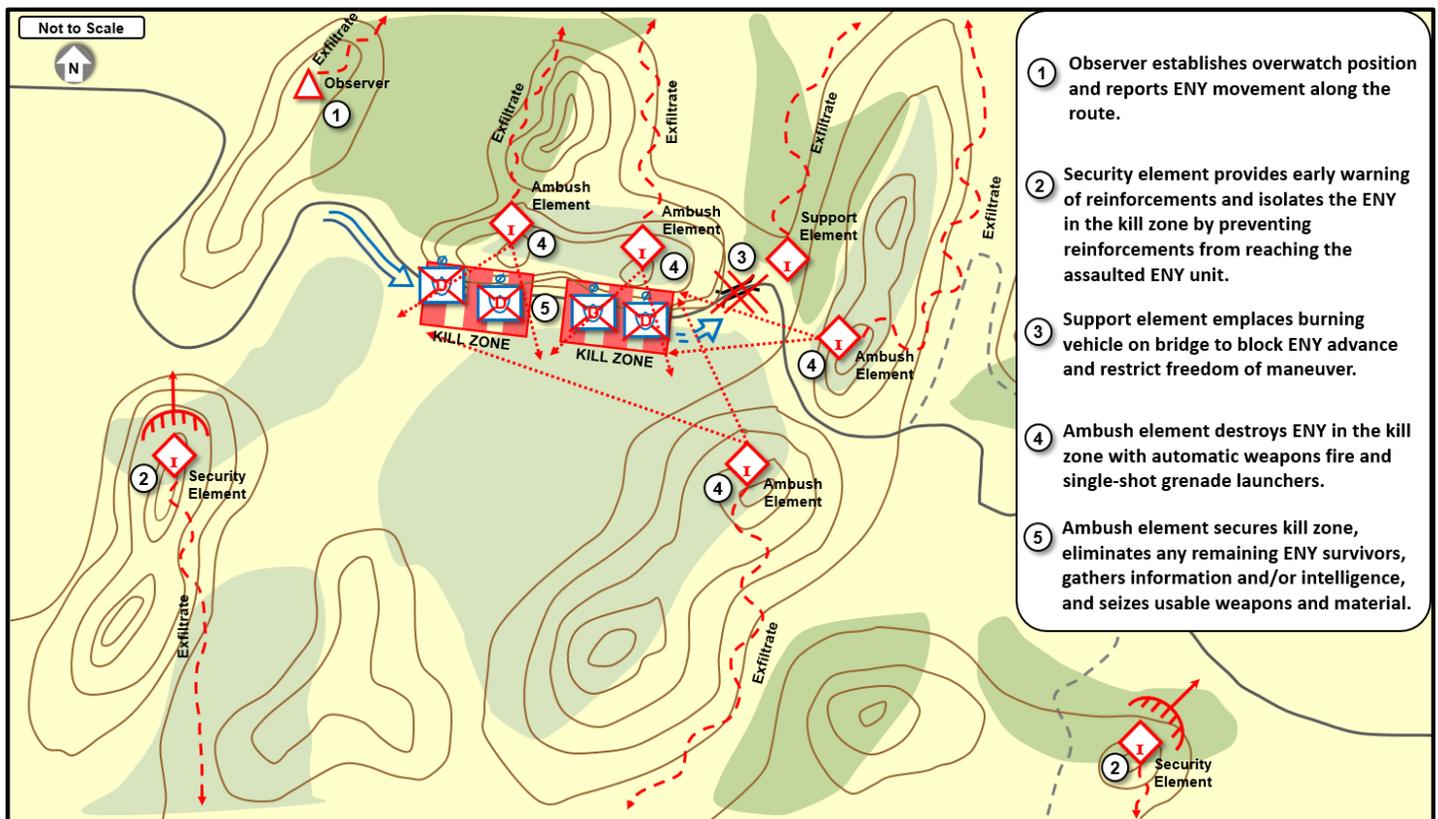


Figure 3: CJNG Annihilation Ambush

In response to the killing of CJNG cell leader Heriberto Acevedo Cardenas (“El Gringo”) after a March 2015 shootout with police, the CJNG retaliated. At approximately 1450 hours, 6 April 2015, an unknown number of CJNG members armed with automatic weapons and grenade launchers ambushed a two-man convoy composed of members from the United Force of Jalisco (a specialized police unit in the western-central Mexican state of Jalisco) on a rural highway in the Sebastian del Oeste municipality of Jalisco state.²² Figure 3 illustrates the analyst’s interpretation of how CJNG could have executed the annihilation ambush.

The attackers established the annihilation ambush on favorable terrain: firing positions were established adjacent to a portion of the two-lane highway that offered the attackers good cover and concealment and fields of fire from the surrounding high ground; the terrain also provided unobservable approach and withdrawal routes. To block the police convoy, the attackers emplaced a burning vehicle on a bridge on the eastern edge of the kill zone. This complemented the already canalizing terrain and further restricted police maneuver. There were also indicators that the attackers had been waiting at the ambush site for some time. Residual debris included clothes, beer cans, empty water bottles, food containers, condoms, and tents.²³ The end result was the deadliest attack on Mexican police since 2010: 15 dead and 5 injured.²⁴

INFOWAR

Threat doctrine defines INFOWAR “as specifically planned and integrated actions taken to achieve an information advantage at critical points and times.”²⁵ DTOs primarily employ the INFOWAR elements of deception and perception management to achieve the tactical tasks of disrupt, deceive, and influence. The proliferation of information and communication technologies has enabled DTOs to communicate their narrative of *plata o plomo* (Spanish for silver or lead) to the majority of relevant actors within the operational environment. Coupled with coercion of the media, low-tech reconnaissance tools (e.g. a *halcone* with a mobile device) and espionage via endemic state corruption, DTO INFOWAR is robust and effective.

INFOWAR can be the impetus for combat action, particularly when the objective is to wage psychological warfare against relevant actors. Grisly recordings of beheadings, public displays of mutilated bodies, mass executions, and even name selection (e.g. *Mata Zetas*, Spanish for Zeta Killers) are all elements of the typical DTO INFOWAR playbook. These abhorrent acts of violence are specifically conducted to influence “the attitudes, emotions, motivations, aggressiveness, tenacity, and reasoning of enemy personnel.”²⁶ The propagation of these acts is sometimes in conjunction with corpse-messaging and narco-banners to further shape the social and environmental conditions in their favor.

Nonlethal examples of perception management activities are manifested in media and recruitment activities. *Narcocorridos* (Spanish for narco-ballad) is a popular music genre that glorifies the *narco* lifestyle and venerates DTO leaders. In a country beset by socioeconomic inequality, disenfranchised Mexican youths gravitate to DTOs for employment and a sense of belonging. In 2007, only eight minors were charged with involvement in organized crime in Mexico; in 2010 that number skyrocketed to 214.²⁷ By highlighting the government’s inability to tackle social and economic issues like endemic corruption, violent crime and poverty, DTOs are able to bolster their ranks with a steady stream of young recruits.

Implications for Training

DTOs are becoming increasingly militarized in the way in which they execute tactical operations, potentially a result of the integration of ex-military defectors into their ranks. Their military capabilities improve as they continue to acquire military-grade weapons like high-powered automatic weapons and sniper rifles; light, medium, and heavy machine guns; grenades and grenade launchers; light anti-tank weapons; rocket-propelled grenades; armor-piercing munitions; 60-mm mortars with high explosive rounds; and improvised explosive devices.²⁸ In light of this threat, joint force units regionally aligned



Figure 4: [Popular narcocorrido band Los Tigres Del Norte performing a hit song](#)

with US Northern Command (NORTHCOM) and US Army Military Police (MP) units that could potentially be tapped to provide security force assistance to Mexican security forces should place a premium on battlefield survivability tasks during training. MP units must be acutely aware of the fact that many Mexican police forces are far less capable than their military counterparts with regards to manning, equipment, training, leadership, and morale. Determining how to address these gaps would be critical to the success of the overall security force assistance mission.

On a macro level, Department of Defense (DoD) justice and security enablers like US Army Criminal Investigations Special Agents, Corrections Specialists, and Judge Advocate General officers may consider preparing to augment existing Merida Initiative programs and activities. The Merida Initiative is a security cooperation partnership between the US and Mexico to disrupt organized crime, sustain the rule of law, increase border security, and build strong and resilient communities.²⁹ It is conceivable that DoD enablers may be integrated into the existing partnership structure to buttress the Mexican security and justice sectors. Integral to the success of the initiative, however, is maintaining a semi-permissive security environment, which continues to be an ongoing challenge.

Notes

- ¹ Cory Molzahn, Octavio Rodriguez and David A. Shirk. "[Drug Violence in Mexico.](#)" Trans-Border Institute at the University of Sand Diego. February 2013.
- ² John P. Sullivan. "[From Drug Wars to Criminal Insurgency.](#)" The VORTEX Foundation. March 2012.
- ³ John P. Sullivan. "[From Drug Wars to Criminal Insurgency.](#)" The VORTEX Foundation. March 2012.
- ⁴ Joint Publication 3-24. "[Counterinsurgency.](#)" 22 November 2013.
- ⁵ John P. Sullivan and Adum Elkus. "[State of Siege: Mexico's Criminal Insurgency.](#)" The Small Wars Journal. 19 August 2008.
- ⁶ Steven Metz. "[Rethinking Insurgency.](#)" Strategic Studies Institute. June 2007.
- ⁷ John P. Sullivan and Adum Elkus. "[State of Siege: Mexico's Criminal Insurgency.](#)" The Small Wars Journal. 19 August 2008.
- ⁸ John P. Sullivan and Adum Elkus. "[Plazas for Profit: Mexico's Criminal Insurgency.](#)" The Small Wars Journal. 26 April 2009.
- ⁹ 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. Para 4-48.
- ¹⁰ Patrick Radden Keefe. "[Cocaine Incorporated.](#)" The New York Times Magazine. 15 June 2015.
- ¹¹ Jason Lange. "[From spas to banks, Mexico economy rides on drugs.](#)" Reuters. 22 January 2010.
- ¹² 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.
- ¹³ 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. Para 6-2.
- ¹⁴ 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. Para 6-7.
- ¹⁵ Lucio R. "[CJNG: killing enemies by dynamite.](#)" Borderland Beat. 15 June 2015.
- ¹⁶ Oscar Martinez. "[How the Zetas Tamed Central America's 'Coyotes.'](#)" InSight Crime. 1 May 2014.
- ¹⁷ Borderland Beat. "[A Nightmare of the Massacre in San Fernando.](#)" 18 April 2011.
- ¹⁸ Oscar Martinez. "[How the Zetas Tamed Central America's 'Coyotes.'](#)" InSight Crime. 1 May 2014.
- ¹⁹ Joint Staff. [Chairman of the Joint Chiefs of Staff Manual 5120.01A.](#) 29 December 2014.
- ²⁰ Headquarters, Department of the Army. [Training Circular 7-100, Hybrid Threat.](#) TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. November 2012. Para 5-18.
 - ²¹ 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.
- ²² John P. Sullivan and Robert Bunker. "[Mexican Cartel Tactical Note # 25: Ambush Kills 15; Injures 5 Police in Jalisco.](#)" The Small Wars Journal. 16 July 2015.
- ²³ Lucio R. "[video: footage of the aftermath of CJNG ambush on state police.](#)" Borderland Beat. 11 May 2015.
- ²⁴ John P. Sullivan and Robert Bunker. "[Mexican Cartel Tactical Note # 25: Ambush Kills 15; Injures 5 Police in Jalisco.](#)" The Small Wars Journal. 16 July 2015.
- ²⁵ 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. Para A-1.
- ²⁶ 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. Para A-33.
- ²⁷ Geoffrey Ramsey. "[Poverty a Recruitment Tool for Mexico's Criminal Gangs.](#)" InSight Crime. 20 July 2011.
- ²⁸ David Kuhn and Robert Bunker. "[Mexican Cartel Tactical Note # 17.](#)" The Small Wars Journal. 17 February 2013; David Kuhn and Robert Bunker. "[Mexican Cartel Tactical Note # 15.](#)" The Small Wars Journal. 14 January 2013.
- ²⁹ United States Diplomatic Mission to Mexico. <http://mexico.usembassy.gov/eng/ata glance/merida-initiative.html/>. 13 October 2015.

Threat Actors in Pakistan

by [Walter L. Williams](#), TRADOC G-2 ACE Threats Integration (DAC)

TRADOC G-2 ACE Threats Integration (ACE-TI) produces Threat Tactics Reports (TTRs) as a method of informing the Army training and education community how a particular state or non-state actor conducts military operations. Unlike an Operational Environment Assessment (OEA) that looks at all of the operational variables of political, military, economic, social, information, infrastructure, physical environment, and time (PMESII-PT), a TTR focuses primarily on the military variable. The purpose of this *Red Diamond* article is to provide a brief look at a TTR currently under development about threat actors in Pakistan.

Strategic Overview

As a country only formed in 1947, Pakistan believes it faces both external and internal threats to its young existence. These threats could usefully be categorized in terms of “*far*” enemy and “*near*” enemy. Externally, Pakistan views its number one nemesis, India, as a near enemy. In relation to this, its internal threats can be characterized as far enemies. Internally, Pakistan face multiple threats from different and at times competing insurgent and militant or jihadist groups and even political turmoil. The term *militant groups* used throughout this article includes jihadist and religious groups and organizations.

In general, the national security threats to Pakistan can be said to include an existential threat from India, separatism from Baluchistan, exceptionalism and religious militancy from the Federally Administered Tribal Areas (FATA), sectarian violence of Sunni against the Shia and other minorities, and political turmoil both at the national and sub-national levels. The ranking and attention—resource and otherwise—paid to these threats correspond to their relative evaluation from a national security strategy perspective. For instance, the threat that emanates from the province of Baluchistan seeks separation or independence from Pakistan. As a relative measure of national security interest, Baluch separatists or insurgent groups are of a higher concern than militant or jihadist groups operating in the FATA but still lower than the overwhelming conventional or nuclear threat posed by India. Accordingly, Pakistan’s security response involves the use of its conventional military under the Ministry of Defense as well as its internally-focused security architecture that is structured from under the Ministry of Interior and combines some federal military with local forces

The Indian threat aside, a view of the militant groups that represent internal or far threats indicates that they can have complex motives, such as economic, ideological/religious, and traditional/tribal, and seems to be geo-spatially self-limiting, meaning that they are focused on particular area of operations. Current and future trends suggest these groups will increasingly cause Islamabad to adopt various diplomatic, information, military, and economic methods to combat the evolving nature of these religious and jihadist groups. The table provides a snapshot of the various militant groups currently conducting operations within Pakistan.

Table 1. Internal Militant Groups

Group Name	Initials	Aliases	Primary Area of Operations
Taliban	Taliban	Pastun Taliban Militia	Afghanistan; Pakistan
Tehrik-e-Taliban	TTP	Tehrik Taliban Pakistan	Pakistan; FATA
Haqqani Network	HQN	Haqqani Militia	Afghanistan; Pakistan
Lashkar-i-Islami	LI	LI	Pakistan
Tehrik-e-Nafaz-e-Shariat-e-Mohammadi	TNSM	Movement for the Enforcement of Islamic Law	Pakistan
Lashkar-e-Taiba	LeT	Jama'at und-Dawa; Al-Mansoorian; Markaz al-Dawa wa al-Irshad; Army of the Pure, Army of the Righteous	Kashmir
Harakat-ul-Mujahideen	HUM	Al-Faran; Al-Hadid; Al-Hadith; Harakat ul-Ansar; Harakat ul-Mujahdeen; HuA; Jamiat ul-Ansar; and the HuM	Kashmir; Afghanistan
Qaeda al-Jihad (al-Qaeda)	AQ	Al-Qaeda of the Lands in the East and West	Pakistan
Islamic Movement of Uzbekistan	IMU	Turkistan al-Islamiyya	Pakistan
Hizb-e-Islami Gulbuddin	HIG		Pakistan
Hizb-e-Islami (Khalis Faction)	Hel-K	Hizb-i-Islami-Yunus Khalis	Pakistan
Islamic Jihad Union	IMU	IMU Faction; Islamic Jihad Group of Uzbekistan and Islamic Jihad Group	Pakistan
Lashkar-e-Janghvi	LJ	Army of Janghvi	FATA; Pakistan
Jaish-e-Mohammed	JeM	Jaish-e-Mujahideen; Army of Mohammed; Jaish-i-Mohammed; Khudamul Islam; Khuddam-ul-Islam; Kuddam e Islami; Mohammed's Army, Tehrik ul-Furaqaan	Kashmir; FATA; Pakistan

Organization

Pakistani militant groups are neither homogenous in nature nor monolithic in thought. Additionally, the organizational structure of the groups is fluid and changes over time in response to external threats such as those posed by forces allied with the United States. A literature review conducted by Center for Strategic and International Studies (CSIS) concluded “that there is no reliable information on the network of offices run by the militant groups across Pakistan and Afghanistan. Furthermore, there is much disagreement over the correct number of individuals who make up the total membership of a militant group and the number of active operatives in this cadre. This is perhaps the case because these organizations are extremely secretive and do not reveal their true strength.”¹

The group's structures range from highly centralized and hierarchal to decentralized, loose networks. Some may be decentralized and cell based. While there is little to no information on the exact organization of a cell, the analyst assessment is the cell structure may consist of a cell leader and cell members. For example, the cell leader assigns tasks, checks on the cell members, and possibly acts as a liaison with other cells. There could be cases of assistant cell leaders based on the size of the respective cell. However, a general consensus is that the cells are kept small to reduce the

possibility of compromise. It is also possible that the cell is compartmentalized in order to protect the militant organization and reduce the vulnerability of its key leaders and members to be captured. Compartmentalization restricts the information any cell member has regarding the identity, background, or current location of other cell members. The decentralized nature of the overall militant group using the cell structure facilitates an autonomy of operations in various parts of the region, layered with security, thus reducing the cell's vulnerability to detection and compromise.

ISIL Attempts to become a Major Player

The Islamic State in Iraq and the Levant (ISIL) has been making attempts to export its organizational brand to Pakistan. As early as September 2014, an ongoing war of words between ISIL and the Afghani-Pakistani militant groups such as the Taliban have been consistently conducted to garner legitimacy and recruitment in region. Specifically, "pamphlets backing ISIL have been appearing in northwestern Pakistan. They appeal to local tribesmen to join ISIL, either in Syria or in Pakistan and fight. This is the only known ISIL activity in Pakistan so far, aside from hundreds of local Islamic terrorists going to join ISIL in Syria over the last year. Most other Islamic terrorist organizations are hostile to ISIL, which is seen as greedy and too extreme for most Islamic extremists. Given the large number of Islamic terrorists already in Pakistan, that would make it difficult get established in Pakistan."²

On 13 September 2015, an anti-Pakistan militant faction allied with ISIL conducted an attack against a Pakistani Border outpost located in the northwest portion of Pakistan. Depending on the location, these outposts face a range of probable incursions by notable groups such as criminals and warlords, Afghan Taliban, al-Qaeda, and tribal miscreants (a bad person or group who is not necessarily an enemy). Figure 1 provides an example or general view of a Pakistani border outpost.

The attack was reportedly conducted in the Damadola district in the Bajaur tribal area. It is the analyst's assessment that the attack was conducted by a small element (possibly 10-20 people) using small arms and rockets. Some groups such as LeT and JeM conduct operations in small teams using *fidayeen* tactics. "Fidayeen attacks, while ultimately acts of suicide, are distinct from the contemporary 'suicide bomber.' Militants armed with ammunition, weaponry, and small-scale explosives infiltrate their targets (often military bases or civilian institutions) and begin to open fire. The attacks continue until the militants run out of ammunition or are killed by security personnel. Escape is possible, and has occurred, but is unlikely and often accidental. Historically, *fidayeen* ('Death-Defying' or 'Commando') squads were introduced by Pakistani radical organizations funneling weapons and personnel in to Kashmir during the 1990s. It was the preferred method of Lashkar-E-Toiba, a Karachi-based extremist group blamed for attacks across the subcontinent."³



Figure 1. Typical border outpost

Despite claims by the anti-Pakistan militant faction that the border post was destroyed, Pakistani intelligence officials confirmed the attack occurred but there were no Pakistani casualties as a result of the attack. Additionally, the militant faction did not acknowledge casualties to its force. Thus, this was a raid that was repulsed by the Pakistani forces occupying the outpost. The rationale for the attack is suspected to be a way for ISIL to attempt to establish a presence in the Afghanistan-Pakistan area through the recruitment of Taliban and al-Qaeda jihads. Figure 2 is a visual concept or of the

attack using the TC 7-100 series Hybrid Threats manuals to serve as a baseline for understanding how this attack was executed. The information warfare (INFOWAR) section in the diagram would more than likely consist of a video crew along with other members to capture material from the outpost to be used in a probable anti-Pakistani media campaign.

Training Implications

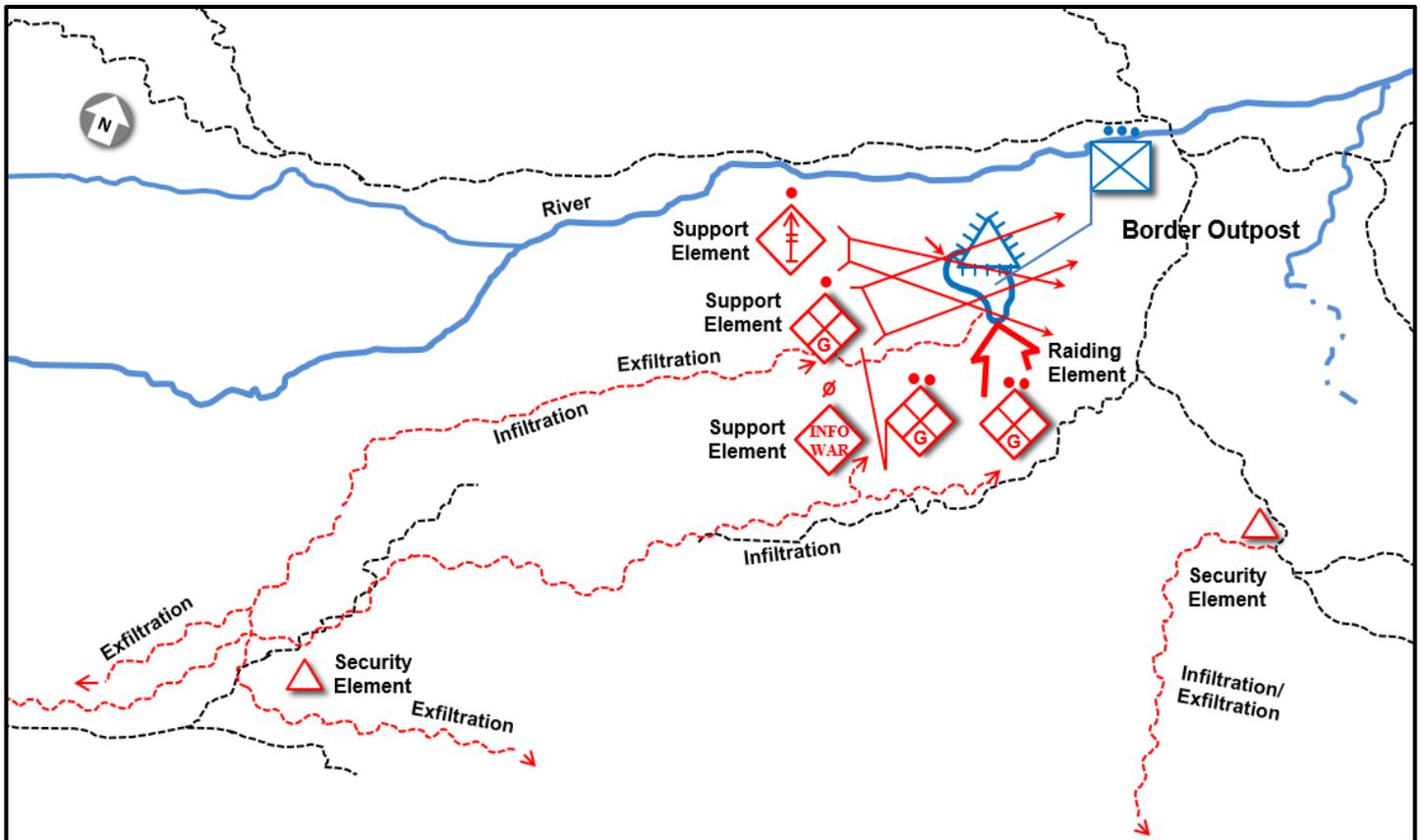


Figure 2. Analyst's visual concept

The alliance of these militant groups demonstrates the high potential for the transfer of tactics and techniques as a countermeasure to the tactics used by forces allied with the US. For example, the use of the improvised explosive devices (IEDs) as a precursor to an attack may show indications of several distinctive groups. IEDs may be used as a barrier or obstacle to a quick reaction force or to severely damage or destroy first or second responders to an attack. Thus, it makes the post attack forensics and analysis a little more challenging. In essence, the militant groups becomes an enemy who constantly observes, picks up patterns very quickly, and determines the best countermeasures.

The implication for training is to present a leader or student with a dilemma or series of dilemmas to resolve over a period of time. It is possible to present the attacks in a generic way to get a "crawl" stage of a probable response. However, to move through a progressive nature of "walk" to "run," the problem sets must become more complex with the outcome not as obvious. The "run" may occur as part of a unit capstone event at a Combat Training Center (CTC) or during a Home Station Training event.

Note. Due to the many spelling and alias names of militant groups listed in various open source publications, the author has chosen to use the group names and aliases as defined by the U.S. Department of State [Country Reports on Terrorism 2014, Chapter 6 Foreign Terrorist Organizations](#). The author also used the [Combatting Terrorism Center at West Point](#) to also determine group names and aliases.

References

- Al Jazeera. "[Afghan leader slams Pakistan over Kabul attacks.](#)" 11 August 2015.
- Aoun, Joy; Danan, Liora; Hameed, Sadika; Lamb, Robert D.; Mixon, Kathryn; and St. Peter, Denise. "[Religious Movements, Militancy, and Conflict in South Asia.](#)" Center for Strategic and International Studies (CSIS). July 13, 2012.
- Hammer, Josh. "[The Age of the Fidayeen: Terror's New Tactic.](#)" Foreign Policy Association. 1 December 2008.
- Hashim, Asad. "[Pakistan's Ismaili community hit by deadly attack.](#)" Al Jazeera. 13 May 2015.
- Hyman, Gerald. "[Will the Taliban School Massacre Change Pakistan's Basic Security Orientation?](#)" CSIS. 28 May 2015.
- Kabul Tolo News in Dari. "[Afghan Deputy Army Chief Says 'Pakistani Generals' Involved in Kunduz Battle.](#)" 5 October 2015.
- Lamb, Robert D. and Mariam Mufti. "[Religion and Militancy in Pakistan and Afghanistan.](#)" Center for Strategic and International Studies (CSIS). June 2012.
- Spencer, Robert. "[Islamic State attacks paramilitary checkpoint along Afghan/Pakistan border.](#)" Jihad Watch. 13 September 2015.
- Strategy Page. "[India-Pakistan: ISIL Comes To Stay.](#)" September 2014.
- Stratfor. "[Pakistan: Militants Attack ISI Building in Peshawar.](#)" 13 November 2009.
- Stratfor. "[Pakistan: Militants Attack Peshawar Checkpoint.](#)" 17 June 2011.
- World Bulletin. "[ISIL Affiliates from Pakistan Attack Military Checkpoint, No Casualties Reported.](#)" 13 September 2015.
- Wilhelm, Thomas P. "Understanding Pakistan's Military Perspective in the AF-Pak Border Region." September 2015.

Notes

- ¹ Robert D. Lamb and Mariam Mufti. "[Religion and Militancy in Pakistan and Afghanistan.](#)" Center for Strategic and International Studies (CSIS). June 2012.
- ² Strategy Page. "[India-Pakistan: ISIL Comes To Stay.](#)" September 2014.
- ³ Josh Hammer. "[The Age of the Fidayeen: Terror's New Tactic.](#)" Foreign Policy Association. 1 December 2008.

TRADOC G-2 ACE Threats US Army TRADOC G-2 Operational Environment Enterprise
Combating Terrorism (CbT) Poster No. 01-16

Remain Vigilant—Antiterrorism Awareness

STAY PROTECTED WHILE CONNECTED

We are Combating TERRORISM

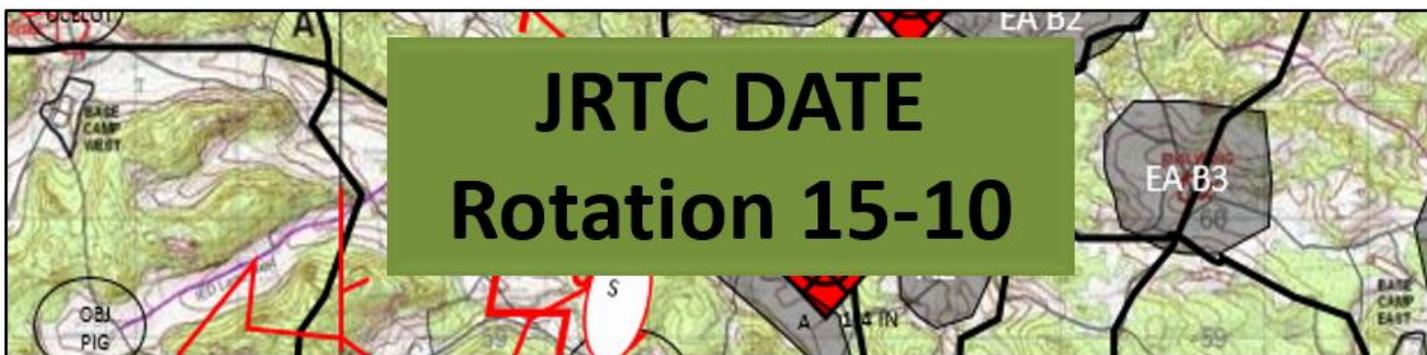
Know the CYBER Threats

People—Processes—Procedures—Protection

For more on Threats and Opposing Forces for Training
Go to <https://atn.army.mil/>
Click "Training for Operations"—"ACE Threats Integration OE Page"
and
"DA Training Environment"—"OPFOR and Hybrid Threat Doctrine"

U.S. ARMY
ATN
Army Training Network

(Photo: US Army Cyber Command)



by [Mike Spight](#), TRADOC G-2 ACE Threats Integration (CGI Ctr)

DATE Rotation 15-10 was conducted at the Joint Readiness Training Center (JRTC), Ft. Polk, LA, 13 August–16 September 2015, with box dates (force-on-force) running from 25 August–11 September. The Rotational Training Unit (RTU) was 2nd Brigade Combat Team (BCT), 3rd Infantry Division. The BCT deployed with its organic three infantry battalions, one reconnaissance squadron, one artillery battalion, one engineer battalion, and one support battalion. A significant element from HQ, 3rd Infantry Division served as HICON during the rotation, and set up a division-level command post under modular tentage in the parking lot next to JRTC's Operations Group. One of the Assistant Division Commanders was present during the rotation.

As last year, this exercise was observed by a Combat Training Center (CTC) Accreditation Team composed of personnel from the G27 OE/OPFOR Program Management TRADOC DCoS G-2, TRADOC G-2 Analysis and Control Element Threats Integration (ACE-TI), and the Combined Arms Center's Combat Training Center Directorate. This accreditation focused on specific areas such as: equipping, manning, and training of the opposing force (OPFOR); replication of the operational environment (OE); replication of the PMESII-PT variables; how well the overall Decisive Action Training Environment (DATE) and Hybrid Threat (HT) are replicated and OPFOR doctrine and tactics planned and executed; and how well is the information environment replicated at the CTC and within the framework of the exercise scenario. This article's focus is on how the OPFOR executed its tactical plan for challenging the RTU commander's training objectives. Note that for this rotation, the Accreditation Team observed only the OPFOR battalion's (Bn's) operations during RTU/BLUFOR Recon/Entry Operations, the OPFOR attack, and was not present for the OPFOR Bn's defense.

As in previous DATE rotations, the OPFOR was built around JRTC's organic unit, the 1st Battalion, 509th Parachute Infantry Regiment. This unit has undergone significant changes to its Modified Table of Equipment (MTOE) and manning documents. It has been increased in strength to a degree that enabled it to stand up a Forward Support Company, and add other personnel to its Headquarters Company. In spite of this, the unit still requires significant augmentation by US Army Reserve and Army National Guard units in order to replicate an Ariania brigade tactical group (BTG). For this rotation, the OPFOR replicated the 171st BTG, consisting of five organic battalion detachments (BDETS) and an aviation detachment. The OPFOR was augmented with three US Army and/or Army National Guard infantry companies. They were also augmented by an Army National Guard artillery battery (-) and a US Army Reserve engineer company.

The RTU commander's training objectives drove refinement of the overall exercise scenario and the tactical tasks selected by the OPFOR, through the process of countertask analysis, which is specifically developed to provide the RTU with a rigorous validation of their training status. For this rotation, the RTU commander's primary focus was on conduct of movement/maneuver (including offensive and defensive operations), sustainment, protection operations, mission command, and employment of fires.

The OPFOR Bn conducted operations in three phases, designed to greatly facilitate the free play that would be significant in this rotation. During BLUFOR's conduct of Phase 1 and 2 Entry Operations (D-1–D+2), the OPFOR Bn was restricted to Threat Level 1 operations. This threat level limits OPFOR to reconnaissance/harassment/probing conducted by SAPA, SPF, or Arianian regular force reconnaissance elements (individuals or fire team-size elements). The intent during Phase 1 was to allow the RTU to bring all its forces into its initial assembly areas in a manner that allows the RTU to establish its support and C4I nodes and begin to move tactical units to their initial objectives, to start off on a relatively level playing field.

Once the RTU was established and began to conduct its own reconnaissance missions, and move to and establish defensive positions (Phase 2 through Phase 3), the OPFOR was permitted to begin Threat Level 2 operations, which included meeting engagements and limited coordinated attacks, but only with squad-size elements (10 men). Note that at this time, the OPFOR Bn began using some of its SAPA assets in a manner that replicated ISIL tactics and techniques currently used in Iraq and Syria. In doing so, the OPFOR Bn mounted some SAPA assets up in OSV MBTs, BMPs, and BRDMs which gave their other foot and technical/commercial vehicle-based SAPA elements a capability that had previously not been seen at JRTC or any other CTC to the Accreditations Team’s knowledge. During the Phase 4 (OPFOR attack on BLUFOR defensive positions, objective to seize the FLS, Dari Lam, and Marwandi Pumping Station [MPS] D+3-D+7), the OPFOR was cleared to use Threat Level 3 operations which include all of the measures in the first two levels and added in decisive operations that could incorporate OPFOR platoon-size elements, and larger. This would include Arianian regular forces, SPF, and SAPA. Figure 1 depicts the plan for the OPFOR attack, with the stated mission as follows: “171 BTG ICW SAPA, attacks to destroy CF in AO Hind to force a USF withdrawal and to facilitate Arianian seizure of key population centers, facilities and resources.” The OPFOR’s decisive objective was to attack along the northern axis and seize the FLS and city of Dari Lam which was also where the US Consulate and staff were located, along with IGO/NGO personnel as well. The OPFOR supporting operation was to attack along the southern axis and seize the MPS, which is the key piece of critical infrastructure for controlling the flow of petroleum through Atropia to the east for export. Figure 1 provides a general view of BLUFOR’s initial movement into The Box, and their objectives. It also depicts the general positions of OPFOR SAPA

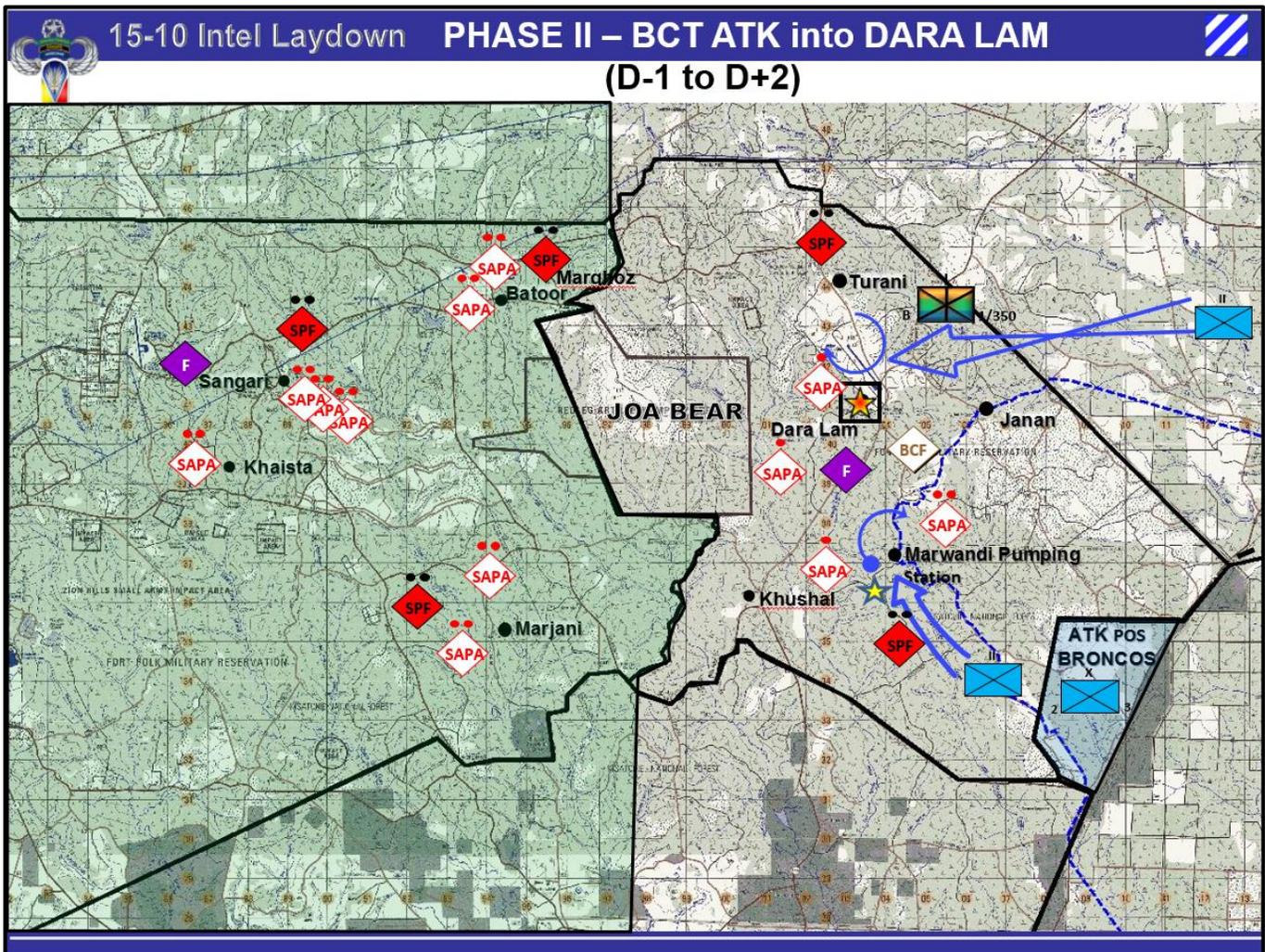


Figure 1. BLUFOR objectives and initial movement

and SPF assets, terrorist cells and a criminal organization. Note that all graphics contained in this article were provided by the Operations Group, JRTC.

Once the OPFOR attack commenced, members of the Accreditation Team were able to move about the maneuver area in admin vehicles driven by personnel assigned to JRTC Ops Grp. The Team had access to OPFOR units in their attack positions prior to initiating their attacks on the RTU on both the northern and southern axis of advance. The attack along the northern axis did stall due to heavy RTU resistance, however the attack along the southern axis pushed through and was not only able to attack the MPS, but part of that column was able to fight their way into Dari Lam and inflict significant damage to BLUFOR assets, to include BLUFOR Attack and Lift rotary wing assets on the FLS. SAPA's role early on in getting "eyes on" BLUFOR HVTs in the area around Dari Lam, to include the BCT TOC and BSA was invaluable in providing significantly greater effect to the OPFOR attack. Figure 2 depicts the general plan for the OPFOR's dispersed attack against BLUFOR's prepared defensive positions, HVT, and OPFOR's objectives.

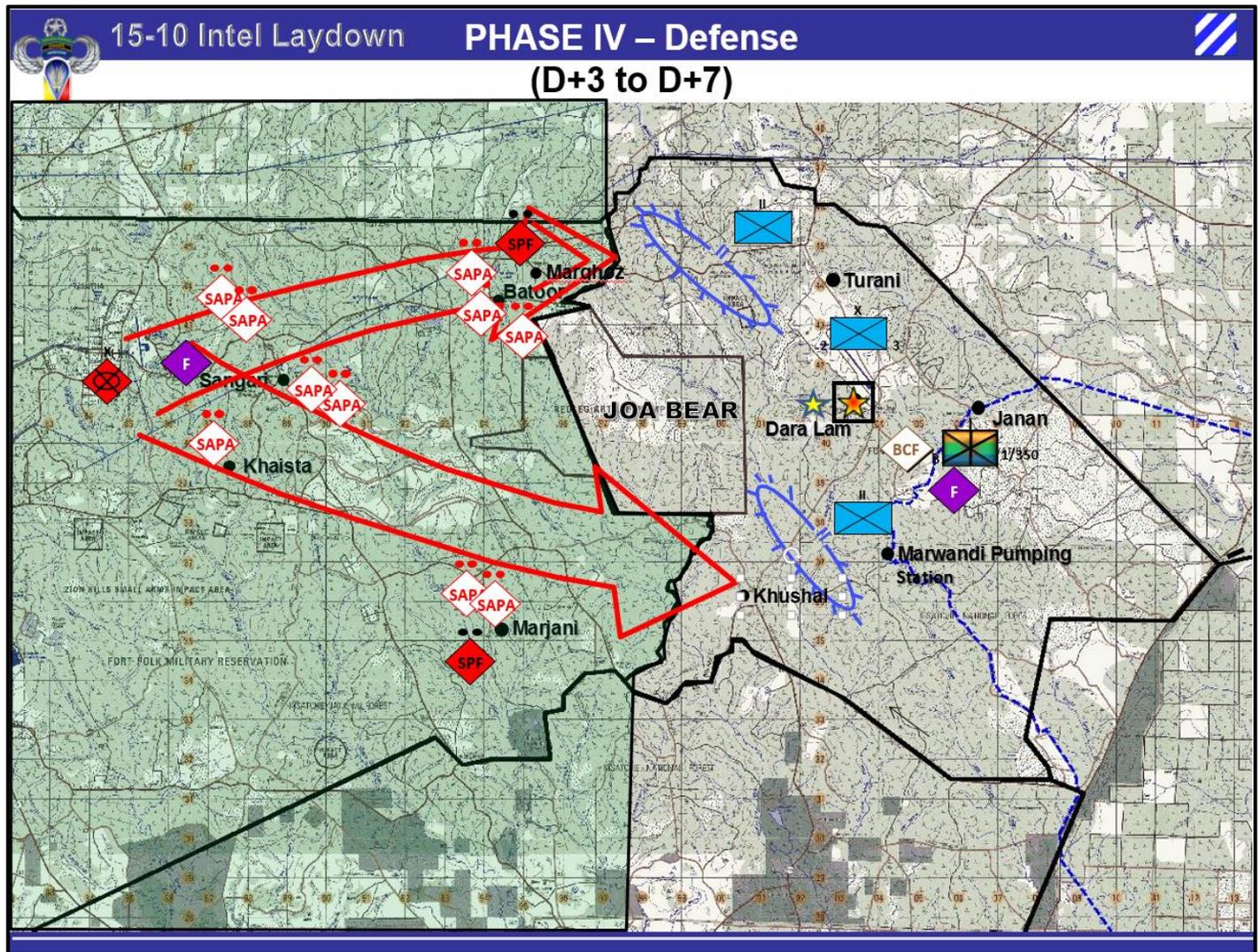


Figure 2. OPFOR's plan for dispersed attack

There was a significant number of civilians on the battlefield (role players) who provided the populations for the town sets that were used in this rotation, and who also replicated US Consulate and IGO/NGO staff personnel, media, etc. during the exercise. Their interaction with BLUFOR and the additional "friction" they provided based on the scenario as written

provided a real challenge to the BCT commander and his staff in balancing all mission requirements with the issues presented in dealing with indigenous and non-indigenous people within the operational environment (OE).

Additionally, the OPFOR were augmented by a World Class Cyber OPFOR team from 1st IO command, and they were able to penetrate BLUFOR's electronic systems and by doing so, provide the OPFOR with a significant advantage.

The OPFOR attack ended once the battle in Dari Lam had culminated, and suspension of battlefield events was declared by the Commander Operations Group. Figures 3 and 4 are pictures taken by the author in Dari Lam. Both BLUFOR and OPFOR MBTs and other vehicles destroyed in the close, urban fight are evident.

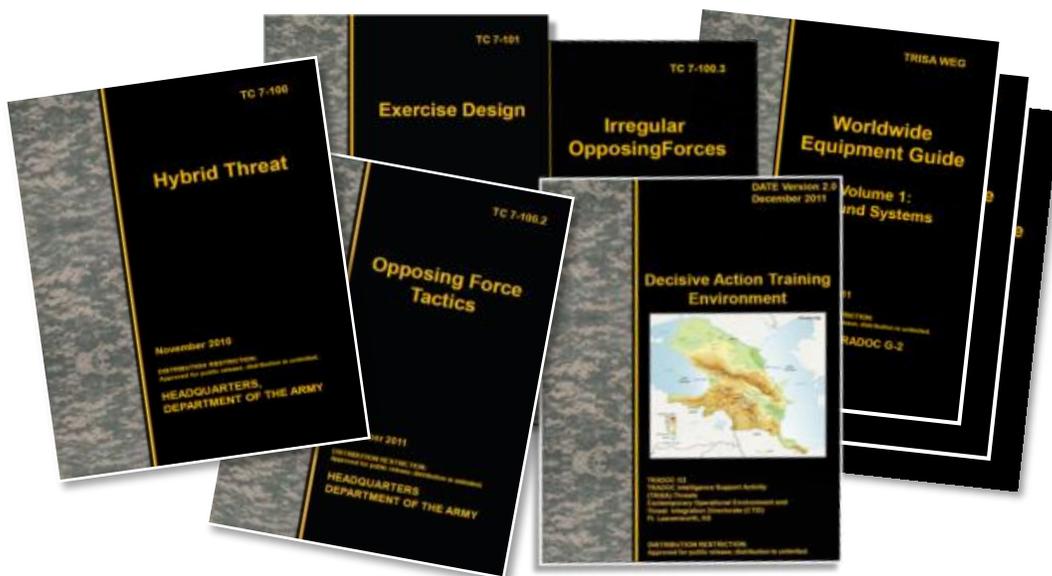


Figure 3. Dari Lam



Figure 4. Dari Lam

This DATE rotation, like all the others this author has observed over the past five years, was an excellent example of how the OPFOR, even with inferior numbers and equipment, can still subject BLUFOR to a serious challenge. As noted earlier in this article, the OPFOR's concept of equipping elements of their company replicating SAPA with OSV MBTs, BMPs, and BRDMs, and conducting ISIL like operations against BLUFOR, created a new dynamic that had not been seen previously in DATE rotations. Considering the impact that ISIL is having in the Middle East (Iraq and Syria), this is certainly an OPFOR capability that is worthy of inclusion in any DATE-based scenario developed by any CTC.



TRADOC G-2 *Worldwide Equipment Guide:* Israeli SpyLite/SkyLite Unmanned Aerial Vehicle (UAV)



by [Patrick Madden](#), TRADOC G-2 ACE Threats Integration (BMA Ctr)

The Israeli SpyLite is a tactical, man-portable, mini-UAV that is designed to be used by small army units or special operations forces (SOF). The SpyLite provides real-time reconnaissance, intelligence, surveillance, and target acquisition (RISTA) at relatively long distances, high altitudes, and in severe weather. These capabilities are possible due to its modular construction which allows quick adjustments prior to launching. Examples of these adjustments are items such as wing tips, battery, and ground control station (GCS) computer software.

Flying for over a decade, the original SpyLite was first revealed by BlueBird Aero Systems during the 2003 Paris Air Show.¹ Briefly named Skylark, the name was changed to SkyLite in 2005 under a partnership with Rafael Advanced Defense Systems in order to prevent confusion with an existing Skylark from the Israeli Elbit Systems company. As enhancements and changes were made, the SkyLite name was changed to SkyLite A, followed by SkyLite B, until BlueBird's partnership with Rafael terminated in 2008.² The SkyLite B was then renamed SpyLite by BlueBird which currently retains ownership.

SpyLite is a proven, reliable mini-UAV that is continually being upgraded and is one of the top performers in its class. As of 2013, the SpyLite had accumulated over 10,000 operational sorties.³ Seven hundred of these sorties were conducted during 24 hour operations under combat conditions as part of Israel's 2014 Operations "Brother's Keeper" and "Protective Edge."⁴ BlueBird also recently announced that its SpyLite broke the world's mini-UAV record for accomplishing the longest successful communication range before returning to its landing site.⁵ BlueBird's primary customer is the Israeli Defense Force (IDF) but it also successfully marketed the SpyLite to several other countries.

Characteristics and System Capabilities

The SpyLite and earlier models are tube shaped with the sensor payload located in the front and a two-bladed electronic engine in the back. The original SkyLite UAVs were shoulder or vehicle launched from a canister with foldable wings and an embedded parachute/airbag landing method. This was later changed to the SkyLite B model which was launched with a portable catapult but retained the original landing method. The landing method was also a significant contributor to the advertised low cost lifecycle since the same UAV can be reused.

The previous and current system components can be carried in two backpacks consisting of a launcher, two to three air vehicles, a laptop GCS, and a ground data terminal (GDT). The current SpyLite system contains an upgraded GCS that is smaller, easier to use, and runs on external electronic sources of power. Also available is a remote video terminal (RVT) that provides real-time video links overlaid on a digital map. The intended users remain tactical or SOF units that are the consumers of the RISTA requested information. It is important to note that a trained unit can operate the entire SpyLite system without external assistance. Autonomous launching, flight, and landing capabilities also significantly decreases the complexity of operating this reusable system.

Key specifications also changed and improved significantly over time. Performance features such as 66 minutes of maximum flight endurance with the SkyLite A increased to four hours with the SpyLite.⁶ Maximum range also increased from 20 kilometers (km) and a maximum flight altitude of 984 feet (ft), to 50 km and a maximum flight altitude of 36,000 ft.⁷ Perhaps the most significant change, mentioned earlier, is the recent, long distance communication range record

between a mini-UAV and its GDT. The SpyLite successfully demonstrated the ability to loiter over a specified target for 40 minutes and transmit 120 km back to the GDT.⁸ This range is normally the capability of much larger UAVs that are not man-portable.

The most important capability of RISTA-based UAVs are their sensor payloads. Without quality sensors all the advanced features mentioned above are somewhat meaningless. The challenge for mini-UAVs is the weight and size of sensors which affect all the capabilities discussed in the previous paragraph. The advancements in micro-electronics and advancements in optics are examples of significant benefits for mini-UAVs.

The current SpyLite is capable of carrying a variety of sensor payloads. The majority of their sensors are manufactured by the Israeli Controp Precision Technologies company. They produce a variety of miniature sensor payloads that are slightly larger than a softball. The most impressive payload is their multi-sensor called M-STAMP. The M-STAMP is a gimballed, gyro-stabilized, triple sensor that provides a daylight color, charge coupled device (CCD) camera with a 10x continuous zoom lens, an infrared (IR) camera with a dual field of view lens, with continuous zoom, and a laser pointer.⁹ Geocoded, marked imagery from both the daylight and IR cameras are combined and transmitted to the GCS for exploitation which includes designated target tracking.

System Proliferation

The largest consumer of the SkyLite/SpyLite continues to be the Israeli Army and Air Force. Use in combat dates back to the 2006 Israeli/Lebanon conflict with Hezbollah.¹⁰ However, during the time that Rafael and BlueBird worked together, their ability to proliferate to foreign countries was not effective despite successful flight demonstrations. Nevertheless, when BlueBird resumed control, foreign proliferation increased. In April 2011, BlueBird was successful in selling its SpyLite to the Ethiopian Army and creating a sustainment compound in Addis Ababa.¹¹ In early 2013 it was revealed that BlueBird was continuing to market its UAV in Africa and again sold to an undisclosed country.¹² BlueBird's most recent sale abroad in 2013 was a competitive win to provide six SpyLites to the Chilean Army.¹³ The results of this recent, successful proliferation provides evidence that BlueBird is marketing world-wide and demonstrating that its SpyLite is competitive in performance and price.

Training and Sustainment Implications

The SpyLite is designed to be lightweight, self-sufficient, and autonomous from launch to landing. The SpyLite is also reusable within a few minutes of landing and operates on rechargeable batteries. The entire system can be carried and operated by two people. Ruggedized GCS laptop software and M-STAMP sensor downlinks also provide real-time, automated targeting, digital video tracking, and battle damage assessment capabilities. Flight operations can also be simplified by setting predesignated weigh-points for a specified flight. All these autonomous and automated features reduce the amount of time required for training and simplify the complexity of operator requirements. The fact that only two personnel are required to carry, launch, operate, and recover the SpyLite also reduces the hours of training compared to larger, more complicated UAVs. Sustainment is also minimized with the ruggedized, reusable design and battery-powered propulsion of the SpyLite system.

Threat Doctrine Manifestations

The primary opposing force (OPFOR) user of SpyLite is the World Class OPFOR (WCOPFOR) from the Mission Command Training Program (MCTP). The SpyLite is used by WCOPFOR special-purpose forces (SPF) in support of their operational strategic command (OSC) during training exercises. The units responsible for operating the SpyLite, listed as [SkyLite B](#), are the SPF UAV Teams located in the Deep Attack and Reconnaissance Platoon, as well as each company of an SPF battalion.¹⁴ The UAV teams and SpyLites are operated and flown competitively in MCTP's Warrior Simulation (WARSIM).

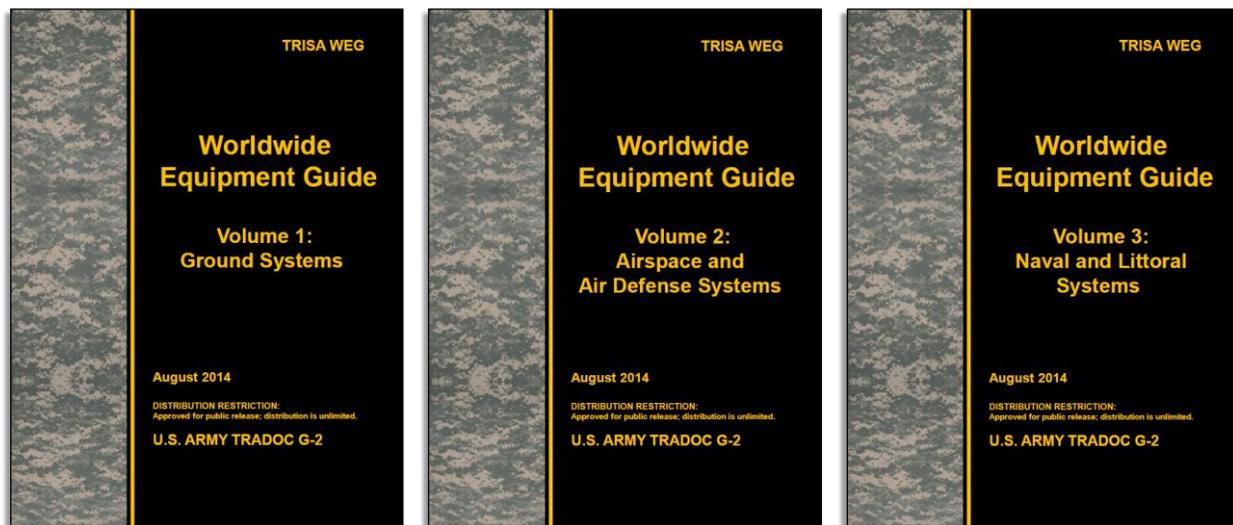
Unique to SPF is that there are no set tactics or techniques.¹⁵ The SPF operates as small teams and uses any method that is necessary for mission accomplishment. That said, the key mission of the UAV team is to provide reconnaissance. SPF UAV teams typically break down into smaller teams and operate deep in enemy-held terrain. They can supplement other SPF teams, operate independently, or support affiliated insurgents or guerrillas in order provide necessary long-range reconnaissance. Other SPF missions the UAV teams can support are direct action, raids, and target acquisition of

key weapon systems, such as Patriot missiles and long-range artillery. Given these mission requirements the man-portable, autonomous, reusable SpyLite provides ideal capabilities for WCOPIFOR mission accomplishment.

NOTE. See corresponding WEG sheet on p 40.

Notes

- ¹ Military Periscope. "[Skylite Miniature Unmanned Vehicle.](#)" 1 December 2013.
- ² Janes Martin Streetly. "IHS Jane's All The World's Aircraft: Unmanned 2013-2014." Slough: IHS Global Limited. 2013. p 83.
- ³ BlueBird Aero Systems News. "[BlueBird SpyLite in Protective Edge.](#)" 19 October 2013.
- ⁴ Bluebird Aero Systems News. "[BlueBird SpyLite in Protective Edge.](#)" 19 October 2013.
- ⁵ Unmanned Systems Technology. "[BlueBird's SpyLite Mini UAV Sets Communication Range Record.](#)" 2 April 2015.
- ⁶ Deagel. "[SkyLite A.](#)" 1 January 2015; Ian Kemp. "Unmanned Air Vehicles," Shephard Unmanned Vehicles Handbook 2010. Slough: The Shephard Press. December 2009. p 34.
- ⁷ Israeli Weapons. "[Skylite.](#)" Undated; Ian Kemp. "Unmanned Air Vehicles." Shephard Unmanned Vehicles Handbook 2010. Slough: The Shephard Press. December 2009. p 34.
- ⁸ Unmanned Systems Technology. "[BlueBird's SpyLite Mini UAV Sets Communication Range Record.](#)" 2 April 2015.
- ⁹ Airforce Technology. "[Spylite Mini UAV System.](#)" Undated.
- ¹⁰ BlueBird Aero Systems News. "[BlueBird SpyLite in Protective Edge.](#)" 19 October 2013.
- ¹¹ BlueBird Aero Systems News. "[Africa; Undisclosed Client Orders BlueBird Spylite UAV.](#)" 13 January 2013; Airforce Technology. "[Spylite Mini UAV System.](#)" Undated.
- ¹² BlueBird Aero Systems News. "[Africa; Undisclosed Client Orders BlueBird Spylite UAV.](#)" 13 January 2013.
- ¹³ Defense Industry Daily. "[Chile Orders SpyLite Mini-UAVs.](#)" 9 April 2013; Airforce Technology. "[Spylite Mini UAV System.](#)" Undated.
- ¹⁴ Army Training Network. "[https://atn.army.mil/dsp_template.aspx?dplD=318.](https://atn.army.mil/dsp_template.aspx?dplD=318)" (Note: format/Skylark undecided).
- ¹⁵ Headquarters, Department of the Army. "[Training Circular 7-100.2, Opposing Force Tactics.](#)" TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. January 2014. pp 15-18.



ACE Threats Integration products are all available on the [Army Training Network](#), as is the information presented in the Threat Tactics Course. Please visit the TRADOC G-2 ACE Threats Integration page on ATN at https://atn.army.mil/dsp_template.aspx?dplD=377.

ISRAELI MINI-UNMANNED AERIAL VEHICLE SPYLITE/SKYLITE



SYSTEM	SPECIFICATIONS	SPECIFICATIONS CONT.	VARIANTS
<p>Designation: The current variant described is a SpyLite.</p> <p>Original Date of Introduction: 2003</p> <p>Proliferation: contracts for at least 4 countries.</p> <p>Description: (SpyLite)</p> <p>Engines: Electric engine</p> <p>Power Plant: Battery-powered with rechargeable lithium-polymer batteries</p> <p>Propulsion: 2-blade pusher propeller</p> <p>Weight (kg): Takeoff: 6.3-8.0</p> <p>Max Payload (kg): 1.3</p> <p>Total System (kg): 39</p> <p>Cruise Speed (km/h): 70-100</p> <p>Max Altitude (ft): 36,000</p> <p>Service Ceiling (m): 3,000</p> <p>Endurance (hr): 4.0</p> <p>Range (km): 50</p> <p>Composition: 2-3 UAVs, catapult launcher, payload, and mission/data control terminal. Optional remote video terminal.</p>	<p>Dimensions (cm):</p> <p>Wing Span: 240</p> <p>Length (fuselage): 110</p> <p>Body Width: 25</p> <p>Deployment:</p> <p>Crew: 2-3 dismounted. Can be vehicle carried and crewed as an alternate duty.</p> <p>Carry: Two backpacks, one pack for 2 UAVs and the other pack for laptop, catapult, and support equipment.</p> <p>Launch Method: 4-kg catapult launch.</p> <p>Recovery Method: Combined parachute and inflatable bag with 30 meter accuracy. The battery, parachute, and bag are replaced prior to reuse (replacement time prior to re-launch: approximately 15 minutes).</p>	<p>Survivability/Countermeasures:</p> <p>Lightweight, composite structure. Small profile with low radar signature and very quiet engine. Excellent flight dynamics for use in all climates and severe weather, with winds of up to 35 knots, and gusts of up to 55.</p> <p>Multi-Sensor Payload Type:</p> <p>Combined, triple axis, gimbaled, gyro-stabilized sensor. Single sensor provides day/night optical zoom lens with auto-tracker, Infrared dual field of lens with auto zoom, and laser pointer.</p> <p>Flight Control System:</p> <p>Ground Control Station (GCS) and ground data terminal using a ruggedized laptop computer with encrypted, digital, real-time downlink. Continuous telemetry transmission with GPS navigation.</p>	<p>SkyLite A: Briefly called Skylark, the SkyLite A was a vehicle or shoulder canister launched UAV for use in tactical units.</p> <p>SkyLite B: variant upgrade has improved cameras, larger wing, longer endurance, and 1.5-kg added weight. Launched by catapult.</p>
			NOTES
			<p>The current SpyLite continues to be successfully marketed globally. The mini-SpyLite set a 2015 record in its class for communicating 120 km between the UAV and its ground data terminal.</p>

Find the Threats and Opposing Force Products on ATN

ATN Army Training Network
Training Solutions to Stay Army Strong

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

2 Click! → Training for Operations

Click! 3 → ACE-Threats Integration Operational Environment Page

Products that describe the PMESII-PT variable conditions of operational environment, threat actors, and threat tactics and techniques for soldiers and trainers to prepare for deployment in a decisive action engagement.

Check this out too! → OPFOR & Hybrid Threat Doctrine

Find TC 7-100 series on Opposing Forces on APD

APD ARMY PUBLISHING DIRECTORATE
<http://www.apd.army.mil/>

Home | About Us | Publications | Forms | Printing | Order Pubs/Forms | Tools | Search

Administrative
Technical and Equipment
Doctrine and Training

TC-Training Circular

TC 7-100	11/26/2010	HYBRID THREAT
TC 7-100.2	12/09/2011	OPPOSING FORCE TACTICS
TC 7-100.3	01/17/2014	IRREGULAR OPPOSING FORCES
TC 7-100.4	06/04/2015	THREAT FORCE STRUCTURE ORGANIZATION GUIDE
TC 7-101	11/26/2010	EXERCISE DESIGN
TC 7-102	11/26/2014	OPERATION ENVIRONMENT AND ARMY LEARNING

What ACE Threats Integration Supports for YOUR Readiness

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

ACE Threats Integration POCs

DIR, ACE Threats Integration jon.s.cleaves.civ@mail.mil	Jon Cleaves 913.684.7975
Dep Director DSN:552 jennifer.v.dunn.civ@mail.mil	DAC Jennifer Dunn 684.7962
Operations-Analyst jon.h.moilanen.ctr@mail.mil	Dr. Jon Moilanen IDSI 684.7928
Product Integration-Analyst angela.m.wilkins7.ctr@mail.mil	Angela Wilkins IDSI 684.7929
Intelligence Specialist walter.l.williams112.civ@mail.mil	DAC Walt Williams 684.7923
Intelligence Specialist (Vacant)	DAC 684.7920
Intelligence Specialist jerry.i.england.civ@mail.mil	DAC Jerry England 684.7934
Intel Specialist-NTC LNO kristin.d.lechowicz.civ@mail.mil	DAC Kris Lechowicz 684.7922
Senior Threats Officer (Military-Vacant)	684.7907
Threat Tactics nickolas.m.zappone.mil@mail.mil	CPT Nikolas Zappone 684.7939
(UK) LNO matthew.j.tucker28.fm@mail.mil	Warrant Officer Matt Tucker 684-7994
Military Analyst richard.b.burns4.ctr@mail.mil	Rick Burns BMA 684.7897
WEG & Military Analyst john.m.cantin.ctr@mail.mil	John Cantin BMA 684.7952
DATE & Military Analyst laura.m.deatruck.ctr@mail.mil	Laura Deatruck CGI 684.7925
LNO to MCTP-Analyst patrick.m.madden16.ctr@mail.mil	BMA Pat Madden 684.7997
Military Analyst henry.d.pendleton.ctr@mail.mil	H. David Pendleton CGI 684.7946
LNO to JMRC & JRTC-Analyst michael.g.spight.ctr@mail.mil	Mike Spight CGI 684.7974
Intel Specialist-Analyst (Vacant)	(TBD)
Intel Specialist-Analyst (Vacant)	(TBD)
Intel Specialist-Analyst (Vacant)	(TBD)