Red Diamond
Threats Newsletter

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

Fort Leavenworth, KS **Volume 8, Issue 05** **May 2017**

INSIDE THIS ISSUE

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

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

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

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

by Angela M. Williams, TRADOC G-2 ACE Threats Integration (DAC)

TRADOC G-2 ACE Threats Integration has completed the most recent update to the Decisive Action Training Environment (DATE) and it will soon be available on the Army Training Network (ATN) at https://atn.army.mil/dsp_template.aspx?dpID=588. As with the last update, an errata sheet will be posted alongside this newest version so that users can track the changes and apply them to their respective training documents. Additionally, changes within the document itself are highlighted with green, italicized text.

Users will see substantive changes in the addition of two new irregular threat actors modeled after violent extremist organizations (VEOs) and a new criminal threat actor with significant information warfare (INFOWAR) capabilities. The VEO-type actors are called One Right Path and The True Believers and the INFOWAR-strong criminal group is named Saints of Cognitio.

All mentions of Kalaria and other regional, real-world countries have been removed, and Donovia has been expanded. Previously, the descriptions of the Donovian physical environment were limited to the part of Donovia that lies in the Caucasus region, but the latest version of DATE expands the physical environment information for the entire country. More details about the additions to Donovia are provided in a March 2017 *Red Diamond* article: "Donovia: Expanding the (Physical) Environment."

The majority of the changes made are driven by the needs of the DATE users, and your feedback is always welcome. TRADOC G-2 analysts at ACE Threats Integration and at the OE Training Support Center are available to support trainers and exercise designers at Centers, Schools, and Home Station with their implementation of the changes in DATE 3.0.

RED DIAMOND TOPICS OF INTEREST

by TRADOC G-2 ACE Threats Integration

This May 2017 *Red Diamond* newsletter leads with recent Russian actions in the Arctic region as an article "Russian Designs of the 80th Separate Motorized Rifle Brigade for Operations in the Artic." The Arctic Ocean region is becoming a potential source of conflict. With the impending ice melts that open up shipping lanes and potential resources, there is a new interest in this barren region. There are five countries with claims in the Arctic Ocean: Russia, United States, Canada, Norway, and Denmark. These five countries' claims have all been based on the UN Convention Law of the Sea (UNCLOS), with the exception of the United States which has not ratified this treaty.

"Threat Tactical Vignette: Delay and Linkup" is the sixth and concluding article in this Red Diamond tactical series at platoon echelon for mission tasks of delay and linkup. Focusing on reconnaissance and counter-reconnaissance as economy of force actions, the vignette mission provides early warning and a degree of protection to the force main body. As the current tactical situation evolves in the independent reconnaissance patrol's zone, actions to delay and linkup challenge the platoon leader and senior sergeant to accomplish the mission and intent while not becoming decisively engaged by the enemy.

The article, "Trends in Attacks against Police and Military in Northwest India 2013–2016," provides a background for situational awareness, and a regional overview of the various threat actors that have impacted the India Administered Kashmir (IAK) in northwestern India operational environment over the past four years. Highlights include some of the major incidents perpetrated by militants during the same timeframe.

"Anti-tank Guided Missile Raid" is the first article of a two-part article series that describes actual incidents that can guide Opposing Force (OPFOR) tactical tasks of raid and ambush. Observations from an anti-tank guided missile (ATGM) video in the ongoing conflict between Yemeni rebels and Saudi Arabian forces provide insight on successful use of ATGMs in these mission tasks. The video footage was reportedly captured near the two countries' borders in the vicinity of Najran province. This article focuses on the tactical actions of an ATGM raid. A subsequent article will emphasize the follow-on ambush to the raid as a planned tactical action.

The present civil war in Syria is the article setting to present the *Sarab* (Arabic for Mirage) family of active protective systems (APSs) against anti-tank guided missiles (ATGMs). Free Syrian Army (FSA) rebels initially had access to only a limited number of ATGMs with most appropriated from the inventories of Bashar al Assad's Syrian Arab Armed Forces (SAA). However, in April 2015 the rebels successfully used ATGMs to destroy about 40 SAA main battle tanks. The arrival of ever-increasing numbers of highly lethal ATGMs translated into daunting tank losses for the Syrian Arab Army. In response, the Syrian high command developed a jamming device capable of interdicting the flight paths of adversary semi-automatic command line-of-sight (SACLOS)-guided ATGMs. The eventual outcome of this effort was a family of soft-kill weapons serially fielded as the Sarab. This article assesses the evolution and fielding of the Sarab family of soft-kill weapons, the recent impact of these weapons on the Syrian operational environment, and the potential implications of soft-kill weapons in future OEs.

RUSSIA DESIGNS THE 80TH SEPARATE MOTORIZED RIFLE BRIGADE FOR OPERATIONS IN THE ARCTIC

by LTC Bryce Frederickson, TRADOC G-2 ACE Threats Integration

The Arctic Ocean region is becoming a potential source of conflict. With the impending ice melts that open up shipping lanes and potential resources, there is a new interest in this barren region. There are five countries with claims in the Arctic Ocean: Russia, United States, Canada, Norway, and Denmark. These five countries' claims have all been based off the UN Convention Law of the Sea (UNCLOS), with the exception of the United States which has not ratified the treaty. The importance for this reason grows with the release of new data and research in the Arctic. The US estimates that about 15% of the world's remaining oil, up to 30% of its natural gas deposits, and about 20% of its liquefied natural gas are stored in the Arctic seabed.[1] As the Arctic warms, Russia is positioning itself to become the dominant player in a resource-rich and strategically positioned region.[2] Russia's will consider the positioning of its forces and developing new force structures to accomplish its goals and objectives.

A potential conflict in the Arctic would require specially trained forces that would be able to manage with the difficulties operating there. The majority of conventional units not trained in this environment would have a steep learning curve to overcome the natural harsh conditions, increasing the difficulties of combat. To ensure Russia remains a dominant force in the Arctic region, Russia has recently invested in a new Separate Motorized Rifle Brigade, designed for operations in the Arctic.

The Russian Northern Fleet has two Separate Motorized Brigades as its land forces. The 200th Separate Motorized Brigade has a traditional force structure and is primarily focused on protection of the Fleet's ports and airfields. The 80th Separate Motorized Rifle Brigade, which was activated in January 2015 and is based in the town of Alakurtti, can also be used for the same purpose as the 200th Brigade, but its organization, equipment, and training exercises indicate a somewhat different mission.[3] Currently, complete composition of the 80th Brigade is unknown, however there are some indications from reports that the composition of this new Brigade continues to evolve and affect how this unit will be used. It is important to note that this will

Figure 1. Arctic region

be a unique unit in the Russian Armed Forces inventory, with a mission focused on Arctic warfare.

Russia reports that a reconnaissance parachute company with the 80th Separate Motorized Rifle Brigade will be trained to fight on drift ice near the North Pole, and troops with the special operations forces have begun to learn to operate in the region too.[4] Additionally, the 80th Brigade is equipped and trained not for forced entry, but for extended independent operations far away from friendly bases on the many islands and archipelagoes of the Arctic theater of operation, such as Novaya Zemlya, Franz Josef Land, and Splitsbergen, and relies mainly on air and sea resupply.[5] The strategic mobility requirement and the need to operate in extreme conditions with limited logistical support means that the 80th Brigade is more lightly equipped than conventional motorized rifle units. It does not have a tank battalion, and its rifle battalions are mounted on *Mashina Transportnaya Legkaya* Boyevaya (MTLB) [Russian transport vehicle for combat] tracked armored personnel carrier (APCs) which have good mobility over snow and tundra.[6]

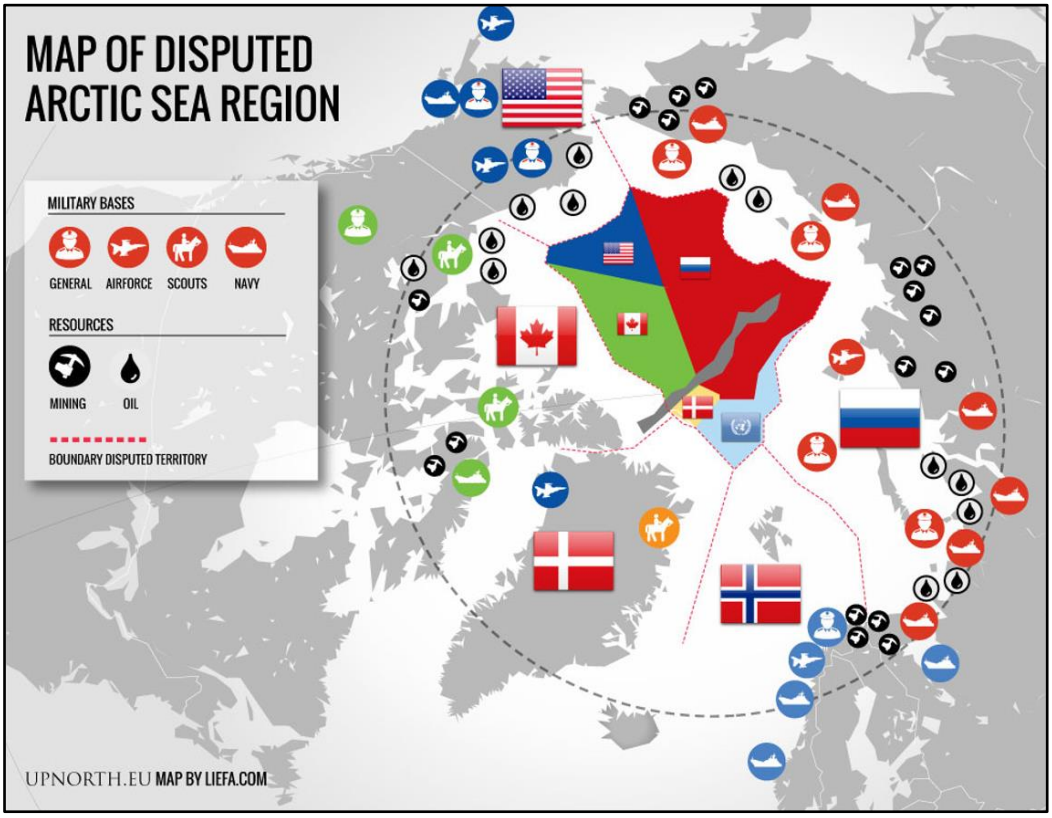


Figure 2. Arctic Council, Arctic Ocean claims

The missions that the 80th Separate Brigade could receive are as diverse as the unit itself. There are some reports it could play both a defensive role, protecting key Russian military infrastructure such as airfields and early warning radar stations against NATO special operations raids, and an offensive one by pre-empting NATO landing on any contested land areas of the Arctic.[7] This force projection role and the associated training and acquisition of exclusive arctic equipment sets this unit apart from the 200th Separate Brigade. Since the 80th Separate Brigade was activated in 2015, it has been conducting training exercises and testing new tactics and equipment for Arctic missions. Tactical operations in Arctic conditions require substantial training and preparation by any force planning for success. The harsh weather conditions to include freezing temperatures, blistering winds, and snow-blindness, along with permafrost terrain

Figure 3. 80th Separate Brigade and reindeer sled mobility

difficulties, requires military units to train and rehearse operations in those conditions to be successful. Military operations require sustainment units that can extend their lines of communication farther than typically required in temperate climates due to the lack of infrastructure.[8] In 2016, the reconnaissance element from the 80th Separate Brigade conducted training operations using snow dogs and reindeer for their movement and equipment.

The Arctic council and its members have been able to negotiate and keep the region on diplomatic terms. However, human nature and the vast resources and economic benefits on shipping lanes means the Arctic presents itself as potential point of conflict in the future. To settle disputes, look to Russia to use the 80th Separate Motor-Rifle Brigade in some capacity since it is clearly postured to project military force into this contested region.

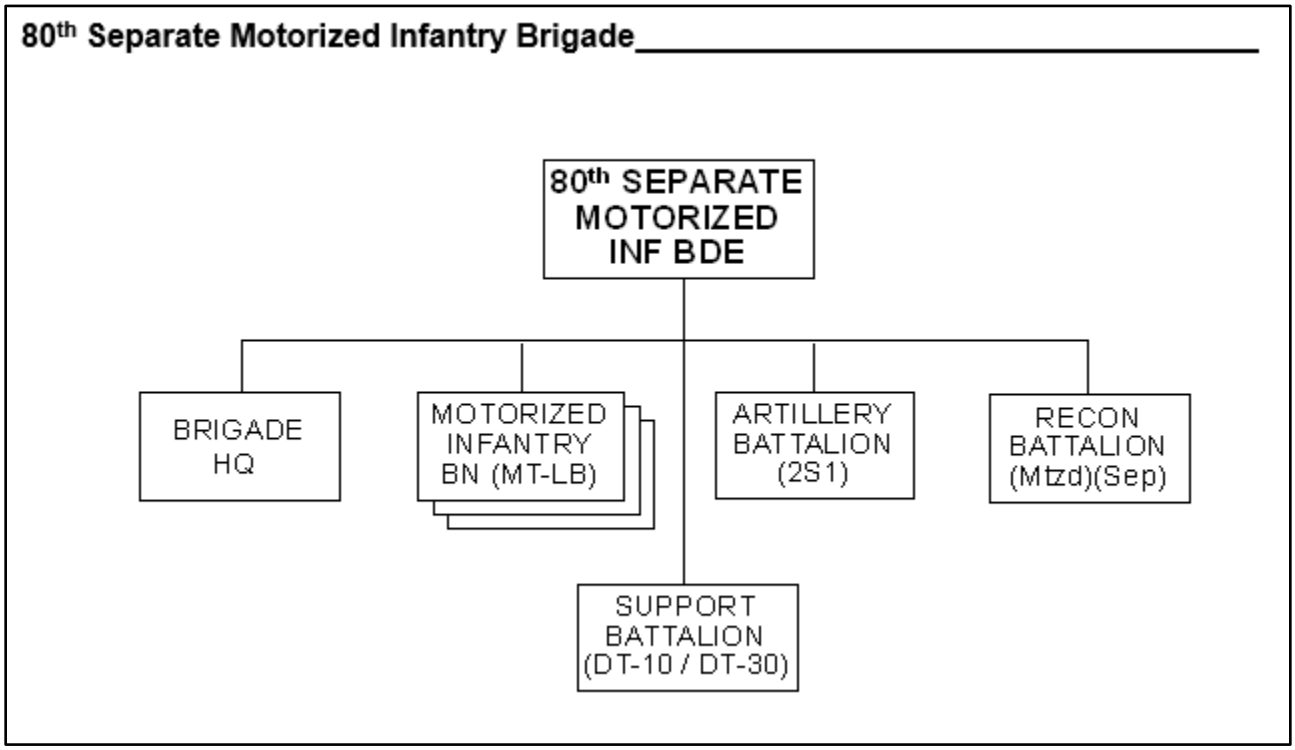


Figure 4. This estimate of the composition of the 80th Separate Motorized Brigade is based on unclassified research conducted by the analyst

Figures

Figure 1. Arctic Region from NOAA, U of Texas Arctic region 2000.
Figure 2. Map of Disputer Arctic Sea Region, UPNORTH.EU.
Figure 3. Russian Northern Fleet's Arctic mechanized infantry brigade conducts military exercises to learn how to ride reindeer and dog sleds at a reindeer farm near the Lovozero settlement. (Photo by Lev Fedoseyev\TASS via Getty Images)

Notes

[1]Jeremy Bender and Mike Nudelman."This map shows Russia's dominant militarization of the Arctic." October 2016.
[2] Jeremy Bender and Mike Nudelman."This map shows Russia's dominant militarization of the Arctic." October 2016.
[3] J. Hawk J. and South Front, "VIDEO: Russia's Northern Fleet in the Arctic. Surface Ships, Submarines, and Aircraft." February 2016.
[4] TASS Russian News Agency, "Russian Spetsnaz Continue Arctic Training." 14 July 2016.
[5] J. Hawk J. and South Front, "VIDEO: Russia's Northern Fleet in the Arctic. Surface Ships, Submarines, and Aircraft." February 2016.
[6] J. Hawk J. and South Front, "VIDEO: Russia's Northern Fleet in the Arctic. Surface Ships, Submarines, and Aircraft." February 2016.
[7] J. Hawk J. and South Front, "VIDEO: Russia's Northern Fleet in the Arctic. Surface Ships, Submarines, and Aircraft." February 2016.
[8] Justin Lynch. "America Needs to Get Serious about the Arctic." January 2017.

Threat Tactical Vignette
Delay and Linkup

by Jon H. Moilanen, TRADOC G-2 ACE Threats Integration (DAC) Part 6 of 6 in RZ-CRZ Series

This May 2017 *Red Diamond* newsletter article is the sixth and final article in this tactical vignette series. Focusing on reconnaissance and counterreconnaissance as economy of force actions, the mission provides early warning and a degree of protection to the force main body attacking to the east. As the current tactical situation develops in the reconnaissance patrol zone, actions to *delay* and *linkup* challenge the platoon to accomplish its mission intent and not become decisively engaged by the enemy.

Recent Tactical Actions

From previous *Red Diamond* newsletter articles-vignettes, the rapid advance of the encirclement operation continues deep into the enemy's rear zone to linkup and close the encirclement along the KRONATZ river line.[1] Threat mechanized and motorized forces of operational strategic commands (OSCs) crossed the international border days ago in preemptive integrated attacks and quickly exploited gaps in the enemy defenses. Division tactical groups (DTGs) and brigade tactical groups (BTGs) are maneuvering to linkup and close the encirclement.

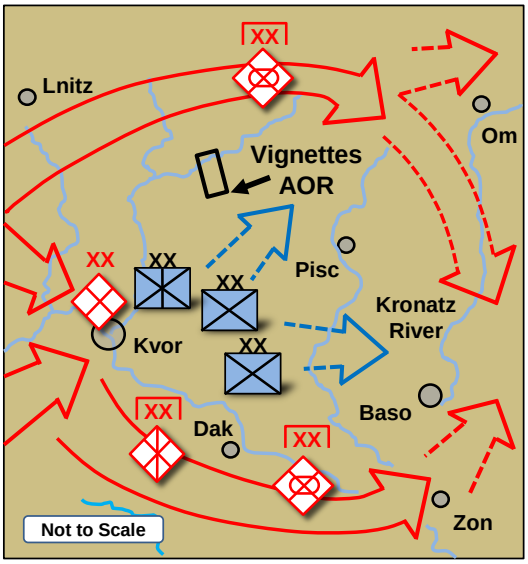


Figure 1. Situational overview

One divisional reconnaissance company with a flank screen mission has intermittent contact with its platoons across a wide reconnaissance zone. The reconnaissance platoon in this tactical vignette, task-organized as an *independent reconnaissance patrol* (IRP), continues its mission tasks of reconnaissance and counterreconnaissance after contact with enemy elements.[2]

Soon after the conclusion of this mission, the platoon leader recalled his initial positioning of elements at or near the village of BEJUNIK. The platoon had crossed its line of departure north of the RADO River, and seized a small bridge over MIN River in a brief firefight at BEJUNIK, but only after enemy militia destroyed the main bridge.

- One scout squad remains on the north bank at the destroyed western bridge. Scouts occupy an observation post (OP) on the south bank.
- The senior sergeant (SS) conducts reconnaissance south of the river to predicted enemy location (PEL) 23 and 25.

Figure 2. Sketch of IRP tactical dispositions and pending actions

- The platoon leader (PL) conducts route reconnaissance along the roadway from the bridge at BEJUNIK toward KOLTE (PEL 27). PEL 26 is the initial objective task focus.
- The combat engineer squad secures the eastern bridge site and is ready to assist the scout squad at the destroyed bridge or respond to the scout section maneuvering south toward PELs 26–27.
- The mortar section remains in position at BEJUNIK ready to assist the platoon with on-call indirect fires.

The platoon leader and scout section maneuvered south of the MIN River, and move cautiously toward their reconnaissance objectives. The senior sergeant conducting reconnaissance south of the MIN River along the western road engaged and destroyed an enemy armored carrier near PEL 23, and suppressed dismounted soldiers with machinegun fire as they attempted to flank his position. The platoon leader directed that the senior sergeant delay into BEJUNIK, adjust defensive fighting positions of the scouts and engineers, and confirm preparation for the subsequent mortar firing positions.

The platoon leader continued south to PEL 26 and observed lead enemy dismounted and mounted elements emerging from KOLTE near Hill 21. A successful ambush and raid temporarily disrupted enemy dismounted maneuver to the north. The more significant patrol loss was destruction of one BTR on Hill 21 from enemy indirect fire. No BTR crew members of the squad survived. Advancing dismounted and mounted enemy caused the platoon leader to delay north toward the operational bridge at BEJUNIK.

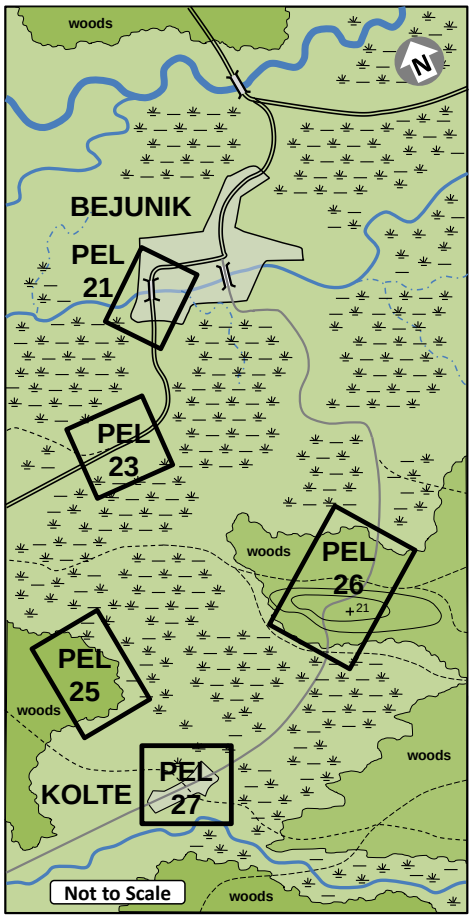


Figure 3. Sketch of IRP PELs

Note. For threat forces presented in the US Army's Training Circular (TC) 7-100 series, an essential component of every military action is reconnaissance. Reconnaissance represents all measures associated with organizing, collecting, and studying an operational environment (OE) in a tactical mission.[3] Even though reconnaissance is often associated with stealth and situational awareness, practical analysis of reconnaissance actions indicates that ground maneuver elements will typically also fight for information in order to obtain relevant intelligence.

Current Tactical Situation

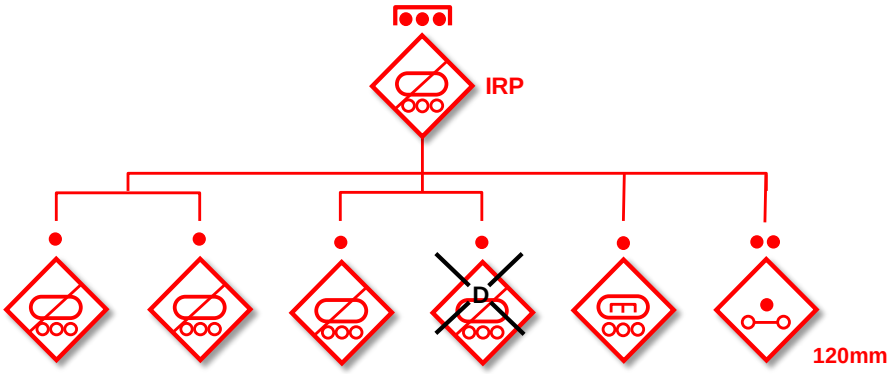


Figure 4. Platoon task-organized independent reconnaissance patrol (current situation)

The scout squad leader near the western ford site supervises emplacement of antipersonnel mines on the northern river bank as the senior sergeant moves in his BTR through BEJUNIK to coordinate with the engineer squad sergeant defending

the useable bridge site.[4] 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 to his rear appears as a vague gray and white mist as his mortar section fires smoke rounds to obscure enemy observation from this high ground. Looking north to the bridge site ahead,

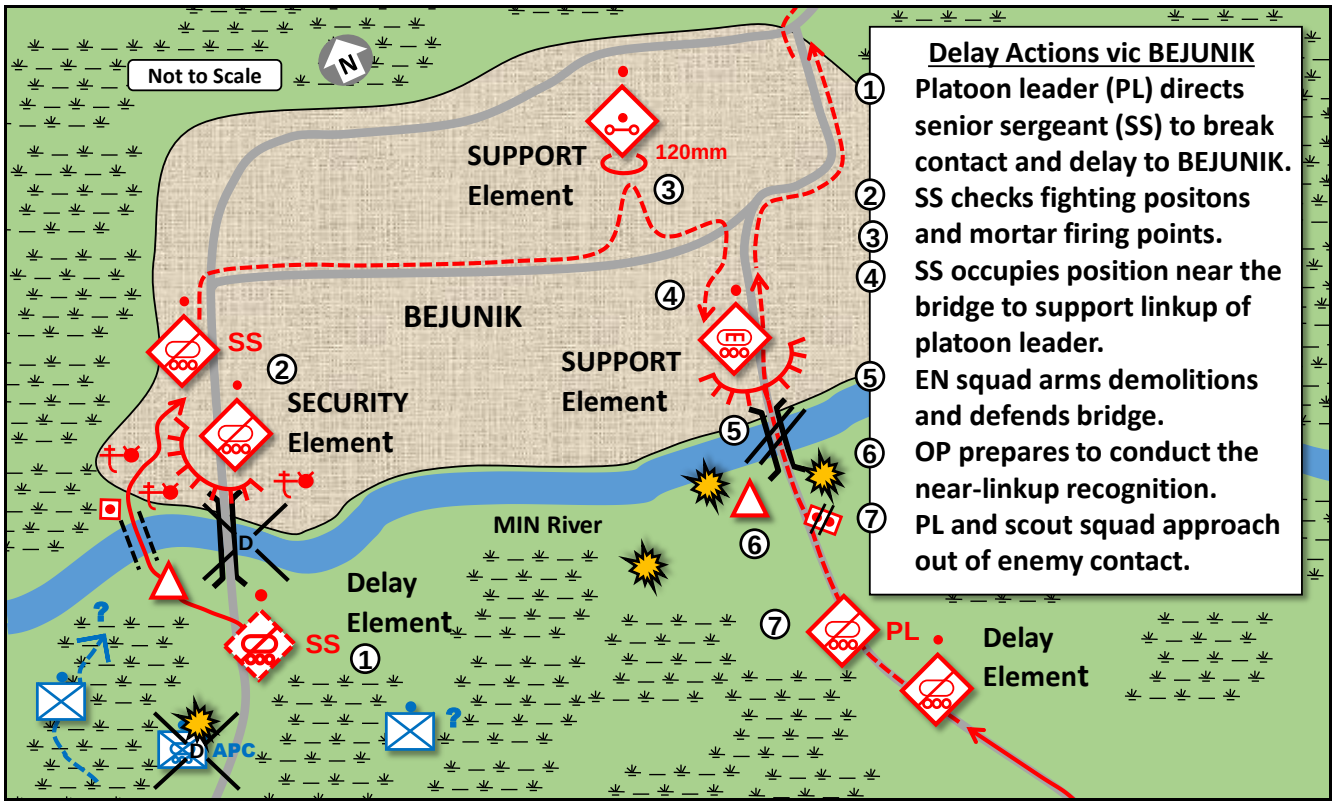


Figure 5. Reconnaissance patrol elements delay to MIN River for linkup and passage

the platoon leader almost feels relieved when suddenly bullets start ricocheting off his vehicle from the left flank.

"Contact 10 o'clock! Suppressive fire—machinegun! Keep moving! Keep moving toward the bridge." The platoon leader jerked down reflexively into the turret as bullets ricocheted off his BTR. His next action was to command "Fire Mission-HE. TRP DELTA 77." The mortar section sergeant was already preparing to shift fires to support the passage when this command echoed from the radio net. Indirect supporting fires occurred within seconds.

As the platoon leader raised his head to view the road ahead, the BTR behind his BTR was already suppressing the left flank area of tall marsh grass with machine gun fire. The BTR commander also attempted to remain alert for any approaching enemy vehicles emerging from the haze and smoke near Hill 21.

Figure 6. Senior Sergeant BTR in position near river

At this moment, the platoon senior sergeant was at the northern bank of the bridge crossing to check the demolitions that the engineer team had armed only minutes earlier. Visibility was decreasing rapidly as rain had increased from a sporadic drizzle to a sudden squall. Mortar rounds were impacting as BTR machinegun fires swept across the marshy area on the left flank.

The soldiers at the observation post south of the bridge were ready for the linkup signal from the approaching platoon vehicles. Timing would be critical to

acknowledge recognition signals and linkup in the limited visibility, and then guide the vehicles around the antitank mines buried in the dirt roadway and embankments. Knowing the normal signal flare recognition was doubtful due the heavy rain, the platoon leader alerted the OP team and senior sergeant of the alternate recognition signal as a reflective panel on his right-front deck. “Two BTRs will pass with turret cannons pointed to the east.”

The soldiers in the OP heard approaching vehicles, updated the platoon on the radio net, and came up from their fighting position with their own recognition panel as the first BTR appeared suddenly only 25 meters distant out of the gray wall of rain.

Figure 7. Observation post preparing for linkup with delay element

The platoon leader brought his BTR to a quick halt, and the second BTR almost slammed into the BTR before coming to a quick halt and orienting his BTR to the left flank and enemy fire. The BTR continued controlled suppressive fire to the left flank. By the time the trail BTR came to a halt, one soldier from the OP had mounted the front deck of the platoon leader’s BTR. He leaned against the turret as he yelled instructions to the platoon leader and pointed to mined areas to avoid.

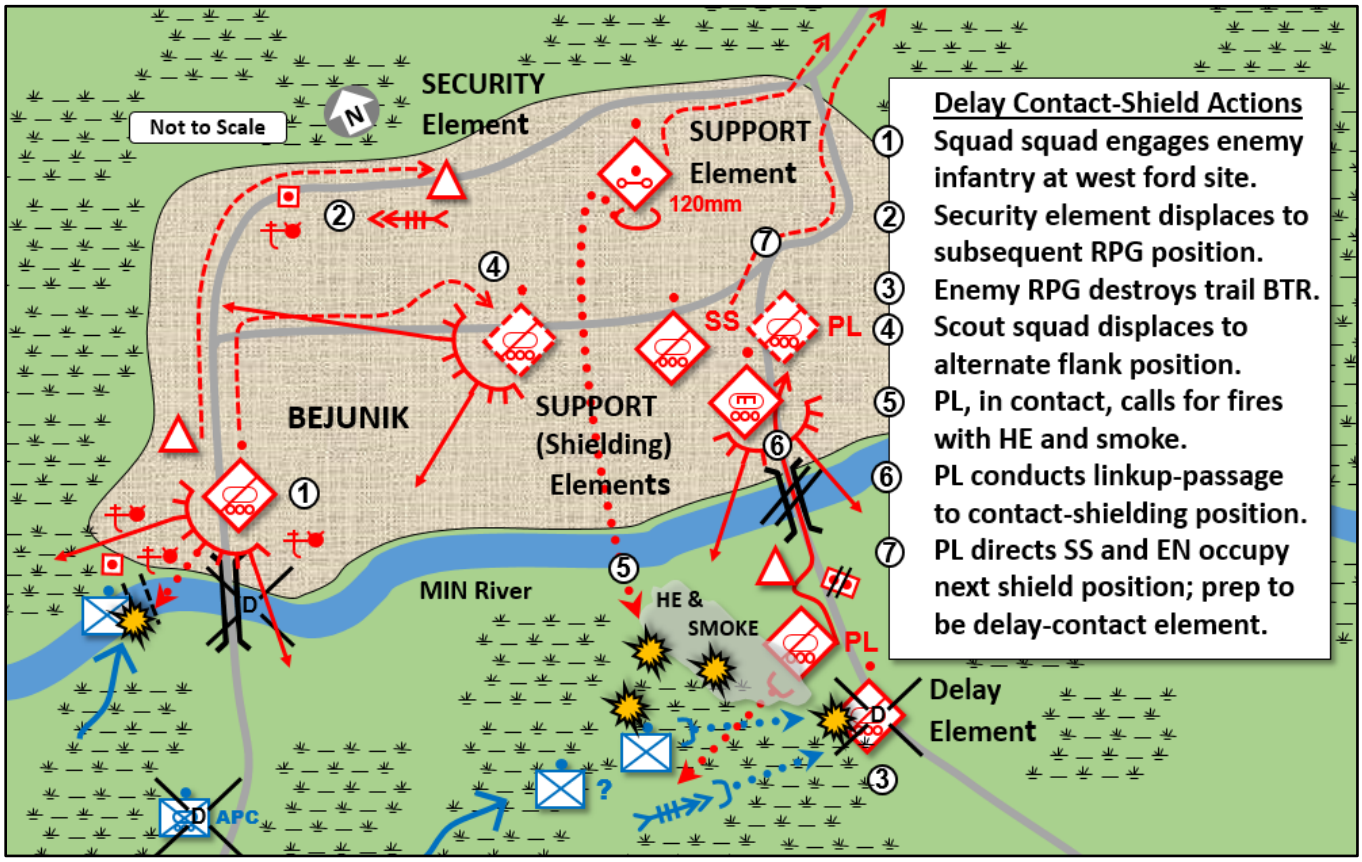


Figure 8. Reconnaissance platoon delay, linkup, and passage at BEJUNIK

The other soldier from the OP was mounting the second BTR when an explosion rocked the left front of the vehicle. “RPG!” rang over the intercom, and the crew burst out of the hatch of the BTR with two of the soldiers dragging a third soldier between them. The vehicle commander continued to fire his turret weapons until all of the crew was clear of the vehicle, and then jumped to the ground to join his crew at the lead BTR. Heavy dark smoke rose from the damaged trail vehicle. The platoon leader yelled into the radio, “One BTR destroyed. One BTR moving now to the bridge.” Mortar rounds were impacting in and near the bridge and road, but the platoon leader could not identify if they were enemy or friendly fires.

Figure 9. RPG hits scout squad BTR at linkup

The platoon leader, having crammed the survivors from the trail vehicle into his BTR, raced his BTR across the bridge and pulled into a fighting position to the flank of the senior sergeant. The security element at the western edge of BEJUNIK reported enemy soldiers were starting to wade across the river ford and were being engaged. The platoon leader directed several actions in quick order: "Western scout squad withdraw to senior sergeant's vehicle and orient west to protect that flank—mortar section displace to firing point CHARLIE just south of the RADO River bridge—senior sergeant and engineer move to subsequent fighting position to the north and cover our delay. I'll update you when I'm moving north on the road toward you."

The platoon leader shifted some of the soldiers from his BTR to the senior sergeant's vehicle and scout squad vehicle. Enemy small arms fire from side streets in the village was increasing in volume of fire, but the rainy haze prevented any effective friendly or enemy fires. "Fire mission—HE—TRP WHISKEY 21," from the platoon leader disrupted any enemy

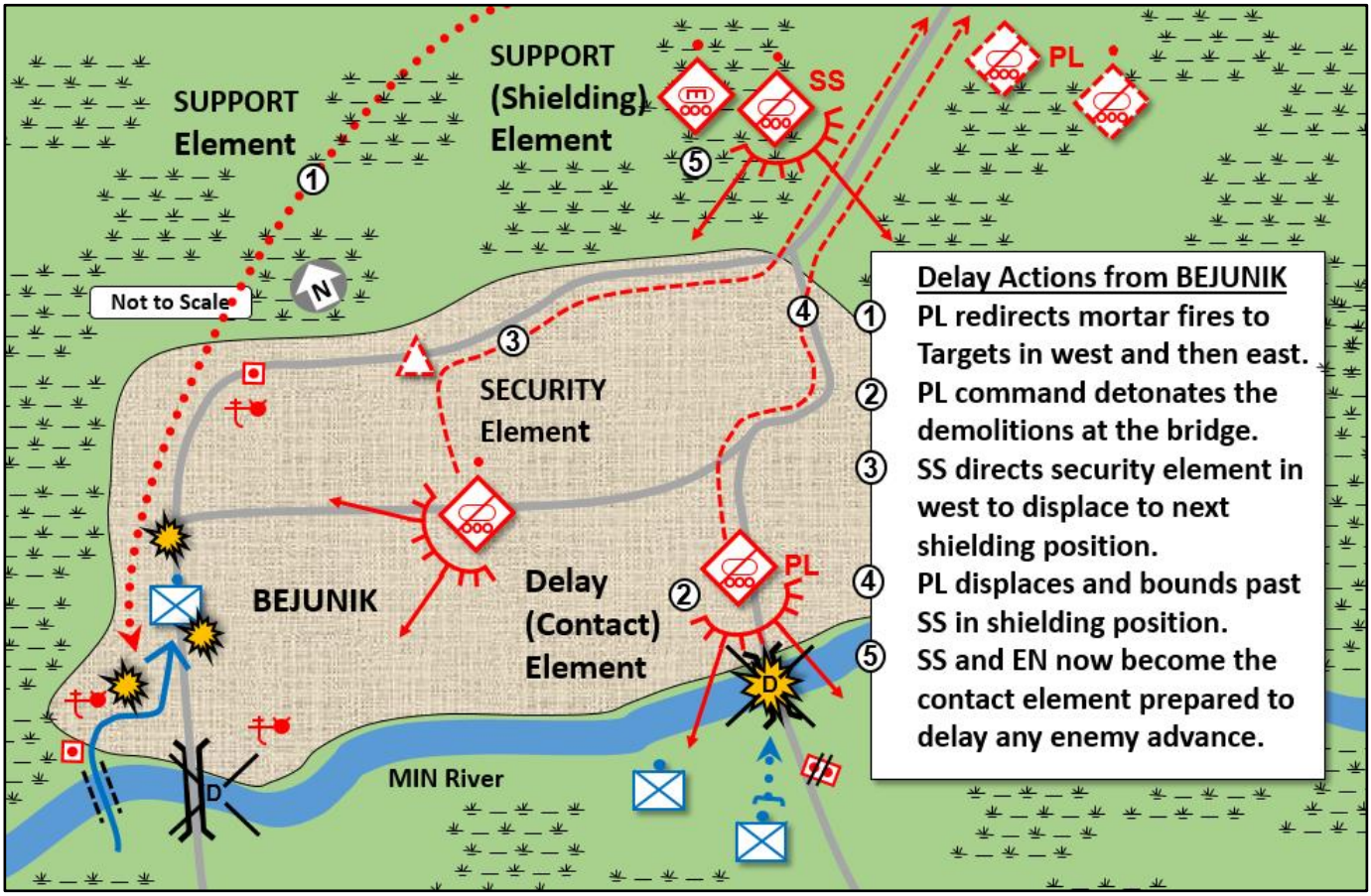


Figure 10. Reconnaissance patrol conducts delay in contact element/shielding element bounds

advance through the village from the west, and allowed the senior sergeant time to move to the next fighting position to the north.

Once he could no longer hear the senior sergeant's BTR engine in the distance, the platoon leader command detonated the demolitions at the bridge. The explosion, although expected, erupted as a sudden flash and deafening noise—probably

amplified by the rainy-haze conditions. The bridge section appeared to rise briefly and then drop suddenly with a gaping hole in the destroyed road surface. The bridge structure canted at a dangerous angle. No enemy vehicle would be coming across the bridge.

Figure 11. Bridge damage

The platoon leader reversed his BTR, and with the scout squad BTR, raced out of the village past the shielding position of the senior sergeant to occupy a subsequent fighting position in order to cover the senior sergeant's next bound to the north. The mortar section shifted fires to the eastern edge of BEJUNIK. The platoon leader and senior sergeant continued to conduct alternate bounds to the north, while the mortar section adjusted its fires along the road trace, on order, to slow any enemy advancing elements.

As the reconnaissance patrol elements approached the RADO River, the platoon leader reestablished radio contact with his reconnaissance company headquarters. Significant enemy irregular element activity north of the RADO River indicated that an alternate route was required to rejoin the reconnaissance company. The platoon leader was directed to move east along the southern bank of the RADO River, and linkup with company reconnaissance elements about fifteen kilometers to the east.

Training Implications

This article highlights tactical actions of the platoon leader and senior sergeant to coordinate a linkup during a delay action and passage across the MIN River, and to continue the mission as an independent reconnaissance patrol in a much larger offensive operation and encirclement of enemy forces. In this independent reconnaissance mission:

- Limitations due to adverse weather, physical environment, and time sensitivity of enemy expected in zone complicated tactical decisions.
- Mission aspects of a higher headquarters flank screening mission depended primarily on a ground-oriented mounted reconnaissance.
- Mission updates stated a high expectation of encountering enemy reconnaissance elements, infantry, or motorized elements attempting to avoid a developing pocket that would contain enemy forces south of the RADO River.

This article demonstrates the value of leader and individual skills proficiency and effective execution of small unit tasks and drills. A tactical opportunity required a ready-response and initiative to enemy contact without becoming decisively engaged. The platoon leader adapted quickly to the changing tactical conditions during his mission. The actions of independent reconnaissance patrol (IRP) noncommissioned officers were instrumental to successful execution of the mission. Decentralized command and control (C2) demands leader initiative with prudent risk-taking and willingness to act, and indicates that leaders and soldiers require experienced judgment and mentorship to develop expertise.

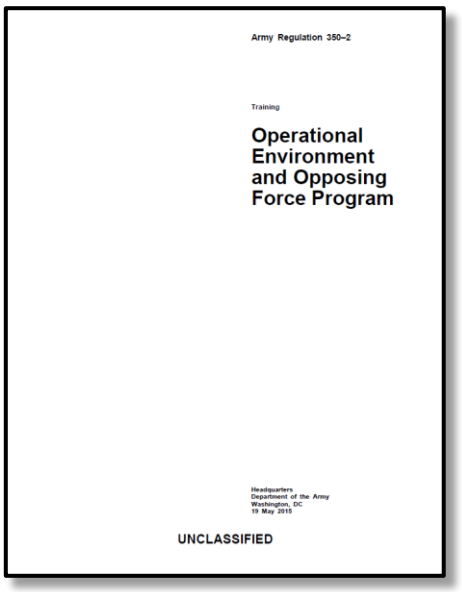


Figure 12. OE and OPFOR Program

Knowing the threat is essential to planning and combating the capabilities and limitations of an adversary or enemy in a training or readiness mission.

- When a specified threat exists in a deployment order, the actual threat force is represented or replicated in training and pre-deployment readiness evaluations.

- When training is not focused on a particular real-world threat, Army activities use an opposing force as stated in Army Regulation 350-2 (2015). This regulation is a 2015 update on the Army 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.

Note. Descriptions throughout the vignette use threat terms from the US Army TC 7-100 series.[1] The task-organized platoon in this article is best understood by knowing the unit and weapon system capabilities presented in TC 7-100.4 and its Threat Force Structure e-folders of units. Another source is the TRADOC G-2 *Worldwide Equipment Guide*. Capabilities and limitations are determined to represent a robust, realistic, and relevant threat/OPFOR as a condition in achieving US Army training objectives and sustained readiness.

The orderly guidance described in doctrine can be—and usually will appear—very different in execution of mission tasks when conditions are likely 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. This vignette demonstrates quality training, teamwork, and leadership with initiative and prudent risk taking by officers and noncommissioned officers in crisis moments of tactical leader decisions.

Independent Reconnaissance Patrol

At the platoon echelon, the threat force structure for reconnaissance is often a task-organized element with combined arms capabilities. This task-organized platoon was an IRP with a specific mission to conduct reconnaissance of the enemy and terrain in a reference zone (RZ).[5] In this tactical vignette, the reconnaissance battalion headquarters coordinated a task organization consisting of a reconnaissance patrol headquarters and two wheeled armored vehicle reconnaissance sections. The combat engineer squad augmented the reconnaissance effort and defensive actions. The attached mortar section was the only dedicated indirect fires for the platoon leader. Soldiers trained in combat lifesaver skills complemented a medic team to provide for immediate medical treatment. Radio communication to company headquarters was disciplined for time intervals but remained flexible to developments.

Mission analysis and a clear understanding by the platoon leader of the mission purpose and intent fortified platoon leader willingness to accept prudent risks in conducting his mission with an expectation that conditions would change from initial situational understanding of the OE and the enemy. Heavy rains and unit movements had already turned underdeveloped roads throughout the zone into muddy ruts. Overcast weather brought aerial reconnaissance to a standstill, and rain or recurring haze severely limited any long-range ground observation.

Delay—Disrupt—Fix—Linkup—Break Contact

Delay **is an action to slow arrival time of enemy forces or capabilities, or alter the ability of an enemy or adversary to project elements/forces or their capabilities.**

Disrupt **is a action to upset an enemy formation or tempo, interrupt an enemy timetable, cause an enemy to commit elements/forces prematurely, and/or cause an enemy to attack in fragmented combat power.**

Fix **is an action to prevent an enemy from moving any part of an element/force from a specific location for a period of time.**

Linkup **is an action between or among friendly elements/forces to meet at a linkup point and coordinate to continue mission tasks.**

Break contact **is an action to disengage elements/forces from an enemy in order to conduct subsequent mission tasks or to avoid decisive engagement**.

Figure 13. Mission task/drill descriptions

Tactics, Techniques, and Tasks/Drills

Situational awareness and understanding of an OE and an adversary or enemy is a continuous series of actions to confirm or deny information and intelligence. In C2 echelons above the platoon, overlapping staff resources gather data to

compare and contrast situation reports, information updates, and intelligence analyses. The platoon leader shapes reconnaissance mission task priorities of effort and coordinates mission preparation with the unit's noncommissioned officers.

- ***Reconnaissance*** is a mission task that represents all measures associated with organizing, collecting, and studying information on the enemy, terrain, and weather in a designated RZ within a zone of reconnaissance responsibility (ZORR). Reconnaissance is part of the threat military function of reconnaissance, intelligence, surveillance, and target acquisition (RISTA).[6]
- ***Counterreconnaissance*** (CR) is a companion task of reconnaissance as a norm of fighting for information and intelligence. Counterreconnaissance locates, tracks, and destroys all enemy reconnaissance operating in a counterreconnaissance zone (CRZ).[7]

When enemy presence is unknown or unconfirmed, analysis of the OE orients leader decisions and guidance on where and when reconnaissance and surveillance is to be conducted. A PEL is an area in the zone where enemy activity, troops, or systems are expected to be operating or will enter during the period of the mission. Analysis of current information and the updated tactical intelligence estimate combines to indicate known, most likely, and/or probable enemy locations and avenues of approach.[8]

Once reconnaissance elements locate and/or maintain surveillance of an enemy reconnaissance effort, the leader determines when and how to counter enemy reconnaissance elements. The specified task may be to continue reporting with situation updates and preclude direct combat actions. However, when the mission includes CR rather than just surveillance, one or more kill zones can be designated by the leader. Indirect fire targets are incorporated into the mission planning, as are tactical task contingencies such as ambush, assault, or raid. Rehearsals and pre-combat checks conducted prior to the mission confirm the actions and possible contingencies at platoon, squad, and team echelons.

- ***Tactics*** are an organized doctrinal arrangement of military or paramilitary forces that work toward achieving a common objective or task. The reconnaissance leader applies tactics and techniques to the mission statement and acts in order to achieve the intent of the mission from the higher-echelon commander.
- ***Techniques*** are the practical application of combat power with skills, experience, and initiative to accomplish mission success. Considering that techniques by nature are non-prescriptive to a distinct way or method of accomplishing a mission or task, the effective execution of tactics uses functional analysis to understand the mission or task requirement.

Of note, control measure and mission task symbols on a sketch or map overlay are neither tactics nor techniques. These graphics assist the leader in visualizing and effectively communicating a planned sequence of actions. Tactical skill and expertise integrate task, purpose, and intent to optimize capability effects with movement and maneuver of the combat power resources allocated to the mission. Understanding function is the underpinning to comprehend and effectively apply tactics and techniques.

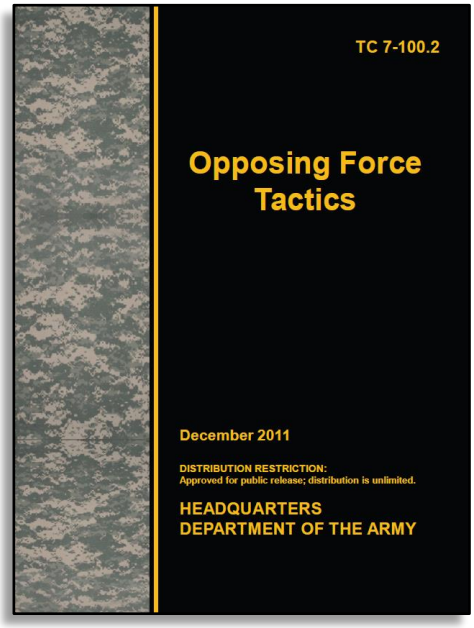


Figure 14. Opposing Force Tactics

Delay and Linkup Dilemma

A delay can be visualized typically as three synchronized elements: a *delay* [action] element, *security* element(s), and *support* element(s). The delay element can be considered a *contact element* in imminent or current contact with an enemy. Depending on how threat elements array for support or security, an element can be considered a *shielding element* that occupies a defensive position to permit a contact element to withdraw or break contact, and reposition into a subsequent fighting position or simple battle position.[9] The principle of security and dedicated elements to provide security can be problematic, especially in small unit/element tactical actions.

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

A small-echelon tactical tasks of conducting a delay with three functional elements—delay element, security element, and support element—relates coordinated actions as follows:[10]

- The ***delay*** element is the *action* element. This element applies defensive fire and maneuver to slow, disrupt, or fix enemy offensive actions, and provide time for other friendly force elements to continue successive support and delay actions that can eventually defeat or destroy enemy elements.
- The ***security*** element provides early warning of approaching enemy forces and prevents them from reinforcing the enemy in contact with the delay element. The threat leader may accept risk and employ a security element that only provides early warning. In either case, security is an *enabling* element.
- The ***support*** element provides the delay action element with one or more of the following but is not limited to: C2, combat service support (CSS), supporting direct fire and/or indirect fire, and mobility or countermobility support. Support is an *enabling* element.

In this article vignette, the *delay* [action] element is in contact with the enemy. Other elements disrupt or fix enemy elements 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. As the action element prepared to maneuver to its alternate or subsequent fighting position, the action element leader coordinates the transfer of delay task responsibility to other friendly elements already positioned to shield the action element as it breaks contact and displaces. This shielding element maintains the enemy under continuous observation, accepts handover of the fire fight, and becomes the delay action element.

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. 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 OE.

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 or fighting position and has coordinated the transfer of main defensive actions to another element now in contact with the enemy, the former delaying element becomes a *support* [enabling] element. These delay maneuvers recur in alternating bounds of the contact and shielding elements.

OPFOR in Training, Professional Education, and Leader Development

An OPFOR is "a plausible, flexible military and/or paramilitary force representing a composite of varying capabilities of actual worldwide forces (doctrine, tactics, organization, and equipment) used in lieu of a specific threat force for training and developing US forces."[11] The OPFOR can represent a particular threat, hybrid threat, and/or an adversary that can morph in capabilities and influence within a relevant population. The threat/OPFOR is not necessarily restricted by law of war protocols or international conventions on armed conflict.

In US Army training, the threat/OPFOR recognizes the value of reconnaissance and counterreconnaissance and employs a disciplined and aggressive approach to plan and conduct these types of mission tasks. Both of these tasks are typical of reconnaissance and security operations. Offensive tasks at platoon echelon anticipate other typical actions of ambush, raid, and assault. Complementary actions include but are not limited to actions on contact, fire and maneuver, disrupt, fix, and break contact.[12]

The threat/OPFOR doctrine and training instill timely and adaptive decisionmaking and leadership that are results focused. Decentralized C2 is a threat norm grounded in a clear understanding of mission task and purpose and the overarching intent of higher headquarters commanders. The threat thinks and acts decisively to achieve tasks with professional execution of individual and collective skills among each element or force level in the tactical mission.

OPFOR Tasks and Drills Update

The TRADOC G-2 Analysis and Control Element, Threats Integration Directorate (ACE-TI) at Fort Leavenworth (KS) is chartered to serve as US Army lead for designing, documenting, and integrating threat [OPFOR] and OE conditions in support of all Army training, education, and leader development programs.[13]

Several OPFOR tasks and drills have been updated as of March 2017. These 17 updated tasks and drills are now posted in the US Army Combined Arms Training Strategies (CATS). For an easy 1-2-3 sequence to retrieve updated OPFOR tasks in CATS, go to the Army Training Network (ATN) with common access card entry, click on the CATS icon, and search using the keyword "OPFOR." Additional OPFOR tasks are in the process of revision and will be incorporated in the revision of TC 7-100.2. See TRADOC G-2 Handbook 1.09, "Opposing Force Tasks: Collective Company/Subordinate Tasks," for the updated 17 tasks and drills.[14]

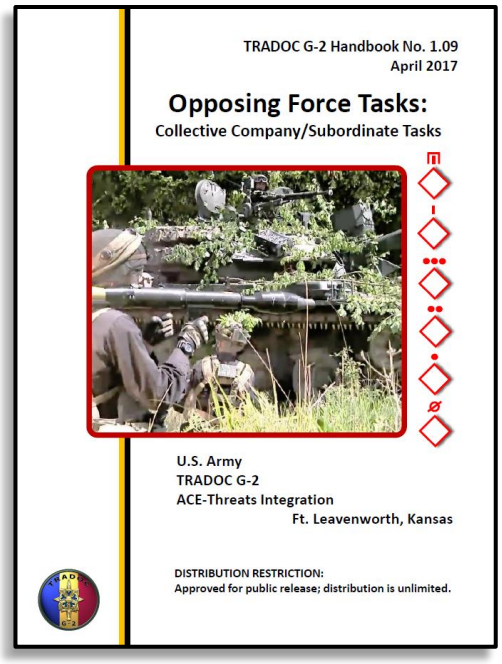


Figure 15. OPFOR Tasks and Drills

These updated tasks are in compliance with the new US Army "Objective T" format, and have a task number sequence in the format 71-CO-85xx, where the last two numerical digits identify the specific OPFOR task number.[15] Several previous OPFOR tasks are being removed gradually from CATS, so look for these 71-CO-85-series company-echelon and subordinate-element tasks and drills for use in home-station training and other readiness venues.

For more information and resources on threat/OPFOR, see US Army TRADOC G-27 Operational Environment Training Support Center (OE TSC) at https://tbr.army.mil/index.html. The **Virtual OPFOR Academy** (VOA) provides OPFOR tasks/drills, references, instructional and immersion videos, and exercise design/support tools to achieve collective training objectives for sustained Army readiness.

Figure 16. TRADOC G-2 Virtual OPFOR Academy learning support resources

In 2017–18, the TRADOC G-2 ACE ACE-TI is reviewing and revising threat/OPFOR tasks. The updated list of tasks and subtasks, with conditions and standards for US Army training readiness, will address traditional offensive and defensive tasks, as well as tasks involving instability in an era of persistent conflict now and for the foreseeable future. See the TC 7-100 series for more information on the threat/OPFOR.[16]

Notes

[1] A series of tactical vignettes based on US Army TC 7-100.2 opposing force tactics conducted by an independent reconnaissance platoon are in the TRADOC G-2 *Red Diamond* newsletter: June 2015 "Reconnaissance;" July 2015, "Reconnaissance and Assault;" August 2015 "Reconnaissance and Ambush;" September 2015, "Reconnaissance and Raid;" October 2015, "Reconnaissance and Delay;" and May 2017, "Reconnaissance Delay and Linkup." The article series emphasizes the basic building blocks of understanding tactics and techniques, and the leadership and expertise required to execute tasks and drills effectively in accomplishment of missions.

[2] Headquarters, Department of the Army. Training Circular 7-100.2, *Opposing Force Tactics*. TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. 9 December 2011. Paras 8-78—8-86.

[3] Headquarters, Department of the Army. Training Circular 7-100.2, *Opposing Force Tactics*. TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. 9 December 2011. Paras 8-1 and 8-21.

[4] BTR. Acronym of Russian word meaning, literally, "armored transporter," and is a common term for any of a family and series of Russian or post-Soviet era military armored personnel carriers produced and fielded by a number of nation-states.

[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. Paras 8-83—8-86.

[6] Headquarters, Department of the Army. Training Circular 7-100.2, *Opposing Force Tactics*. TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. 9 December 2011. Paras 8-21—8-28.

[7] Headquarters, Department of the Army. Training Circular 7-100.2, Opposing Force Tactics. . TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. 9 December 2011. Paras 6-8; 8-39.

[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. Paras 6-11–6-13; 8-38; 8-58–8-59.

[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. Paras 4-62, 4-70—4-74. The principles described in these paragraphs address tactics at division and brigade group echelons; however, the concept of mutually supporting and successive bounds is also applicable to small unit tactical actions.

[10] Headquarters, Department of the Army. Training Circular 7-100.2, Opposing Force Tactics. . TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. 9 December 2011. Paras 4-1, 4-11, and 4-70—4-71.

[11]Headquarters, Department of the Army. Army Regulation 350-2. Operational Environment and Opposing Force Program. 19 May 2015 with effective date 19 June 2015. Para 1-5b.

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

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

[14]Headquarters, US Army Training and Doctrine Command. Opposing Force Tasks: Collective Company/Subordinate Tasks. TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. April 2017.

[15]Headquarters, Department of the Army. G-3/5/7. *Leader's Guide to Objective Assessment of Training Proficiency*, 15 March 2017.

[16]Headquarters, Department of the Army. Training Circular 7-100.2, Opposing Force Tactics. TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. 9 December 2011. Headquarters, Department of the Army. Training Circular 7-100.3, Irregular Opposing Forces. TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. 17 January 2014. Headquarters, Department of the Army. Training Circular 7-100.4, Hybrid Threat Force Structure Organization Guide. TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. June 2015. Headquarters, Department of the Army. Training Circular 7-101, Exercise Design Guide. TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. November 2010. Headquarters, Department of the Army. Training Circular 7-102, Operational Environment and Army Learning. TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. November 2014. US Army, TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. US Army, TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. Worldwide Equipment Guide – Volume 1: Ground Systems. December 2016.

TRENDS IN ATTACKS AGAINST POLICE AND MILITARY IN NORTHWEST INDIA, 2013–2016

by H. David Pendleton, TRADOC G-2 ACE Threats Integration (CGI Contractor)

All insurgencies are local, and the techniques used are often tailored to the region where the uprisings take place. Each region often faces its own peculiar mix of issues, and a solution that works in one area may not work in another. While improvised explosive devices (IED) are often a weapon of choice in Afghanistan, the same is not true for India Administered Kashmir (IAK) in northwestern India. While this part of India lies less than 500 km from Afghanistan, IEDs rarely detonate in the IAK. The Naxalites, who have been fighting government forces in other parts of India for years, have shown a preference for IEDs; yet the first known command-detonated IED attack on an Indian military or police target in the IAK occurred less than six months ago in December 2016.[1] Between January 2013 and December 2016, only nine other IED attacks against the military or police occurred in the IAK with none reported in a single year—2015.[i]

Figure 1. Kashmir and the disputed areas between India, Pakistan, and China

This article provides a background for situational awareness, and a regional overview of the various threat actors that have impacted the IAK operational environment (OE) over the past four years. It then touches on some of the major incidents perpetrated by militants during the same timeframe. The bulk of the article is an examination of the interaction between militants and Indian security forces to identify trends that have emerged in the IAK insurgency. The article concludes with an analysis of these trends to determine what clues they offer regarding the future course of the insurgency.

Background

Territorial disputes related to its borders with Pakistan and China rank in the top tier of challenges confronting India's government. These disputes most often revolve around the Indian state of Jammu and Kashmir (a single entity often abbreviated as J&K). Generally speaking, with the 1947 withdrawal of Great Britain from the Asian sub-continent, the primarily Muslim-occupied areas were assimilated into the country of Pakistan, while those with predominantly Hindu populations joined together to form India. The J&K maharaja (ruler)—a Hindu who formerly governed the majority Muslim region—was permitted to choose between independence and joining either country. When invaded by Pakistani forces, the Maharaja decided to join India, and the region's status has been contested since that time. In the ensuing decades, Pakistan consistently has attempted to alter the territorial status quo. India Defeated Pakistan in three wars (1947–48, 1965, and 1971) fought over this disputed territory, with little change emerging as a result of the violence.[2]

[i] An important source of information on the militant activity in the IAK is the South Asia Terrorism Portal (SATP). The SATP lists over 550 events in IAK between 1 January 2013 and 31 December 2016. Although an attempt was made to find corroborating sources for each event, approximately 20 (about 7%) of these sources could not be accessed from a government computer. Since all SATP-reported events discussed in this article were confirmed as factual the 20 events remain part of the article's background source material. This is not to say that no other events occurred besides those reported by SATP. When other events were discovered, they too were assimilated into the article's background material, although the need to avoid undue redundancy meant that not all of them could be cited. Upon request the author will furnish a complete listing of over 550 events and their corresponding sources.

Although the entire territory, often simply called Kashmir, is claimed by both India and Pakistan, the area is actually divided between the two countries—with each side controlling part of the land: IAK and Pakistan administered Kashmir (PaK). A fence marks the boundary, but does not extend across the entire border. This is especially true in areas that contain rivers or significant bodies of water. Both sides patrol the border and maintain guard posts along a dividing line, or Line of Control (LoC). Of the 22 districts that comprise the Indian state of J&K, ten are contiguous with PaK.

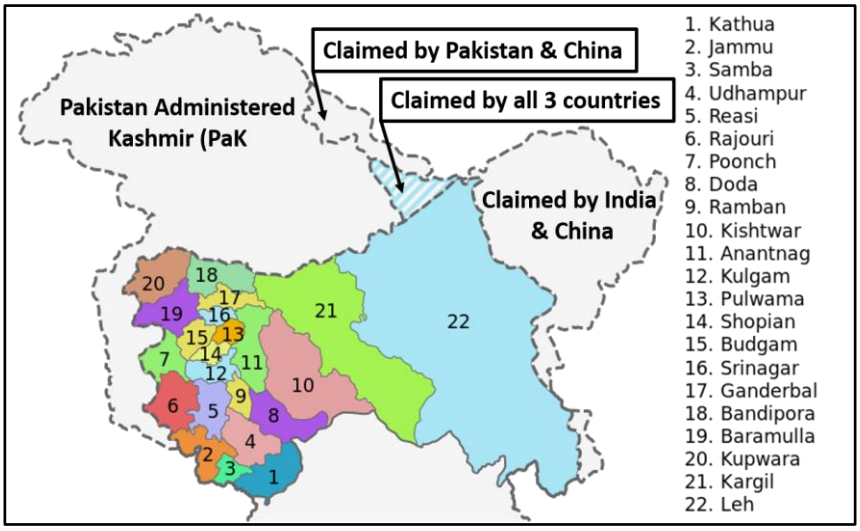


Figure 2. Jammu and Kashmir's districts

Insurgent Groups

A number of insurgent groups operate in the J&K/IAK/PaK region. A number of recorded attacks, however, cannot be linked to any of these groups for a variety of reasons: no organization claimed these actions, Indian governmental officials refused to release information on perpetrators, or the perpetrators successfully made their escape. With rare exceptions, the groups typically do not work together.[3] India claims that many of these groups train in eastern Pakistan, supported by the Pakistani government, and then cross the LoC to attack Indian governmental officials and infrastructure. Most but not all of these actions take place in J&K state. An analysis of attacks perpetrated over the past four years reveals the existence of two major and two minor insurgent groups operating in J&K, with a fifth group that ranges somewhere between these pairs of groups along the broad spectrum of militant activity. The number of attacks attributed to the two largest groups—Lashkar-e-Taiba (LET) and Hizb-ul-Mujahideen (HM)—have remained relatively consistent over the past two years. Events that cannot be attributed to a specific organization, however, have increased significantly rising from 30 to 100 events over the past four years.[4]

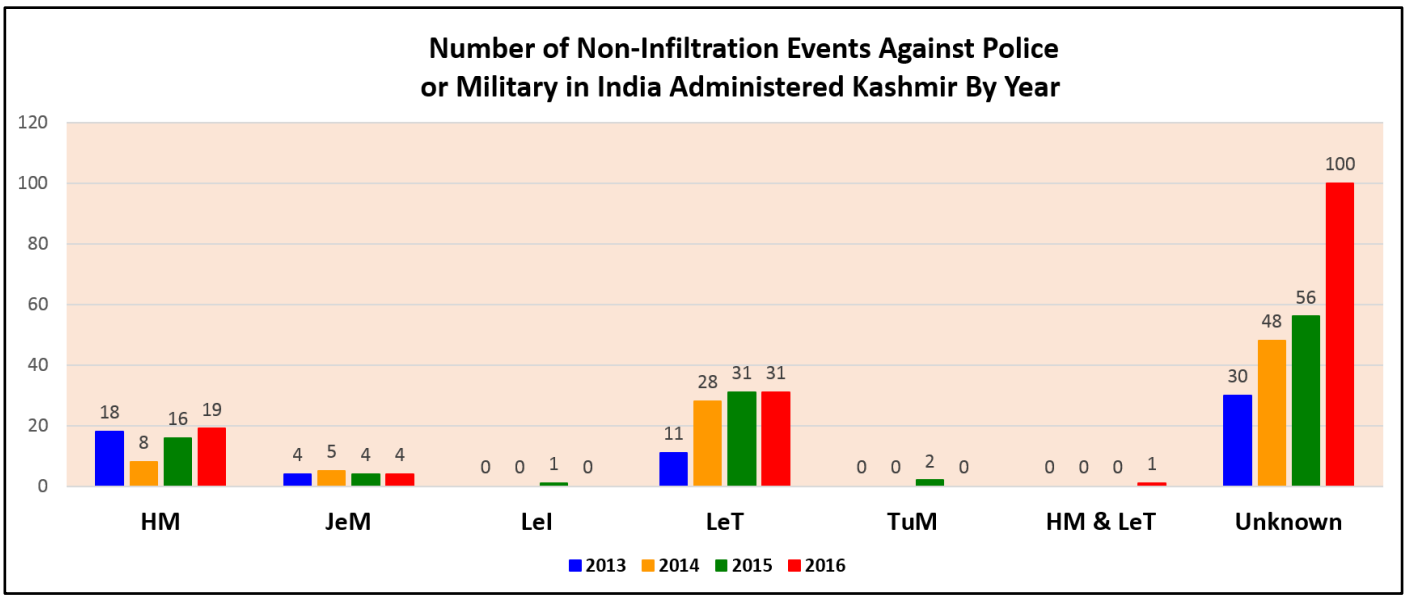


Figure 3. Activity levels by militant groups, 2013–2016

Lashkar-e-Taiba (LeT)

One of the most active insurgent groups in the IAK is the Lashkar-e-Taiba, more commonly known as LeT. Founded in 1990 in Afghanistan, its headquarters is in Muridke, near Lahore, Pakistan. LeT initially crossed the LoC in 1993 and continues to operate not only in J&K, but throughout all of India. In one of its most successful actions, LeT set off a series of explosions on 29 October 2005 that killed 62 persons in New Delhi, India. In its literature, LeT states that its mission is to not only impose Islamic rule over all parts of India, but to unite all the Muslim majority regions in the countries that surround Pakistan. LeT is against democracy and nationalism and draws its cadre from the radical Wahabi school of Islamic thought. LeT is geographically organized, with district commanders in charge of their respective units/cells. LeT, through its training camps located in Pakistan, conducts courses for militants that run up to several months in duration. LeT is known to have connections to both the Taliban and al-Qaeda (AQ).[5]

Hizb-ul-Mujahideen (HM)

The region's second most active insurgent group is the Hiz-ul-Mujahideen, usually shortened to HM. This group is sometimes described as a militant offshoot of the Jammat-e-Islami (JeI) that first surfaced in Kashmir in 1989. HM's stated purpose is the reunion of all of Kashmir with Pakistan. Headquartered in Mzaffarabad, Pakistan, the HM is well organized. Its five geographically aligned divisions operate across the J&K: in Central (Srinagar district); Northern (Kupwara, Bandipora, and Baramulla); Southern (Anantnag and Pulwama); Chenab (Doda and part of Udhampur); and PirPanjal (Rajouri and Poonch) districts. HM's information warfare dimension encompasses the Kashmir Press International—its own news agency—which enjoys a substantial support base in several parts of J&K. HM is also known to have connections to the JeI within the IAK OE and to other Muslim organizations outside of India.[6]

Jaish-e-Mohammed (JeM)

The third most active insurgent group in IAK is Jaish-e-Mohammed, abbreviated as JeM. JeM is an Islamist splinter group that began operating in Karachi, Pakistan in 2000 after India released Maulana Masood Azhar as part of a hostage swap arrangement. The stated purpose of JeM is to use violence to force India to withdraw its security forces from J&K. JeM's primary technique is to launch *fidayeen* (suicide) attacks against selected targets. JeM members typically undertake a mission knowing they will likely die, and often conduct raids against military or police bases, camps, convoys, or patrols. After neutralizing their initial target, JeM attackers often establish a defensive perimeter, intending to kill as many indigenous security force personnel and civilians as possible before they die themselves. JeM maintains strong connections with both AQ and the Taliban.[7]

Lashkar-e-Islam (LeI) and Tehreek-ul-Mujahideen (TuM)

Over the past four years, the Laskar-e-Islam (LeI) and Tehreek-ul-Mujahideen (TuM) have claimed responsibility for a small number of attacks in IAK. The Indian government has also accused these organizations of perpetrating or sponsoring a variety of militant events. While LeI normally operates in northwest Pakistan along the Afghanistan border, the TuM publically stated it will no longer claim responsibility for any future attacks.[8]

Major Attacks in Northwest India: 2013–2016

The two most serious militant attacks against police/military targets in Northwest India both happened in 2016. Early in the morning hours of 18 September 2016, militants used grenades, small arms, and arson to attack an Indian army brigade's administrative camp near Uri in Baramulla District, J&K. Before the army could eliminate the four attackers, the militants killed 19 soldiers and support staff while injuring 35 others.[9] This attack occurred less than a year since the attack on an Indian Air Force base at Pathankot in nearby Punjab state that demonstrated the vulnerability of military posts in Northwest India to militant raids.[10]

Over the past four years, casualties produced by each militant attack on Indian security personnel reached double digits on three other occasions. At around noon on 26 September 2013, personnel dressed in military uniforms attacked a police station in Hiranagar, Kathua district with grenades and small arms fired from a motorized rickshaw, killing a total of 14 police officers and civilians caught in the crossfire.[11] On 5 December 2014, six militants divided into groups to launch simultaneous attacks on multiple targets in different locations. They conducted an early morning raid on an ordnance unit's camp near Mohra in Baramulla district killing twelve people, including ten military personnel, before security forces eliminated the assailants.[12] In the early evening hours of 13 March 2013, two militants dressed as cricket players attacked

a Central Reserve Police Force (CRPF) camp near Srinagar City in Srinagar district. The attackers pulled weapons from their equipment bags, threw grenades, and fired indiscriminately, killing ten people and injuring seven others before other soldiers killed the cricketer impersonators.[13]

Infiltration Trends: 2013–2016

There appears to be an increase in infiltration attempts during the past four years, but a case could be made that better security measures created a perceived increase in illegal cross-border attempts. What is not known is how many

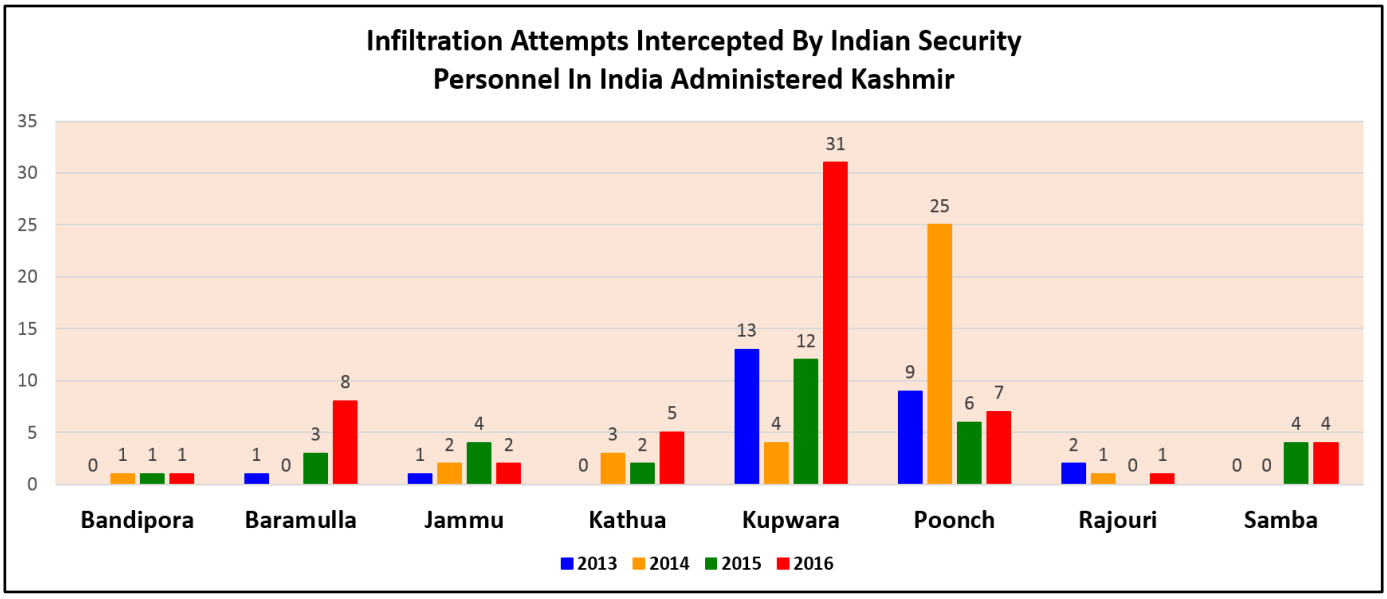


Figure 4. Infiltration attempts intercepted by district, 2013–2016

infiltrators crossed the LoC without detection by Indian security personnel. The reason for varying numbers of infiltration attempts in a district is quite simple: militant groups seek the easiest place to illegally cross the border without interference from Indian officials. When the Indian security personnel increased their vigilance in one location, the militant groups pursued alternative safer routes into the IaK, usually found in a different district. Ten of the 22 districts in J&K are contiguous with IAK territory, but there are varying levels of illegal crossings of the LoC by the militants. No South Asia Terrorism Portal (SATP) documentation confirms infiltration through two of these districts—Leh and Kargil—both large districts that lie near to contested areas close to the Chinese border. Four other districts—Bandipora, Jammu, Kathua, and Rajouri—demonstrate a relatively consistent number of infiltrations over the past four years. Two of the districts—Baramulla and Samba—show an increase in infiltration activity over the past two years. The number of known infiltrations in these latter two districts, however, never exceeded five attempts in any given year. An examination of the SATP database revealed no cross border activity in Samba district in 2014, but showed four attempts in each of the last two years. Kupwara and Poonch represent the most active districts for infiltration attempts from Pakistan over the LoC since 2013, garnering the highest numbers for all four years. Since 2013, infiltrations in the most active district each year were always at least double the attempts in the second most active district for that year.

Militant Attacks against Police and Military Targets: By District Trends, 2013–2016

The level of militant activity in J&K depends on the district. Srinagar District endured the brunt of these attacks, most likely because Srinagar City is the capital of J&K state. The militants probably believed that attacks in the state capital—the area's largest city—symbolically underscore the Indian government's inability to protect is own officials, not to mention the population at large. After Srinagar district suffered at last 15 incidents in 2013, the Indian government increased its security presence in the city and the surrounding area. The measure reduced the number of attacks in Srinagar, both city and district, during the next two years. In 2016, however, the number of attacks in Srinagar district doubled relative to the previous year. There are four districts where the SATP reported no militant activity of any kind against police or military

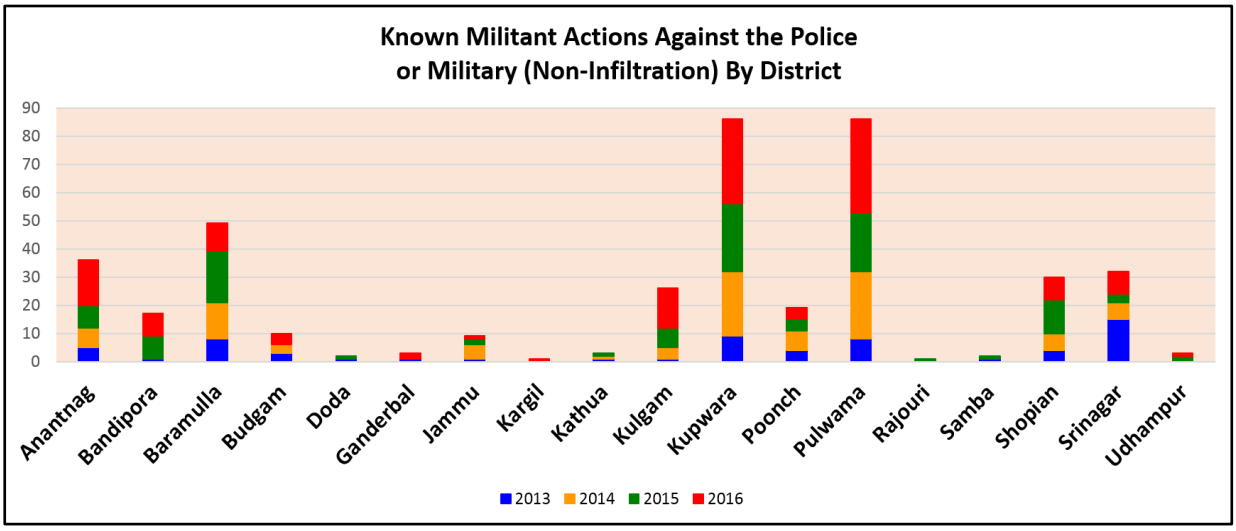


Figure 5. Militant activity by district, 2013–2016

forces over the past four years: Kistwar, Leh, Reasi, and Ramban. Most militant activity in J&K since 2013 occurred in just seven districts: Anantnag, Baramulla, Kulgam, Kupwara, Pulwama, Shopian, and Srinagar. Except for Bandipora and Poonch, all the remaining districts saw fewer than five militant acts against security targets in any single year. The proximity of the district to the LoC, however, does not always correlate to the number of attacks on police or military personnel. Rajouri, Samba, and Kathua districts all touch PaK, but the militant groups operating in those areas rarely targeted security personnel. Conversely, the districts of Anantnag, Shopian, and Srinagar are separated from PaK by other districts, but their police and military were the focus of an intense targeting effort by the militants. Kupwara and Pulwama districts suffered the most anti-police/military activity over the past three years, including over 30 incidents in both districts during 2016.

Militant Activity against Police and Military: 2013–2016

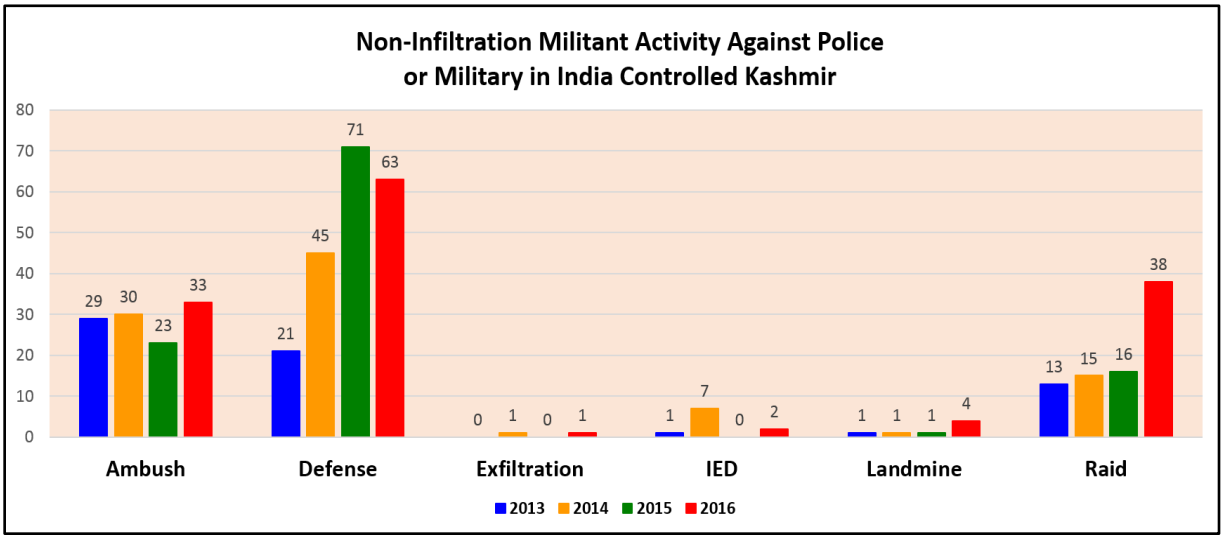


Figure 6. Militant tactics by district, 2013–2016

SATP statistics regarding violent engagements between militants and indigenous security forces in J&K can be broadly grouped into six categories: ambushes, defensive actions, raids, exfiltrations, IED attacks, and emplacement of landmines.

The first three categories comprise over 95% of the (approximately 400) non-infiltration events, while only 19 events during the last four years were attributed to landmines, IEDs, and exfiltration attempts. Ambushes are of two types: the first type is an attack against a single vehicle or convoy, while the other is an ambush against a foot patrol. Defense is a broad category including indigenous security personnel detecting militants and forcing them into a violent engagement, typically a firefight. In these situations, security units were on the offensive, and the militants—even if merely trying to escape—are cast in a defensive role. Events that entailed the nonviolent capture of militants by security forces are not reflected in these statistics. The increasing number of confrontations wherein militants fought defensive actions may reflect increased Indian security force efforts over the past two years to eliminate militants operating in J&K. The increased effort to aggressively pursue any tips has caused a rise in confrontations between security units and militant groups. These clashes have caused collateral damage to innocent bystanders as well as property. The raid category includes situations wherein an individual or group either attacked a police station or camp with the intent to escape with weapons, or an attack intended to inflict as many casualties as possible before the attacking element could be captured or killed. The most likely reason for the increase in raids in 2016 is that stronger security throughout the LoC reduced the flow of weapons from Pakistan into India. These increased security measures leave militants little choice other than ambushing police patrols or raiding police stations as their most viable means of obtaining arms and ammunition. Often, the militants forbear conducting raids against highly trained and proficient security personnel, preferring instead to focus on personal body guards, security guards, or individual police officers whose weapons and/or lesser training present a significantly lower risk to the attacking element. Exfiltrations occur when individuals or groups unsuccessfully attempt to cross the LoC and re-enter PaK. IED and landmine statistics relate to similar events that typically involve members of foot patrols causing detonations by stepping on devices that are usually hidden underground. Except for the one example cited earlier, command detonated IEDs do not usually occur in J&K.[14]

Militant Group Activity Preferences against Police and Military: 2013–2016

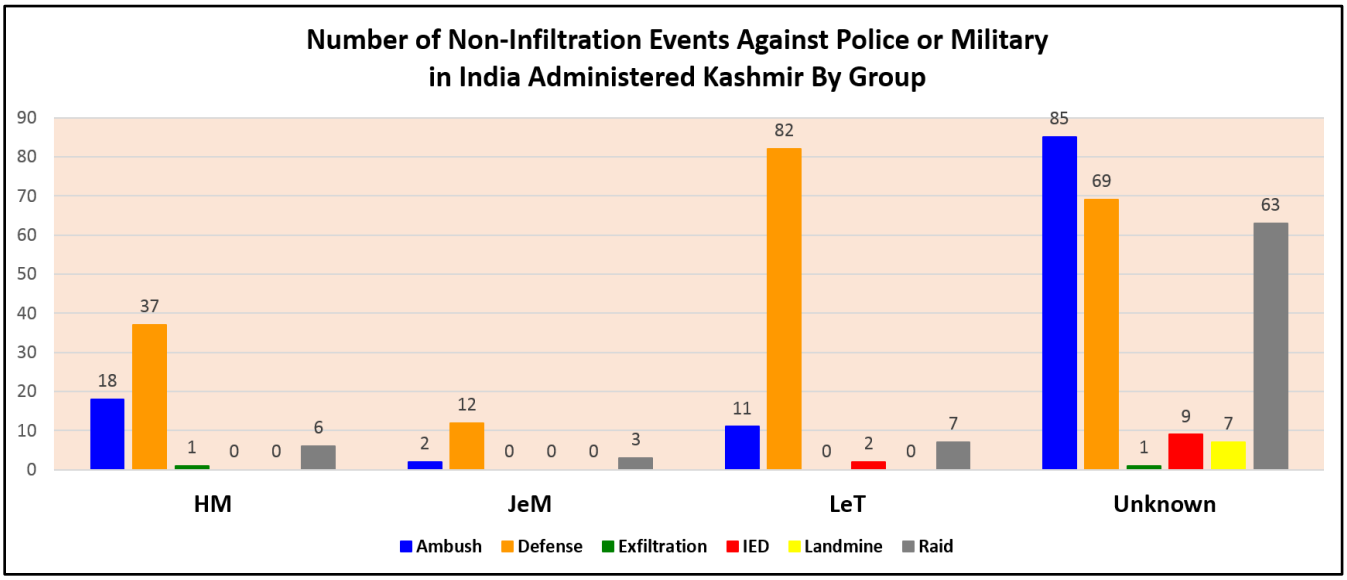


Figure 7. Militant activity by group and activity type, 2013–2016

Ambushes are the primary technique used by militant groups in J&K, with raids coming in at second place. Normally ambushes are less risky than other types of actions because if planned properly, the perpetrators have already prepared an escape route. Often the only way the ambush perpetrator's identity becomes known is if a group later claims responsibility for the attack.[15] Defense is not usually a planned technique by a group, but arises out of necessity when a security patrol successfully flushes out militants. When cornered, whether in a building or in rural areas, the militants' survival depends on engaging the security force, usually with small arms.[16] Sometimes, when the decisively engaged militant cell is sufficiently large enough, the group may leave behind one or two individuals to fight a delaying action in hopes of holding the Indian security force at bay long enough to permit escape by the remaining cell members.[17] These militants often die to save their comrades. A number of reasons account for why many militant actions are perpetrated

with no group claiming responsibility. In the first place, security forces are often unable to pinpoint responsibility for a successful ambush or raid because the perpetrators successfully made their escape. Secondly, in the last few years groups have grown increasingly reticent in taking credit for an attack, even if it proved successful. Finally, the Indian media is focusing less attention on naming the groups believed to be responsible for terrorist incidents. It is unknown whether this turn of events reflects a lack of knowledge on the part of Indian officials, or that the latter have decided to withhold information from the media.

Tactic: Harassment Ambush

Drive-by motorcycle shootings of buses carrying security personnel is an ambush technique used by the militants during the past four years is a type of harassment ambush tactic.[18] Often, the victims of these ambushes are weaponless. Since 2013, this motorcycle ambush technique has been used about a half-dozen times in the approximately 25 ambushes of police/military vehicle(s) ambushes in J&K. On 21 March 2013, motorcycle-riding militants ambushed a Border Security Force (BSF) bus, killing one passenger and injuring two other guards near Rawalpora in Srinagar district.[19] Over four years later, the militants again used a variation of the same technique. At about 1400 hours local time on 18 December 2016, a motorcycle carrying two riders pulled alongside an army bus in Pampore (Pulwama district), and began peppering the bus with small arms fire. The vehicle carried unarmed soldiers returning from leave in Jammu district to their base in Srinagar. The shooters killed three soldiers and wounded two others, including the bus driver, during this ambush. The casualties were not higher because the bus driver chose not to stop and instead fled the ambush site as best he could.[20]

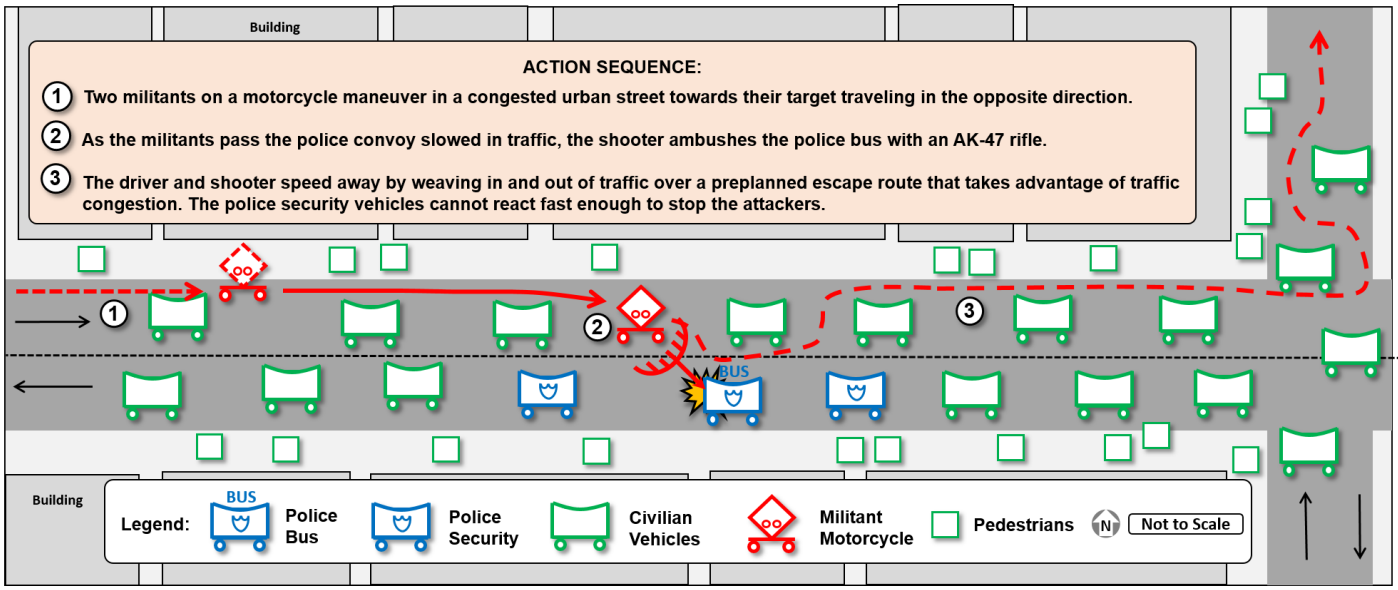


Figure 8. J&K motorcycle ambush technique

The diagram in figure 8 depicts a representative sample of this harassment ambush technique similar to the attack on 18 December 2016. The militants purposely choose a congested area to make their attack, and select a time when heavy traffic makes it difficult for police in four-wheeled vehicles to chase a motorcycle weaving in and out of traffic lanes. The militants often choose soft targets such as unarmed soldiers or policemen riding in buses. The two militants are on a motorcycle, an everyday sight in India. As the motorcycle approaches the bus, the passenger raises the muzzle of his semi-hidden machine gun and fires through the bus windows as the motorcycle passes the larger vehicle. The motorcycle then weaves through the civilian vehicles to avoid any police security vehicles and speeds off over a pre-planned escape route. A variation of this technique entails the perpetrators, once they have distanced themselves from their target, abandoning their motorcycle and transferring to another escape vehicle. If the Indian security forces find the perpetrators' motorcycle, they usually cannot obtain a description of the second getaway vehicle.

Connections to Opposing Force Tactics

The ambushes, raids, and defensive actions by the J&K militants are similar to the tactics found in Training Circular (TC) 7-100.3, *Irregular Opposing Forces*.[21] While the techniques used by the militants operating in J&K may be different than those in TC 7-100.3, the tactics are the same as those found in the manual. In the absence of a known deployment location, studying TC 7-100.3 will generally prepare a Soldier for what to expect from militants. Upon notification of the actual deployment location, however, an additional study of the local militant techniques will be needed to ensure mission success.

Analysis

Despite the increase in infiltration attempts thwarted over the past four years, most likely due to increased vigilance on the part of Indian security personnel along the LoC, the number of attacks aimed at police and military personnel continues to climb. Since the Pathankot Airbase attack in January 2016, India has not only increased its BSF patrols along the Pakistani border, but is also installing additional fencing as well as electronic devices to detect illegal crossings in areas where fencing is problematic. These security improvements caused the infiltrators to search for other routes into the IAK as reflected by the changes in locations of where security personnel caught the most illegal border crossers. The rise in attacks on security forces in IAK, despite the reduction in militants crossing the LoC from Pakistan, is most likely due to an increased effort by militants to recruit from Muslims already living in J&K.

Many of these home-grown militants lack weapons, creating a necessity for them to attack individual security personnel or isolated outposts in order to obtain arms. This is the most likely reason for the increase in raids focused on stealing weapons from police and security personnel over the past few years. Weapons obtained from these raids, combined with equipment brought over the LoC in successful infiltration attempts, enable the various militant cells to conduct ambushes against soft targets. The militants often choose unarmed police, whether a group on a bus or a single police officer in a neighborhood store, as their target. These victims, who symbolize the authority of the Indian state, present attackers with the added advantage of an increased chance for escape.

Due to the greater targeting of police and military personnel, Indian security forces continue to intensify their pressure on the various anti-government groups in J&K by swiftly acting on any tips pertaining to militants. As a by-product of conducting vigorous searches, the Indian security forces have generated a surge in civilian collateral casualties and property damage. This upswing in collateral damage probably alienated some of the neutral J&K Muslims, engendering a collective anti-government mindset that makes Islamic militant propaganda resonate among young and marginalized elements of the population.

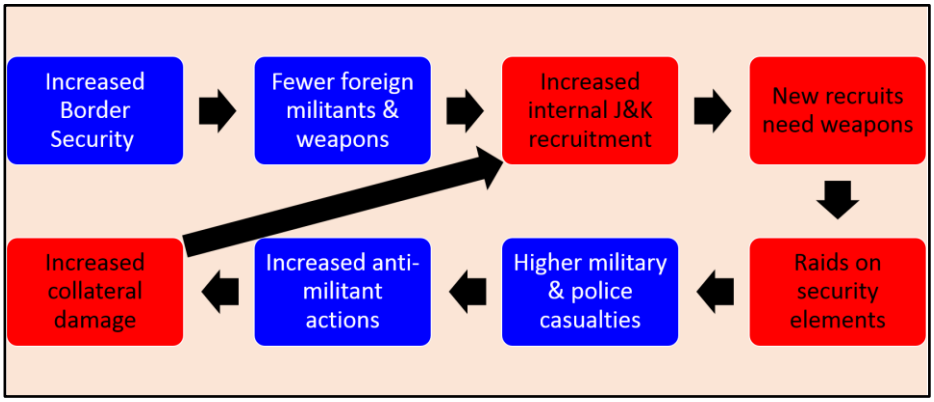


Figure 9. J&K negative causal loop

Militant groups previously would publically claim a successful ambush to the media, but they are now less likely to do so because of a fear that the Indian security personnel will surge personnel and resources in an all-out effort to apprehend or neutralize perpetrators of a successful ambush. This trend is demonstrated in the rising number of militant attacks perpetrated with no claim of responsibility.

Summary

The Indian security force/militant situation in J&K is a negative causal loop as shown in Figure 9. As more of the militants come from J&K, they will need weapons they are having difficulty in obtaining from the other side of the LoC. The violence against security forces to obtain weapons only increases the crackdown on militant groups creating more collateral

damage. The additional collateral damage generates more sympathy among the locals and makes them more susceptible to the militants' recruiting pitch. Breaking this cycle is the Indian government's best hope for peace in J&K, but how to do so is a conundrum without any simple solutions. It is likely that any successful outcome acceptable to the Indian government for J&K will prove impossible as long as the Islamic militant groups persist in their demand for the merger of IAK with Pakistan as the requirement for these groups to end hostilities against the Indian government in Kashmir.

Figures

Figure 1. Kashmir and the disputed areas between India, Pakistan, and China. CIA Map from Wikipedia Commons, Kashmir Region 2004.
Figure 2. Jammu and Kashmir districts. Map from Wikipedia Commons. Permission granted under GNU Free Documentation License, Version 1.2 or later.
Figure 3. Activity levels by militant groups, 2013–2016. Primary source is the South Asia Terrorism Portal (SATP) with additional sources from media outlets.
Figure 4. Infiltration attempts intercepted by district, 2013–2016. Primary source is the South Asia Terrorism Portal (SATP) with additional sources from media outlets.
Figure 5. Militant activity by district, 2013–2016. Primary source is the South Asia Terrorism Portal (SATP) with additional sources from media outlets.
Figure 6. Militant tactics by district, 2013–2016. Primary source is the South Asia Terrorism Portal (SATP) with additional sources from media outlets.
Figure 7. Militant tactics by group and technique, 2013–2016. Primary source is the South Asia Terrorism Portal (SATP) with additional sources from media outlets.
Figure 8. J&K motorcycle ambush technique. Created by ACE-TI, 22 March 2017.
Figure 9. J&K negative casual loop. Created by ACE-TI, 6 April 2017.

Notes

[1] Firstpost. "Security forces in Kashmir Valley targeted using Naxal-style IED." 11 December 2016.
[2] Thomas A. Marks. "Jammu & Kashmir: State Response to Insurgency – The Case of Jammu." National Counter Terrorism Center (NCTC). 14 March 2017.
[3] India Today. "ISI brings LeT, Hizbul Mujahideen, JeM together to bleed India." 26 November 2015.
[4] South Asia Terrorism Portal (SATP), India Assessment – 2016. 10 April 2017.
[5] South Asia Terrorism Portal. "Lashkar-e-Taiba: "Army of the Pure." 14 March 2017.
[6] South Asia Terrorism Portal. "Hizb-ul-Mujahideen." 14 March 2017.
[7] South Asia Terrorism Portal. "Jaish-e-Mohammed (Army of the Prophet)." 14 March 2017.
[8] South Asia Terrorism Portal. "Tehreek-ul-Mujahideen." 14 March 2017; South Asia Terrorism Porta. "Terrorist and Extremist Groups of Pakistan." 14 March 2017. Dera Ismail Khan. "Pakistani splinter group rejoins Taliban amid fears of isolation." Reuters. 12 March 2015.
[9] The Hindu. "18 jawans killed in pre-dawn strike at Uri." 18 September 2016.
[10] For details on the attack on the Uri base, see the Red Diamond article from January 2017 titled, "Uri, India attack—18 September 2016." For details on the Pathankot attack, see the Threat Tactics Report, "Pathankot, India Airbase Attack: 2 January 2016."
[11] India Today. "Terrorists attack police station and army camp in Jammu." 26 September 2013.
[12] Pakistan Kakhuda Hafiz. "Lt Col, 10 Security Men, 8 Militants Among 21 Killed in 4 Attacks." 6 December 2014.
[13] Muzaffar Raina. "Terror leaps out of cricket kit." The Telegraph. 14 March 2013.
[14] Firstpost. "Security forces in Kashmir Valley targeted using Naxal-style IED." 11 December 2016.
[15] Mufti Islah. "Militants Hurl Two Grenades at Police, 9 Security Personnel Injured in Pulwama." News 18. 24 August 2016.
[16] Xinhuanet. "Indian troops kill militant in Kashmir gunfight." 3 October 2014.
[17] Fayaz Bukhari. "Gun battle rages in Lolab forests, one militant killed." Daily Excelsior. 18 December 2013.
[18] Headquarters, Department of the Army. Training Circular (TC) 7-100.3, "Irregular Opposing Forces." January 2014. Paragraph 7-26 to 7-30, p. 7-6.
[19] NDTV. "One BSF jawan killed in militant attack on convoy in Srinagar." 21 March 2013; Getty Images. "BSF Convoy Attacked By Terrorists in Kashmir." 21 March 2013; The Kashmir Walla. "Suspected militants attack Indian forces in Kashmir; 3 injured." 21 March 2013; South Asia Terrorism Portal. "India Timeline – Year 2013." 16 March 2017.
[20] Toufiq Rashid and Ashiq Hussain. "Militants on motorbike target army bus in Kashmir, 3 soldiers killed." Hindustan Times. 18 December 2016.
[21] Headquarters, Department of the Army. Training Circular (TC) 7-100.3, "Irregular Opposing Forces." January 2014.

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

This is the first article of a two-part series that examines the Opposing Force (OPFOR) tactical tasks of raid and ambush by extracting tactical vignettes from an anti-tank guided missile (ATGM) video originating from the ongoing conflict between Yemeni Rebels and Saudi Arabian forces. The video footage was reportedly captured near the two countries' borders in the vicinity of Najran province. This article focuses on the initial raid that extended over a period of time. The subsequent article will emphasize the follow-on ambush as a tactical action. This article compares OPFOR doctrine from Training Circular (TC) 7-100.2 *Opposing Forces Tactics* and the 24 OPFOR Tactical Task List from appendix B from TC 7-101, *Exercise Design.* The video footage has the ATGM system(s) as the primary action element engaging a number of different targets in both the raid and a follow-on vehicle ambush that theoretically could be a quick reaction force (QRF).

Figure 1. Overview of Simple Fighting Position

The video begins with an ATGM raid by Yemeni rebels that engage three different stationary targets on a small outpost.[1] This article provides a real-world example for the training community and scenario developers with related concepts for ATGM threat replication as precision-guided system against smaller or isolated combat outposts. The video represents a real-world example that is cross referenced with threat doctrine. This article is the third collaborative effort between the

TRADOC G-2 ACE Threats Integration Directorate and the Defense Intelligence Agency's Missile Space Intelligence Center (MSIC). MSIC provided ACE-TI with a basic analysis of the ATGM video.

Video Background[2]

- Date: between July and August 2016
- Location: Najran, Yemen
- Rebel Group: Houthi Rebels (ATGM offensive tactical actions)
- Weapon System: ATGM (Unknown)
- Weapon Systems Location: Elevated
- Target(s): Saudi Arabian Army (Raid)—1st "Access Point," 2nd Simple Battle Position (fixed structure), 3rd Tracked Vehicle, Shots were fired over an unknown time period.
- Missile Firing Time to Target: UNK
- Endstate: 1 burning vehicle; 1 fighting position burning and 1 position with unknown damage

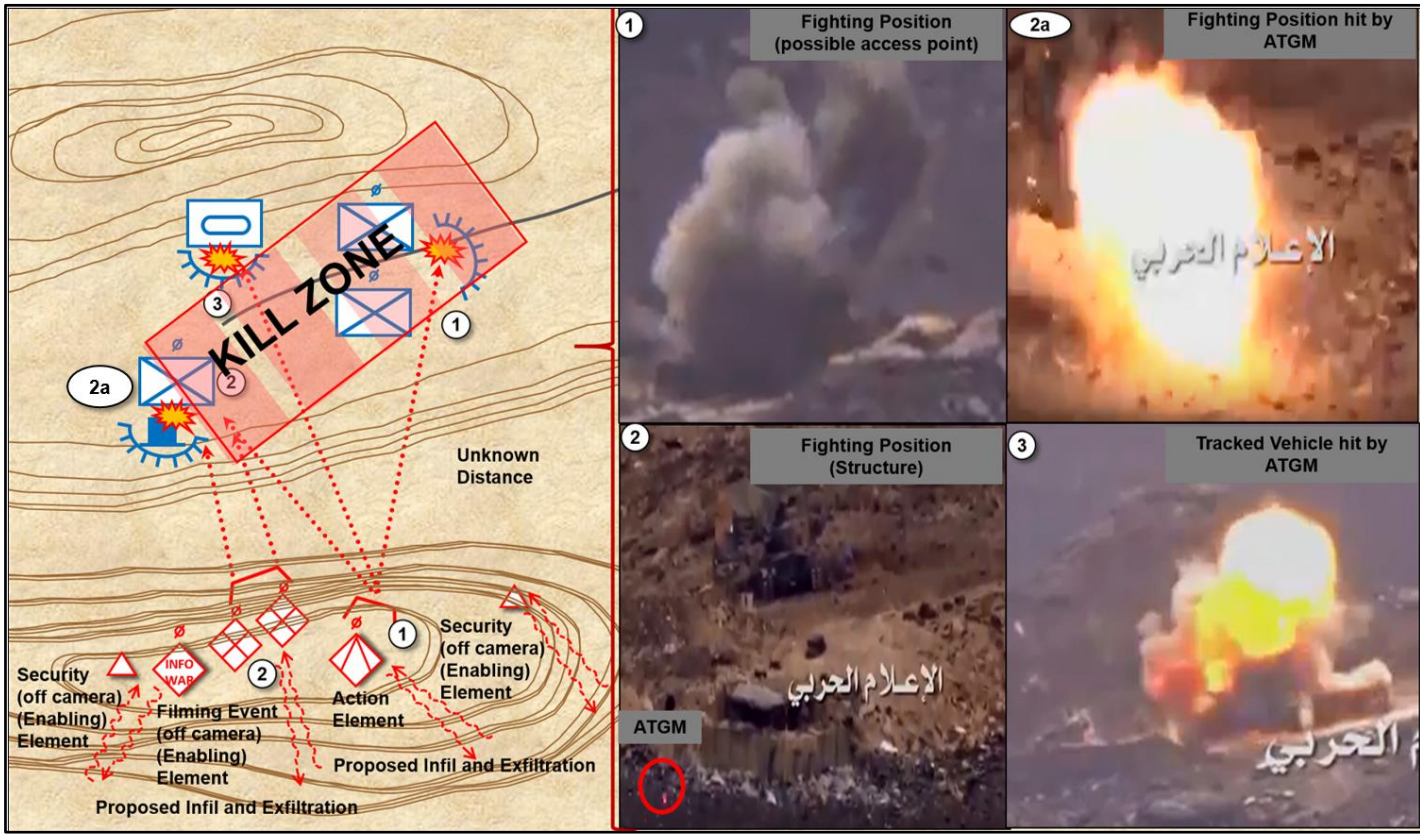


Figure 2. ATGM Raid diagram and video graphic

The video provides a good example of an ATGM as a versatile precision weapon against multiple types of targets. The US military and coalition forces may encounter a similar type of threat in future conflicts due to ATGM proliferation in the strategic environment. The ATGM's crew in the video appeared fairly proficient with the systems capabilities. The crew successfully hit three targets out of three ATGM missiles fired over different time periods, causing a wide range of damage.

The action element (rebels) within the video likely conducted reconnaissance and/or human intelligence gathering information about the outpost. Even though not witnessed on film, the rebels likely moved as a small hunter-killer team construct armed with small arms and multiple ATGMs. The teams moved to an elevated vantage point overlooking the outpost, which provided good line of sight for the engagements. For additional information on hunter-killer teams see TC

7-100.4 and its associated Threat Force Structure. (TC) 7-100.2 *Opposing Forces Tactics* discusses the tactics of hunter killer teams that can be duplicated for the training community.

The outpost's isolated position (with a steep drop off facing the target) on a hill capitalized on the ATGM's range for the rebels' tactical action element to engage multiple targets from a relatively safe standoff distance from an elevated position on different hilltop. The terrain also prevented the rapid deployment of a vehicle QRF to interdict the rebels' position or to support the outpost. The rebels also appeared to wait until Soldiers reinforced their fighting position with more ammo before targeting the second fighting position with another ATGM. The priority of targeting was the following:

1. The Saudi soldiers' access point (which appeared to be vehicles)
2. The simple battle position
3. The tracked vehicle

It is unclear why the rebels choose this targeting sequence. It could be hypothesized that this action was taken to further isolate the outpost and decrease the remaining forces' mobility. It could be argued that the small arms fire after the first ATGM launch was to "fix" the Soldiers in the fighting positions to follow on with another ATGM missile.

Table 1. OPFOR tactical task drill: Raid

TACTICAL TASK 2.0 RAID		
No.	**Scale**	**Measure**
01	Yes/No	Unit infiltrates without detection.
02	Yes/No	Unit isolates enemy from assistance.
03	Time	To seize or destroy raid target.
04	Time	To extract/exfiltrate.
05	Percent	Of friendly forces available to continue mission.

OPFOR Implications and Training Support

The OPFOR Tactical Task List formally consisted of 24 OPFOR-specific tactical tasks (such as raid or ambush), which are similar in theory to the US Army's Universal Task List but unique to the OPFOR. The OPFOR Tactical Task list can be found in Appendix B of TC 7-101, *Exercise Design.* The rationale for these 24 distinctive tasks for the OPFOR is to reduce mirror imaging and to provide challenging conditions for the spectrum of the training community. The following defines the tactical task *raid* that has been taken directly from appendix B of TC 7-101, *Exercise Design.* The OPFOR Tactical task list has been recently updated.

UPDATE: OPFOR Tasks in US Army Combined Arms Training Strategies (CATS)
Several OPFOR tasks in TC 7-101 have been updated as of March 2017 to 17 tasks and drills. These updated tasks are posted in CATS. See the special bulletin in this newsletter at p. 30 for an easy 1-2-3 sequence of how to find, with common access card entry, updated OPFOR tasks in CATS. As outdated OPFOR tasks are gradually removed from CATS to support the new "Objective T" charter, current OPFOR tasks have a task number in parentheses of (71-CO-85xx). The last two numerical digits identify the specific OPFOR task number.

Figure 3. Update to OPFOR Tasks in US Army Combined Arms Training Strategies (CATS)

Tactical Task 2: Raid[3]

A raid is an attack against a stationary target for the purposes of its capture or destruction that culminates in the withdrawal of the raiding detachment to safe territory.[4] Raids can also be used to secure information and to confuse or

deceive the enemy. The keys to the successful accomplishment of any are raid surprise, firepower, and violence.[5] The raid ends with a planned withdrawal upon completion of the assigned mission. The subtasks for raid are the following:[6]

INFILTRATE

- Conduct undetected movement through and/or into an area occupied by enemy forces to occupy a position of advantage.

ISOLATE

- Maneuver and deploy security element(s) to ensure additional enemy forces do not join the battle unexpectedly. (Security elements may become fixing elements.)
- Continue to provide early warning.
- Prevent the enemy from gaining further information.
- Prevent enemy maneuver.

SEIZE OR DESTROY

- Attack to destroy or seize personnel or equipment.

EXFILTRATE

- Conduct undetected movement from areas under enemy control by stealth, deception, surprise, or clandestine means.

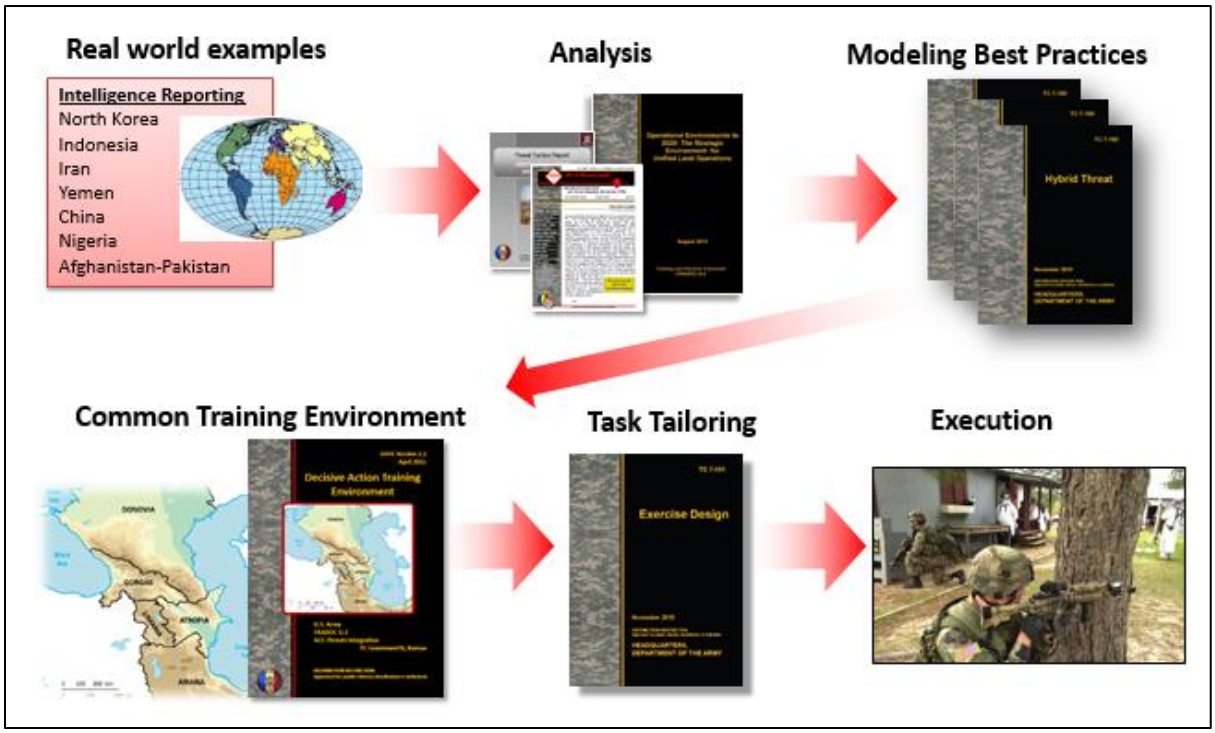


Figure 5. ACE-TI's Support Products to the Training Community

OPFOR Replications and Training Support

The Yemeni attack video depicts an ATGM raid on an isolated outpost that demonstrates the connectivity between real world examples and the OPFOR used in US training. This type of tactical action represents a real-world threat and a formidable challenge for training or deploying units. The considerable ranges on many modern ATGMs in a dual-use role provide a potential threat for commanders and unit staffs to consider in decision making and force protection issues. Combat Training Center (CTC) scenario developers and home station trainers can find additional information on ATGM units, organization, or weapons systems in TC 7-100.4, its associated Threat Force Structure, and the Worldwide Equipment Guide (WEG). These type of real-world examples are key for the training community to include into scenario development and training.

References

Headquarters, Department of the Army. Training Circular 7-100.2, Irregular Opposing Forces. TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. August 2011.

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

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

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

Notes

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

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

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

[4] US Department of the Army. Training Circular 7-100.2, Opposing Force Tactics. 9 December 2011 Pg 3-38.

[5] Headquarters, Department of the Army. Training Circular 7-100.2, Irregular Opposing Forces. TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. August 2011.

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

***Note*: The current 17ea tasks have a collective task number with the following sequence (71-CO-85xx). The last two numerical digits are the specific task number 01 through 17.**

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

The nemesis of Syrian Arab armor

At the outset of the present civil war in Syria, Free Syrian Army (FSA) rebels had access to only a limited number of anti-tank guided missiles (ATGM), mostly appropriated from the inventories of Bashar al Assad's Syrian Arab Armed Forces (SAA). The meager casualties initially inflicted by Russian-made 9M113 Konkurs and 9K115-2 Metis-M ATGMs that had fallen into FSA hands at first presented no insurmountable problem to Bashar al Assad's army, which absorbed the losses and overwhelmed its adversaries with the shock, firepower, and mobility typically associated with seasoned armored forces.[1] That began to change shortly after the second battle of Idlib in April 2015, when the rebels successfully used ATGMs to destroy about 40 SAA main battle tanks (MBT). Clearly, the arrival of ever-increasing numbers of coalition-supplied 9M113 Konkurs; HJ-8 Red Arrow; and BGM-71 tube-launched, optically tracked, wire-guided (TOW) ATGMs in the theater of operations was beginning to translate into daunting tank losses for the Syrian Arab Army.[2] Despite the logistical limits of their availability in the Syrian operational environment (OE), these ATGM weapons were widely considered to be the nemesis of Syrian armored vehicles, and produced a predictable effect on SAA combat effectiveness and soldiers' morale.

As the regime's leadership sifted through the possible courses of action to alleviate the unacceptably high attrition rates for its armored forces, the Syrian high command hit upon the idea of developing a jamming device capable of interdicting the flight paths of adversary semi-automatic command line of sight (SACLOS)-guided ATGMs. The eventual outcome of this effort was a family of soft-kill weapons serially fielded as the Sarab (Arabic for Mirage) 1, 2 and 3. Essentially this system employs an Infrared jammer and/or laser technology designed to disrupt SACLOS guided missiles commonly found in the Syrian theater of operations.[3] This article assesses the evolution and fielding of the Sarab family of soft-kill weapons, the recent impact of these weapons on the Syrian operational environment, and the potential implications of soft-kill weapons for future OEs.

The Syrian Scientific Studies and Research Center (SSRC)

The agency that developed this ATGM-defeating system—the Syrian Scientific Studies and Research Center (SSRC)—was originally established in 1969, at the height of the Cold War, under the regime then headed by Bashar al Assad's father, Hafez al Assad. The SSRC's purpose is "to advance and coordinate scientific activities in Syria."[4] Although ostensibly independent from other government agencies, some Western analysts "believe the SSRC to be linked to the [country's] military establishment, where it is allegedly responsible for new research and development [R&D] of nuclear, biological, chemical, and missile-related technology."[5] The SSRC is also "considered…the best-equipped research center in Syria, possessing better technical capacity and equipment than the four Syrian universities."[6]

The SSRC's formal ties to the Syrian military date to October 1993, when a presidential decree mandated an upgrade of its respective departments to research institute status. The same directive elevated the SSRC's director general to ministerial rank in the Syrian cabinet. Most importantly, the decree stipulated that henceforth the Syrian president "would appoint members to the board of the SSRC, as well as its technical staff."[7]

In 2005, five years after Bashar al Assad succeeded his father to the Syrian presidency, US President George W. Bush placed the SSRC on the US Treasury Department's Specially Designated Nationals List by issuing Executive Order 13382: "Blocking Property of Weapons of Mass Destruction Proliferators and their Supporters."[8] By that time the Treasury Department had identified the SSRC as the "Syrian government agency responsible for developing and producing non-conventional weapons and the missiles to deliver them."[9] Recently the SSRC made headlines that both shocked the world and once again garnered the negative attention of the Treasury Department's Office of Foreign Assets Control. The latter recently imposed "one of the largest sanctions actions in its history," a penalty levied in response to "the April 4, 2017 sarin [gas] attack on innocent civilians in Khan Sheikhoun, Syria by the regime of Syrian dictator Bashar al-Assad."[10]

Infrared countermeasure (IRCM) technologies on the modern battlefield

Based on the agency's demonstrated and highly visible track record for developing and producing non-conventional weapons and the means to deliver them, it is hardly surprising that Assad's Syrian Arab Army turned to the SSRC to help meet its pressing ATGM challenge. Infrared countermeasure (IRCM) technologies have been present on the battlefield since the early 1990s, when US and allied forces deployed to the First Gulf War, Bosnia, and Kosovo. In 2011, an analyst writing for a monthly magazine specializing in laser, photonics, and opto-electric technologies observed, "An infrared countermeasure—a device designed to prevent a heat or plume-seeking missile from reaching its target—generally consists of a flare, laser, or other bright illumination source and optics combination that when placed on an aircraft or marine craft, confuses a missile's target acquisition system…. Today, IRCM systems are standard equipment for most military aircraft."[11] Meanwhile the same technologies were evolving in a direction that enabled their application in a ground combat role. Israeli Defense Forces first employed this capability in Lebanon during the 1990s.[12] IRCMs that are designed primarily to neutralize incoming enemy ordnance by disrupting electronic navigation systems—as opposed to directly striking enemy targets—are considered "soft kill" weapons. Because the countermeasure essentially accomplishes the same end result as a hard kill system, however—namely destruction of the enemy target—it is considered an active protection system.

By 2005, Russian T-90 MBTs were rolling off the production line equipped with a SHTORA-1 Active Defense System. Besides mounting hard-kill laser-homing weapons to engage incoming targets, the SHTORA protects the tank against SACLOS guided missiles by generating an IR signal and laser beam rider that mimics the flare on the back of incoming missiles.[13]

Figure 1. Sarab-1 mounted on a "tactical"

This kind of integrated defense system—built into the design of a new (T-90) MBT tailored for use by a rapidly modernizing Russian army—was one thing; adapting something akin to the SHTORA system to legacy Russian T-72s, T-62s, and even T-55s still present in large numbers in the Syrian OE was more problematic. Still, since Russia has long been an ally of Syria in the Middle East, it is possible if not probable that SSRC researchers were able to tap into evolving Russian R&D SHTORA technology during their efforts to overcome the Free Syrian Army ATGM threat.

Mounting armored casualties and the necessity of avoiding prohibitive R&D costs combined to create an overriding need to field large numbers of an

effective ATGM defense system in the shortest possible period of time. The SSRC soon pursued the course of developing "an infrared jammer designed to disrupt the optical command [signals] used by second generation…SACLOS guided missiles."[14] Accomplishing this task required procuring TOW technology then in the almost exclusive possession of Syrian rebel forces. Accordingly, the Syrian regime's intelligence arm arranged to clandestinely purchase 18 TOW ATGMs from Free Syrian Army sources.[15] These weapons provided the SSRC the means to validate its findings through testing against an adversary's weapons system. The outcome of this process was an operational active defense system designated the Sarab-1.

A new family of soft-kill systems

The first tranche of this system made its appearance in Latakia Province in early 2016. Mounted on tacticals (i.e. gun-carrying pickup trucks), T-62s, and miscellaneous other tracked, wheeled, and towed vehicles/weapons in more or less ad hoc fashion, the Sarab-1 used powerful light-emitting diode (LED) lights and magnifying lenses that offered formidable protection against their adversaries' ATGMs. Based on battlefield testing conducted in the Khanaser District in southern Aleppo Province as well as engagements in Latakia Province, the Sarab-1 was found to be over 80% effective against all SACLOS ATGMs (see Figure 1, above). Based on that determination, the Syrian Ministry of Defense directed large-scale production of the system in tandem with a concurrent effort to develop future upgrades. Thus within a fairly short timeframe and at relatively low cost, the SSRC transitioned from a theoretical R&D venue to a practical battle-tested protection system.[16]

The need for additional R&D to occur simultaneously with large-scale production of the Sarab-1 underscored some of the system's initial drawbacks. Since its emitters could only cover a frontal arc for defense, the Sarab-1 was incapable of slewing to provide 360 degree protection. Another disadvantage involved a run-time restricted to only about six hours, a limitation imposed by the system's power source: most often a vehicle battery. Toward the end of 2016, Syrian soldiers received delivery of the promised upgrade: Sarab-2. "The Sarab-2 improved over the first generation by using multiple emitters that could mimic the vertical movement [of ATGMs]."[17] In addition, the Sarab-2's design reduced power consumption, allowing the system to operate for about 10 hours between battery re-charges. Finally, the Sarab-2 came enclosed in a protective casing to enhance its battlefield survivability.[18]

Figure 2. Sarab-2 mounted on a Syrian T-72 toward the end of 2016

In mid-December 2016, as the battle of Aleppo wound down, it became clear that the Sarab-2 had rendered effective service to Bashar al Assad's army. "According to Syrian sources, the Sarab-2 was completed and successfully deployed in the battle of Aleppo, effectively defeating the Free Syrian Army (FSA) TOWs."[19] The same sources claimed that in the later stages of the battle, SAA tanks ranged Aleppo's streets with impunity because they were virtually immune to FSA ATGM threats, and forced FSA fighters to direct their fire exclusively at infantry and non-armored targets (see Figures 2, 3, and 4).[20]

Despite its more advanced features, protective casing, and extended battery operating life, the Sarab-2 still could cover only a frontal arc facing the enemy of about 180 degrees. Following the successes scored at year's-end 2016, the SSRC fielded a third generation soft-kill weapon—the Sarab-3—equipped with additional emitters (possibly including laser power sources) to provide still more active protection for tanks and other armored vehicles. This newest version featured a full 360 degree slew capability (see Figure 5).[21]

Survivability in a multi-domain environment requires an ability to detect and outmaneuver an opponent before friendly units can be detected, acquired, and destroyed by an enemy force. Neutralizing an adversary's weapons systems does not always require superior munitions or heavier armor. At times the same effect can be achieved by frustrating an opponent's

Figure 3. A close-up view of the Sarab-2 system, featuring stacked IR diodes and protective shield

ability to gather and process information that guides munitions to their intended targets. A naval warfare analyst writing for the United Kingdom (UK) *Defence Journal* argues that "this ability to disrupt an opponent's ability to actively engage you is a hugely important capability…. The reason [such capabilities] are not taken into consideration by the casual observer is because of a failure…to realize that not all weapons systems actually fire anything."[22] The same observer stated the obvious in adding, "modern warfare is in some ways a lot more complex than it used to be, when [an] engagement was decided purely on the size and number of its guns and the competence and bravery of [a ship's] crew. Those days are gone forever."[23] The SSRC appears to have applied a similar logic to engagements between tanks and ATGMs: the ATGM-defeating weapons systems did not actually fire anything, and instead relied on IRCM and laser technologies to defeat weapons furnished by backers of the Free Syrian Army.

Figure 4. SAA armor and infantry in downtown Aleppo

Relevance to Threat Doctrine/Training Applicability

The SSRC's development, deployment, and proliferation of the Sarab family of soft-kill defense systems provides a real-world example of "Electro-optical and other systems defeated by obscurants," covered in Table 13-1 of TC 7-100.2, *Opposing Force Tactics*.[24] As the table explains, such obscurants can "counter or degrade…use of IR band illumination—including spotlights, flares, and night vision systems."[25] The continuing back-and-forth of evolving armor/anti-armor capabilities between adversary proxies in the Syrian OE relates to the concept of opposing force (OPFOR) "survivability activities [that can be implemented] when fighting a more powerful opponent."[26] First on a list of examples of unique engineer measures to enhance OPFOR survivability are "screening, protective, and C3D [command, cover, concealment, and deception] techniques…to passively deny the enemy the ability to acquire OPFOR positions for targeting."[27] This, essentially, is what Assad's Syrian Arab Army was able to do throughout 2016 through an R&D project that significantly contributed to the FSA's defeat in the Battle of Aleppo.

In those waning days of 2016, the results of a recent presidential election and its attendant controversies seized first place in US media coverage, and tended to eclipse other major events unfolding on the world stage. Most domestic coverage of the Syrian conflict predictably focused on the human tragedy that accompanied the debacle in Aleppo. Yet somewhere in

Figure 5. Sarab-3 system with 360 degree slew capability, stacked IR light sources, and possibly laser diodes

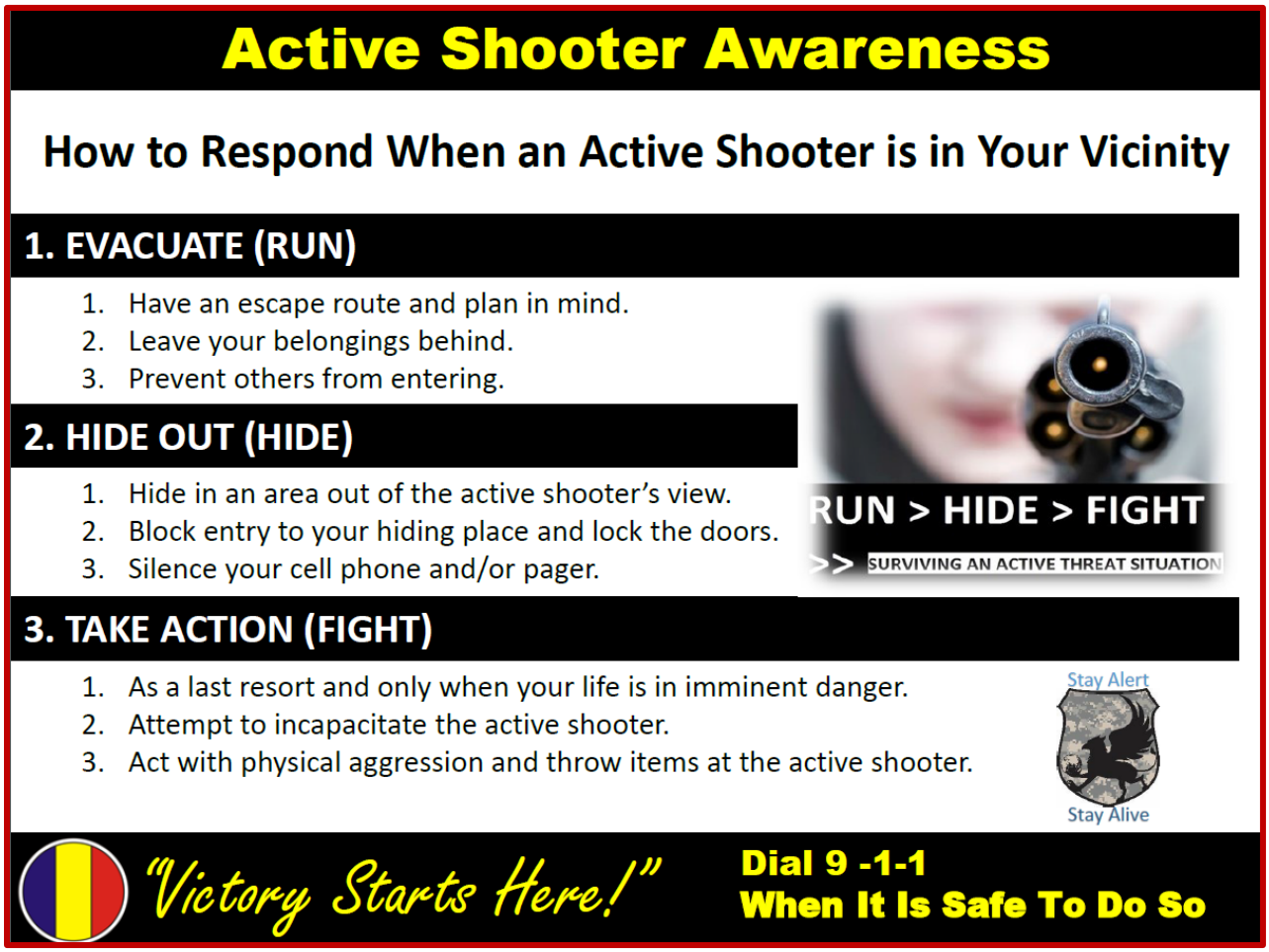
the mix a major backstory was inadvertently obscured: the chronicle of how a think tank sponsored by the Syrian high command undermined the technological edge of a superpower to achieve a tactical if not strategic victory in an unglamorous slugging match that pitted ATGMs against Cold War-era armor. Chapter 4, "Main Battle Tanks," of Volume 1 of the 2016 *Worldwide Equipment Guide* is instructive in placing this episode of the Syrian Civil War in context; it addresses the three functional categories that are used to gauge overall MBT effectiveness: mobility, survivability, and lethality, and defines survivability as "the aggregate of protective measures which allow the MBT to complete its mission."[28] Among these measures are "obscurant systems" that "include methods for reducing detection by optical, infrared, and radar technologies."[29] In developing the Sarab family of soft-kill systems, the SSRC essentially reverse engineered both US and Russian ATGM technologies, then selectively repurposed an existing ATGM defense system—the SHTORA-1—for use with legacy weapons commonly found in the Syrian OE.

Worthwhile lessons are embedded in developments that occurred within the Syrian OE throughout 2016. As explained in the Introduction to TC 7-100.2, "the nature of real-world OEs and potential OEs is extremely fluid, with rapidly changing regional and global relationships…the OEs change…. Therefore, the nature of the COE for training is [also] adaptive and constantly changing. As the Army applies the lessons learned from training, the OPFOR and potential real-world adversaries will also learn and adapt."[30] The SSRC's use of the black market as a conduit for procuring world class weaponry furnishes an apt example of such adaptation. Just as the SAA found work-arounds to neutralize the effects of superior ATGM technologies possessed by the FSA, it is highly likely that future deployments will again witness frenetic enemy R&D surges intended to attrit and degrade the technological advantages of the US and its allies. Developments similar to those recently seen in the Syrian OE are likely to recur. When that happens, commanders and staffs at tactical and operational levels need to be ready.

Notes

[1] Within Syria: About the Syrian Arab Army. "Sarab 1, 2 & 3 Active Protection System." 26 February 2017.
[2] Within Syria: About the Syrian Arab Army. "Sarab 1, 2 & 3 Active Protection System." 26 February 2017.
[3] Tamir Eshel. "Home Grown Syrian Soft Kill System Successfully Defeated TOW Missiles." Defense Update. 1 March 2017.
[4] Nuclear Threat Initiative. "Scientific Studies and Research Center." 1 March 2011.
[5] Nuclear Threat Initiative. "Scientific Studies and Research Center." 1 March 2011.
[6] Nuclear Threat Initiative. "Scientific Studies and Research Center." 1 March 2011.
[7] Nuclear Threat Initiative. "Scientific Studies and Research Center." 1 March 2011.
[8] Nuclear Threat Initiative. "Scientific Studies and Research Center." 1 March 2011.
[9] Nuclear Threat Initiative. "Scientific Studies and Research Center." 1 March 2011.
[10] US Embassy in Damascus. "Treasury Sanctions 271 Syrian Scientific Studies and Research Center Staff in Response to Sarin Attack on Khan Sheikhoun." 24 April 2017.
[11] Gail Overton. "Photonics Applied: Defense: IR Countermeasures Aim For Safer Flights." Laser Focus World. 1 August 2011.
[12] Tamir Eshel. "Home Grown Syrian Soft Kill System Successfully Defeated TOW Missiles." Defense Update. 1 March 2017.

[13] Defense Update. "SHTORA -1 Active Defense System." 12 October 2005; US Army, Training and Doctrine Command (TRADOC) G-2 Analysis and Control Element (ACE) Threats Integration. Worldwide Equipment Guide—Volume 1: Ground Systems. December 2016.
[14] Tamir Eshel. "Home Grown Syrian Soft Kill System Successfully Defeated TOW Missiles." Defense Update. 1 March 2017.
[15] Tamir Eshel. "Home Grown Syrian Soft Kill System Successfully Defeated TOW Missiles." Defense Update. 1 March 2017.
[16] Within Syria: About the Syrian Arab Army. "Sarab 1, 2 & 3 Active Protection System." 26 February 2017; Tamir Eshel. "Home Grown Syrian Soft Kill System Successfully Defeated TOW Missiles." Defense Update. 1 March 2017; Arthur Dominic Villasanta. "New Syrian Army Infrared Jammer Protects Tanks vs TOW and Other ATGMs." China Topix. 2 March 2017.
[17] Tamir Eshel. "Home Grown Syrian Soft Kill System Successfully Defeated TOW Missiles." Defense Update. 1 March 2017.
[18] Tamir Eshel. "Home Grown Syrian Soft Kill System Successfully Defeated TOW Missiles." Defense Update. 1 March 2017.
[19] Tamir Eshel. "Home Grown Syrian Soft Kill System Successfully Defeated TOW Missiles." Defense Update. 1 March 2017; Laila Bassam, Angus McDowall, and Stephanie Nebehay. "Battle of Aleppo Ends After Years of Bloodshed With Rebel Withdrawal." Reuters. 13 December 2016.
[20] Tamir Eshel. "Home Grown Syrian Soft Kill System Successfully Defeated TOW Missiles." Defense Update. 1 March 2017.
[21] Tamir Eshel. "Home Grown Syrian Soft Kill System Successfully Defeated TOW Missiles." Defense Update. 1 March 2017.
[22] Kieran Locke. "In Defence of Soft-Kill Defences." UK Defence Journal. 22 April 2014.
[23] Kieran Locke. "In Defence of Soft-Kill Defences." UK Defence Journal. 22 April 2014.
[24] 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. Pg. 13-18.
[25] 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. Pg. 13-18.
[26] 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. Pg. 12-30.
[27] 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. Pg. 12-30.
[28] US Army, Training and Doctrine Command (TRADOC) G-2 Analysis and Control Element (ACE) Threats Integration. Worldwide Equipment Guide—Volume 1: Ground Systems. December 2016.
[29] US Army, Training and Doctrine Command (TRADOC) G-2 Analysis and Control Element (ACE) Threats Integration. Worldwide Equipment Guide—Volume 1: Ground Systems. December 2016.
[30] 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. Pg. xv.



What ACE Threats Integration Supports for YOUR Readiness

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

ACE Threats Integration POCs

DIR, ACE Threats Integration	Jon Cleaves	jon.s.cleaves.civ@mail.mil 913-684-7975
Dep DIR & DATE	DAC Angela Williams	angela.m.williams298.civ@mail.mil -7962
Intel OPS Coordinator	DAC Nicole Bier	nicole.n.bier.civ@mail.mil DSN:552 -7907
Intell Specialist	DAC Dr. Jon H. Moilanen	jon.h.moilanen.civ@mail.mil -7928
UK LO to ACE-TI	WO2 Danny Evans	daniel.j.evans92.fm@mail.mil -7994
Threats Officer	LTC Bryce Frederickson	bryce.e.frederickson.mil@mail.mil -7930
Threats Officer	CPT Frank Reyes	francisco.j.reyes6.mil@mail.mil -7991
Threats Officer [Replacement Programmed]		
Threat Models	DAC Jerry England	jerry.j.england.civ@mail.mil -7934
Threat Tactics Course	DAC Kris Lechowicz	kristin.d.lechowicz.civ@mail.mil -7922
Training-Edu-Ldr Dev	DAC Walt Williams	walter.l.williams112.civ@mail.mil -7923
Threat Analysis	CGI Brian Allen	brian.d.allen44.ctr@mail.mil -7948
Threat Analysis	IDSI Dr. Jim Bird	james.r.bird.ctr@mail.mil -7919
Threat Analysis	BMA Rick Burns	richard.b.burns4.ctr@mail.mil -7987
Worldwide Eqmt Guide	BMA John Cantin	john.m.cantin.ctr@mail.mil -7952
Thr Analysis & Editing	CGI Laura Deatrick	laura.m.deatrick.ctr@mail.mil -7925
Threat Analysis	CGI Jay Hunt	james.d.hunt50.ctr@mail.mil -7960
ACE-TI LO to MCTP	BMA Pat Madden	patrick.m.madden16.ctr@mail.mil -7997
Threat Analysis	CGI Mike Marsh	michael.g.marsh3.ctr@mail.mil -7897
Threat Analysis	CGI Brad Marvel	bradley.a.marvel.ctr@mail.mil -5963
Threat Analysis	CGI Dave Pendleton	henry.d.pendleton.ctr@mail.mil -7946
ACE-TI LO to JRTC/JMRC	CGI Mike Spight	michael.g.spight.ctr@mail.mil -7974
Threat Analysis	CGI Jamie Stevenson	james.e.stevenson3.ctr@mail.mil -7995
Threat Analysis	CGI Wayne Sylvester	vernon.w.sylvester.ctr@mail.mil -7939
ACE-TI LO to NTC	ThreatTec Marc Williams	james.m.williams257.ctr@mail.mil -7943