Red Diamond
Threats Newsletter

TRADOC G-2 Operational Environment Enterprise
ACE Threats Integration

Fort Leavenworth, KS | Volume 7, Issue 06 | JUN 2016

INSIDE THIS ISSUE

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

Send suggestions to:
ATTN: *Red Diamond*
Jon H. Moilanen (IDSI Ctr), Operations, ACE-TI
and
Laura Deatrick (CGI Ctr), Editor, ACE-TI
and
Angela McClain-Wilkins, Guest Editor (DAC)

2016 THREAT TACTICS COURSE ENROLLMENT NOW OPEN!

by **Kristin Lechowicz**, TRADOC G-2 ACE Threats Integration (DAC)

ACE-TI is currently taking enrollment for the fall offering of the Threat Tactics Course (TTC) at Fort Leavenworth, tentatively scheduled for 15–19 August 2016. The course topics are beneficial for S-2/G-2 sections by enabling them to understand and describe the threat in the real world or training exercises. They are also vital to a wide audience throughout the training community, to include scenario developers at the combat training centers and home-station training planners.

The course provides a 40-hour block of instruction based on the Training Circular (TC) 7-100 series of products on opposing force doctrine. Instructors define and explain threat concepts and functional tactics; operational environment variables; hybrid threat in complex and persistent conflict; threat actors, including regular and irregular forces and elements; offensive and defensive tactics and techniques; and emerging threats. The course consists of a number of classes on the hybrid threat's methodology taken from real-world examples. It also introduces students to the Decisive Action Training Environment, which is an integral part of the course, particularly in the capstone practical exercise. Instructional methodologies included lectures, videos, discussions, and practical exercises. The course includes doctrinal presentations, OPFOR role-playing, and table-top or computer-assisted practical exercises.

For information about course offerings or to request an MTT, contact Kristin Lechowicz at (913) 684-7922 or kristin.d.lechowicz.civ@mail.mil.

RED DIAMOND TOPICS OF INTEREST

by **Jon H. Moilanen**, TRADOC G-2 ACE Threats Integration, Operations, *Red Diamond* Newsletter (IDSI Ctr)

This issue of *Red Diamond* opens with an article on the April 2015 Afghan Taliban summer military operations in the north with a particular focus on Kunduz Province and its capital city, Kunduz. Over a period of months, the Taliban encircled Kunduz City and easily captured it. The fall of the city represented the biggest military victory for the Taliban since 2001.

A farewell article by the inaugural British Foreign Liaison Officer to TRADOC G-2 ACE Threats Integration (ACE-TI) recalls the last two and a half years at Fort Leavenworth as the main effort of liaison between the British Collective Training Group and TRADOC G-2 has been to support the decisionmaking process for the British Army's validation and subsequent implementation of the Decisive Action Training Environment (DATE).

An article on crime in current OEs reviews recent Russian military incursions in Eastern Ukraine and Crimea and assesses crime groups masquerading as pro-Russian separatist and local militias.

Information warfare (INFOWAR) in the 8 May 2016 Cairo ambush and the October 2015 downing of Russian Metrojet Flight 9268 share an ISIL-SP controlled narrative. The two attacks described in this article demonstrate how terrorism in Egypt is in an evolutionary process to align with overarching ISIL objectives.

Another article examines the opposing force (OPFOR) antilanding operations (ALO) tactical task from Training Circular (TC) 7-100.2, *Opposing Forces Tactics*, and the OPFOR tactical task list from appendix B of TC 7-101, *Exercise Design*. It compares the OPFOR ALO doctrine to a video derived from the ongoing Syrian conflict.

The last article presents an example for US Army training of opposing force (OPFOR), as described in the US Army Training Circular (TC) 7-100 series, and representing the realistic, robust, and relevant types of regular and irregular threats and actions currently observed in Russian regular military and irregular forces and surrogates in OEs such as Ukraine, the Russian Federation, and the Middle East**.** These OPFOR actions and other conditions will be incorporated in the fiscal year 2017 update of US Army Training Circular 7-100.2.

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

Dr. Jon H. Moilanen (IDSI Ctr)
TRADOC G-2 ACE Threats Integration, Operations
jon.h.moilanen.ctr@mail.mil

More on the *Threats Tactics Course* TTC—Coming 15–19 AUGUST 2016

The course is open to a wide spectrum of students, including contractors, government employees, and military personnel—both US and foreign. There are currently 25 seats remaining. The graduates from the course receive a certificate from ACE-TI. The TTC block of instruction is also offered as a mobile training team (MTT) product, provided that instructor travel costs are funded by the hosting unit**.**

The Taliban Capture of Kunduz City

by **Rick Burns**, TRADOC G-2 ACE Threats Integration (BMA CTR)

In April 2015, the Afghan Taliban began its summer military operations in the north with a particular focus on Kunduz Province and its capital city, Kunduz. Over a period of months, the Taliban encircled Kunduz City and easily captured it on Monday, 28 September 2015. The fall of the city represented the biggest military victory for the Taliban since 2001. It also boosted the Taliban's information warfare campaign, lending credibility to the recently-installed head of the Taliban, Mullah Akhtar Mohammad Mansour, as one who can deliver victory to the Taliban.[1] This article details the fall of Kunduz City to the Taliban. A forthcoming Tactical Action Report: *Kunduz, Afghanistan*, will provide a more detailed analysis of the attack and the subsequent retaking of Kunduz by Afghan security forces, supported by NATO-led Resolute Support assets.

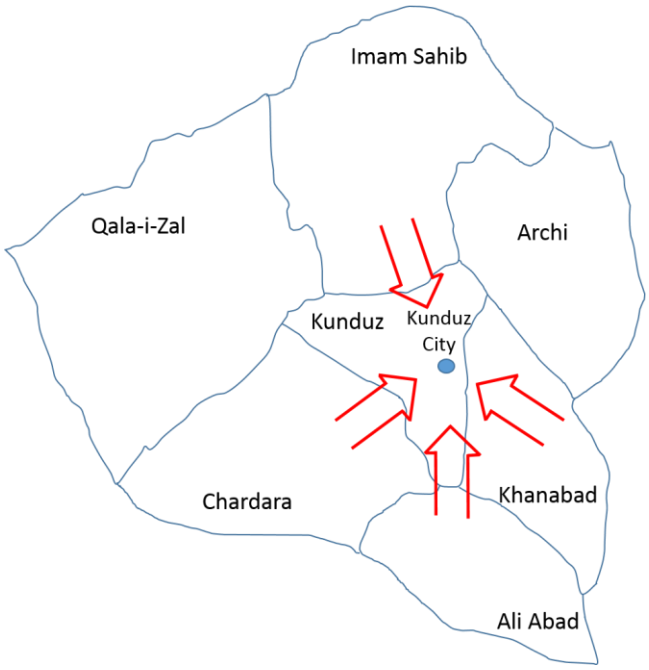


Figure 1. Taliban attack routes

Kunduz Province is one of the wealthiest in Afghanistan. With a population estimated at just under 225,000, the capital and fifth-largest Afghan city, Kunduz City, is on a major international trade route, with Pakistan, Iran, and Tajikistan as its primary international trading partners. It is also the closest provincial capital to the Tajikistan Shir Khan border crossing, an entry into Central Asian markets.[2] In addition, the city is the hub for trading routes throughout Afghanistan.[3] Its geographic location makes Kunduz City a lucrative target for Taliban leaders.

Prior to the successful attack on Kunduz, the Taliban gained control of key ground surrounding the city. Through a deliberate effort, beginning in April 2015, Taliban forces secured almost all of the government's land supply routes into Kunduz City while maintaining control of their own supply routes. In April 2015, the Taliban captured Gortepa, an area composed of 40–50 villages extending northwest of Kunduz for about 15 kilometers. Bordered on either side by rivers, Gortepa connects Chardara and Qala-i-Zal districts. A decision by Afghan forces to not clear this region and only set up outposts to protect the city allowed the Taliban to thrive in this area.[4] Additionally, Taliban forces strengthened their hold on the surrounding Imam Sahib district to the northeast, Khanabad district to the southeast, and Ali Abad district to the south.[5]

On Monday, 28 September 2015, several hundred Taliban fighters conducted a dispersed attack on the city of Kunduz, defended by an estimated 7,000 Afghan security and militia forces.[6] Taliban elements attacked from positions of strength in the surrounding districts and quickly overwhelmed Afghan security forces. Previous Taliban attacks on urban areas had been limited to suicide attacks by individuals or small groups. The Taliban's well-organized attack on Kunduz and its intent on holding the city surprised the Afghan security forces and the Afghan government.[7]

The dispersed attack consisted of Taliban fixing, assault, and exploitation elements. For two days, the Taliban fixing elements blockaded around 200 Afghan security soldiers within the Bala Hisar hilltop fortress that overlooks the city, preventing them from supporting the town's defense. The Taliban finally forced the Afghan units to withdraw under pressure after running out of food and ammunition.[8] A Kunduz police spokesman stated the withdrawal occurred at about

1700 on 30 September with Afghan military, police, and intelligence cooperation and assistance. Taliban leaders offered amnesty to those who surrendered, but afterwards claimed all government military personnel had been killed during the attack.[9]

Taliban assault elements attacked from multiple directions. The attacks focused first on combat outposts, often referred to as checkpoints, which served as a defensive perimeter around the city. Some resistance continued as these outposts fell and government forces persisted in fighting within the city. Once the Taliban entered the city, it focused on civilian, government, and military infrastructure. Taliban fighters targeted the Médecins Sans Frontières (Doctors Without Borders) hospital, where they searched for possible wounded or hiding security personnel; police stations and other security-related buildings; the prison, from which they released inmates; and municipal and provincial government buildings.[10]

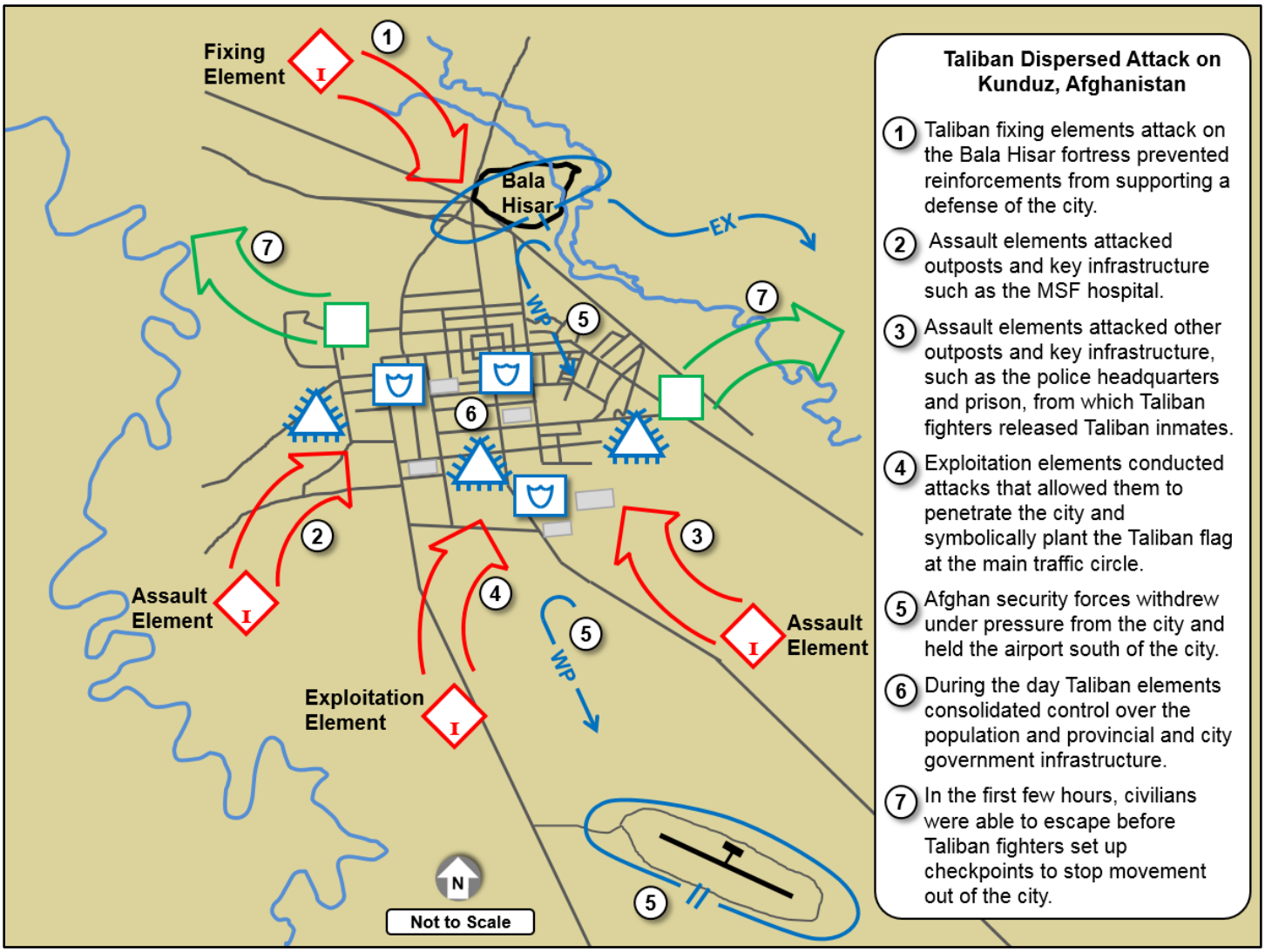


Figure 2. Taliban dispersed attack on Kunduz

Exploitation elements penetrated into the city and planted the Taliban flag in the central traffic circle, symbolically announcing the group's triumph over government security forces. There is also evidence of Taliban fighters infiltrating the city, hiding in homes, and disguising themselves in Afghan security uniforms ahead of the attack. Other reports indicate that citizens disenchanted with the government may have also joined Taliban fighters.[11] With insider information, Taliban fighters sought key government, military, police, intelligence, non-governmental organization (NGO), and other officials, particularly those deemed a threat to the occupation.[12] Taliban fighters took money from the Kunduz banks and seized

weapons and armed vehicles. Soon after occupying the city, they sought to control the population by setting up checkpoints to block civilians who were trying to leave the city, and instituting and enforcing rules.[13]

Despite being heavily outnumbered, Taliban fighters took control of the city with relative ease. Afghan security forces withdrew under pressure to the safety of the airfield south of the city. In the first few hours of the attack, many civilians, to include government officials and NGO workers, escaped the city as well. The Taliban quickly shut down escape routes through the use of checkpoints. Poor coordination and communication between Afghan security forces further facilitated Taliban control of the city by the end of the day.[14]

A number of lessons can be learned from the Taliban capture of a major Afghan urban area. An organized use of dispersed attack tactics with fixing, assault, and exploitation elements contributed to Taliban success. Taliban fighters spent weeks consolidating their control of the areas surrounding Kunduz City. Prior to the attack, the Afghan security forces chose to create a defensive perimeter around the city and failed to clear areas outside the main city, allowing Taliban fighters to thrive while building up their strength. The Taliban infiltrated the city with fighters who, prior to and during the attack, provided intelligence and facilitated success. Discontent with the government created other readily-available partisans. Neglect and poor communication and coordination on the part of the Afghan security forces leadership also factored into the Taliban success.

Notes

[1] Sune Engel Rasmussen. "Taliban Capture Key Afghan Provincial Capital." The Guardian. 28 September 2015.
[2] UN Habitat. "State of Afghan Cities Report." 2015.
[3] Rod Nordland. "Taliban End Takeover of Kunduz After 15 Days." The New York Times. 13 October 2015.
[4] Joseph Goldstein and Mujib Mashal. "Taliban Fighters Capture Kunduz City As Afghan Forces Retreat." The New York Times. 28 September 2015; Patricia Gossman. "Afghanistan: After Kunduz." The Diplomat. 16 December 2015.
[5] Borhan Osman. "The Fall of Kunduz: What Does it Tell Us about the Strength of the Post-Omar Taleban?." Afghanistan Analysts Network. 30 September 2015; Joseph Goldstein and Mujib Mashal. "Taliban Fighters Capture Kunduz City As Afghan Forces Retreat." The New York Times. 28 September 2015.
[6] For a description of a dispersed attack, see: Headquarters, Department of the Army. Training Circular 7-100.2, Opposing Force Tactics. TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. 9 December 2011. Paras 3-74 through 3-84.
[7] Rod Nordland. "Taliban End Takeover of Kunduz after 15 Days." The New York Times. 13 October 2015.
[8] BBC. "Taliban Tighten Grip on Afghan City of Kunduz." 30 September 2015.
[9] Hidayatullah Hamdard. "Security Forces Retreat from Kunduz City's Bala Hisar." Pajhwok Afghan News. 30 September 2015.
[10] Rod Nordland. "Taliban End Takeover of Kunduz After 15 Days." The New York Times. 13 October 2015; Ayaz Gul and Fern Robinson. "Taliban Seizes Kunduz, Afghanistan." Voice of America. 28 September 2015; Joseph Goldstein and Mujib Mashal. "Taliban Fighters Capture Kunduz City As Afghan Forces Retreat." The New York Times. 28 September 2015; Lynne O'Donnell. "The Taliban Takes over Kunduz." US News & World Report. 29 September 2015.
[11] Patricia Gossman. "Afghanistan: After Kunduz." The Diplomat. 16 December 2015; Rod Nordland. "Taliban End Takeover of Kunduz After 15 Days." The New York Times. 13 October 2015; Sune Engel Rasmussen. "Taliban Capture Key Afghan Provincial Capital." The Guardian. 28 September 2015.
[12] Patricia Gossman. "Afghanistan: After Kunduz." The Diplomat. 16 December 2015.
[13] Krishnadev Calamur. "The Fall of Kunduz." The Atlantic. 28 September 2015; Lynne O'Donnell. "The Taliban Takes over Kunduz." US News & World Report. 29 September 2015.
[14] Sune Engel Rasmussen. "Taliban Capture Key Afghan Provincial Capital." The Guardian. 28 September 2015.

by **WO2 Matthew Tucker**, TRADOC G-2 ACE Threats Integration (UK LO)

Having served for the last two and a half years at Fort Leavenworth as the inaugural British Foreign Liaison Officer to TRADOC G-2 ACE Threats Integration (ACE-TI), it is with sadness that I announce that my tour is soon to be over. This sadness is lessened by the knowledge that I am to be replaced by an equally capable warrant officer from the British Military Intelligence and that I will use the knowledge and experience I have gained in my new post as an observer, controller, and trainer at the Command and Staff Trainer in Catterick, England.

During my time at ACE-TI, I have been focused on the development of the Decisive Action Training Environment (DATE) and growing my understanding of threat portrayal using the Training Circular 7-100 Series. The main effort of my liaison between the British Collective Training Group and TRADOC G-2 has been to support the decisionmaking process for the British Army's validation and subsequent implementation of DATE. The last three years have witnessed the British Army evaluate DATE in the constructive and live environment to ensure that it meets our requirements for foundation training.

Figure 1. WO2 Tucker interacting with students during an offering of the Threat Tactics Course

During an extended trial, the British Army has conducted two division-level exercises with the 3rd UK Division (Exercise Iron Resolve 14 and Exercise Iron Resolve 15) and five brigade-level exercises that included the new Intelligence, Surveillance, and Reconnaissance Brigade. DATE has also been chosen as the training environment for use at the British Army Training Unit Suffield, the principal armored battlegroup training area located in Canada. All of the exercises conducted during the evaluation period were a success and reinforced the utility and scalability of DATE.

In a letter dated March 2016, British Commander of the Field Army (CFA) LTG Everard wrote to the TRADOC commander, informing him that DATE was being formally adopted across the Field Army. This decision delivers an army-wide unified approach to foundation training and a training environment that can meet the highest expectations and standards into the future. As close allies, the adoption of DATE reinforces the US-UK interoperability agenda and allows our armies to train together with greater familiarity and fewer logistical constraints. Overt training activities and agreements such as

the multinational use of DATE, synchronized with strategic messaging, provides a powerful deterrent effect on possible adversaries.

Foundation Training

A period of individual and collective training that allows units to achieve tactical competence on core equipments, usually culminating in combined arms field training.

British Army Field Manual, Volume 1, Part 7, Training (2013)

The success of both the British formal adoption of DATE and my tour in ACE-TI has been due to a lot of support from numerous organizations within the US Army. I would personally like to thank all those that have supported this mission, especially within the TRADOC Operational Environment Enterprise, but also officers from the Mission Command Training Program, the Joint Multinational Readiness Center, and the Combined Arms Center. The future will present many more opportunities for multinational integration across all aspects of training and provide a greater level of interoperability during deployed operations.

US Army-British Army Readiness with the Decisive Action Training Environment

TRADOC G-2 Analysis and Control Element (ACE-TI) welcomes Warrant Officer (WO) Danny Evans (UK) as the newly arrived British Foreign Liaison Officer (LNO) to G-2 ACE-TI. The continuation of this superb liaison in military intelligence and professional partnership builds on the foundational success of Warrant Officer Matthew Tucker during his over two years of UK LNO duty with us at Fort Leavenworth, Kansas. WO2 Tucker's personal presence, insights, and recommendations on the fidelity and utility of the *Decisive Action Training Environment (*DATE) were instrumental to British Collective Training Group validation of the DATE, and enabled British Army senior leader decisions to implement the DATE for British Army training conditions in support of army, joint, coalition, and allied operations.

WO2 Danny Evan's arrival as an LNO signals our mutual commitment to training excellence with challenging and realistic environmental conditions and opposing forces representative of actual regular and irregular threats in complex operational regions throughout the world today and into the near future.

Jon S. Cleaves Director, TRADOC G-2 ACE-TI

by **CPT Nickolas Zappone**, TRADOC G-2 ACE Threats Integration

Recent Russian military incursions in Eastern Ukraine and Crimea have spawned a resurgence of analysis aimed at our former Cold War foe. In that vein, this article will seek to illuminate an often-overlooked auxiliary employed as part of Russia's greater operational approach—crime groups masquerading as pro-Russian separatists and local militias. This article will first take a posterior look at the use of crime groups during previous conflicts in Georgia in 2008 and Crimea in 2014. It will then conclude with a discussion on the military implications for land force components. It is important to remember when digesting this article that, although criminal organizations are primarily concerned with power and profit, they may at times be affiliated with nation-state military and/or paramilitary actors.[1] Because of their high level of covert capability and operational reach into deep areas of the battlespace, opposing force special purpose forces are particularly adept at orchestrating criminal activity to help achieve military objectives and operational environment conditions via instability actions.

The 2008 Russo-Georgian War

The sinews between Russian intelligence services, such as the Main Intelligence Directorate (GRU), and the maelstrom of irregular forces and noncombatants within the operational environment perceptively follow the same contours, irrespective of which conflict is being analyzed. Hallmarks of Russian unconventional warfare include a slew of former KGB officers and ex-Soviet military officers; well-connected and inordinately-wealthy oligarchs; the stable of corrupt politicians, government administrators, law enforcement officers, and customs officials; seemingly-legitimate white-collar criminals; freelance hackers; and the expansive networks of local smugglers and crime groups.

The 2008 Russo-Georgian War is one example of how Russia has put these armed actors to use. In July 2008, approximately one month before Russia's invasion began in earnest, a series of bomb blasts and assassination attempts resulted in the death of an Ossetian village police chief and a South Ossetian citizen, and injury to the head of the pro-Georgian

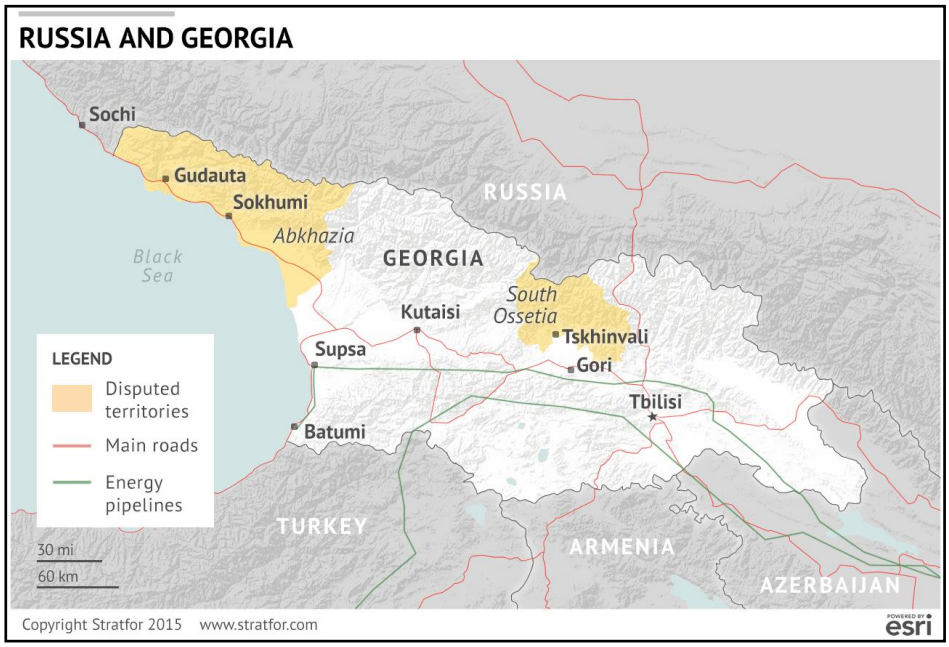


Figure 1: The breakaway regions of Abkhazia and South Ossetia

government in South Ossetia and five Georgian police officers.[2] The Georgian government blamed these attacks on Abkhaz organized crime groups, but these reports appear to be unverified.[3] This string of violent and provocative activity gave way to the intermittent cross-border shelling of checkpoints and villages in both South Ossetia and Georgia, followed by intense clashes between "paramilitary volunteers" from 2–4 August 2008 that eventually precipitated a full-scale conflict that began on 7 August 2008. It is difficult to say who was responsible for what amounts to deep direct action, but given the typical skill-set of criminals (namely murder and assassination), it is entirely plausible they were the perpetrators acting on orders from Russian GRU operatives that were deployed prior to the outbreak of the war and likely conducting deep reconnaissance operations.[4]

In order to visualize how Russia—specifically the GRU—leverages diverse criminal groups to its advantage, one must understand the symbiotic relationships that had been developed and nurtured prior to the onset of hostilities. The conclusion of the First South Ossetian War (1991–1992) was marked by a Russia-brokered ceasefire, which established "peacekeeping" units comprised of Russian, Georgian, and Ossetian forces.[5] The dissolution of the Soviet Union and fragmentation of its armed forces spawned an unprecedented era of military crime, corruption, and abuse of power and authority within the officer corps and military leadership. Access to, and demand for, highly-sought-after weaponry and military material provided the impetus for these quasi-military mafias to establish, maintain, and improve transnational smuggling networks.[6] On the one hand, Russian "peacekeepers" in the breakaway regions of Abkhazia and South Ossetia were the benefactors of Georgia's geographic location (strategically situated between Turkey, Iran, and the Middle East to its south and Russia to its north), their ability to pilfer military equipment, and the fact that these breakaway regions were in effect ungoverned spaces from which they could operate with impunity. On the other hand, corrupt local officials, indigenous security forces and customs officials "on the take," smugglers, and local crime groups were the benefactors of the illegal patronage networks that facilitated much of the economic activity (albeit highly illegal) brought into the impoverished region by the military mafia.

Figure 2: Abkhaz militiamen in the village of Chkhalta

Over time that nexus has most likely evolved, integrating unsavory characters from all sides of the equation. For example, tribal warlords such as Emzar Kvitsiani and his Monadire militia were ethnic Georgian Svans who resisted Abkhaz militias in the Upper Kodori Gorge before switching sides pursuant to the 2003 Rose Revolution that deposed Georgian President Eduard Shevardnadze. For years, Shevardnadze allowed local strongmen like Kvitsiani to operate their fiefdoms with little to no interference from the Georgian government, in return for political favor at the ballot box. Furthermore, Kvitsiani's enclave was exempt from paying taxes and Kvitsiani was allowed to operate his timber smuggling operation free and clear.[7] Clientelism between the two sides came to an abrupt end when Kvitsiani and his militia were labeled *persona non grata* by the new Georgian government after they refused to disarm and disband. In 2006, Kvitsiani and his militia were besieged during an operation spearheaded by Georgian special police forces and were forced to abscond. During the 2008 war, Russian and Abkhaz forces retook the gorge, and rumors that Kvitsiani's militia is back at the helm with the backing of the Russian military have begun to swirl.[8]

While it is difficult to draw inferences from the limited information available on Kvitsiani and his Monadire militia, they represent the type of irregular force Russia could leverage to its benefit. More specifically, these types of groups—mostly tribal or clan-based, yet partially criminal, and operating under the guise of a Nationalist paramilitary—help their regular force actors (in this case Russia) achieve regular-irregular synergy to present the Georgian military with multiple dilemmas.

The 2014 Annexation of Crimea

In February 2014, local crime group thugs, identifiable by red armbands, helped seize strategic locations across Crimea in concert with Russian Spetsnaz forces, insignia-stripped marines and paratroopers, the "Berkut" riot police force, and, most likely, clandestine operatives from Russia's GRU and Federal Security Service.[10] These locations included the Supreme Council (Crimea's local legislature), police stations, local businesses, and key border-crossing points. While some of the "local self-defense volunteers" were probably no more than armed citizens, many were rank-and-file members of the peninsula's Bashmaki and Salem crime gangs, who provided valuable military and political muscle.[11] Dr. Mark Galeotti, a clinical professor of global affairs at New York University's Center for Global Affairs and director of Keele University's (United Kingdom) Organized Russian and Eurasian Crime Research Unit, has written extensively on this topic. In a November 2014 article published on Radio Free Europe Radio Liberty's website, Galeotti claims that, as it became apparent that President Victor Yanukovych's position in Kiev was increasingly untenable, Moscow began reaching out to potential local allies in Crimea through the Moscow-based crime group *Solntsevo* in an effort to gauge the disposition of local crime groups.[12]

> *"…Russia's geopolitical position is dependent upon its ability to corrupt: to corrupt outsiders; to use organized crime outside of Russia, ranging from the thugs in Crimea who suddenly emerged as 'local self-defense volunteers' alongside the Special Forces 'polite people' in the annexation and, indeed, some of the militants in the Donbas who are clearly no more than local organized crime gangs…"*
>
> *– Dr. Mark Galeotti*
> *"Crime, Kleptocracy, and Politics: Developments in Modern Russia"*
> *October 2015* [9]

For local crime groups like Bashmaki and Salem, corrupt politicians like the recently "elected" Prime Minister Sergey Aksyonov—himself a former Salem group member during the 1990s—and local elites, the decision to throw their lot in with the Kremlin was a no-brainer. In Crimea, the most lucrative criminal enterprises, such as trafficking Afghan heroin or smuggling counterfeit cigarettes, are largely reliant upon working relationships with Russian criminal networks. Additionally, members of the Crimean underworld launder much of their ill-gotten gains through Russian banks, which are often deeply penetrated by Russian organized crime.[13] Crimea-based groups may have leveraged their willingness to augment Russian forces in Crimea for sweetheart deals down the road, such as opportunities in infrastructure development and the tourism industry, particularly casino complexes in the city of Yalta, situated on the Black Sea coast.[14] It also appears that in exchange for their support, the Kremlin will back their play against non-Slavic gangs—particularly the Georgians, Chechens, and Tatars—attempting to encroach on their territory. To add yet another layer of complexity, the ranks of militarized criminal groups in the Donbas region were replenished when Russian President Vladimir Putin amnestied convicts from prisons in eastern Ukraine in July 2014.[15]

Figure 3: Aksyonov (center) leaving a polling station in Simferopol

Military Implications

Threats employ armed criminals as auxiliaries to achieve regular-irregular synergy in order to present their adversaries with multiple dilemmas. These groups are often difficult to characterize as they are often not purely criminal in the traditional sense. Rather, they are a complex combination of multiple identities—ethnic, religious, tribal, clan, familial, and village-based—that, at times, may don the

accoutrements of a local militia or nationalist paramilitary. Complicating matters further, these criminal threats' motivations, alliances, and degrees of affiliation are constantly shifting due to merging or diverging interests. Armed criminal auxiliaries ensure freedom of action by providing the threat a capability that is indigenous; executing a broad range of missions, ranging from assassinations to smuggling operations to bombing campaigns; maintaining anonymity to facilitate plausible deniability (e.g. Russia's takeover of Crimea); and being self-sustaining due to their diverse illegal entrepreneurial endeavors.

The employment of armed criminal auxiliaries falls squarely into the gray zone of warfare, a concept recently published by the Army's Special Forces community. In the concept paper, the author defines gray zone challenges as "competitive interactions among and within state and non-state actors that fall between the traditional war and peace duality."[16] Threats deliberately choose to employ armed criminal auxiliaries as part of regional campaigns in concert with the great equalizers of 21st century warfare—mass media, public opinion, and the inherent rigidity of democratic, consensus-building governments and coalitions—to pursue courses of action that convolute realties on the ground, thus stymieing efforts to create situation understanding. As a result, these gray zone activities help confuse and delay decisionmaking, enabling the threat to maintain the initiative and achieve its objectives.

Threats are, and will likely continue to be, less encumbered by artificial rules-based systems, enabling them to act, adapt, and evolve with greater speed and creativity than their adversaries. To prepare for this reality, Army units should consider placing a premium on designing operational approaches during training that achieve balance between offense, defense, and stability in order to effectively counter irregular threats and the instability they foment. This will require leveraging intelligence tools (e.g. tools that enable social network analysis and geospatial information systems) and processes to accurately identify, map, and target the geography of the irregular threat's sanctuary. To that end, Army units must better integrate and leverage the expeditionary forensics and biometrics capabilities of military police criminal investigation units, forward-deployed forensics labs ran by the Defense Forensics Science Center, and the biometric exploitation capabilities of the Defense Forensics and Biometrics Agency. This forensics and biometrics data can be alchemized with criminal intelligence gathered by military police units, human intelligence, and signals intelligence to facilitate evidence-based targeting. Russia has operationalized crime as an integral component of statecraft in its near abroad, an important—yet all too often overlooked—consideration for the Army.

Notes

[1] Headquarters, Department of the Army. Training Circular 7-100.3, Irregular Opposing Forces. TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. January 2014. Para 4-4.
[2] Jim Nichol. "Russia-Georgia Conflict in South Ossetia: Context and Implications for U.S. Interest." Congressional Research Service. 24 October 2008.
[3] Jane's Country Risk Daily Report. "Abkhazia closes boundary with Georgia after bomb attacks." Jane's Intelligence Review. 1 July 2008.
[4] Ariel Cohen and Robert E. Hamilton. "The Russian Military and the Georgia War: Lessons and Implications." Strategic Studies Institute. June 2011.
[5] Jim Nichol. "Russia-Georgia Conflict in South Ossetia: Context and Implications for U.S. Interest." Congressional Research Service. 24 October 2008.
[6] Graham H. Turbiville. "Mafia in Uniform: The Criminalization of the Russian Armed Forces." TRADOC G-2 Foreign Military Studies Office. 1995.
[7] Kimberly Marten. "Russia, Chechnya, and the Sovereign Kadyrov." PONSARS Eurasia Policy Memo No. 116. 2010.
[8] Kimberly Marten. "Russia, Chechnya, and the Sovereign Kadyrov." PONSARS Eurasia Policy Memo No. 116. 2010.
[9] Mark Galeotti. "Crime, Kleptocracy, and Politics: Developments in Modern Russia." YouTube. 13 October 2015.
[10] Mark Galeotti. "Hybrid, ambiguous, and non-linear? How new is Russia's 'new way of war'?" Small Wars & Insurgencies. Volume 27, Issue 2, 2016.
[11] Mark Galeotti. "Crime and Crimea: Criminals as Allies and Agents." Radio Free Europe Radio Liberty. 3 November 2015.
[12] Mark Galeotti. "Crime and Crimea: Criminals as Allies and Agents." Radio Free Europe Radio Liberty. 3 November 2015.
[13] Mark Galeotti. "Crime and Crimea: Criminals as Allies and Agents." Radio Free Europe Radio Liberty. 3 November 2015.
[14] Mark Galeotti. "How the Invasion of Ukraine Is Shaking Up the Global Crime Scene." VICE News. 7 November 2014.
[15] Yuliya Zabyelina. "Ukraine's criminal gangs thrive on separatism." Jane's Intelligence Review. 24 March 2015.
[16] United States Special Operations Command. "The Gray Zone." 9 September 2015.

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

In the wee hours of Sunday morning, 8 May 2016, eight police officers drove through the deserted streets of Helwan, a southern suburb of Cairo, conducting what should have been a routine round of security checks. Suddenly a pickup truck darted in front of the police van, forcing it to stop. The truck's four masked occupants jumped out and sprayed the police van with automatic weapons fire, killing all eight Egyptian policemen. The perpetrators of this terrorist attack then methodically searched the corpses of their victims, seized the policemen's weapons, and faded into the darkness with no interference or molestation from stunned authorities.[1] In the immediate aftermath of the incident an organization affiliated with the Islamic State of Iraq and the Levant (ISIL) claimed responsibility, declaring that "soldiers of the caliphate" carried out the attack in retribution for the Egyptian government's incarceration of "pure women"—a pretext commonly used by Islamic militants to justify acts of violence.[2] Although the ISIL claim could not be independently verified, the group's statement had identified one of the slain officers and images on social media "showed the bloodied bodies of the officers, dressed in shirts and jeans, slumped in and around a white vehicle that was raked with bullet holes."[3]

Figure 1. Police van ambushed by ISIL-SP

Getting the World's Attention

The group that perpetrated the Helwan ambush calls itself *Wilayat Sinai* (Sinai Province; ISIL-SP), a name that alludes to an insurgency that the Egyptian military has been fighting for several years, which has greatly increased in severity since President Mohammed Morsi was forced from power in July 2013. Formerly known as Ansar Beit al Maqdis (*Supporters of Jerusalem*), the group that became ISIL-SP first appeared in the Gaza Strip following the overthrow of Egyptian President Hosni Mubarak in September 2011. It took its present name in November 2014—coinciding with its pledge of allegiance to ISIL—and became the focus of world attention after downing a Russian airliner over the Sinai in October 2015.[4]

Much of the notoriety on that occasion stemmed from the scale of the atrocity. The downed aircraft was a civilian jet carrying 224 passengers and crew; all on board lost their lives. Within hours of the crash, ISIL-SP published a statement claiming that "soldiers of the caliphate were able to bring down a Russian airplane."[5] Meanwhile, US, UK, French, and Russian counterterrorism and intelligence officials were busy drawing similar conclusions. Investigators early on ruled out technical failure, pilot error, and impact by some external object as likely causes. The emerging consensus was that an explosive device had been planted on the plane; and in early November 2015 British Prime Minister David Cameron said that the planted bomb scenario was "more likely than not."[6]

In an interview with Newsweek, geopolitical consultant Michael Horowitz offered other considerations that lent credibility to ISIL-SP's claim of responsibility. For one thing, the timing of the terrorist attack was probably no accident: it came almost exactly one year after the group swore allegiance to ISIL, and also came on the heels of Russian airstrikes that began hitting ISIL targets in Syria in September 2014. ISIL responded to the Russian intervention in Syria by calling for a holy war against both Russia and the US. Moreover, Horowitz argued that ISIL's reputation is based on making credible claims for attacks, and that the group would not risk damaging its image by making a false claim.[7] According to H. A. Hellyer, an associate of

the Royal United Services Institute—a UK think tank—the media coverage generated by the attack gave ISIL-SP an unprecedented "level of prominence . . . in the international extremist universe. They've controlled the narrative [of the crash]—that's a victory in and of itself."[8]

The INFOWAR Dimension

The information warfare (INFOWAR) dimension is what both the 8 May 2016 Cairo ambush and the October 2015 downing of Russian Metrojet Flight 9268 share in common. In both instances, ISIL-SP controlled the media narrative. The two attacks also demonstrate how the group is undergoing an evolutionary process that is bringing it into alignment with overarching ISIL objectives. As explained in the February 2016 ACE-TI Threat Tactics Report, *Islamic State of Iraq and the Levant*, "most Wilayat Sinai attacks target security forces in the northern part of the area [Sinai Peninsula] in an attempt to create a zone where the group can operate freely without interference from national security forces."[9] Although the statement accurately described the situation that existed throughout most of 2015, circumstances have changed since then. ISIL-SP's zone is still expanding.

An Adaptive Enemy with Long-Term Goals and Objectives

A growing body of evidence suggests that ISIL-SP is making a concentrated effort to extend its geographical reach deeper into the Egyptian heartland. The expanding sphere of influence includes the greater Cairo area, especially the South Cairo suburb of Helwan, where the 8 May 2016 ambush occurred. The previous November, ISIL had claimed responsibility when four police officers were gunned down at a security checkpoint, also in Cairo.[10] The subsequent terrorist attack of May 2016 suggests that killing so many policemen so close to Cairo indicates an escalation in violence.

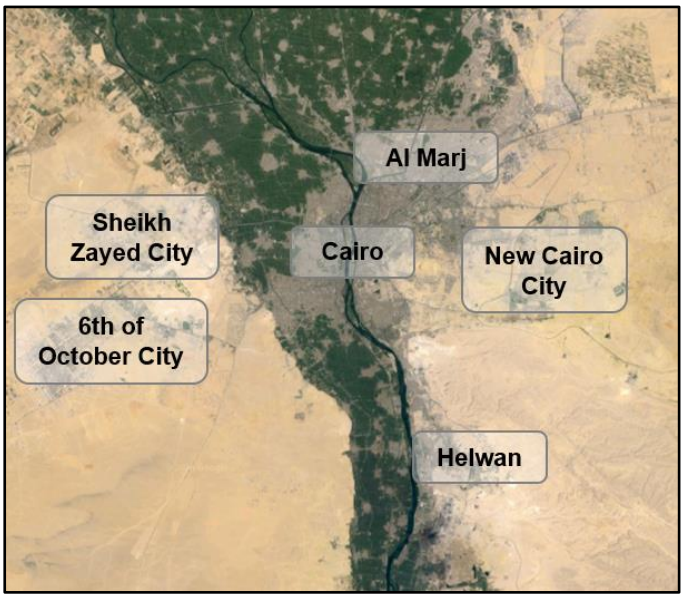


Figure 2. View of Cairo and selected suburbs

Zack Gold, a contributor to West Point's CTC Sentinel publication, underscores another indicator of organizational evolution in his discussion of ISIL-SP's decision to bring down Metrojet Flight 9268. Gold contends that the bombing was the capstone of "the group's self-declared economic war against the state and was [consistent with] a year-long trend of rhetorically attacking the local interests of nations working against the Islamic State."[11] Gold goes on to explain that on 18 November 2015, after stonewalling for nearly three weeks on the need to provide hard evidence to substantiate its involvement in the Russian jetliner bombing, ISIL-SP published a photo of the IED it used in ISIL's English-language magazine, *Dabiq*. British analyst Michael Horowitz declared that "the propaganda campaign surrounding the Russian jet crash is proof of the close links between the Sinai Province and ISIS."[12]

In the aftermath of the Russian Metrojet crash, some experts thought that perhaps ISIL-SP had alienated its popular base of support by wreaking havoc with a tourist industry on which many Egyptians depended for their livelihood.[13] Recent developments, including the police van ambush, provided evidence of a more likely scenario: that the group is capitalizing on popular discontent with recent measures taken by the Egyptian authorities to quell anti-government protests and political opposition. Although ISIL-SP militants do not actually control territory in Egypt, according to the BBC they are "thought to be aiming to take control of the Sinai Peninsula in order to turn it into an Islamist province run by IS [ISIL]."[14] During the period immediately preceding the 8 May 2016 Cairo ambush, Mokhtar Awad, a contributing author to West Point's CTC Sentinel, had already drawn similar conclusions:

> Nearly 18 months after the Islamic State [ISIL] injected itself into the Egyptian jihadi landscape . . . the contours of an Islamic State expansion strategy in the Egyptian mainland are becoming clearer. The Islamic State has escalated activity in the Western Desert, Upper Egypt, and found new cells in the Greater Cairo area. The group is exploiting its Egypt presence to project terror by targeting Western interests as part of

> its broader external operations campaign. It is also steadily laying the groundwork for a mainland insurgency to link the Libyan and Sinai theaters and to consolidate control over a fragmented Nile Valley militant landscape made up of al-Qa'ida-aligned militants and violent actors associated with some factions inside the Muslim Brotherhood and their Islamist supporters.[15]

Such broad-based goals as those described above suggest that adjustments made by the Sinai Province franchise of ISIL transcend short-term adaptations geared to day-to-day survival on the battlefield. Instead, they reflect a long-term evolutionary trend consistent with an intent to overthrow the ruling Egyptian government. First estimated to number about 300, ISIL-SP is now believed to have between 1,000 and 1,500 members.[16]

Wellsprings of Discontent: Turmoil, Poverty, and Marginalization

Egypt has been a staunch ally of the United States since the late 1970s when US President Jimmy Carter brokered the Camp David Accords, which led to the 1979 Egypt-Israeli peace treaty. Hosni El Sayed Mubarak, a former Egyptian general, served as Egypt's vice president during President Anwar Sadat's tenure in office, then assumed the mantle of president following Sadat's assassination in October 1981. Mubarak brought considerable stability to the US-Egyptian relationship, remaining in power for nearly 30 years before finally being forced to step down after 18 days of demonstrations during the Egyptian revolution of January 2011. Following Mubarak's fall, Mohammed Morsi, Egypt's first democratically-elected president, assumed office in June 2012. As chairman of the Freedom and Justice Party, Morsi drew much of his support from members of the Muslim Brotherhood, an organization originally founded in 1928, only a few years after Egypt gained its independence from Great Britain. Since that time the Brotherhood has come to represent a center of gravity for political Islam, not only in Egypt but elsewhere throughout the Middle East. According to the New York Times, it "has prided itself for decades on a nonviolent and election-oriented approach to political change. Some of its [followers] founded moderate Islamist parties in Turkey and Tunisia, while others, like Ayman al-Zawahri, the ideologue of Al Qaeda, have broken with the brotherhood to form anti-Western militant groups."[17] During the 2012 Egyptian presidential election campaign that followed Hosni Mubarak's fall from power, Morsi presented himself as a hedge against any return by the old guard, and promised to head a government that would represent the interests of all Egyptians.[18]

In accordance with the provisions of the 1979 Egyptian-Israeli treaty, over time the Sinai Peninsula was to become a buffer zone that would help establish peace and mutual trust between the two signatories. Instead, the area degenerated into a hotbed of international crime and Islamist militancy. Consequently, since the days of Mubarak's presidency, the Egyptian government has been fighting a number of extremist factions in the Sinai. The peninsula is a strategic land bridge that links Africa with Asia. It forms a triangular geographical land mass bounded by Gaza, Israel, and the Gulf of Aqaba on the east; the Mediterranean Sea to the north; and the Suez Canal to the west. The north and south Sinai comprise about 7% of Egypt's territory, and are sparsely inhabited, accounting for only about 0.7% of the country's population. Its natives are mostly nomadic Bedouins, an ethnic group sometimes scorned by other Egyptians because of alleged collaboration with Israeli authorities during their 15-year-long military occupation of the Sinai Peninsula following the 1967 Arab-Israeli war. Since the end of that occupation, the central government in Cairo has tended to doubt the loyalty of the Bedouins, looking down on them as a potential political fifth column.[19]

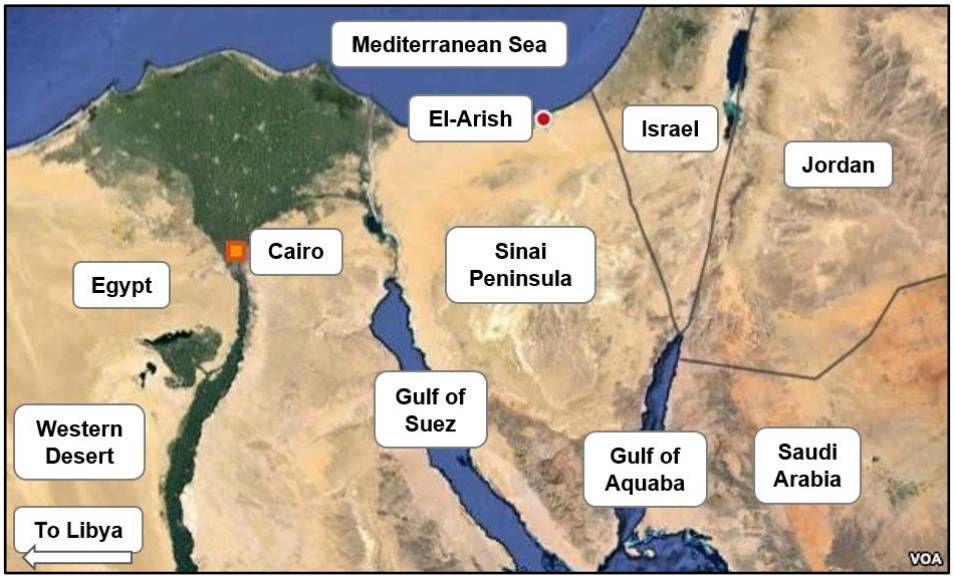


Figure 3. Voice of America map as modified by ACE-TI

Consequently, over time some parts of Egypt's Sinai Peninsula became a neglected no man's land, whose population the state power structure regarded as second-class citizenry, with native Bedouins excluded from tourism and energy development projects.[20] Steven Cook, a Senior Fellow with the Council on Foreign Relations, recalled that "the United States and Israel were telling Mubarak for years that neglect of the Sinai was going to come back to haunt" the Egyptians.[21] The haunting occurred in the form of an underground economy where Bedouins "found opportunities for economic survival in cannabis and narcotics production, gun running, and smuggling goods as well as people."[22] Human trafficking increased significantly during the mid-2000s, when refugees from sub-Saharan Africa flooded the Sinai in a desperate attempt to reach Israel, or perhaps even Europe. All too often while crossing the peninsula they encountered abduction, rape, torture, and extortion for ransom.

During Mubarak's near 30-year rule, many Bedouins dependent on the underground economy grew increasingly frustrated with the central government in Cairo. They perceived its secular-oriented state security apparatus as corrupt and detrimental to their own well-being, an entity that preferred conspiring with Israel over improving the quality of life of local residents in the Sinai. Although tribal leaders generally rejected violence, a rift developed between them and radicalized Bedouin youths, who believed armed resistance against the state was a better option than accepting the tenets of the Israeli-Egyptian peace treaty. It is hardly surprising that this radicalized faction included Salafi jihadis who felt justified in waging holy war against infidels and insufficiently-pious Muslims. This was the state of affairs that prevailed in the Sinai on the eve of the Egyptian revolution of January 2011.[23]

In early 2011, after prolonged demonstrations in Cairo's famous Tahrir Square and elsewhere across Egypt had forced President Mubarak to relinquish power, government security forces drastically reduced their presence in the Sinai in order to project as much power as possible along the trace of the Nile River Valley. Then in March 2011 NATO began its bombing campaign in neighboring Libya. As NATO air operations west of the Egyptian border forced the Libyan military to leave sizeable caches of arms virtually unguarded, many Bedouins seized the opportunity to smuggle large quantities of weapons and ammunition into the Sinai region, as a hedge against the day when Egyptian security forces might return to restore order. At this point a state of near anarchy prevailed in large parts of the Sinai. Israeli intelligence identified as many as 15 militant Islamist factions, including Ansar Beit al Maqdis, operating there. Most were in a position to defy the central government's authority with impunity.[24]

A Withered Arab Spring

As noted earlier, following the first free elections in Egypt's recent history, Mohammed Morsi, representing the interests and views of the Muslim Brotherhood, became president in June 2012. Many of the Brotherhood's long-suffering followers felt vindicated that their years of patient organizing, sometimes in the face of state-sponsored repression, had paid off by demonstrating that an Islamic government could indeed be brought to power through a peaceful electoral process. Conversely, the Brotherhood victory also amounted to a rebuke to militant groups who had insisted that an Islamic state could only be created through violent means. After his election, Morsi took a conciliatory approach to crafting a reconciliation between Egypt's central government and its wayward Sinai region. He promised that the relationship between the two entities would witness a new start, and personally visited the Sinai to demonstrate support for its future development.[25]

Despite Morsi's promise to govern in the interest of all Egyptians, his tenure in office disappointed many of his fellow countrymen. The BBC reported that he failed to deliver on many of his promises and that critics "accused him of allowing Islamists to monopolise the political scene [by] concentrating power in the hands of the Muslim Brotherhood."[26] In addition to those complaints, the economy remained problematic, and Morsi's track record on civil rights and social justice issues fell far short of meeting public expectations. Opposition to his regime increased in November 2012, when the Islamist-dominated parliament vacillated in drafting a new constitution and Morsi published a decree granting himself far-reaching powers. The public furor subsided temporarily after 15 December 2012, when voters approved the draft constitution through a referendum.[27]

Although President Morsi deployed the Egyptian military to the Sinai to demonstrate the authority of the central government, he hesitated to use force to restore order in the restive region. A climate of insecurity and lawlessness prevailed there until May 2013, when militants kidnapped seven soldiers, an act that set the stage for massive protests

across Egypt the following month and created conditions favorable for a military coup. The thirtieth of June 2013 marked the first anniversary of Mohammed Morsi's swearing-in as president. On that day, millions of demonstrators took to the streets in protest, prompting military authorities to issue an ultimatum warning Morsi that it would intervene within 48 hours to impose its own way forward if public demands were not satisfied. The deadline passed and, as reported by BBC, "on the evening of 3 July the army suspended the constitution and announced the formation of a technocratic interim government."[28]

The Egyptian Army's War on Terror

President Morsi's removal brought General Abdul Fattah al Sisi to the pinnacle of power in Egypt. As former head of the armed forces, he led a military establishment whose relationship with the Muslim Brotherhood dated to the early 1950s, when members of that organization formed a temporary alliance of convenience with the Nationalist Free Officers' movement to rid the country of British rule. Later, however, the two factions became bitter adversaries in the struggle for political power in Egypt. Just hours after President Morsi's ouster, military helicopters appeared over Cairo's Tahrir Square, then dropped thousands of Egyptian flags over protesters assembled there, inspiring them to chant, "the people and the army are one hand!"[29] Mr. Sisi boasted a reputation as a soft-spoken yet charismatic leader, with a knack for giving emotional speeches. CNN reported that on one occasion, at a concert in 2012, "his words . . . had artists on the stage with him in tears."[30]

Many Egyptians were supportive of a military-led government they hoped would re-stabilize the country after the chaos that brought down Hosni Mubarak's regime and persisted during President Morsi's rule through the first half of 2013. A new crackdown on political Islam soon revealed that the Sisi government made no distinction between moderate and militant factions within the Muslim Brotherhood: all were regarded as threats to the state. When government security forces stormed two pro-Morsi protest camps in August 2013, killing hundreds in the process, a wave of violent backlash washed across Egypt. Pro-Morsi elements attacked government buildings and torched dozens of Coptic Christian churches, causing government authorities to declare a state of emergency and outlaw membership in the Muslim Brotherhood.[31]

Predictably, Egyptian militant groups interpreted the Islamists' fall from grace as solid evidence that the goal of an Islamic state could only be realized through violence, and not through the ballot-box. In October 2013 one militant jihadist, calling himself al Shinqiti, wrote that anyone advocating nonviolence "is a criminal thug who wants the Ummah (Muslim community) to be eradicated and to be slaughtered . . . Every attempt to avoid fighting the Egyptian Army is like treating a disease with the wrong medicine."[32] ISIL-SP's parent organization, Ansar Beit al Maqdis, had formed in Egypt following the ouster of Mubarak, and numbered among the armed groups that rejected the Sisi regime's crackdown on Islamist opponents. The US State Department declared it a terrorist organization in October 2014 following attacks in the North Sinai that killed 33 security personnel. The group changed its name the following month to Sinai Province and concurrently pledged allegiance to ISIL.[33]

Figure 4. ISIL-SP logo

Thus the set of conditions were created that led to the ISIL-SP attack on Sheikh Zuweid in the Sinai Peninsula, discussed in the previously mentioned Threat Tactics Report, "Islamic State of Iraq and the Levant." The New York Times described the fight at Sheikh Zuweid as the most audacious attack launched by the group in the first half of 2015. "To finally overcome the militants," said the Times, "the military called in warplanes and helicopters, conducting airstrikes that left the remains of the militants still sitting in their pulverized vehicles, witnesses said."[34] The affair at Sheikh Zuweid was the capstone of more than 700 attacks launched against Egyptian security forces in the Sinai Peninsula during the first half of 2015.[35]

On 8 September 2015 the Egyptian army launched operation Martyr's Right, said to be "the largest and most comprehensive operation aimed at rooting out and killing militants in the North Sinai."[36] It consisted of two phases, conducted in serial fashion: a kinetic phase that ran from 8–22 September, in which security forces attacked and destroyed personnel, vehicles and equipment; and a second phase beginning on 8 October that entailed stability operations designed

to "pave the road for creating suitable conditions to start development projects in the Sinai."[37] The government's information campaign presented Martyr's Right to the Egyptian public as a resounding success, and timed the end of the operation to coincide with the 6 October anniversary of the country's victory in the 1973 war against Israel. Despite positive government interpretations, a series of four terrorist attacks perpetrated during the last ten days of October, in addition to the shoot-down of Metrojet Flight 9268 on the last day of the month, speaks for itself as testimony to Wilayat Sinai's resilience and capacity for adaptation.[38] The 8 May 2016 ambush of the police van in the Cairo suburb of Helwan, as previously discussed, is a further indication that the threat posed by ISIL-SP is far from being eradicated and instead may be expanding.

Figure 5. Russian leaders meet after loss of Metrojet Flight 9268

Recent Developments and the Way Ahead

A survey conducted by a London-based news website revealed that ISIL-SP had perpetrated over thirty attacks across the Sinai Peninsula during a two-week period in March 2016. The group also kept up the tempo of its ongoing media campaign, in September releasing a video, "Soldiers' Harvest," that portrayed several attacks carried out against security forces. Another video, released in March 2016, purportedly showed camps in a desert location where ISIL-SP members received combat training. Before President Morsi's downfall the group scorned the nonviolent wing of the Muslim Brotherhood for embracing the "infidel democracy" and the electoral process; but in early 2016, just a few days prior to the fifth anniversary of the 25 January 2011 revolution, ISIL-SP softened its tone toward the Muslim Brotherhood's "supporters of peacefulness," calling on them to abandon their former stance in favor of taking up arms against the regime of President Abdul Fattah al Sisi.[39]

In April 2016, President Sisi's government ran into additional rough sailing when Egypt transferred authority over two Red Sea islands to Saudi Arabia. In the midst of allegations that the islands' giveaway was no more than a deal concocted by the Sisi and Saudi Arabian regimes to funnel additional aid to Egypt, security forces arrested approximately 1,200 people in the wake of public protests against the arrangement. Of the 1,200 arrested, about 600 were formally charged. These most recent incidents have further tainted Sisi's popularity, and added more fuel to public anger already simmering over alleged police brutality involving deaths stemming from trivial matters such as taxi fares or the price charged for a cup of tea. Recent arrests of journalists have also tarnished police reputations and spawned violent public protests. On 8 May 2016—the same day of the Cairo police van ambush—issues of due process and other allegations against the police were scheduled for debate by the Egyptian parliament.[40]

If President Sisi's government has a less-than-perfect track record on human rights, the fact remains that Egypt has been a dependable US ally in the war against ISIL, regardless of the country's troubled internal politics. It has also lived up to its obligations under the Egypt-Israeli peace accord of 1979, making it the first Arab state to formally acknowledge the sovereignty of Israel. Declan Walsh of the New York Times correctly observed that "fears over the spread of the Islamic State, which is based in Syria and Iraq but also has a muscular presence in Libya, have helped ensure Western support for Mr. Sisi even as he faces renewed criticism for a harsh, police-led crackdown on political dissent in Egypt."[41]

Before the month of May 2016 ended, Western support assumed the guise of providing the Egyptian government with 762 US-manufactured mine resistant ambush protected (MRAP) vehicles, scheduled for delivery in increments, free of charge. The first consignment is already in Egypt, with the remainder to be shipped in coming months. The MRAP shipments will occur in addition to the $1.3 billion in US military aid allocated to the Sisi regime this year. As to the future, it may be significant that, as a recent Washington Post article points out, the Obama administration "has asked Congress to remove all political and human rights conditions on military aid to Egypt in next year's budget."[42] Because defeating ISIL

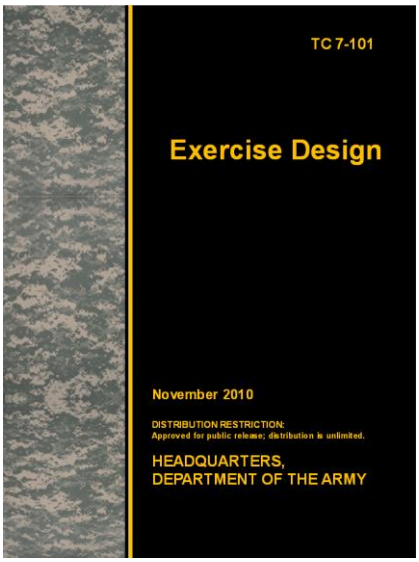
is in the interest of both the United States and Egypt, developments in the Sinai Peninsula warrant the attention of combatant commands as a potential future operational environment. Currently-deployable US units would do well to keep informed of the ongoing and apparently burgeoning threat posed by ISIL-SP; it constitutes yet another front in the war against ISIL and the level of US support will, in all likelihood, continue.

Notes

[1] BBC. "Egyptian Policemen Killed In Ambush South of Cairo." 8 May 2015; Thomas Joscelyn. "Russians Say Improvised Explosive Device Brought Down Jet In Sinai." Long War Journal. 17 November 2015.
[2] Declan Walsh. "Ambush Kills 8 Police Officers in Egypt." New York Times. 8 May 2016.
[3] Declan Walsh. "Ambush Kills 8 Police Officers in Egypt." New York Times. 8 May 2016.
[4] Conor Gaffey. "What Is The Sinai Province, The ISIS Affiliate In Egypt?" Newsweek. 5 November 2015.
[5] Thomas Joscelyn. "Russians Say Improvised Explosive Device Brought Down Jet In Sinai." Long War Journal. 17 November 2015.
[6] Conor Gaffey. "What Is The Sinai Province, The ISIS Affiliate In Egypt?" Newsweek. 5 November 2015.
[7] Conor Gaffey. "What Is The Sinai Province, The ISIS Affiliate In Egypt?" Newsweek. 5 November 2015.
[8] Conor Gaffey. "What Is The Sinai Province, The ISIS Affiliate In Egypt?" Newsweek. 5 November 2015.
[9] US Army, TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. "Threat Tactics Report: Islamic State of Iraq and the Levant." Version 1.6. February 2016. Pg 30.
[10] Voice of America. "8 Egyptian Police Killed in Ambush Near Cairo." 8 May 2016; Declan Walsh. "Ambush Kills 8 Police Officers in Egypt." New York Times. 8 May 2016.
[11] Zack Gold. "Wilayat Sinai Risks Backlash After Metrojet Bombing." CTC Sentinel. 15 December 2015.
[12] Conor Gaffey. "What Is The Sinai Province, The ISIS Affiliate In Egypt?" Newsweek. 5 November 2015.
[13] Zack Gold. "Wilayat Sinai Risks Backlash After Metrojet Bombing." CTC Sentinel. 15 December 2015.
[14] BBC News. "Sinai Province: Egypt's Most Dangerous Group." 12 May 2016.
[15] Mokhtar Awad. "The Islamic State's Pyramid Scheme: Egyptian Expansion And The Giza Governate Cell." CTC Sentinel. 22 April 2016.
[16] Conor Gaffey. "What Is The Sinai Province, The ISIS Affiliate In Egypt?" Newsweek. 5 November 2015; BBC News. "Sinai Province: Egypt's Most Dangerous Group." 12 May 2016.
[17] David D. Kirkpatrick and Mayy El Sheikh. "Push for Retribution in Egypt Frays Muslim Brotherhood." New York Times. 5 August 2015.
[18] BBC News. "Profile: Egypt's Mohammed Morsi." 21 April 2015.
[19] Zachary Laub. "Egypt's Sinai Peninsula And Security." Council On Foreign Relations. 12 December 2013.
[20] Bethan Staton. "Sharm el-Sheikh: How The Luxury Resorts On Egypt's Perfect Beaches Turned Into Abandoned 'Ghost Hotels'." Quartz.com. 4 June 2016.
[21] Zachary Laub. "Egypt's Sinai Peninsula And Security." Council On Foreign Relations. 12 December 2013.
[22] Zachary Laub. "Egypt's Sinai Peninsula And Security." Council On Foreign Relations. 12 December 2013.
[23] Zachary Laub. "Egypt's Sinai Peninsula And Security." Council On Foreign Relations. 12 December 2013.
[24] Zachary Laub. "Egypt's Sinai Peninsula And Security." Council On Foreign Relations. 12 December 2013.
[25] Zachary Laub. "Egypt's Sinai Peninsula And Security." Council On Foreign Relations. 12 December 2013.
[26] BBC News. "Profile: Egypt's Mohammed Morsi." 21 April 2015.
[27] BBC News. "Profile: Egypt's Mohammed Morsi." 21 April 2015.
[28] BBC News. "Profile: Egypt's Mohammed Morsi." 21 April 2015
[29] BBC News. "Egypt: Abdul Fattah Al-Sisi Profile." 16 May 2014.
[30] BBC News. "Egypt: Abdul Fattah Al-Sisi Profile." 16 May 2014.
[31] BBC News. "Egypt: Abdul Fattah Al-Sisi Profile." 16 May 2014.
[32] Vivian Salama. "What's Behind The Wave Of Terror In The Sinai." The Atlantic. 22 November 2013.
[33] Conor Gaffey. "What Is The Sinai Province, The ISIS Affiliate In Egypt?" Newsweek. 5 November 2015; Zachary Laub. "Egypt's Sinai Peninsula And Security." Council On Foreign Relations. 12 December 2013.
[34] Kareem Fahim and David D. Kirkpatrick. "Jihadist Attacks on Egypt Grow Fiercer." New York Times. 1 July 2015.
[35] Conor Gaffey. "What Is The Sinai Province, The ISIS Affiliate In Egypt?" Newsweek. 5 November 2015.
[36] Dr. Shaul Shay. "Egypts Counter Terror Operation 'Martyr's Right' in North Sinai." International Institute for Counter-Terrorism. 1 November 2015. (Link is not accessible from a US government computer.)
[37] Dr. Shaul Shay. "Egypts Counter Terror Operation 'Martyr's Right' in North Sinai." International Institute for Counter-Terrorism. 1 November 2015. (Link is not accessible from a US government computer.)
[38] Dr. Shaul Shay. "Egypts Counter Terror Operation 'Martyr's Right' in North Sinai." International Institute for Counter-Terrorism. 1 November 2015. (Link is not accessible from a US government computer.)
[39] BBC News. "Sinai Province: Egypt's Most Dangerous Group." 12 May 2016.
[40] Declan Walsh. "Ambush Kills 8 Police Officers in Egypt." New York Times. 8 May 2016.
[41] Declan Walsh. "Ambush Kills 8 Police Officers in Egypt." New York Times. 8 May 2016.
[42] Jackson Diehl. "America Gives Egypt Free Armored Vehicles. Egypt Gives America A Slap In The Face." Washington Post. 29 May 2016.

by **MAJ Michael Trujillo**, (US Army) Defense Intelligence Agency's Missile Space Intelligence Center and **Kristin Lechowicz**, TRADOC G-2 ACE Threats Integration (DAC)

This article examines the opposing force (OPFOR) antilanding operations (ALO) tactical task from Training Circular (TC) 7-100.2, *Opposing Forces Tactics*, and the OPFOR tactical task list from appendix B of TC 7-101, *Exercise Design*. It compares the OPFOR ALO doctrine to a video derived from the ongoing Syrian conflict. This video consists of a standoff ambush using an antitank guided missile (ATGM) on a temporarily-halted helicopter. This article will also explore ATGM systems as dual-use weapons against aircraft for training scenarios. The intent is to provide the training community and scenario developers with concepts for replication from real-world threats to aircraft or airbases and to cross-reference ALO threat doctrine. It is also to allow training units to draw lessons learned from the Syrian video and plan accordingly in order to counter such threat techniques. This article is the second collaborative effort between the TRADOC G-2 ACE Threats Integration Directorate and the Defense Intelligence Agency's Missile Space Intelligence Center (MSIC). MSIC provided the video with a basic analysis of the ATGM attack from Syria.[1] ACE-TI then used this primer as a case study to introduce OPFOR ALO doctrine as a comparison to current real world threats in Syria for the training community.



Video Background[2]

- Date: 8 September 2014
- Location: Idlib Province, Syria
- Rebel Group: Sham Legion, based on icon in video
- Type of Event: ALO offensive tactical action
- Weapon System: Kornet ATGM
- Weapon Systems Location: Level with target adjacent (estimated) 5,000–5,077 meters in an open field beyond airbase perimeter
- Target: Recently-landed MI-8 helicopter (Syrian Arab Army)
- Acquisition to Target Hit: 3 minutes 20–22 seconds
- Overview of Events: The video shows the helicopter descending, taxiing, and coming to a temporary halt. Support elements move toward the helicopter. The Kornet missiles strike the target as the helicopter starts to spin. The helicopter then combusts.
- Result: MI-8 helicopter destroyed

The video provides an example of the Kornet ATGM system used in a non-standard method against aircraft. ATGMs against air threats are not a new technique, but an example of the threat logically utilizing available weapon systems in a different function. The Syrian Civil War's operational environment is inundated with ATGM systems based on the attack videos reported by MSIC.[3] The Kornet system provides both the range and accuracy for the rebel's action element in the video to engage the target on the airfield from a relatively safe standoff distance. Training developers could include the Kornet ATGM in training events by using the Kornet's capabilities as given in the Worldwide Equipment Guide (WEG).

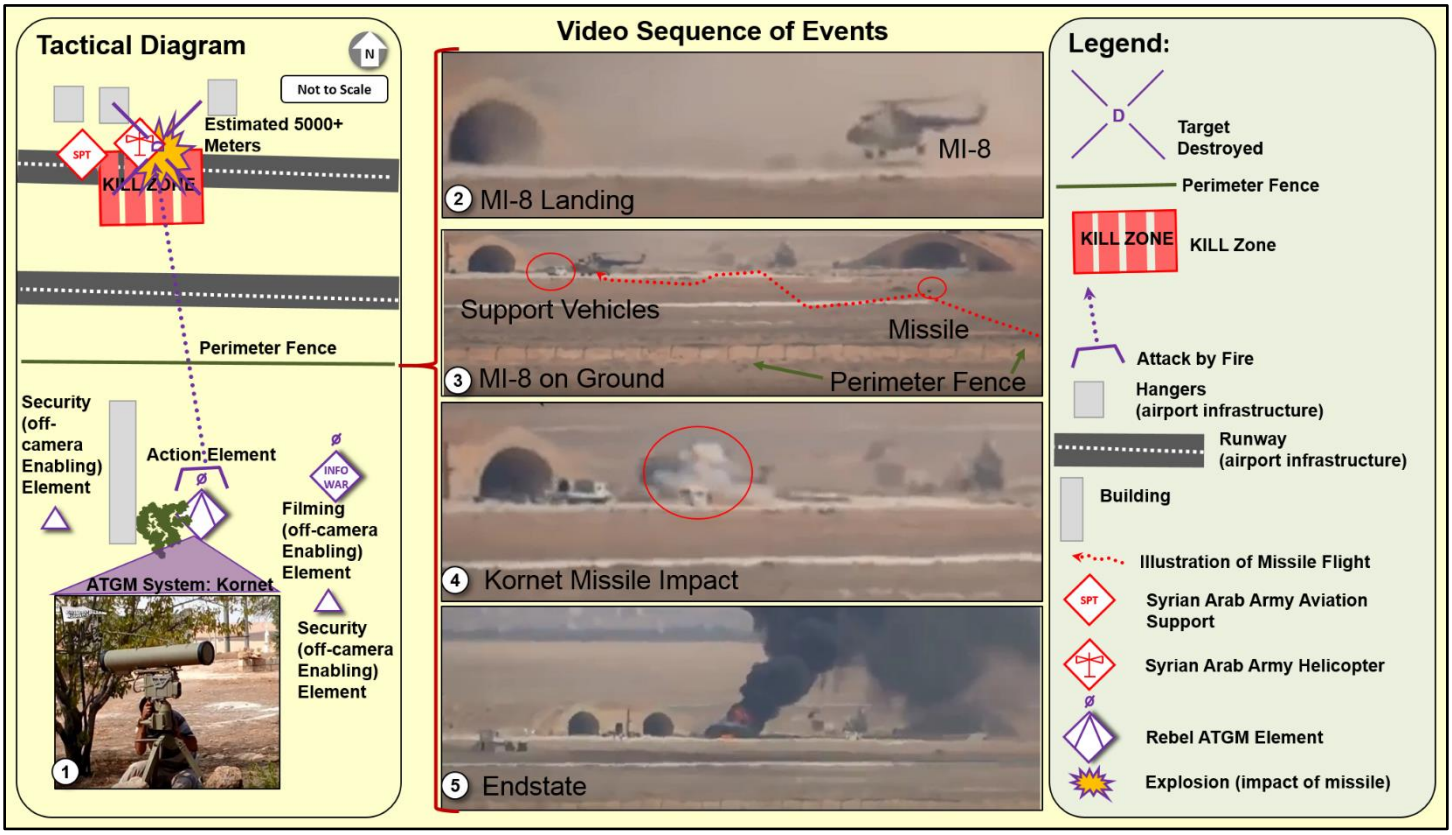


Figure 1. ALO (ATGM) diagram and graphic[4]

Another piece of information extracted from the video shows that the Kornet just short of its maximum range.[5] Choosing such a distance illustrates that the ATGM's crew was quite proficient and confident in the system's capabilities. The action element (rebels) within the video likely conducted reconnaissance and tracked other incoming flights to learn aircraft landing patterns, which allowed the ATGM crew to set up the Kornet in a most advantageous site. For scenario replication, the threat could also use a number of smaller hunter-killer teams in different positions around an airbase perimeter. For additional information on hunter-killer teams see TC 7-100.4, Appendix E-1, and its associated Threat Force Structure. Chapter 16 of TC 7-100.2, *Opposing Forces Tactics*, discusses the tactics of hunter-killer teams that can be implemented by the training community. The combat training centers' (CTCs') OPFOR, like the Syrian rebels in the video, employ a similar technique of targeting a rotational training unit's (RTU's) aircraft—either landing or taking off—by sending smaller irregular elements, often 2–3 individuals, to monitor the airfield from the perimeter. These threat teams wait for targets of opportunity to strike if left unchallenged by the RTU.

The ATGM team in the video appeared confident that base patrols would not compromise its position. This confidence might occur due to early-warning security elements or the lack of patrols from the base, a common RTU mistake at the CTCs. Another possibility is that the airbase in the video is isolated in rebel-controlled territory, similar to the two-year siege of the Abu al-Duhur airbase in Syria. During the rebels' operations against the Abu al-Duhur airbase, the base defenders became dependent on helicopters as their only means of resupply. From the threat's point of view, ALO makes perfect sense, with threat doctrine using the denial of resupply to the defenders in order to gain control of key terrain.

OPFOR Implications and Training Support

TC 7-101, *Exercise Design*, Appendix B, contains the OPFOR Tactical Task List. This is comparable to the US Army's Universal Task List (AUTL); however, there are currently only 24 OPFOR specific tactical tasks. Of note, the list is currently being revised and rewritten in the updated version of TC 7-100.2, *Opposing Forces Tactics*. These 24 tasks are unique to the OPFOR in order to reduce mirror-imaging of US Army tactics and to provide challenging conditions for the full spectrum of the training community. The following is tactical task 19, ALO, taken directly from TC 7-101, *Exercise Design*.

Tactical Task 19.0 Antilanding Actions[6]

Antilanding actions are those methods used to prevent landings by airborne or heliborne troops or to destroy enemy landing forces on the ground as soon after landing as possible. Antilanding actions can and will be executed by any force with the capability to affect the aircraft or the landing forces. However, this is a combined-arms action that primarily falls to the antilanding reserve (ALR) for execution. The subtasks for antilanding actions are the following:[7]

PLANNING

- Locate and predict drop and landing zones (DZs and LZs).
- Determine need for window of opportunity.
- Backwards plan from destruction of landing forces back to the current time.
  - Destruction of landing forces.
  - Detection of landing forces.
  - Maneuver to firing position and/or placement of obstacles.
  - Use of concealment, cover, camouflage, and deception, and window(s) of opportunity.
  - Disruption force(s) execute disruption of enemy.
  - Rehearsals.
  - Preparation.
  - Planning.
- Identify complex terrain in the vicinity of identified targets and potential cache sites.
- Identify affiliated forces (such as insurgent groups, groups with ethnic ties to the OPFOR, groups that sympathize with the OPFOR for political reasons, individual sympathizers, terrorist groups and criminal organizations) that can perform or support antilanding functions.
- Determine potential means and routes of infiltration and potential sources of supply.
- Determine the decisive point for destruction of landing forces.
  - On the ground, before air transport (using indirect fire, WMD, direct action, or precision munitions).
  - En route to or in the vicinity of LZs or DZs (using air defense weapons, directed-energy weapons, direct fire, obstacles, or anti-helicopter mines).
  - In a LZ or DZ (using indirect fire, WMD, direct fire, direct action, precision munitions, or infantry with antitank weapons).

PREPARATION

- Create one or more ALRs.
- Create task organization and command and control (C2) of action element(s), support element(s), security element(s), and deception force.
- Assign attack zone(s) and kill zone(s).

REHEARSAL

- The ALR rehearses actions in the vicinity of the LZs or DZs as well as movement between assembly areas, hide positions, and attack positions, and between LZs or DZs.

EXECUTION

- Transmit early warning from the main command post to the ALR.

- ALR moves to positions in the attack zone from which it can engage transport aircraft and destroy landing forces on the ground.
  - Disruption force(s) execute disruption of the enemy; focus on preventing detection of action element(s).
  - Security element(s) maneuver and fire to ensure the decisive point is isolated to ensure additional enemy forces do not join the battle unexpectedly. (Security elements may become fixing elements.)
  - Support element(s) conduct action to set conditions for action elements' success.
  - Action element(s) destroy targeted enemy.

Table 1. OPFOR tactical task: Antilanding actions

TACTICAL TASK: ANTILANDING ACTIONS		
No.	**Scale**	**Measure**
01	Yes/No	Mission accomplished.
02	Yes/No	Support element(s) created correct conditions for action elements' success.
03	Time	To complete mission.
04	Yes/No	Security element(s) isolated decisive points.
05	Yes/No	Disruption force(s) accomplished their mission.
06	Percent	Of friendly forces available to continue previous mission.
07	Percent	Combat effectiveness of enemy force.
08	Percent	Correctness of initial assessment of enemy.

OPFOR Replications and Training Support

Even though the Syrian attack video does not show a number of the exact steps in the OPFOR's ALO tactical task, it does not mean that they did not take place in some sort of fashion. The rebels in the video located and predicted the LZ. There was likely some sort of planning cycle for the infiltration of the team, weapon choice, and the target choice in the kill zone. There were likely other elements off-camera providing security, early warning, and C2 in support of the operation. These real-world events provide great examples for scenario developers to replicate and simulate for the training community.

The Syrian Kornet attack video on the airbase provides an example of a daunting challenge for training or deploying units. A commander needs to consider a five-kilometer threat from an ATGM on all his vehicles, including aircraft, and how to successfully mitigate the risk to the unit/base. The ATGM in a dual-use role also provides a new dimension for a training unit's S-2 section to consider. The standard thought process of weapons systems falling into defined categories can potentially be dangerous. Just because a system is designated as an ATGM does not mean that intelligence should eliminate the weapon as a threat against other targets—especially effective systems like the Kornet.

The training community, such as the CTCs or home station scenario developers, can reference ACE-TI's TC 7-100.2 and TC 7-100.3 in order to prepare units for ALO or other threats in order to enhance training. The previous article in this month's publication of the *Red Diamond* discusses the future rewrite of ALO doctrine as a tactical action that will be included in the updated TC 7-100.2. CTC scenario developers and home station trainers can find additional information on air defense or the duel use of ATGM/air defense artillery units, organization, or weapons systems in TC 7-100.4, its associated Threat Force Structure, and the Worldwide Equipment Guide (WEG). The *Red Diamond* also includes articles on real-world threats, such as ALO tactical actions, in order to inform and stimulate the training community and scenario development.

References

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] Missile and Space Intelligence Center. "Kornet ATGM Destroys SAF Helicopter." Liveleak. Posted 12 September 2014. (Video is no longer accessible; an alternative site is Military.Com.)

[2] Missile and Space Intelligence Center. "ATGM Firings in the Syrian Conflict as of 3 June 2016." 3 June 2016.

[3] Missile and Space Intelligence Center. "ATGM Firings in the Syrian Conflict as of 3 June 2016." 3 June 2016.

[4] Adapted from MSIC video from Live leak. Graphic Created by TRADOC G-2 ACE Threats on 22 May 2016.

[5] US Army, TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. Worldwide Equipment Guide – Volume 1: Ground Systems. December 2015. Pg 87.

[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-17.

[7] 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-17.

Antilanding Actions
Anti-Air Assault and Anti-Airdrop Defense

by **Jon H. Moilanen** (IDSI Ctr) and **Angela M. Wilkins** (DAC), TRADOC G-2 ACE Threats Integration

INTRODUCTION

A myth continues to obtain unwarranted attention that the US Army's *Opposing Force* (OPFOR) is somehow not adequately representative of the types of operational environment (OE) threats witnessed during current military operations in regions such as Ukraine or the Middle East. Some viewpoints suggest that the increased overt and covert acts of aggression by the Russian Federation in regional conflicts are not sufficiently addressed in OPFOR force structure and adaptive capabilities for US Army training readiness, professional education, and leader development. Other opinions seek to find "new" threat tactics for use in US Army combined arms training strategies.

> **The simple truth is the opposing force (OPFOR), as described in the US Army Training Circular (TC) 7-100 series, represents the realistic, robust, and relevant types of regular and irregular threats as currently observed of Russian military and paramilitary forces and surrogates in OEs such as Ukraine, the Russian Federation, and the Middle East. The tactics employed are not new—techniques evolve with available means and methods in a particular OE, but tactics remain an established functional foundation for action.**

A comparison of current Russian army brigade-echelon doctrine and current OPFOR doctrine in the TC 7-100 series verifies the accurate representation and additional tactical description and detail of characteristics, tactics, and techniques in the OPFOR conduct of threat military operations. In many cases, the TC 7-100 series on the OPFOR provides more information than is generally available on how the threat fights in actual battles and engagements. (See section below "Case Vignette: OPFOR Antilanding Actions and Russian Anti-Air Assault Actions.")

As the US Army continues to research, observe, and study ongoing conflicts involving the Russian Federation and possible impacts on US military abilities to dissuade, deter, or defeat Russian aggression, the US Army's OPFOR is an accurate composite of real-world threats in doctrine, tactics and techniques, organization, and equipment. The fidelity of OPFOR and OE conditions are readily adaptable to challenge a US Army unit commander's mission essential tasks or other specified mission tasks for unit, Soldier, and leader evaluation of readiness.

BACKGROUND

US Army Regulation (AR) 350-2, *Operational Environment and Opposing Force Program*, (2015) defines:

> An OPFOR is a plausible, flexible, and free-thinking mixture of regular forces, irregular forces, and/or criminal elements representing a composite of varying capabilities of actual worldwide forces and capabilities (doctrine, tactics, organization, and equipment). The OPFOR is used in lieu of a specific threat force for training and developing U.S. forces. The OPFOR is tailored to replicate highly capable conventional threats and unconventional threats that combined can replicate hybrid threats and their strategies further described in the Training Circulars (TC) 7-100 series.[1]

Headquarters, Department of the Army recently published Execution Order (EXORD) 001-16 to detail requirements and direction on how the US Army will establish an enduring process for sustainable readiness. Annex B of this EXORD states a critical factor in order to provide consistency in Army unit training products, such as collective and individual tasks, Combined Arms Training Strategies (CATS), and associated learning methods. The Army directs that its training and education proponents use the Decisive Action Training Environment (DATE) as the foundation to describe operational environment (OE) conditions. The

Army Training and doctrine Command (TRADOC) G-2 authors the DATE and applies the TC 7-100 series to describe the several OPFORs comprising regular and irregular force antagonists, adversaries, and enemies in the DATE.

The DATE utilizes PMESII-PT [political, military, economic, social, information, infrastructure, physical environment, and time] variables to frame the OE conditions for training. As in the TC 7-100 series, the conditions in DATE represent a composite of real-world conditions that allow trainers and scenario developers to design training exercises that replicate threats that can look like what the Russian Federation would bring to a fight as well as all types and sizes of regular and irregular forces and environments in which they exist. The options available through the use of DATE are numerous to ensure that military training remains robust and relevant. ACE-TI works to ensure the relevance of DATE through feedback and collaboration with a wide audience of users who are integral to the production and regular updating of the document.

US Army TRADOC G-2 and the OPFOR

The TRADOC G-2 is the Army's lead for the operational environment and opposing force program in accordance with AR 350-2. The TRADOC G-2 Analysis and Control Element (ACE) Threats Integration Directorate (ACE-TI) serves as the lead for designing, documenting, and integrating threat, OPFOR, and OE conditions in Army doctrine, training, professional education, and leader development, as well as concepts and capabilities development for the US Army. ACE-TI collaborates closely with the TRADOC G-27 OE Training Support Center to provide the resources that enable Army leader initiatives that embed robust, realistic, and rigorous conditions to train and educate to Army standards. The TRADOC G-2 ACE-Threats Integration authors the US Army TC 7-100 series on the OPFOR.

Opposing Force for Sustained Readiness in US Army Training

The basis of developing the TC 7-100 series (circa 2000+) was a deliberate process involving the TRADOC G-2 staff, functional experts, reviews by military officers from several nations, and evolving Russian military doctrine of the era. The additional extensive study and analyses of several nations' military doctrine and operations resulted in the composite model of the current OPFOR doctrine, tactics and techniques, organizational force structure, and systems. The majority of this OPFOR data incorporates post-Soviet Russian military doctrine and subsequent additions on actions of state and non-state actors as observed in recent and current real-world conflicts.

CASE VIGNETTE: OPFOR ANTILANDING ACTIONS AND RUSSIAN ANTI-AIR ASSAULT ACTIONS

US Army TC 7-100.2, *Opposing Force Tactics*, compared and contrasted with a translation of Russian Federation military doctrine at the brigade echelon, presents a fully representative state and non-state threat in current OPFOR organizations for training to US Army readiness standards.

For example, OPFOR antilanding actions of an antilanding reserve (ALR) in TC 7-100.2 parallel a Russian doctrinal description of "integrated air assault/air drop defense" or "anti-air assault defense reserve" capabilities. The OPFOR description for this type of tactical action presents a credible baseline for use in US Army training with an OPFOR, and is a prime US Army resource for knowing, understanding, and training against sophisticated regular and irregular force threats now and into the near-term and midterm future. The OPFOR includes hybrid capabilities of regular and irregular units and organizational combinations; willing, coerced, or unanticipated support by a relevant population; and the specter of terrorism and a threat not normally constrained by international conventions or law of war protocols.

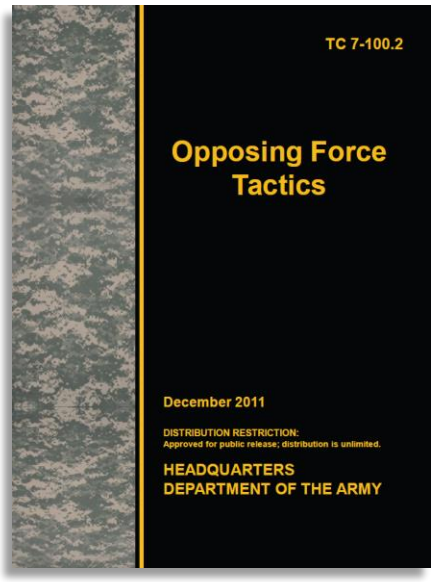


Figure 1. US Army TC 7-100.2

Russian Anti-Air Assault and Antilanding Actions

Current Russian independent brigades—some regimental and division units remain in Russian army structure—doctrinally identify an anti-air assault defense reserve as part of a unit's

integrated air assault defense in offensive and defensive operations. At brigade echelon, a company is typically the basic maneuver element headquarters that can include task-organized capabilities for:

- rapid mobility to probable landing zones, drop zones, or other objectives,
- direct fires,
- indirect fires,
- air attack,
- air defense, and
- countermobility with "antilanding obstacles."

Russian doctrine describes an antilanding element mission task to prevent enemy air assaults and destroy enemy forces *before* they land, *during* their landing, and *after* they land, as well as countering airborne and airmobile sabotage and reconnaissance efforts.

Beyond a brief indication of an assembly area location in offensive and defensive operations in the second or third echelon of the brigade, no other significant discussion of antilanding actions resides in a translated sample of doctrinal training material from Russian military college and academy curricula.

OPFOR Antilanding Actions

To train an OPFOR for use in US Army training, TC 7-100.2 describes organizing and conducting antilanding actions, and states an ALR mission task to—

> Prevent landings by enemy airborne or heliborne forces or elements through destruction of the troop transport aircraft *in flight,* effects to enemy *aircraft in the landing* of forces, and destruction to enemy forces *on the ground as soon after landing* as possible. Antilanding actions are a combined arms action executed typically by an antilanding reserve (ALR).[2]

The OPFOR trains with a methodology of evaluating tactical tasks and drills to specified but tailorable conditions with established and rigorous standards of performance. The ongoing 2016 update of OPFOR tasks and drills is being integrated into the TRADOC G-2 Virtual OPFOR Academy (VOA) for live, virtual, constructive, and gaming (LCVG) simulations. A framework of OPFOR tactical tasks in TC 7-101, *Exercise Design*, is currently being updated for a revision of TC 7-100.2 in fiscal year 2017. Antilanding actions in TC 7-100.2 present topic areas currently as follows:

Antilanding Reserve

Because of the potential threat from enemy airborne or heliborne troops, an OPFOR commander may designate an antilanding reserve (ALR). While other reserves can perform this mission, the commander may create a dedicated ALR to prevent destabilization of the defense by enemy vertical envelopment of OPFOR units or seizure of key terrain. ALRs are resourced for rapid movement to potential drop zones (DZs) and landing zones (LZs).

An ALR commander has immediate access to operational and tactical intelligence systems for early warning of potential enemy landing operations. ALRs typically include maneuver, air defense, and engineer units, but may be allocated any unit capable of disrupting or defeating an airborne or heliborne landing, such as smoke or information warfare (INFOWAR). They rehearse and plan for rapid mobility and combat at DZs or LZs.

Simple battle positions (SBPs) and complex battle positions (CBPs) employ both active and passive air defense measures to protect the OPFOR defender from airlanding threats. Antiaircraft guns and shoulder-fired surface-to-air missiles (MANPADS) and other air defense systems may be found interspersed throughout battle positions, and may include antilanding ambushes. Integrated air defense or fires systems may be present when allocated to the defending force from higher-echelon supporting units.

An antilanding reserve can be located as part of a disruption or security force or element, main defense or attack force or element, or be a contingency planning mission task of a reserve.

Organizing Terrain for Antilanding Actions

Antilanding forces or elements are assigned a zone to control their actions against enemy landing forces. An attack zone may only be activated for the duration of an antilanding action or may be assigned permanently to an ALR. Kill zones are used to control both ground and air defense engagements. Anticipated enemy landing zones (LZs) or drop zones (DZs) are included in the listing of predicted enemy locations (PELs) similar to a named area of interest (NAI) or target area of interest (TAI).

Organizing Forces or Elements for Antilanding Actions

OPFOR commanders form one or more antilanding reserves to conduct antilanding actions during or after an enemy airlanding operation. ALRs can consist of any units that commander and staff analyses determine necessary to destroy an enemy airborne or heliborne landing. Typical ALRs may include unit capabilities of—

- Air defense gun and missile units,
- Infantry with rapid mobility, heavy machine guns, and antitank weapons,
- Armor,
- Smoke,
- Engineers,
- Aviation, and
- Artillery.

ALRs are typically OPFOR detachments. OPFOR doctrine describes task-organized units at battalion and company echelon as a battalion detachment (BDET) and company detachment (CDET). A detachment commander can organize his force or elements into—

- Disruption elements to disrupt the enemy and prevent detection of action elements,
- Security elements to maneuver and fire to isolate a decisive point and prevent additional enemy forces or elements from linkup with an airlanded enemy,
- Support elements to conduct actions to set conditions for action element success, and
- Action elements to destroy the enemy landing force.

However, an ALR for an anticipated major enemy landing operation may be a brigade tactical group (BTG) or a division tactical group (DTG). Both BTG and DTG are OPFOR terms of reference for task-organized brigades and divisions. In these two echelons, the ALR would consist of functional forces rather than elements.

Planning Antilanding Actions

An ALR plans actions to attack enemy transport aircraft in flight prior to and in the vicinity of an LZ or DZ. This planning typically requires coordination with a higher headquarters and task-organized units for timely intelligence updates from reconnaissance, surveillance, intelligence, and target acquisition (RISTA) resources; integrated fires; and integrated air defense systems.

Camouflage, cover, concealment, and deception (C3D) actions improve the ability of an ALR to surprise and defeat or destroy an enemy airlanding attempt. Countermobility obstacles can be are openly emplaced as decoys, hidden with C3D, or arrayed in obvious patterns to dissuade use of an LZ or DZ. The OPFOR uses antilanding mines at possible LZs or DZs as explosive, nonexplosive, and combination obstacles. The OPFOR uses all types of mines and follows minefield doctrine, but adapts emplacement to optimize command and control and mine effects. At LZs and DZs, fragmentation and directional antipersonnel mines are a norm. Tripwire patterns or command detonation can improve multiple simultaneous mine effects. Antitank mines can be part of an LZ or DZ mining pattern. Anti-helicopter mines can be emplaced with tilt rods and small chutes to trigger mines from blade wind pressure.

Rehearsals of ALR antilanding actions in the vicinity of the LZs or DZs confirm readiness. An ALR also plans and rehearses movement between assembly areas, hide positions, and attack positions with a priority of effort among multiple possible LZs or DZs in an assigned zone.

Executing Antilanding Operations

Early warning of an approaching enemy airlanding and possible or probable LZs or DZs is transmitted from a higher headquarters, as well as from available integrated fires and air defense connectivity within the task-organized ALR. The ALR moves rapidly to designated battle positions from which it can engage and defeat transport aircraft as they approach an LZ or DZ, are attempting to deploy airborne or air assault forces or elements, or destroy airlanding forces if they reach the ground.

OPFOR TRAINING TO STANDARDS: ANTILANDING ACTIONS

ACE-TI provides documented and approved OPFOR task and drill training packets to the TRADOC G-27 OE Training Support Center for implementation into the G-2 Virtual OPFOR Academy (VOA) resources such as instructional videotapes and VBS3 visualizations. These same OPFOR training packets, composed of a narrative task, conditions, standard, and performance measures evaluation are being entered into the US Army's Combined Arms Training Strategies (CATS) as additional data for planning and training OPFOR tasks to standards and in support of Army training.

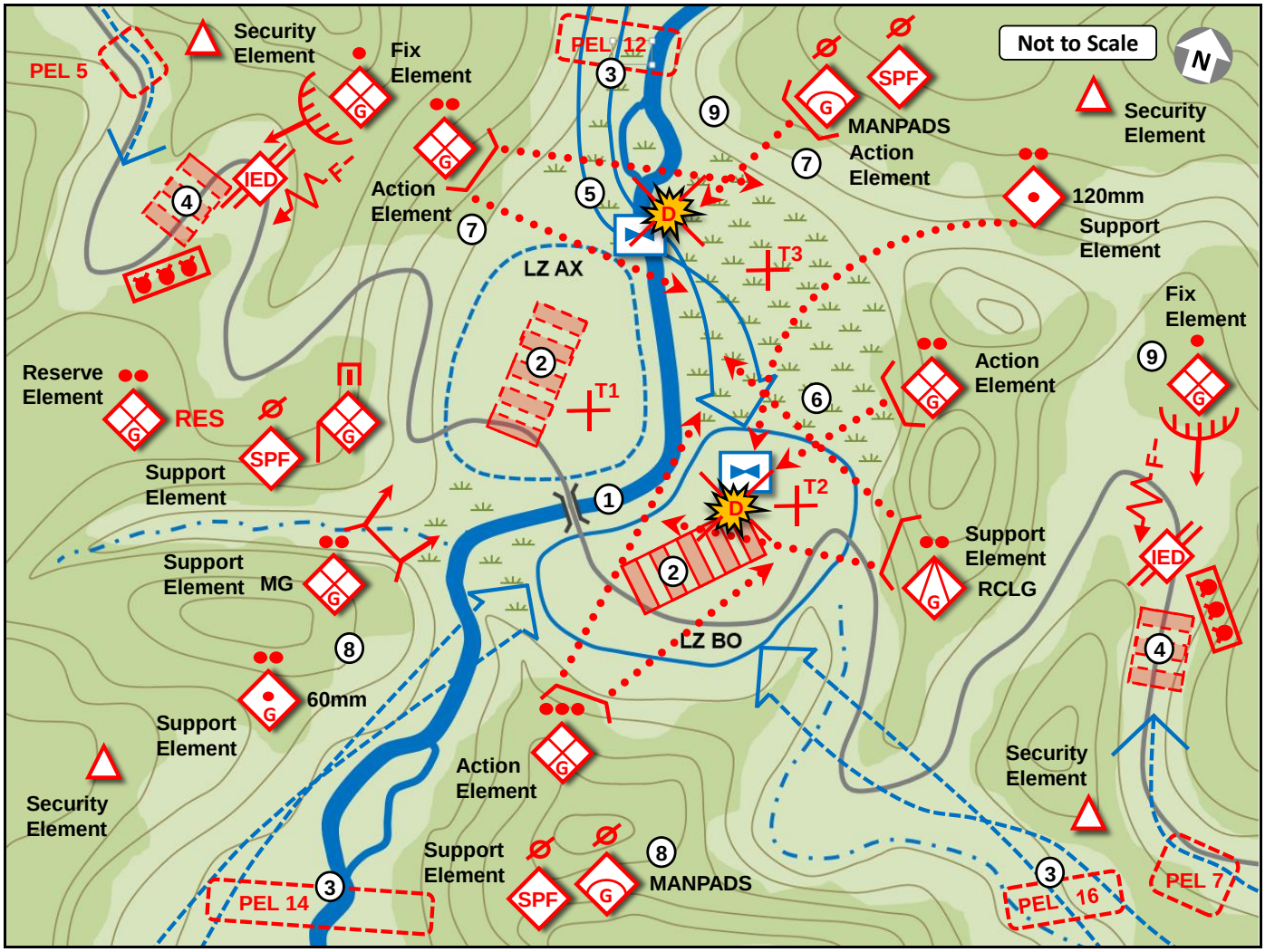


Figure 2. Antilanding actions tactical sketch (example)

① A task-organized guerrilla company protects a bridge from enemy antilanding actions. Augmentation includes three SPF advisory teams with MANPADSs, 120mm mortar section, and 12.7mm HVY MG squad.

② Probable landing zones are targeted as kill zones with direct and indirect fires. Mines and obstacles are arrayed and camouflaged in each LZ and marsh.

③ Security elements focus on PELs on probable aerial avenues of approach.

④ PELs on two ground approaches to the bridge site focus security and fix elements to prevent linkup of enemy ground and airlanding elements.

⑤ Observers allow enemy UAS to enter and depart area in support of C3D. PEL 12 confirms two rotary-wing utility aircraft maneuvering north to south along the river trace. Action elements allow the lead helicopter to continue into LZ. Action elements track the trail helicopter as it follows the lead helicopter.

⑥ On order, action and support elements covering LZ engage the lead helicopter as it hovers to disembark enemy infantry. The lead helicopter crashes and explodes with all enemy aboard.

⑦ Simultaneously, the infantry section and MANPADS team with SPF advisors engage the trail helicopter.
The missile hit on the trail helicopter and heavy machine gun fire cause it to spiral rapidly and crash in the river bed. There are no enemy survivors.

⑧ Guerrilla elements not in the engagement remain in location to protect the bridge site while some elements reposition or resupply.

⑨ Security and fix elements are prepared to ambush any ground maneuver toward the bridge.
The guerrilla CDET continues antilanding actions to include reconnaissance and surveillance of the bridge site, and counterreconnaissance actions in zone. The CDET CO continues the mission.

Figure 3. Antilanding actions sequence (example)

The collective task narrative training packet for antilanding actions progresses through a task description, training conditions, and standards that list six main tasks for antilanding actions with supporting sub-tasks, and uses 15 performance measures to assess and evaluate satisfactory conduct of OPFOR antilanding actions. A sample concept tactical sketch (see figure 2) illustrates how a training environment could be visualized at company or subordinate unit echelons to train and evaluate antilanding actions readiness.

A sequence of actions in the antilanding actions tactical sketch (above) is an example of incorporating an integrated and all-arms air defense approach to protecting a bridge site by an affiliated guerrilla company detachment. The accompanying description (see figure 3) of sequential and concurrent actions realizes that an airlanding action is associated typically with a linkup of forces or elements for subsequent operations. Defeating or destroying the linkup is an implied task in destroying the enemy airlanding operation.

To view OPFOR tasks and drills already posted to the TRADOC G-2 Virtual OPFOR Academy, use common access card (CAC) to enter the TRADOC G-27 OE Training Support Center e-site http://www.tradoc.army.mil/g2/oetsc/ and its "Operational Support" button to retrieve Virtual OPFOR Academy resources.

DISCUSSION

The OPFOR, as described in the US Army Training Circular (TC) 7-100 series, represents the realistic, robust, and relevant types of regular and irregular threats as currently observed of Russian military and paramilitary forces and surrogates in OEs such as Ukraine, the Russian Federation, and the Middle East. The tactics employed are not new—however; *techniques* evolve with available means and methods in a particular OE. Basic tactics with adaptive execution of techniques remain the established functional foundation for successful tactical actions.

Numerous requests for information from commanders, Centers of Excellence, exercise designers, curriculum developers, trainers, and educators want data on the former Warsaw Pact or Russian Federation forces to represent in training and education that span live, virtual, constructive, and gaming (LVCG) venues.

A potential concern is any presumption that actions occurring between Ukraine and the Russian Federation are representative of how conflict would occur if the US Army, in a coalition, confronts the Russian Federation.

Similarities of a specific regional contest may exist in a future conflict; however, enemies will not necessarily fight US military forces the way they fight a regional opponent with significantly fewer capabilities in a particular OE. Adversaries and opponents will adapt, shape OE conditions to their advantage, and attempt to avoid or counter overmatch capabilities of US military forces.

Another potential concern is a recurring claim that the OPFOR for training needs to be "more Russian." The hybrid threat OPFOR already includes a substantial level of Russian post-Soviet representation in its composite model of actual worldwide forces and adaptable capabilities in doctrine, tactics, organization, and equipment. Russian thinking and experience arguably accounts for more of the hybrid threat OPFOR than any other single actor. The OPFOR, a composite model of worldwide threat best practices, can be tailored to replicate the tactics, techniques, and comprehensive operations of any highly capable threat, including that posed by the Russian Federation.

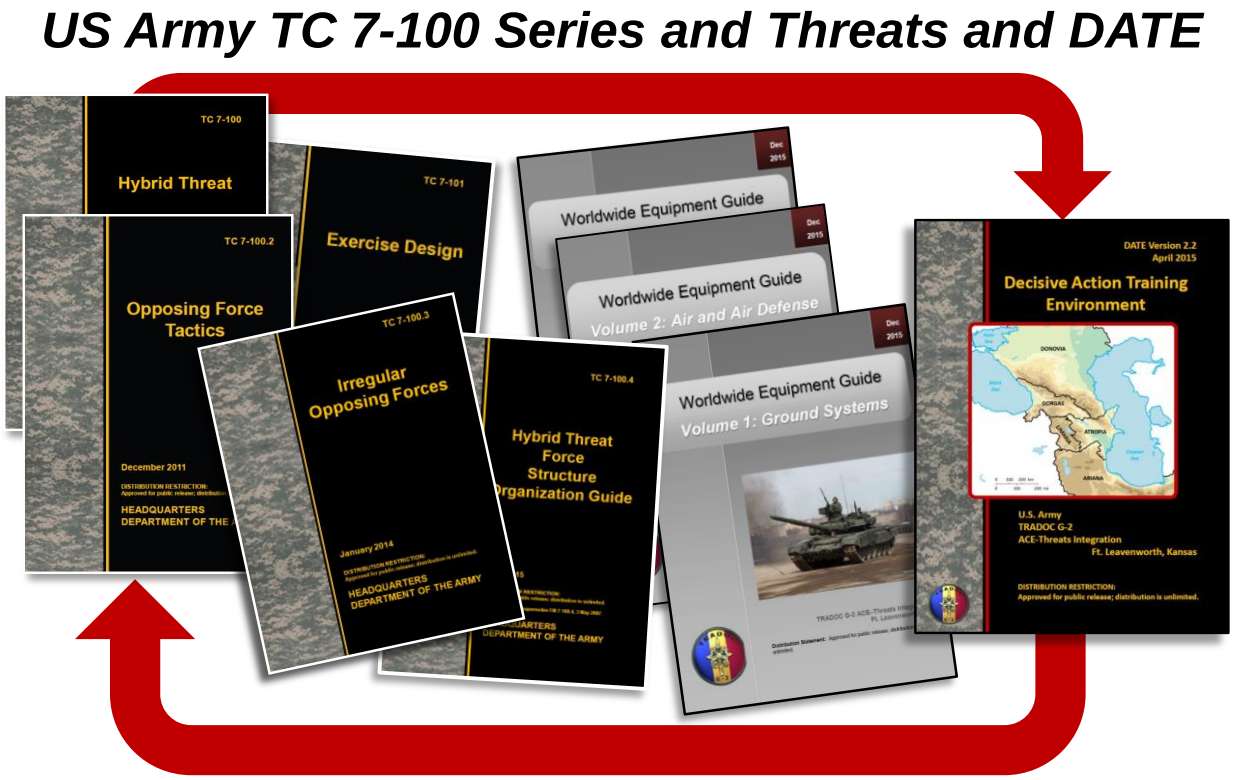


Figure 4. The OPFOR—Robust, Realistic, Relevant, and Representative of Current Threat Actors

A WAY AHEAD

ACE-TI continues to collect and analyze threats in various levels of conflict throughout the US combatant commands. Several of the recurring means of collaboration and continual improvement to a robust, realistic, relevant, and representative OPFOR include but are not limited to the following:

- Continue to collect observations from US Army and Joint forces, allies, and partners on threats in current real-world conflicts among state and non-state actors in varied OEs, and incorporate appropriate threat capabilities and limitations into the fiscal year 2017 update to TC 7-100.2, *Opposing Force Tactics*.
- Continue to collect observations from US Army and Joint forces, allies, and partners on threats in current real-world conflicts among state and non-state actors in varied OEs, and incorporate appropriate threat capabilities and limitations into the next version update of the US Army's *Decisive Action Training Environment*, Version 3.0.
- Sustain TRADOC G-2 threats information exchange to an active military observation and lessons learned program in coordination with Combatant Commands (CCOMs), Army Component Service Command (ASSCs), and allies and partners in conflict zones.

- Sustain TRADOC G-2 threats information exchange with organizations such as HQDA G-2, Center for Army Lessons Learned (CALL), and the US Army's Asymmetric Warfare Group (AWG).
- Sustain TRADOC G-2 threats information and intelligence exchanges with organizations such as the National Ground Intelligence Center (NGIC) and Defense Intelligence Agency (DIA).
- Improve the fidelity of the US Army Training Circular (TC) 7-100 series on opposing force (OPFOR) as representative of realistic, robust, and relevant types of regular and irregular threats and actions through regular review and update of real-world threats in all US combatant commands.

TRAINING IMPLICATIONS

- Understand Complex Operational Environments. The US Army's training and education proponents use the Decisive Action Training Environment (DATE) (current version is 2.2, dated April 2015) as the Chief of Staff of the US Army approved foundation to describe operational environment (OE) conditions.
- Know the Opposing Force (OPFOR). The US Army TC 7-100 series provides complex and dynamic operational conditions, and OPFOR organization, weapon systems and equipment, doctrine, tactics, and techniques as a composite of real-world threats, adversaries, and enemies.
- Use Virtual OPFOR Academy (VOA) and OPFOR training resources in in the US Amy's Combined Arms Training Strategies (CATS). Train-educate and leader develop with the TRADOC G-2 VOA and OPFOR Training and Evaluation Outlines (T&EOs) in CATS resources.
- Train to Army Standards with the OPFOR. An OE and the OPFOR, as stated in Army Regulation 350-2, *Operational Environment and Opposing Force Program* (2015), are integral to complex and dynamic training conditions as challenging operational variables to assess and evaluate US Army collective and individual task proficiencies.

References

Headquarters, Department of the Army. Army Regulation 350-2, *Operational Environment and Opposing Force Program*. 19 June 2015.

Headquarters, Department of the Army. Training Circular 7-100, Hybrid Threat. TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. November 2010.

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

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

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

Headquarters, Department of the Army. Training Circular 7-101, 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.

Headquarters, US Army Training and Doctrine Command. TRADOC Regulation 10-5-1, *Organization and Functions*. 20 July 2010.

Headquarters, US Army Training and Doctrine Command. TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. Decisive Action Training Environment. Version 2.2. April 2015.

Headquarters, US Army Training and Doctrine Command. TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. Worldwide Equipment Guide – Volume 1: Ground Systems. December 2015.

Headquarters, US Army Training and Doctrine Command. TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. Worldwide Equipment Guide – Volume 2: Airspace and Air Defense Systems. December 2015.

Headquarters, US Army Training and Doctrine Command. TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. Worldwide Equipment Guide – Volume 3: Naval and Littoral Systems. December 2015.

Notes

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

[2] Headquarters, Department of the Army. Training Circular 7-100.2, Opposing Force Tactics. TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. 9 December 2011. Para 6-31.

What ACE Threats Integration Supports for YOUR Readiness

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

ACE Threats Integration POCs

DIR, ACE Threats Integration	Jon Cleaves	jon.s.cleaves.civ@mail.mil	913.684.7975
Dep Director DSN:552	DAC Jennifer Dunn	jennifer.v.dunn.civ@mail.mil	684.7962
Military Analyst/Operations	Dr. Jon Moilanen IDSI	jon.h.moilanen.ctr@mail.mil	684.7928
Intelligence Specialist	DAC Jerry England	jerry.j.england.civ@mail.mil	684.7934
Senior Threats Officer	MAJ Jay Hunt	james.d.hunt50.mil@mail.mil	684.7960
Intel Specialist-NTC LNO	DAC Kris Lechowicz	kristin.d.lechowicz.civ@mail.mil	684.7922
(UK) LNO	Warrant Officer Matt Tucker	matthew.j.tucker28.fm@mail.mil	684-7994
Intelligence Specialist-DATE	DAC Angela Wilkins	angela.m.mcclain-wilkins.civ@mail.mil	684.7929
Intelligence Specialist	DAC Walt Williams	walter.l.williams112.civ@mail.mil	684.7923
Threat Tactics	CPT Nikolas Zappone	nickolas.m.zappone.mil@mail.mil	684.7939
Military Analyst	Dr. Jim Bird IDSI	james.r.bird.ctr@mail.mil	684.7919
Military Analyst	Rick Burns BMA	richard.b.burns4.ctr@mail.mil	684.7897
Military Analyst & WEG	John Cantin BMA	john.m.cantin.ctr@mail.mil	684.7952
Military Analyst-Editing	Laura Deatrick CGI	laura.m.deatrick.ctr@mail.mil	684.7925
Mil Analyst-MCTP LNO	BMA Pat Madden	patrick.m.madden16.ctr@mail.mil	684.7997
Military Analyst	H. David Pendleton CGI	henry.d.pendleton.ctr@mail.mil	684.7946
Mil Analyst-JMRC LNO	Mike Spight CGI	michael.g.spight.ctr@mail.mil	684.7974
Mil Analyst-JRTC LNO Threat Tec	Marc Williams	james.m.williams257.ctr@mail.mil	684-7943
Military Analyst (Vacant)	CTR (TBD)		
Intel Specialist-Analyst (Vacant)	DAC (TBD)		