U.S. TRADOC G2 Intelligence Support Activity

Red Diamond

Complex Operational Environment and Threat Integration Directorate

Fort Leavenworth, KS Volume 4, Issue 12 DEC2013

INSIDE THIS ISSUE

TRISA *Red Diamond* is published monthly by TRISA at CTID. Send suggestions to CTID
ATTN: *Red Diamond*
Dr. Jon H. Moilanen
CTID Operations, BMA
and
Mrs. Angela Wilkins
Chief Editor, BMA

by Jon H. Moilanen, CTID Operations (BMA Ctr)

The TRISA *Red Diamond* is a monthly newsletter that presents topics on an opposing force (OPFOR) threat for training and observations from ongoing or historical conflicts in complex environments. The value of rigorous and realistic threats in Army training, professional education, and leader development is evident in the quality of performance by our Soldiers, Army leaders, and Department of Army Civilians (DACs) in the daily conduct of missions and mission support. This December issue of the *Red Diamond* is a selective collection of TRISA articles from 2013 that addresses the diverse and challenging threats and related conditions of complex operational environments (OEs). These threats and conditions remain a significant factor in military missions today and for the foreseeable future.

Preparation and Readiness

Today we stand at a historical inflection point: the end of a decade-plus of war while facing an uncertain and dangerous future. The kind of conflict we will fight next is as unknown as the location or date. What is certain is that our Army will again be called on to deploy and engage our nation's foes—perhaps sooner, perhaps later.

General Robert W. Cone (2013)

RED DIAMOND TOPICS OF INTEREST

by Jon H. Moilanen, CTID Operations and Chief, *Red Diamond* Newsletter (BMA Ctr)

This issue of TRISA ***Red Diamond*** spotlights a selection of articles authored within the TRADOC G2 Intelligence Support Activity (TRISA) with a focus on opposing forces (OPFOR) as a threat or hybrid threat for training readiness.

See p. 46 for the 2013 INDEX of *Red Diamond* articles. The articles of 2013 address issues that are applicable today and very likely to continue for the foreseeable future in various operational environments (OEs).

TRISA-CTID values collaboration to present rigorous and realistic threats in Army training, professional education, and leader development of our Soldiers, Army leaders, Department of Army Civilians (DACs), as well as our multinational and interagency whole-of-government partners. Current incidents, historical vignettes, and threats tactics, techniques, and procedures (TTP) complement the deliberate actions to prepare for and conduct successful institutional and operational missions in complex operational environments and conflict with dynamic and committed threats.

Email your topic recommendations to:

Dr. Jon H. Moilanen, CTID Operations, BMA CTR
jon.h.moilanen.ctr@mail.mil
and
Mrs. Angela M. Wilkins, Chief Editor, BMA CTR
angela.m.wilkins7.ctr@mail.mil

What is Your Situational Awareness?

US Army Antiterrorism Quarterly Theme:1st Q/FY 2014
Army Antiterrorism Risk Management

BEST OF 2013 INTRODUCTION: *RED DIAMOND* IN REVIEW

Complex Operational Environment and Threat Integration Directorate

by CTID Operations

The December 2013 issue of the *Red Diamond* presents the articles listed below. The topics are critical to the situational awareness and understanding of the threat. The various forms of article presentation include focused case study, regional incident review, new equipment and/or weapon system development or upgrade to support the documentation, validation, and application of a hybrid threat for training as integral to CONDITIONS present in operational environments (OEs).

"Menagh Airbase Siege: Menagh, Syria" by Rick Burns is a tactical action in August 2012 with insurgents fighting the Syrian government. Insurgents conducted a siege and executed multiple attacks on the Menagh Airbase. On 5 August 2013, insurgents finally captured it. After a three-day long barrage of artillery, mortars, and machinegun fire, a Saudi suicide bomber detonated a specially-outfitted BMP loaded with explosives close to where the last remnants of the government troops were concentrated. The insurgents showed an aptitude for using "old weapons" in innovative ways. Realizing a prematurely-detonated VBIED would not be effective, the insurgents welded homemade appliqué armor protection to the sides of the BMP, which also served to stabilize the cylindrical explosives on top of the vehicle as it attacked the target.

Figure 1. BMP configured as a VBIED

"Integrating Crime and Criminal Elements into Training" by Ari Fisher reviews issues of how to accurately and effectively integrate crime and criminal elements into training scenarios within given constraints. Factors to consider include—first, a structured criminal organization does not need to exist for crime to be common, especially when some illicit acts are culturally relative; second, members of government are far from immune from criminal acts and may be in collusion with, or are, a hybrid threat actor; and third, profit is the primary motivator for criminal activity by a threat actor. The article also lists Army Universal Task List (AUTL) tasks that can be used to leverage crime and criminal organizations against Army forces.

"Decoys and Deception TTP in a Defense" by Kris Lechowicz is a combat multiplier used in threat training at the US Army's combat training centers (CTCs). A series of threat tactical diagrams illustrates how decoys can deceive and disrupt an enemy's offensive plan. Successful deception creates conditions that place an enemy at a significant tactical disadvantage. In the article's example based on a rotation engagement at a CTC, the threat defeats lead units of a battalion-size task force. As lead enemy reconnaissance and security elements enter a kill zone, threat detonations near a decoy tank platoon draw immediate attention. Simultaneously, indirect fires land in the kill zone as a threat platoon commences direct fires in support of the "tanks." The enemy vehicles orient to the north and return direct fires and call for indirect fires at "tanks" in the tree line and infantry positions. Threat infantry and tank platoons to the enemy flank hold any direct fires initially as enemy vehicles attempt to maneuver and expose its flank and rear to the main combat power of the threat. Massed threat tank main gun fires and indirect fires are devastating—the enemy reconnaissance platoon is destroyed in the kill zone and stalls the enemy task force advance. US Army Training Circular 7-100.2, *Opposing Force Tactics,* is a source for threat training principles, tactics, and techniques.

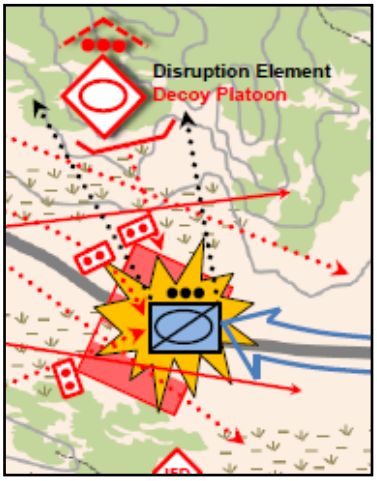


Figure 2. Decoy in ambush (extract)

"Aircraft Threats" by Marc Williams presents various threats to aircraft such as ground fire from small arms, man portable air defense systems (MANPADS), and gun-missile systems. Relatively recently, the threats have included laser "dazzlers" fired at cockpits and high-energy laser systems for countering rockets, artillery, and mortar shells (C-RAM). Other threats include IEDs used as anti-aircraft IEDs. These are used to deny landing access and to disrupt flight patterns for rotary wing aircraft. While not common, anti-aircraft IEDs have the potential of becoming more effective weapons in a long term counterinsurgency environment.

"Abiding Threat at Camp Chapman" by Jim Bird examines a recent terrorist attack at Forward Operating Base (FOB) Chapman, Afghanistan, as well as its implications for the information warfare (INFOWAR) arena. It drives home the point that no static facility is ever totally secure, especially if a threat actor is willing to die in an attack. It also reminds readers that a small force or single individual can inflict serious damage, either in a physical sense, or by undermining the credibility of security forces. Finally, it suggests that this type of suicide bombing is easily replicated, needs few role players, and requires minimal logistical support.

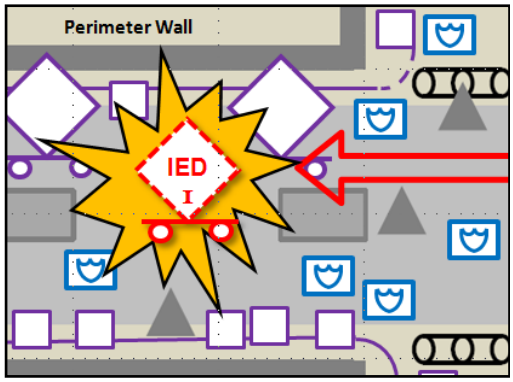


Figure 3. VBIED at Chapman (extract)

"Hybrid Threats and the Art of Reconstitution of the Force" by Walt Williams discusses strength percentages for a hybrid threat to remain combat effective and will provide a brief overview of the methods to reconstitute the unit. The article also serves as a beginning point in discussions that try to answer the elusive question of quantifying acceptable attrition rates necessary for commanders and staffs to use in modeling, training, and actual combat situations and still accomplish their mission.

"IED Attacks in Pattani" by David Pendleton reviews a 20-hour period on 16-17 February 2013 when insurgents acting against the ruling Thai national government attempted 11 improvised explosive device (IED) attacks in Pattani, Thailand. These actions were possibly retaliation against the government for the deaths of 16 of their fellow Islamist insurgents the week before in Pattani Province. The vigilance of several civilians, the ineptness of some of the bomb makers, and the rapid response of the Thai first responders all played major roles in the mitigation of the potential damage from the Islamist insurgents' IED attacks.

"The PK Series of General Purpose Machineguns" by Mike Spight highlights the development and current uses of the former Soviet Union General Purpose Machineguns (GPMG), culminating with Kalashnikov's design of the Pulemyot Kalashnikova, ("Kalashnikov's Machinegun" – PK) in the early 1960s which was accepted for issue by the Soviet Ministry of Defense in 1965. It is estimated that in excess of 50 nations currently use the PK/PKM or its domestically manufactured copy as their issued GPMG. This level of distribution clearly indicates that, like the AK-47/AK-74M and other Soviet era/Russian Federation weapons systems, the potential for future threats and their allies to be equipped and armed with the PK/PKM/PKP is very, very high. Knowing and understanding its capabilities is essential for every tactical leader in the US Army.

"Kidnapping in Katsina" by Laura Deatrick recounts the night of 19-20 December 2012, when several gunmen simultaneously attacked the police station and a residence in Rimi, Nigeria. Attackers killed two Nigerians, wounded a third, and kidnapped a French engineer at the residence. Several aspects of this incident can be useful to trainers and scenario writers. The small number of attackers and materiel allow for efficient use of role players and readily available training aids. Finally, additional complexity is the two-pronged attack, the foreign national target, and the possible insider threat angle.

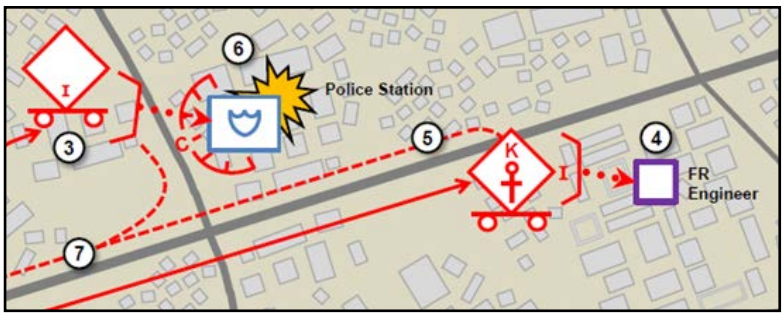


Figure 4. Kidnapping sequence in Katsina (extract)

"The Threat of Fire Producing TTP and Weapons on the Battlefield" by Jennifer Dunn presents threat capabilities and information available to implement the threat of fire producing TTP in training programs. The hybrid threat for training is a representative composite model of the threat, and uses OPFOR doctrine to set the proper conditions for effective training. The threat of fire producing TTP and weapon systems is more relevant than ever. The threat is increasingly gaining access to fire producing weapon systems through arms proliferation. Training implications include—new fire producing TTP and weapon systems continue to appear as globalization and technological advancements continue; an entire spectrum of the hybrid threat (irregular forces, regular forces, and criminal elements) has access to fire producing TTP and weapon systems; proliferation of fire producing weapon systems is increasing; and, threat OPFOR doctrine contains fire producing TTP and weapon systems so trainers can design exercises to train US soldiers against these threats.

Figure 5. TOS-1 flamethrower system

"Challenging Concepts and Capabilities" by Mike Sullivan demonstrates the threat training support to the US Army and joint community via the Wargame, Experimentation, and Threat Emulation Directorate (WETED) of the TRADOC Intelligence Support Activity (TRISA). Training events in 2013 provided many useful insights in hybrid threat and a rigorous and dedicated enemy. An example of evolving threat capabilities includes threat unmanned aerial vehicle (UAV) warfare and the increasing challenge for deploying forces by 2020. Proliferation of relatively inexpensive but highly capable UAV systems with reconnaissance, intelligence, surveillance, and target acquisition (RISTA) sensors and/or lethal laser-guided munitions will complicate airspace command and control and threaten US forces, allies, and coalition partners, and their cyber and sustainment assets as vulnerable to detection and attack by a persistent enemy UAV threat.

"Insurgent Dismounted RAID on a Tank Platoon" by Jon H. Moilanen describes the tactics and techniques of a threat OPFOR *raid* as an attack against a stationary target for the purposes of its capture or destruction that concludes with the withdrawal of the raiding force to safe territory. A training vignette is based on a dismounted insurgent raid on a tank platoon defensive position in Syria. With active reconnaissance and surveillance to confirm enemy vulnerabilities, a dismounted, infantry-like insurgent cell conducted a raid and destroyed an enemy force of three main battle tanks in a platoon-size defensive position. Information warfare (INFOWAR) used the Internet to exploit effects of a successful raid. Training implications for US Army forces are as stated in US Army Training Circular 7-100.2, *Opposing Force Tactics*.

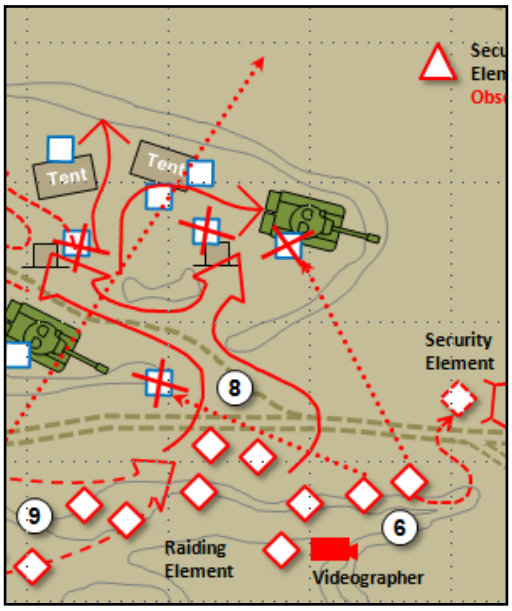


Figure 6. Insurgent raid concept (extract)

As the Army adapts for the future, it will retain its ability to dominate on land across the range of military operations to prevent and deter aggression and shape the security environment. This will include the use of combined arms, campaign-quality forces, power projection capabilities and regionally aligned, mission-tailored forces. The United States does not seek war, but others must never doubt our ability to wage it and win decisively when it occurs.
***Army Strategic Planning Guidance 2013*, p.1**

MENAGH AIRBASE SIEGE: MENAGH, SYRIA

by Rick Burns, OE Assessment Team (BMA Ctr)

For a year beginning in August 2012, insurgents fighting the Syrian government conducted a siege and executed multiple attacks on the Menagh Airbase. On 5 August 2013, insurgents finally captured it. After a three-day long barrage of artillery, mortars, and machinegun fire, a Saudi suicide bomber detonated a specially-outfitted BMP loaded with explosives close to where the last remnants of the government troops were concentrated. The Islamic State of Iraq and the Levant (ISIL) claimed it had taken the lead in attacking the airfield, supported by other units from the Free Syrian Army (FSA) and other Islamist organizations. The airbase was little more than an outpost with only about 75-100 defenders still remaining when it finally surrendered to the insurgent forces.

Figure 1. Specially-outfitted BMP VBIED with explosive containers

By the time the airbase fell, the Syrian Air Force no longer enjoyed air superiority and took to the skies with much less bravado than it had earlier in the Syrian civil war, making the airfield less important as a base from which to strike the insurgents. What started out as a very strategic and critical target for the insurgents became much less important and much more a psychological and symbolic target. The anti-government forces gained ammunition and a few weapons, but the surrender of Menagh Airbase represented much more of a symbolic victory. It also showed that groups with disparate political goals and tactics can band together to force the surrender of a much more organized and homogenous force.

The following is an outline detailing some of the events leading up to the final assault and subsequent capture of the Menagh Airbase.

2 August 2012: The Free Syrian Army and affiliated groups attacked the Menagh Airbase in Aleppo Governate, using a combination of small arms, rocket-propelled grenades (RPGs), and four tanks captured at the Battle of Anadan. This attack was repelled by entrenched government troops.

27 December 2012: Insurgents assaulted the besieged airbase with a night of heavy fighting. The government responded with bombing attacks on rebel positions.

January 2013: Approximately 300 government defenders remained at the airbase with supplies and medical evacuations delivered via helicopters. Over time, delivery of supplies became problematic as rebel forces eventually gained access to weaponry capable of shooting Syrian aircraft from the sky. (For more information, see TRISA-CTID's *The Free Syrian Army: From Rifles to MANPADS* Threat Report, 15 Nov 2012.)

8 February 2013: The Syrian Air Force bombed parts of the airfield where insurgents had gained access, resulting in a rebel retreat.

28 April 2013: Insurgent forces overran parts of the base in an attack, but were repulsed and forced to retreat.

5 May 2013: The largest assault to that point was launched by the insurgents under heavy aerial bombardment by the Syrian Air Force. The rebel forces captured a large portion of the airfield and a tank. Reports indicated that there were about 200 defenders concentrated in the administration building and guarded by a few tanks.

9 May 2013: Due to heavy airstrikes, the insurgents were forced to retreat from the airbase.

28 May 2013: The government conducted a successful resupply mission while thousands of insurgents left the siege to launch an attack on the Kurdish Popular Protection Units (YPG) in the Afrin region.

10 June 2013: Rebel forces attacked government troops and by the next day had secured the airbase control tower. Government forces responded by shelling insurgent-held positions.

17 June 2013: Insurgents clashed with pro-government fighters from Nubbul and Zahra who were moving to reinforce those defending the airbase.

23 June 2013: Insurgents detonated a vehicle-borne improvised explosive device (VBIED) in a government-held area of the airfield, killing 12 soldiers and destroying the surrounding buildings. The explosion was reportedly followed by missile firings on regime force positions.

5 August 2013: An assault led by ISIL was launched against the remaining 70-100 defenders left at the airbase. Two suicide bombers drove a modified armored personnel carrier to the command center and detonated explosives facilitating a final assault. The explosion destroyed buildings and killed or scattered the last defenders. There were reportedly 40 government and 21 insurgent soldiers killed in the operation.

The following description corresponds to the figure below. Some positions may not be exact due to limited available open source information, but are representational.

1. The final assault began with a three-day barrage of artillery, mortars, and heavy machineguns.
2. A Saudi suicide bomber drove the specially prepared BMP VBIED close to the buildings where the government troops resided and then detonated it.
3. Insurgent troops, attacking along three axes that converged where the government forces had consolidated at the airbase, prevailed after a day of heavy fighting.

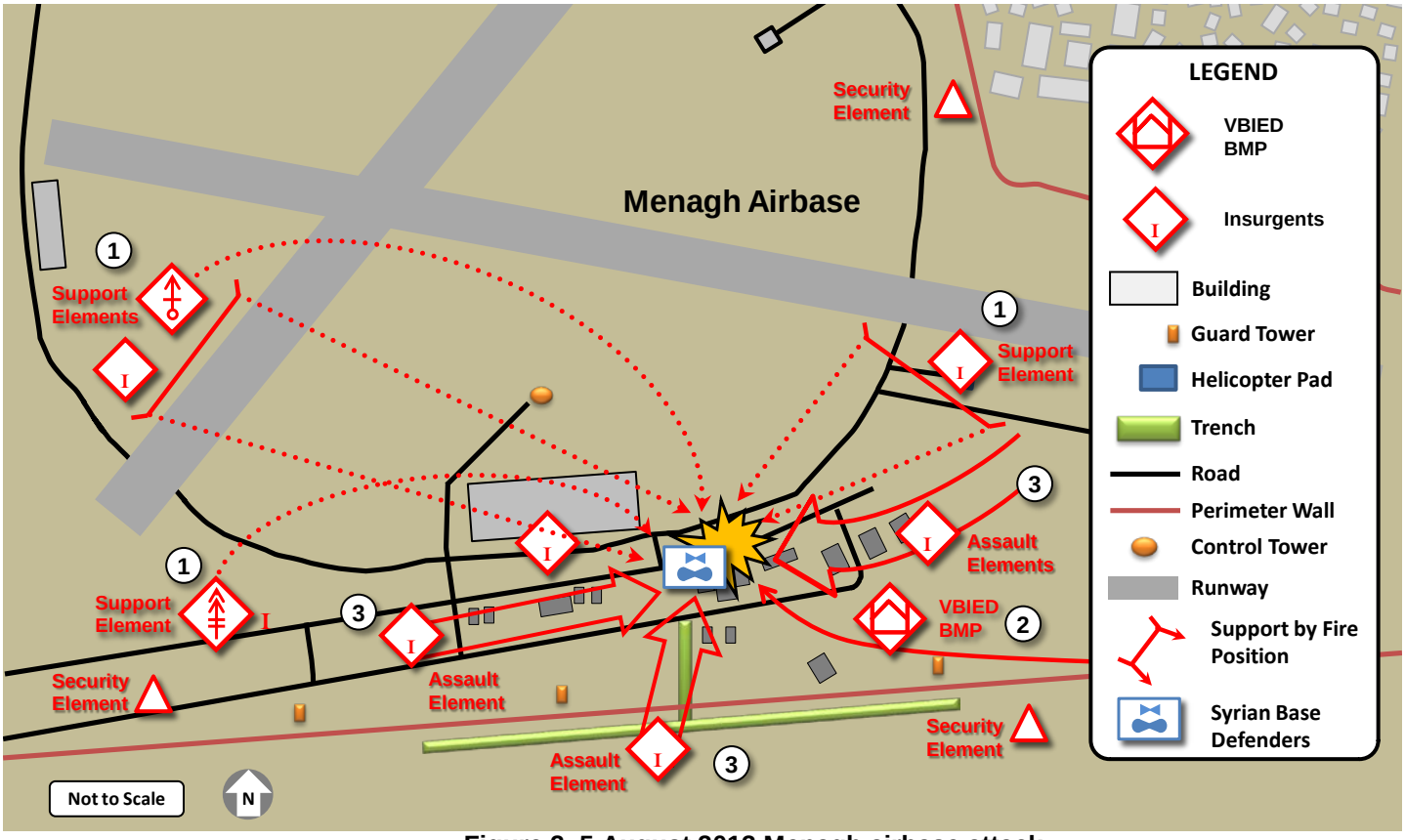
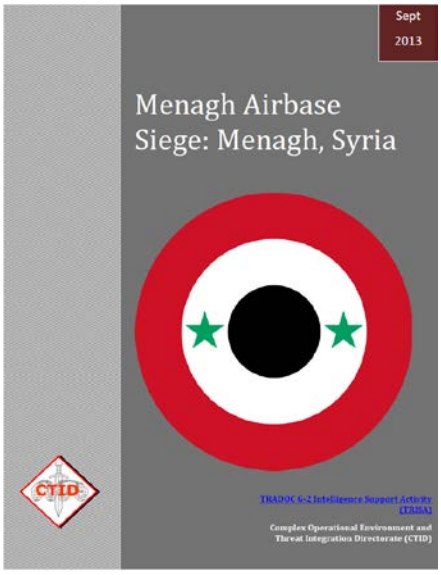


Figure 2. 5 August 2013 Menagh airbase attack

ISIL reportedly formed the vanguard of the attack, with other units supporting. Nine brigades participated in the final attack on Menagh Airbase. The exact number of insurgents, however, is not known, as insurgent unit manning does not correlate with conventional organizational constructs. A brigade, for example, may not be more than a company-size

element. It is certain that the number of insurgents outnumbered the small contingent left to defend what had become a barebones Menagh Airbase outpost.

The siege of the Menagh Airbase by insurgent forces is important for a number of reasons. First and foremost, it showed the tenacity of the insurgents. Far from a homogenous group of fighters with clear and agreed-upon tactics and desired outcomes, the insurgents were a disparate group with very different views on how the war should be conducted and a variety of post-war political goals. In the case of the Menagh Airbase siege, they were able to put these differences aside in order to prosecute a cooperative and coordinated mission over a long period of time.



The Menagh Airbase siege transitioned from a strategic operation to a psychological one. During the early days of the Syrian civil war, the regime owned the skies and used this capability to exact a terrible toll on insurgent forces. Airbases such as Menagh were critical strategic targets for the insurgents, who desperately needed to reduce the advantage enjoyed by the Syrian Air Force. As the insurgents gained the capability to shoot Syrian aircraft from the sky and the Syrian Air Force became more timid in using its air assets, the airbases became less strategically important. Capturing the airbase netted the insurgents abandoned ammunition and a few weapons; however, the psychological impact remains a significant accomplishment. The insurgents would not be able to hold the airbase if the Syrian military decided to retake it, but the victory is significant nonetheless.

The insurgents also showed an aptitude for using old weapons in innovative ways. Realizing a prematurely-detonated VBIED would not be effective, the insurgents welded homemade appliqué armor protection to the sides of the BMP, which also served to stabilize the cylindrical explosives on top as the vehicle ambled toward the guarded target. Seeing a BMP modified in this manner may have been, in and of itself, intimidating to government forces that were painfully aware they were the few defenders left in an increasingly disproportionate and disadvantageous situation.

Finally, the insurgents demonstrated an ability to grasp basic military tactics. Over time, they consistently improved their battle positions and enlarged their trenching systems. This allowed them to harass government forces from multiple angles. They also created sandbagged battle positions on the airfield, which allowed them to surround regime troops and slowly constrict the defensive perimeter. In the end, their patience won the day as Menagh was reduced to an outpost that became almost impossible to resupply and defend. For more details about the events at the Menagh Airbase, please see the Threat Report *Menagh Airbase Siege: Menagh, Syria*.

INTEGRATING CRIME AND CRIMINAL ELEMENTS INTO TRAINING

by CPT Ari Fisher, Training, Education, and Leader Development Team

Students attending September's Hybrid Threat Train the Trainer course expressed that they are trying, with varying degrees of success, to accurately and effectively integrate crime and criminal elements into scenarios within given constraints. Recently, a Combat Training Center demonstrated initial success by using a criminal element to smuggle arms to an insurgent force as well as provide information to Opposing Forces (OPFOR) on training unit activities. The criminal organization presented opportunities, which were not taken, for the training unit to leverage their influence. While this is a fine example, there is more we can do to add realism and complexity to training. Although often considered low-level white noise, as an irregular force actor, criminals and crime are often inextricably linked to the other threat actors.

Themes

As an analogy, the Decisive Action Training Environment (DATE) is to a pantry as your scenario is to dinner. Therefore, exercise designers should not feel pressure to develop the criminal threat by creating more force structure just because the option exists within DATE. When considering crime and criminal organizations, there are certain themes to ponder.

First, a structured criminal organization does not need to exist for crime to be common, especially when some illicit acts are culturally relative. Second, members of government are far from immune from criminal acts and may be in collusion with, or are, a hybrid threat actor. Third, profit is the primary motivator for criminal activity by a threat actor. Important to note is the reason may not wholly be individual greed or graft but could also be increased organizational influence, increased operational capacity, and decreased dependence upon a sponsor. Fourth, trafficking is multidirectional and modular. Relationships and links in the chain can form, break down, and re-form for multiple purposes. Often, however, physical routes and terrain use may be repetitive. Also, the modularity of interchangeable links within a trafficking chain may result in commodity payment versus money payment and multi-way transactions. For instance, Group A has drugs and needs weapons, Group B has transportation assets and weapons but needs money, and Group C has money and needs drugs. Therefore, Group B transports the drugs to Group C for money releasing weapons to Group A. Group C then sells the drugs on black market to earn more money.

Finally, crime is often not singular in nature. Interconnected criminal activity supports the main effort. It is not uncommon for those other criminal acts to resonate within the local populace. For instance, theft supports trafficking and kidnapping, and bribery or extortion can force or enable government official complicity. Ultimately, nesting story lines over common individuals will accurately reflect the common nexus between crime and criminal elements with other actors. The forthcoming are examples to serve as departure points for other ideas.

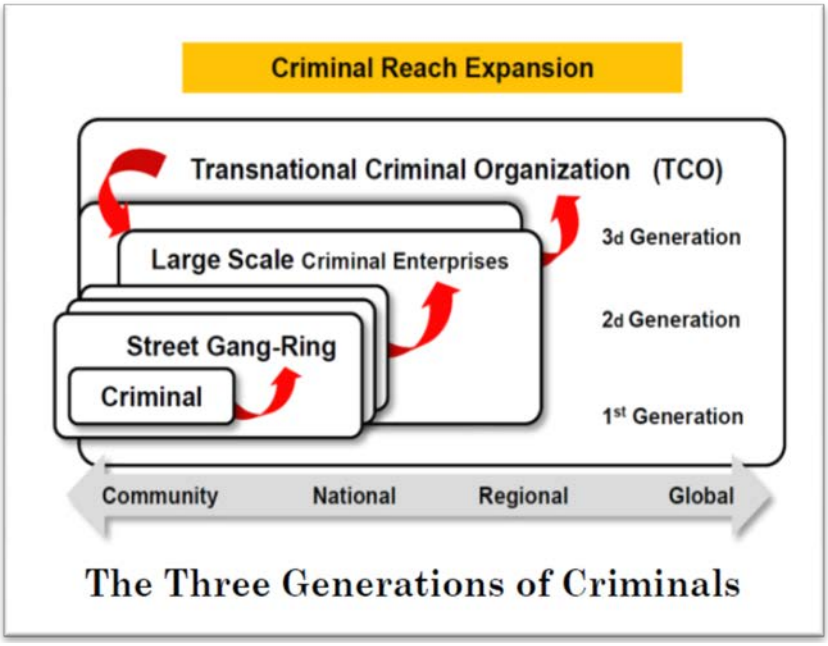


Figure 1. Criminal echelons (example) *Source: DATE 2.0*, pg 2B-2-10

Integrating Crime

This first example integrates only criminal activity: Create a police or government official that is also a guerrilla company commander. He or a close associate may also be the owner, possibly in name only, of a private business. For the sake of argument, let's say that business is a fuel distribution point or some other resource that holds significant value. To protect that resource, our corrupt official employs a guerrilla platoon that doubles as private security. There are many ways to further complicate this scenario. For instance, indicate that the fuel distribution point or resource mining site frequently siphons product to smuggle it to other regions, charges at an inflated rate, and possibly launders money with

proceeds that benefit and directly sustain guerrilla or other threat operations. Finally, consider the treatment of business employees by the owner or guerrilla security element that can be further integrated into the storyline and facilitate or drive other reporting or action. For instance, do they pay well and take care of families or are they abusive and commit atrocities?

Charles Taylor of Liberia serves as a real-world example. He had a proxy establish the Liberian Forest Development Company (LFDC) in Monrovia. On paper, the FDC was a subsidiary of two other companies, one of which Taylor owned. Concurrently, Taylor declared his brother head of a government agency titled the Forest Development Authority (FDA). As director of the FDA, he gave Taylor's company and the LFDC the rights to log three million acres, the largest plot granted, which increased state exports threefold. To secure these logging sites, Taylor used his own militia whose commanders committed human rights abuses.[1]

Integrating One Criminal Organization

This second example integrates both criminal activity and at least one criminal organization: Consider in this case that the criminal organization is classified as a transnational criminal organization (TCO) and takes on a primary roll of trafficking. With significant earnings, TCOs are capable of owning or controlling vast resources such as shipping companies and assets and have access to governmental officials who can provide official documentation authorizing commodity trading and transfer. To build upon the previous example, this TCO ensures the trafficking of fuel or other resources out while the same assets and logistics lines traffic arms, personnel, or other sustainment back to threat actors. The criminal organization benefits in at least two ways. The first is of course the money earned during the transfer of goods. The second is the link to a government official who can guarantee official documents. This gives the TCO's transportation fleet and front companies the appearance of legitimacy and facilitates regional operations.

Viktor Bout, an infamous arms trafficker, serves as a real-world example. Furthermore, his ties to Charles Taylor will further expand on the aforementioned sketch. Viktor Bout, also referred to as the "Merchant of Death," was arming several sides of several conflicts. Through his significant air fleet, Bout was capable of delivering large amounts of weapons and weapon systems, to include attack helicopters, around the world. In mutual benefit, Taylor allowed Bout to register dozens of his aircraft in Liberia. In a circular fashion, timber flowed out of the country while money flowed back to Taylor, which was used to purchase weapons for transport back to armed militants.[2]

The late Hugo Chavez and Venezuela serve as another real-world example. Chavez granted the Revolutionary Armed Forces of Colombia (FARC) access to territory and documentation. The FARC retained freedom of movement for cocaine shipments out to Europe and the United States to pay for sophisticated weapons to combat the Colombian government. In return, Chavez, through the FARC as a proxy, kept pressure on the Colombian government and military.[3]

Integrating Multiple Threat Organizations

This third example links multiple threat organizations together: Expanding upon the prior two examples, we introduce a third organization that provides mediation, another commodity required to complete the trafficking chain, or to serve a specific function. Our guerrillas were successful in securing the fuel or resource to the TCO, but the TCO cannot or does not use that commodity. Therefore they provide it to a third organization, perhaps a gang they exert control over that is able to sell it on the streets in another region. The money earned goes back to the TCO allowing it to grow as a regional player. To add further complexity, consider the size and breadth of this organization. Perhaps this TCO physically controls multiple trafficking routes within a region and is also profiting from everything else that travels along those routes regardless of their personally supported operations. Now any organization transporting even licit material in this region must account for additional fees or tolls extorted by the TCO along the route. Also consider how that gang interacts or seeks to control the local populace. What other crimes are they committing to support the main effort of drug sales?

Again the FARC serves as a real-world example. They reportedly enjoy a relationship with al-Qaeda in the Islamic Maghreb (AQIM). AQIM agrees to secure cocaine shipments through Mali to users in Spain for approximately $2,000 per kilogram. In at least one instance, the Malian military found an abandoned aircraft capable of lifting 20 tons of cocaine; the flight originated in Venezuela.[4] Also, in Afghanistan the Haqqani organization is familiar with criminal activity, specifically extortion. Haqqani controls areas in Loya Paktia on both sides of the Durand line. Transport trucks carrying

supplies, including those contracted by coalition forces, pay fees along the way that vary depending upon the cargo.[5] Finally, consider Mara Salvatrucha (MS-13) as an example of gang activity. MS-13 has links with Los Zetas Cartel managing human trafficking routes north through Central America. Similarly, gangs of the like serve as a source of personnel which often results in armed factions that, in addition to committing less lucrative crimes, assist larger groups' wage conflict to gain power.[6]

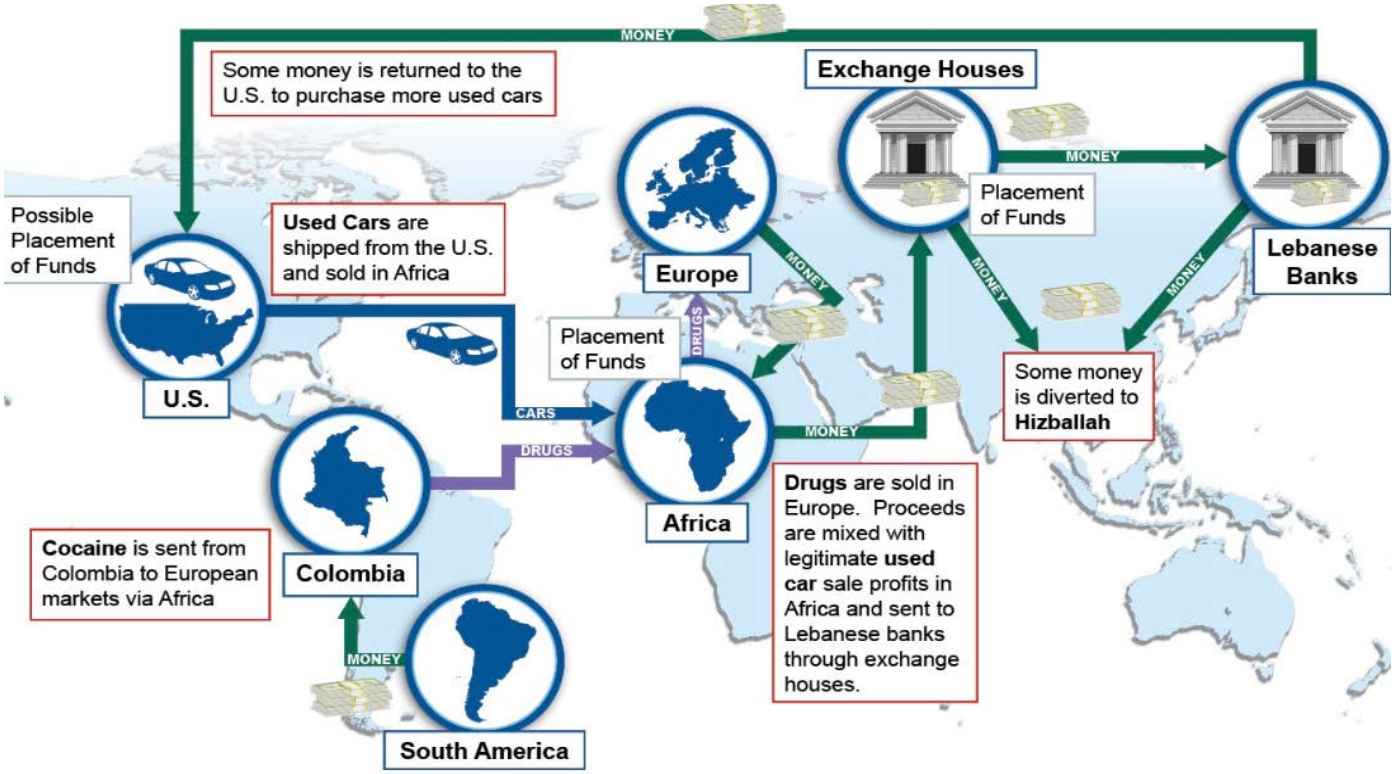


Figure 2: Hezbollah crime to fund operations (example) *Source:* Financial Crimes Enforcement Network, US Department of Treasury, 4 April 2013 as used in TRISA's Train-the-Trainer slides

Exercise Design Considerations

The subsequent discussion only serves to highlight certain considerations within the exercise design process to facilitate the use of crime and criminal organizations. When developing detail within operational variables, crime fits very well into the economic variable, but can also be prevalent within the political and social variables. Understandably, the amount of actual "play" time may limit the extent and breadth of criminal operations. Consider building additional detail into the road to war especially in regard to their current relationships, alliances, and control or pervasiveness within the populace. Knowing the criminal element's primary motivation of profit, developing great detail early will not restrict follow on play as these elements readily shift alliances to best posture themselves for future earnings and power gain.

A cursory review of the Army Universal Task List (AUTL) reveals several tasks in which leveraging crime and criminal organizations against may prove useful. These tasks, and some of their subordinate tasks, include but are not limited to the following tasks. (See callout box of AUTL sample tasks at right.)

Crime and criminal organizations may only seem pertinent when conducting stability operations. However, like any threat actor, training units must consider second- and third-order consequences of the operational effect they seek to

Army Universal Task List (AUTL) SAMPLE TASKS

ART 1.6.2
Enhance Movement and Maneuver
ART 2.0
Intelligence Warfighting Function
ART 4.1
Provide Logistics Support
ART 4.5.2
Enable Logistics
ART 5.7
Integrate, Inform, Influence Activities
ART 5.8
Establish and Maintain Discipline
ART 6.5
Conduct Operational Area Security
ART 7.3
Conduct Stability Operations
ART 7.4
Conduct Civil Support Operations
ART 7.6
Operational Themes

achieve. For instance, consider how the construction of combat roads and trails, the development of traffic control plans, enforcement of highway regulations, or area security during offensive or defensive operations purposefully or inadvertently impact criminal operations and what could be threat responses.

Integrating crime and criminal organizations into scenarios will yield a more complex and realistic scenario. The aforementioned examples build upon trafficking successes demonstrated at one CTC, which is also important due to its prevalent practice. However, integrating other forms of crime, many of which can be found in TC 7-100.3, *Irregular Opposing Forces*, and showing their support to each other or even criminal civic action is also effective. Build the threat as it best suits the training unit's objectives and task list, but do not feel the pressure to build additional force structure to do so as integrating crime is just as important. Ultimately, making a great dinner doesn't always mean using everything in the pantry.

Notes

[1] Douglas Farah, "Fixers, Super Fixers and Shadow Facilitators: How Networks Connect," International Assessment and Strategy Center, 20 April 2012.
[2] Douglas Farah, "Fixers, Super Fixers and Shadow Facilitators: How Networks Connect," International Assessment and Strategy Center, 20 April 2012.
[3] Douglas Farah, "Terrorist-Criminal Pipelines and Criminalized States: Emerging Alliances," 1 June 2011.
[4] Douglas Farah, "Terrorist-Criminal Pipelines and Criminalized States: Emerging Alliances," 1 June 2011.
[5] Gretchen Peters, "Haqqani Network Financing: The Evolution of an Industry," July 2012.
[6] Patrick Corcoran, "How Street Gangs Have Complicated Mexico Security," 10 September 2013.

DECOYS AND DECEPTION TTP IN A DEFENSE

by Kris Lechowicz, Threat Assessment Team (DAC)

This series of threat tactical diagrams presents an example of how decoys can deceive and disrupt an enemy's offensive plan. Successful deception creates conditions that place an enemy at a significant tactical disadvantage. In this example, the threat defeats lead units of a battalion-size task force.

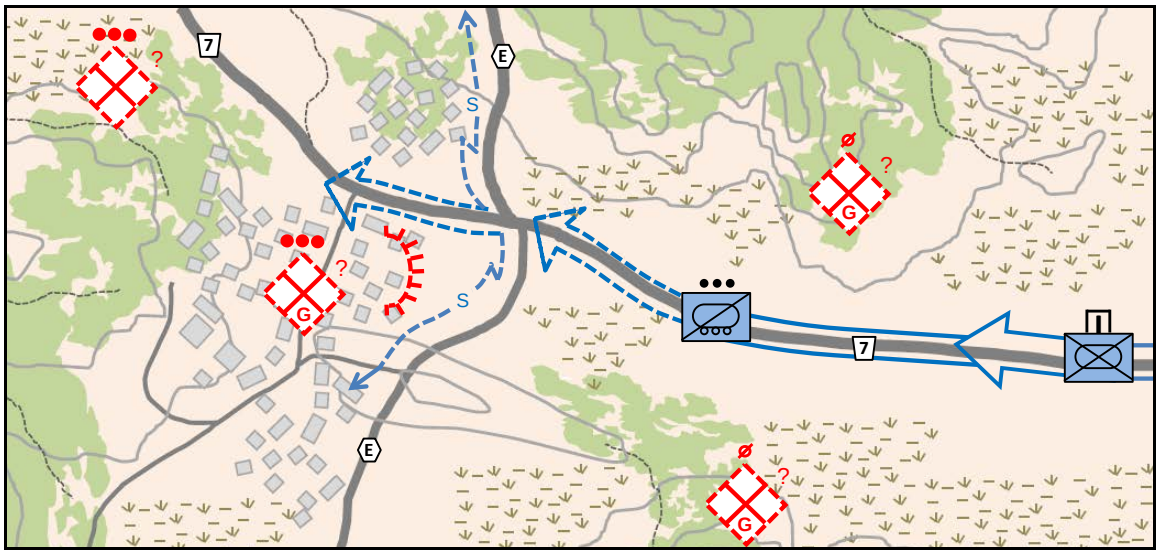


Figure 1. Enemy situational awareness of the axis of advance

Create an Enemy Vulnerability

The threat is conducting a withdrawal to the west in order to establish an area defense along the west side of a major river. East of the river line, threat units occupy defensive positions along main avenues of approach to slow the enemy advance. Deception and use of decoys are a key aspect of this defense. Radio intercepts indicate that the enemy is

unsure of threat strength east of the river and will conduct offensive actions to reestablish contact with threat main defenses or rear guard forces. Threat intelligence reports estimate that up to an enemy mechanized task force may attempt to attack west along the canalized terrain of Highway 7 (see figure 1).

Defending the Highway 7 approach, Team JANOS is an ad hoc company-size unit task organized with two understrength infantry platoons, one self-propelled howitzer, an air defense (MANPADS) squad, and one armor platoon. A guerrilla platoon from the local insurgent organization is integrated into the defense of the village and highway-road network and provides security observation posts to the east.

The team commander also has a number of main battle tank decoys that he arrays as a disruption element along a tree line to the north of the main highway intersection. Effective deception of portraying a threat tank platoon to the north of Highway 7 and east of Route E is critical to the initial area defense.

The Team JANOS commander organizes his defense on a kill zone in restrictive terrain along the highway (see figure 2). He emplaces obstacles of antitank mines and improvised explosive devices (IEDs) on primary and probable enemy approaches. The IEDs are armed and have assigned teams with orders of when to detonate the munitions. His infantry platoons provide overlapping direct fires coverage of the kill zone and the howitzer has registered on target reference points in the battle zone. The actual armor platoon is in reserve with contingency priorities to move, on order, to an attack by fire position in support of the primary kill zone on Highway 7. A secondary contingency is to be prepared to move south and ambush enemy elements approaching from the south on Route E.

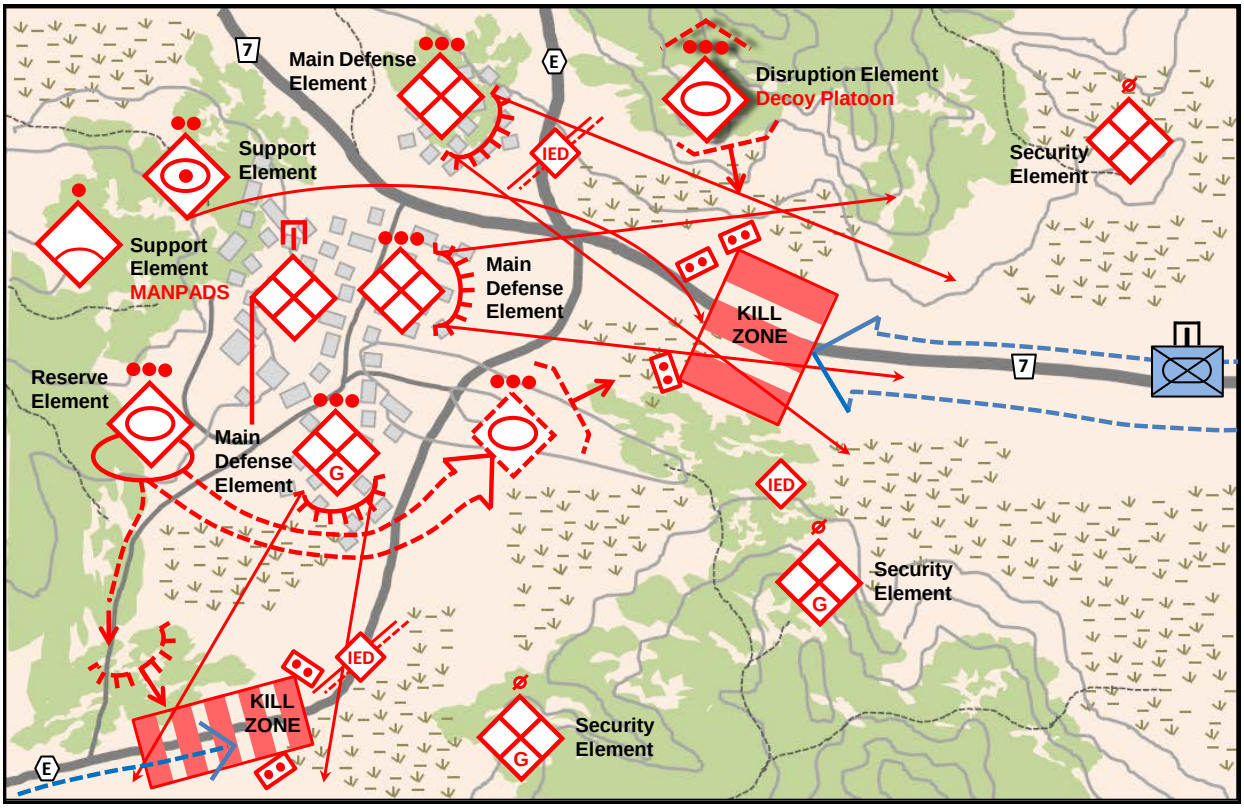


Figure 2. Threat defensive plan with decoys

The threat team commander plans to deceive lead enemy elements with the decoy armor platoon and cause the enemy to deploy its combat power focused on the tree line to the north. This orientation will create a vulnerable enemy flank and rear in the kill zone (see figure 2).

Deceive Enemy Decisionmaking

Threat security elements report that armored wheel vehicle reconnaissance at platoon strength is approaching along Highway 7. The terrain restricts their lateral movement and enemy actions appear focused on route reconnaissance with no dismounted action to either flank.

As the lead reconnaissance elements enter the kill zone, threat detonations near the decoy platoon draw immediate attention. Simultaneously, indirect fires land in the kill zone as the northern threat platoon commences direct fires in support of the "tanks." The enemy vehicles orient to the north and return direct fires and call for indirect fires at "tanks" in the tree line and infantry positions in the village north of Highway 7.

The threat infantry platoon in the center holds any direct fires initially as enemy vehicles attempt to maneuver. One vehicle quickly hits an antitank mine and is immobilized. The enemy reconnaissance unit appears to be fixed in the kill zone. The center platoon remains silent in its village positions as part of the threat team commander's deception on his relative defensive strength. The enemy platoon leader remains focused on threat direct fires and "tank" fires from the north and northwest (see figure 3).

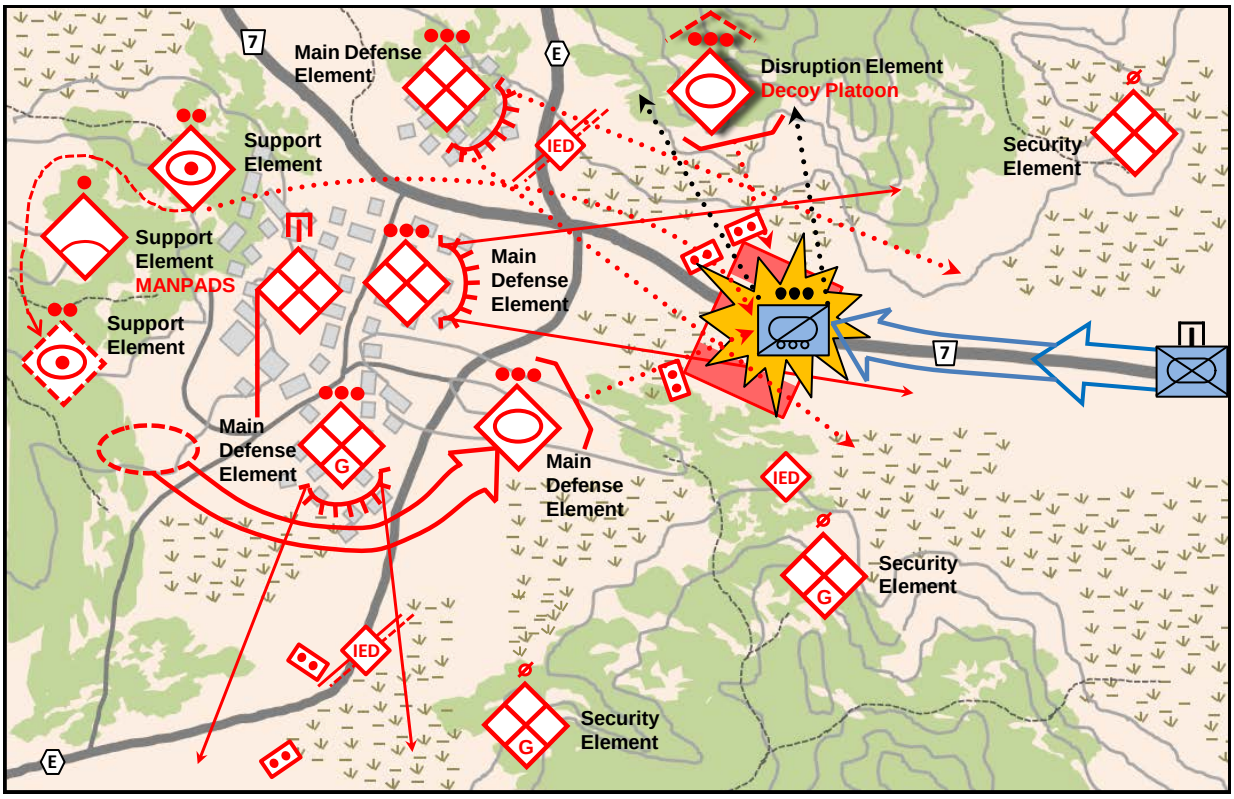


Figure 3. Successful threat use of decoys in a defense

With the guerrilla platoon reporting no enemy activity on approaches from the south, the threat team commander directs his reserve to occupy the pre-planned attack by fire position and support the team defense. Having rehearsed its movement route and direct fires plan into the kill zone, the tank platoon arrives within minutes below the hill crest. The tank platoon leader issues final instructions as he orders the tanks to move up to hull defilade positions together and commence main gun fires.

Achieve Engagement Success

The massed tank main gun fires into the enemy flank and rear are devastating. The enemy reconnaissance platoon is destroyed in the kill zone as a combination of massed direct fires from the tank platoon, infantry platoon, and supporting indirect fires of the howitzer. The entire engagement lasts less than 15 minutes.

The Team JANOS commander assesses his unit losses and reorganizes positions for the continued defense. Two soldiers were killed and three wounded in the engagement. One wounded soldier required immediate medical evacuation. Almost all of the antitank mines remain intact. None of the IEDs were detonated. One tank has a transmission problem and cannot move from the hill position; however, it is in hull defilade and can shoot its main gun into the kill zone. The other tanks move back down the reverse slope into hide positions. Ammunition resupply is underway at the infantry simple battle positions (SBP) as soldiers continue to improve fighting positions.

Threat security elements to the east report that enemy mechanized elements are forming along Highway 7 but have only just started to move west along the highway. The howitzer has repositioned while the air defense squad is alert for any rotary or fixed wing enemy aircraft. Team JANOS is ready for the next engagement.

Decoys and Deception

Note. **This TTP example incorporates several observations from a recent training rotation of coalition forces at a combat training center (CTC). Decisive action and prudent decisionmaking in use of decoys by a threat commander was instrumental to defeating an enemy mechanized infantry task force attack.**

AIRCRAFT THREATS

by Marc Williams, Training, Education, and Leader Development Team (CGI Ctr)

"If it flies, it dies" is the adage of the air defense branch and one that holds uncomfortable truth for aviators. The US goes to great lengths to ensure it has air superiority in conflict zones, and this includes air-to-air combat as well as neutralizing ground-to-air capabilities through suppression of enemy air defense (SEAD) missions. Some of the threats to our aircraft are ground fire from small arms, man portable air defense systems (MANPADS), and gun-missile systems. Relatively recently, the threats have included laser "dazzlers" fired at cockpits and high-energy laser systems for countering rockets, artillery, and mortar shells (C-RAM).

C-RAM

Since the invention of the laser, military application has been the goal of many researchers. However, the energy requirements for such a weapon have been considered too high. In October 2012, MBDA Germany completed a further major step toward a laser weapon system capable of providing air defense. For the first time, the company's high-energy laser demonstrator was used to demonstrate the complete deployment sequence in C-RAM. Using 40 kilowatts (kW) of laser power, the laser demonstrator successfully acted on airborne targets at a range of over 2,000 meters. For these tests, MBDA Germany's laser demonstrator was equipped with a new, improved performance, significantly more compact and lighter optical system which was integrated in a transportable container. During the tests, the illumination and effect laser was pre-targeted using a radar (SPEXER™ 2000) and an IR optronics system (MEOS II) supplied by Cassidian. A multi-stage control system, incorporating an in-house developed image processing system, was used to lock onto the target at close range.[1] This was tested against multiple artillery shells in a wide variety of flight paths at an altitude of 1,000 meters. This implication is that it will also be effective against manned aircraft within range.

In November 2012, Rheinmetall successfully tested a 50kW laser weapon in Switzerland against steel girders, nose-diving target drones, and 3.2-inch steel projectiles moving at 50 meters per second. Designed for air defense, asymmetric warfare, and C-RAM operations, the Rheinmetall laser isn't a single weapon, but two laser modules mounted on Oerlikon Revolver Gun air defense turrets with additional modules for the power supply. The lasers are combined using Rheinmetall's Beam Superimposing Technology (BST) to focus a 30kW and a 20kW laser on the same spot. This gives it the destructive power of a single 50kW laser. Rheinmetall claims this laser works in snow, dazzling sunlight, ice, and rain. Currently this is a stationary system which could be used for static air defense of military installations and forward operating bases. Rheinmetall looks to develop a mobile system in the future.[2]

On 12 December 2012, Lockheed-Martin successfully tested a tactical-level system named Area Defense Anti-Munitions (ADAM). Providing short-range defense of high-value areas including forward operating bases, the ADAM system is designed to track targets at a range of

more than 5 kilometers and to destroy targets at a range of up to 2 kilometers. It is specifically designed as defense against rocket and unmanned aerial systems (UAS), but may also prove effective against manned aircraft.[3]

Dazzlers

Lasers are especially dangerous to human eyes and there are multiple cases of people shining them at pilots while in flight or on final approach. In June 2011, three men in their 20s were arrested in Chicago for shining a green laser at a police helicopter.[4] According to the FBI, there were 10 reported laser incidents in Virginia Beach during 2011 and 98 in Virginia. January 25, 2012 marked the first felony conviction in a laser-pointing case in Virginia.[5]

Russia has developed harsh laws concerning the use of laser pointers against airplanes. The Criminal Code provides three years in prison or an 80,000 ruble fine (approximately $2,600) for "laser hooliganism." If the airplane's crew is blinded by laser pointers, which may disorient pilots, those responsible will face up to seven years in prison. If laser hooliganism causes the jet's crash, the sentence will increase to 10 years in prison.[6] There were 50 such cases in Russia in 2011.

Gun Systems

"Small arms" in air defense parlance includes heavy machineguns such as the US M2 .50 caliber and the Russian DsHK 14.5mm machinegun. Small arms were extremely effective against rotary wing aircraft in the Vietnam War, and were responsible for multiple aircraft downings and damage in Operation Urgent Fury (Grenada), Operation Just Cause (Panama), Operation Gothic Serpent (Somalia), and the Battle of Najaf in 2003 (Iraq). Not classed as an air defense weapon, the RPG-7 has been proven effective against low flying or hovering aircraft when fired in volley. During the Vietnam War, enemy squads were drilled in downing low-flying US helicopters using nothing more than AK-47s.

The current rebellion in Syria has provided video evidence of ground fire downing both rotary wing and fixed wing aircraft. The Free Syrian Army (FSA) has used anti aircraft weapons, such as the ZU-23-2, to bring down Syrian aircraft. For more information on the ZU-23-2 weapon system, refer to the *Worldwide Equipment Guide,* Vol 2: Airspace and Air Defense Systems, p. 6-49.

Below are examples of successful FSA attacks on Syrian aircraft. (Compilation from the CTID OEA Team Threat Report, *The Free Syrian Army: Rifles to MANPADS*, November 2012.)

June 26, 2012
A helicopter was shot down in Maardebseh, Idlib. The Suqour al-Sham Brigade and the Shuhada Jebel al-Zawiyah Battalion both claimed responsibility. Video Source

July 7, 2012
A surveillance aircraft was shot down by members of the Jafar al-Tayyar Battalion in Deir Ezzor.

Air Threats

Threats to aircraft include ground fire from small arms, man portable air defense systems (MANPADS), and gun-missile systems. In relatively recent attacks, the threats have included laser "dazzlers" fired at cockpits and high-energy laser systems for countering rockets, artillery, and mortar shells (C-RAM).

August 13, 2012A MiG jet was shot down in the town of Mohasan, Deir Ezzor. Video Source

August 27, 2012
A helicopter was shot down in the vicinity of the Jobar neighborhood. Video Source

August 31, 2012
A MiG jet was shot down by the Shuhada Jebel al-Zawiyah Battalion during a week-long attack on the Abu Dhuhur airport. Video Source

September 4, 2012
A second MiG jet was shot down by the Shuhada Jebel al-Zawiyah Battalion during the week-long attack on the Abu Dhuhur airport.

September 5, 2012
A helicopter was shot down over Damascus by the Saif al-Islam Battalion of the al-Islam Brigade.

MANPADS

Man-portable air defense systems (MANPADS) were originally developed in the 1940s to provide air defense to ground troops (German *Fliegerfaust*). The first generation of missiles was infrared guided, developed in the 1960s, which lock-in on an aircraft's exhaust

plume. These include the American Redeye, the Chinese HN-5, and Soviet SA-7 and were referred to as "tail chasers" or "revenge weapons." Second generation MANPADS including the Russian SA-14 and Chinese FN-6 permit head-on and side engagements, and the US Stinger includes a UV target-detection mode. Third generation MANPADS include the French Mistral, Russian SA-18, and US Stinger B. These can recognize and reject decoy flares. Fourth generation missiles (Stinger Block 2) use advanced sensor systems and have greater range.

Command line-of-site (CLOS) missiles require a gunner to visually acquire a target and "fly" the missile to that target. These include the British Blowpipe, Javelin, and Starburst. Laser guided missiles require a highly trained gunner to keep a laser trained on the target while the missile flies the beam. These include the Swedish RBS-70 and the British Starstreak.

Twenty-five countries, including the United States, produce man-portable air defense systems. Possession, export, and trafficking of such weapons are officially tightly controlled, due to the threat they pose to civil aviation, although such efforts have not always been successful. This was especially true following the Russia-Afghan War when the US provided Stinger missiles to Afghan mujahedeen. Use of MANPADS against civilian aircraft is an especially sensitive issue and not without precedence as the incidents listed below show.

Figure 2. MANPADS hit, Iraq (2003)

Known civilian aircraft incidents:

03 September 1978: A Rhodesian Vickers Viscount was struck by a Soviet-made Strela 2 fired by Zimbabwe People's Revolutionary Army (ZIPRA) cadres near Karoi. 38 killed in the crash, another 10 killed on the ground by guerrillas.

12 February 1979: Air Rhodesia Flight 827 was shot down by ZIPRA guerrillas using a Strela-2 surface to air missile (SAM). 59 killed (55 passengers, four crew). After this incident, Air Rhodesia modified the exhaust pipes of their aircraft and painted aircraft with low-radiation paint.[7]

21 September 1993: A Transair Georgia airliner on final approach was shot down by a SAM fired by rebels in Sukhumi, Abkhazia, Georgia. 27 killed (22 passengers, five crew).

29 September 1998: Lionair Flight 602 from Sri Lanka was shot down by a MANPAD fired by Liberation Tigers of Tamil Eelam (LTTE). 55 killed (48 passengers, 7 crew).

28 November 2002: Two SA-7b Mod 1 "Grail" SAMs were fired at an Arkia Airlines Boeing 757 as it departed Mombasa, Kenya. Both missiles missed and the aircraft continued its flight to Israel with Israeli Air Force fighter escort. Police found the launcher assemblies and missile casings 2 km from the airport.[8]

22 November 2003: A DHL Airbus A-300B was hit by a SA-7 SAM at 10,000 feet over Iraq. The crew managed to land the aircraft at Baghdad International Airport (see figure 1 on previous page).

23 March 2007: A TransAVIAexport Airlines Ilyushin Il-76 aircraft was shot down outside Mogadishu, Somalia. Eyewitnesses reported seeing a SAM strike the aircraft. The MANPAD was reported to be a Strela-3 (SA-14). 11 killed (4 passengers, 7 crew).

Known military aircraft incidents:

17 November 1991: A USAF F-16 and an RAF Tornado GR1 were shot down by Strela-3 SAMs during Operation Desert Storm in Iraq.

06 April 1994: A SAM shot down a Dassault Falcon 50 carrying the Rwandan and Burundian presidents in Kigali, Rwanda. 12 killed.

16 April 1994: A RAF Sea Harrier was shot down by a MANPAD during Operation Deliberate Force in Serbia while attacking two Bosnia Serb tanks.

27 May 1999: AmiG-21 and a MiG-27 of the Indian Air Force were shot down during the Kargil Conflict by a Pakistani Anza Mark II MANPAD.

19 November 2000: A Su-27 was shot down by a Strela-3 in Angola fired by UNITA forces during final approach.

19 August 2002: An Igla SAM hit a Russian Mi-26 helicopter in Khankala, Chechnya. 127 killed.

27 November 2012: Videos from Syria appear to show first confirmed hit of aircraft by surface-to-air missile by Syrian rebels (see figure 3).

Anti-Aircraft IEDs

Just like IEDs are used against troops and ground vehicles, there have been instances of anti-aircraft IEDs. In 2006 the Army's Aviation center was discussing insurgent use of devices being fired into the air and exploding with proximity fuses at US helicopters. On 15 May 2009, a scout helicopter operating near Mosul, Iraq was damaged and forced to land by an anti-aircraft IED.[9] These are used to deny landing access and to disrupt flight patterns for rotary wing aircraft.[10] While not common, they have the potential of becoming more effective in a long term counterinsurgency environment.

Training Readiness

Threats to aircraft remain a significant aspect of uncertain, complex environments.

Threats against US aircraft are numerous and must be replicated in training. Allowing aircraft to operate freely in a hostile area is unrealistic and teaches the wrong lessons to air crews. At the same time, the weapons systems deployed against aircraft must be realistic; this means no less lethal, and no more lethal, than the real-world systems they replicate.

Figure 3. MANPADS kill, Syria (2012)

Application in Training

The threats against US aircraft are numerous and must be replicated in training. Allowing aircraft to operate freely in a hostile area is unrealistic and teaches the wrong lessons to air crews. At the same time, the weapons systems deployed against aircraft must be realistic. This means no less lethal, and no more lethal, than the real-world systems they replicate.

This can be controlled by the number of air defense systems in the training area and ensuring the hit-to-kill indicators match real-world capabilities. Recognizing the abilities of conventional systems requires pilots to be experts on their counter-systems and will reinforce the need to adapt their tactics as the opposing forces shift theirs.

Notes

1. MBDA Germany's laser demonstrator proves its air defence capabilities, accessed 15 November 2012.
2. Rheinmetal successfully tests 50kW high-energy laser weapon, accessed 06 January 2013.
3. Lockheed Martin's New Killer Laser Puts Israel's Iron Dome to Shame, accessed 19 December 2012.
4. UPI.com, 3 arrested for pointing laser at helicopter, accessed 17 May 2012.
5. FBI, Virginia Beach man pleads guilty to using laser to endanger aircraft, accessed 17 May 2012.
6. ITAR-TASS, Duma seeks criminal responsibility for "laser hooliganism," accessed 17 May 2012.
7. Peter Petter-Bowyer, "Winds of Destruction," Trafford Publishing.
8. David A. Kuhn, "Mombasa attack highlights increasing MANPADS threat," Jane's Intelligence Review, February 2003.
9. Daniel W. Smith, Iraq Slogger; Mosul: US helicopter hit by "anti-aircraft IED," accessed 20 May 2009.
10. Small Wars Journal, accessed 04 December 2012.

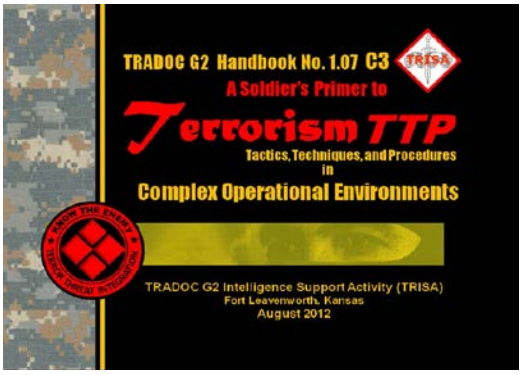
THREAT TTP: SUICIDE VEHICLE BORNE IMPROVISED EXPLOSIVE DEVICE

by Jim Bird, OE Assessment Team (Overwatch CTR)

Veterans of Operation Enduring Freedom (OEF) know only too well that improvised explosive devices (IEDs) and suicide bombings are anything but a novelty in the Afghan theater of operations. A new OEA Team Threat Report, *Abiding Threat at Camp Chapman*, examines a recent terrorist attack at Forward Operating Base (FOB) Chapman, Afghanistan, as well as its implications for the information warfare (INFOWAR) arena. The connection between a vehicle borne IED (VBIED) that killed four Afghan nationals (and wounded several others) on 26 December 2012, and an insider attack that occurred almost exactly three years earlier at the same general location, lies essentially in interpretations given both events by the international news media.

VBIED Attack

The day after Christmas 2012, a suicide bomber detonated a VBIED at the main entrance to FOB Chapman near Khost City, Afghanistan. The attack occurred as Afghan National Security Force (ANSF) personnel halted a minivan entering the compound, in accordance with the base's standard operating procedure. After pausing briefly at the checkpoint, the minivan driver advanced a few yards farther before setting off the device that killed himself, a security officer nearest the vehicle, a civilian passerby, and two unfortunate local drivers who made their living by bringing passengers to and from their daily workplaces on the FOB. Although the blast shook windows in buildings two miles from the scene, the base perimeter remained intact, and no US personnel were killed or wounded in the incident (see figure 1 next page).



The 26 December 2012 suicide bombing at FOB Chapman is an excellent example of a strike and detonate VBIED attack depicted in the TRADOC G2 Handbook No. 1.07 C3, *A Soldier's Primer to Terrorism TTP: Tactics, Techniques, and Procedures in Complex Operational Environments*. The following FOB Chapman illustration shows a close-up graphic representation of the incident based on available open source descriptions. The graphic is not to scale, and all locations are approximate:

Aside from what this tactical VBIED attack teaches about enemy TTP, there are INFOWAR considerations also. Statements issued by the Taliban in the immediate aftermath of the December 2012 incident gave no indication that it was timed to draw public attention to a previous suicide bombing that occurred at Camp Chapman three years earlier. On 30 December 2009, an insider attack killed seven Central Intelligence Agency (CIA) employees and the Chief of Jordan's General Intelligence Directory. The 2009 bombing inflicted more casualties on the CIA than any other single incident in the previous 25 years, and caused the temporary shutdown of the CIA office in Khost City until a replacement team could be assembled and dispatched to the area. Predictably, it also made a big splash with international news agencies.

Al Jazeera was hardly alone in suggesting a linkage between what in actuality were two distinct events separated in time by three years. By following suit and portraying the 2012 attack on FOB Chapman as a sequel to the earlier bombing, the collective effect of media coverage conferred strategic significance on what in fact amounted to little more than an unsuccessful enemy attempt to penetrate a FOB perimeter.

Training Implications

Tactically and operationally, the latest attack on Camp Chapman will have little if any impact on the outcome of the Afghan war. Viewed from the perspective of information warfare, however, the December 2012 episode should serve as a reminder to commanders of the media's potential power to impart strategic significance to relatively minor tactical occurrences. Published accounts of the after-Christmas suicide bombing emphasized a perceived undiminished ability of the Taliban to attack targets almost at will throughout Khost Province over a decade into the OEF deployment.

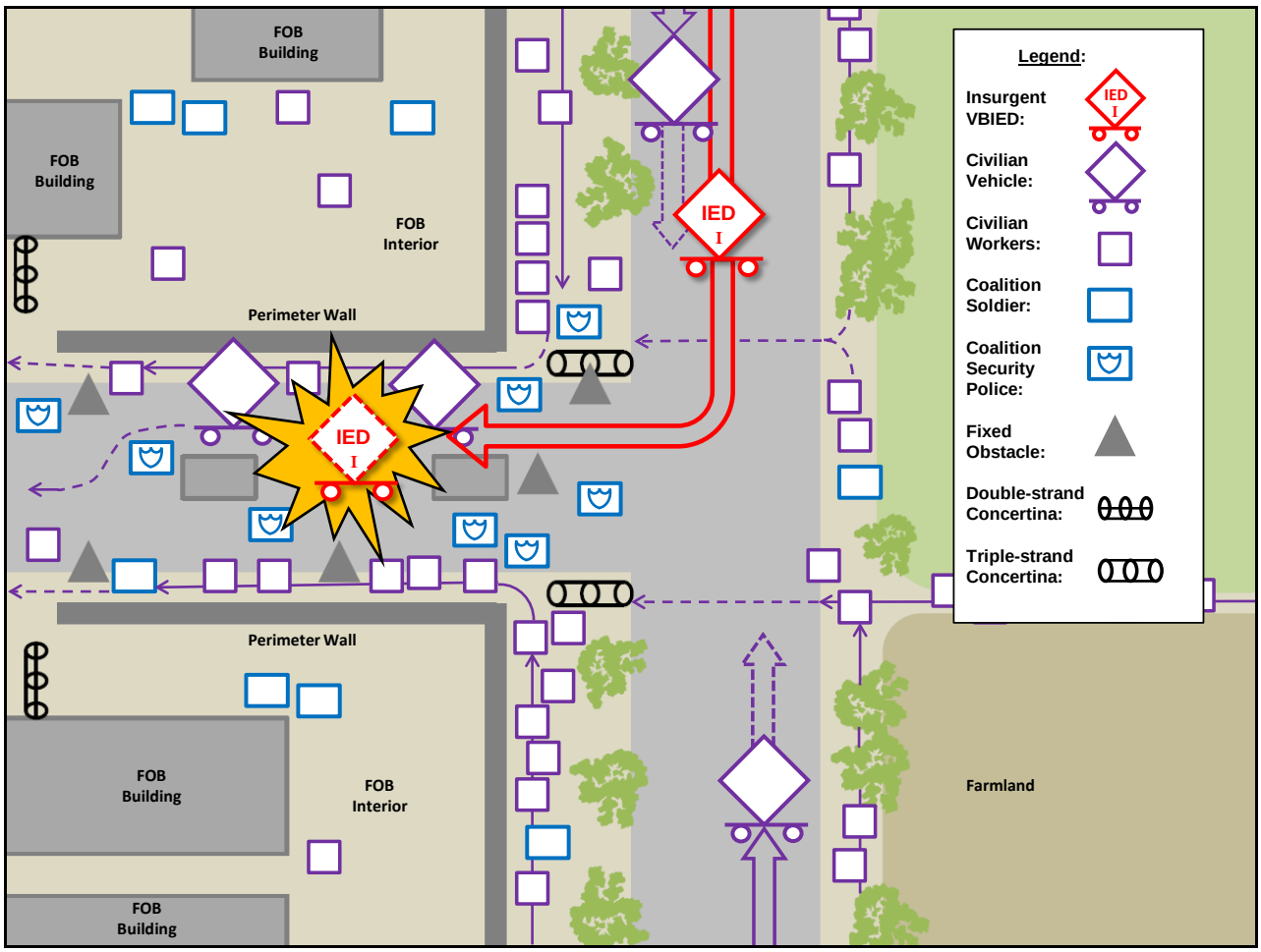
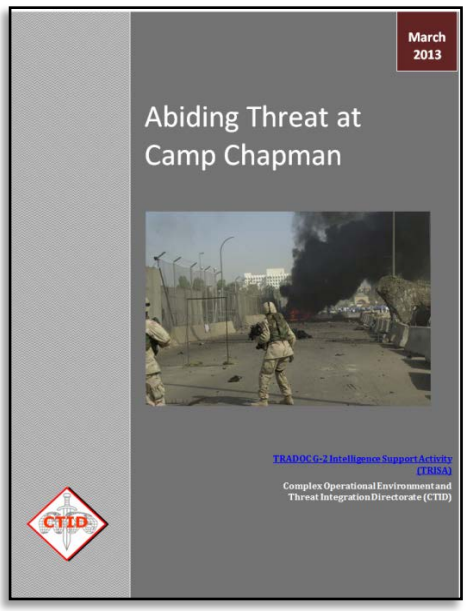


Figure 1. Camp Chapman suicide VBIED TTP

The 26 December suicide bombing at FOB Chapman also illustrates the potential of a single individual to instill fear in a local population, out of all proportion to the small number of casualties actually inflicted. The VBIED blast occurred between 0730 and 0800, indicating that it was timed to inflict a maximum number of casualties as local nationals employed by the US arrived at the FOB to begin their workday. This interpretation meshes with the Taliban spokesman's comment attributing the motivation behind the attack to a desire to kill and injure Afghans who work for the Americans and who support the regime of President Hamid Karzai. Finally, the 26 December terrorist attack at FOB Chapman underscores the need for deployed forces to keep their guard up as the Coalition drawdown continues, especially on the anniversaries of previous terrorist attacks.



Several aspects of this event will make it of interest to the Army training community. It drives home the point that no static facility is ever totally secure, especially if a threat actor is willing to die in an attack. It also reminds readers that a small force or single individual can inflict serious damage, either in a physical sense, or by undermining the credibility of security forces.

Finally, it suggests that this type of suicide bombing is easily replicated, needs few role players, and requires minimal logistical support. In sum, the *Abiding Threat at Camp Chapman* Threat Report provides information to the Army training community on the December 2012 attack on FOB Chapman, and examines it from the information warfare implications.

HYBRID THREATS AND THE ART OF RECONSTITUTION OF THE FORCE

by Walter L. Williams, Training, Education, and Leader Development Team Leader (DAC)

A unit may be considered combat ineffective because of number of equipment losses, casualties, morale, unit cohesion, leadership, and training. One could easily make the case that the culture or sub-culture of a force could be a factor in the combat effectiveness of a force. Discussing strength percentages to estimate if a hybrid threat remains combat effective is fundamental to applying methods in the art of unit reconstitution. Consideration of strength percentages also serves as a "beginning point in discussions that try to answer the elusive question of quantifying acceptable attrition rates necessary for commanders and staffs to use in modeling, training, and actual combat situations and still accomplish their mission." [1]

reconstitution – Extraordinary actions that commanders plan and implement to restore units to a desired level of combat effectiveness commensurate with mission requirements and available resources.

In his article, "Attrition and Combat Breakpoint Decisions," Gerald Halbert defines a breakpoint as "any action that causes a commander to change his combat posture due to enemy activity. It is important that commanders and their staffs understand how a simple maneuver or attrition can cause a breakpoint." For example, an 80% strength attacking force may encounter a 50% to 40% strength defending force reinforced or supported by indirect and aerial fires (as well as effective use of the terrain) that causes the attacking force to transition from an offensive posture and to a defensive posture due to attrition of a force. However, throughout the course of history "there [have been] indications that it is not the absolute number of casualties that causes a force to break off an attack or give up the defense, but rather the number of casualties inflicted during a given period. The great range of casualty rates possible before reaching a breakpoint indicates that there may be no magic or single number of casualties that a military force can take and remain combat effective."[2]

Attrition of a force can occur either by attacking a force or defending against a force. In some cases the skillful art of maneuver can make it obvious to an enemy force that it cannot execute its assigned mission as planned. Thus, the issue for a commander becomes do we really have to attrite the force or execute a maneuver in such a way the enemy either retreats or surrenders.

Such was the case of the large British-led coalition surrendering to a numerically smaller Japanese assault force in Singapore during the World War II Malayan campaign. The British Imperial garrison on Singapore consisted of 146,000 troops who were well trained, equipped, and had sufficient ammunition and supplies. They were facing a Japanese assault force of 35,000 troops who were exhausted and severely depleted of key logistical supplies such as ammunition and food. It seemed that the Japanese assault force was on its last leg or gasping for breath, but 130,000 British, Australian, and Indian officers and soldiers surrendered to the Japanese on 15 February 1942. During the entire Malayan campaign the Japanese suffered 9,000 casualties out of 60,000 troops. On the other hand, the British-led coalition force suffered 16,000 casualties out of a force of 146,000. This translated to the Japanese loss of 15% to a British coalition loss of 11%. The surrender of the British-led coalition could be attributed to a combination of equipment losses, casualties, morale, unit cohesion, leadership, training, and water.

It is important to recognize that during the design of an exercise a trainer or modeler may seek a specific strength percentage or number to use in describing the overall posture for an attacking or defending force. The desired strength percentage becomes even more difficult as a trainer employs a force that is not only representative of a composite of tactics, techniques, and procedures (TTP) found worldwide, but is hybrid in nature as well.

Table 1, Hybrid Threats Unit Combat Effectiveness, presents a series of strength percentages (developed by TRISA-Threats) to use during the design of an exercise employing a hybrid threats force. Table 1 also provides a summary of

actions that may be employed by a hybrid threat commander as the strength percentage decreases. A discussion of the tactics that a hybrid threats force may employ can be found in the TC 7-100 series of publications.

Table 1 – Hybrid Threats Unit Combat Effectiveness

STRENGTH LEVEL	STATUS	REMARKS
80% or greater	Combat Capable	
70% - 80%	Combat Capable with minor deficiencies or losses	Unit uses adaptive tactics to compensate for losses or deficiencies
30% - 69%	Combat Capable with significant deficiencies or losses	Unit is assigned a special mission or role combined with adaptive tactics to compensate for losses or deficiencies
Less than 30%	Unit requires reconstitution	Generally the unit is withdrawn from the battle for reconstitution

Hybrid Threat Force Reconstitution

Reconstitution is performed in support of all combat operations. Although it is mainly a command and operations function, the actual refitting, supply, personnel fill, and medical actions are conducted by logistics units. There are two methods for conducting reconstitution: reorganization and regeneration.

Reorganization is action taken to shift resources internally within a degraded unit to increase its level of combat effectiveness. Reorganization is normally done at unit level and requires only limited external support such as supply replenishment, maintenance assistance, and limited personnel replacement. When continuity of the mission is of paramount importance, composite units may be formed from other units reduced by combat operations.

Regeneration is an action taken to rebuild a unit through large-scale replacement of personnel, equipment, and supplies. Additionally, it is action taken to restore command and control (C2) and conduct mission-essential training. Overall, the effort is directed at restoring the unit's cohesion, discipline, and fighting effectiveness.

The hybrid threat personnel and equipment replacement operations are based on unit strength reports and include the coordinated support and delivery of soldiers or warriors returning from medical facilities. The unit strength report is used to assess a unit's combat power, plan for future operations, and assign replacements on the battlefield. The unit strength report includes both personnel and equipment readiness status. The following are methods employed by the hybrid threat to reconstitute personnel losses.

- ***Individual Replacements.*** The hybrid threat can use the system of individual replacements in both peacetime and wartime. The sources of the replacement personnel are school graduates, reserve assignments, medical returnees, and normal assignments.
- ***Incremental Replacements.*** The hybrid threat can incrementally replace entire small units such as weapons crews, squads, and platoons. The replacements may be obtained from training units or reserve forces. They may be also composed of medical returnees and individual replacements during wartime.
- ***Composite Unit Formations.*** Composite units may be formed from other units reduced by combat operations. Composite units may be constituted up to operational strategic command (OSC) level.
- ***Whole-Unit Replacement.*** The hybrid threat uses whole-unit replacement when massive losses occur as a result of combat operations. Company-level and above units are brought forward from reserve forces to replace combat forces rendered ineffective.

Weapon systems replacement is simply a procedure for providing a weapon system to a combat unit. It involves processing the vehicle or equipment from a storage or transportation configuration to a ready-to-fight condition. It also involves the integration of a completely trained crew with the weapon system. For example, a battle damaged or maintenance incapable weapon system such as an APC or SP howitzer may be replaced and delivered to the unit by a maintenance crew. The maintenance crew returns to the maintenance or supply area once via an accompanying vehicle. Or, the weapon system may be delivered by a crew composed of incremental replacements. Equipment replacement such as trucks, radios, and individual and crew-served weapons may be either by individual systems or components.

It is important to note that this article is the tip of the iceberg in a discussion of attrition rates for combat effectiveness and methods of reconstitution of a hybrid threats force. The issue of quantifying an attrition rate or strength percentage to determine a units' combat effectiveness will continue to be elusive for years to come. What is required is a general consensus on a start point to determine combat effectiveness.

Notes

[1] Gerald A. Halbert, "Attrition and Combat Breakpoint Decisions," *How They Fight: Armies of the World,* NGIC-1122-203-98, 6 March 1998, p 1.
[2] Gerald A. Halbert, "Attrition and Combat Breakpoint Decisions," *How They Fight: Armies of the World,* NGIC-1122-203-98, 6 March 1998, p 1.

THE PK SERIES OF GENERAL PURPOSE MACHINE GUNS

Weapons in an Operational Environment

by Mike Spight, Training, Education, and Leader Development Team (CGI Ctr)

Figure 1. CAMP YASSIR, AL ASAD, Iraq – Iraqi Army Soldiers spend a day at the range, firing the PK machine gun as part of the School of Infantry
Source: Cpl. Adam Johnston, Photo ID: 2007442010, Submitting Unit: 2nd Marine Division[1]
Also see TRADOC G2 *Worldwide Equipment Guide*, Volume 1, for PKM data. Chapter 2, p. 2-18

There is little doubt that Germany's work in firearms development prior to and during WW2 has and continues to influence the development of military small arms in both the latter half of the 20th century and well into the 21st century. This influence can be seen in weapons designed in both the former Soviet Union and within Western nations and NATO.

Not only Germany's development of the StG-44 (Sturmgewehr 44–Assault Rifle-44, the inspiration for Mikhail Kalashnikov's AK-47), Germany would (with their MG-42 (Maschinengewehr-42—Machine Gun-42) also provide the design foundation for a series of Soviet General Purpose Machine Guns (GPMG), culminating with Kalashnikov's design of the Pulemyot Kalashnikova, ("Kalashnikov's Machine Gun"–PK) in the early 60s which was accepted for issue by the Soviet Ministry of Defense in 1965. To date, in excess of one million PK series machine guns have been manufactured and issued to Russian military and security forces.

Designed with the intent to fill multiple roles, GPMG are belt fed, and primarily utilized from their organic bi-pod, but can also be mounted on a tripod, and used in conjunction with a Traversing and Elevation (T&E) Mechanism from fixed defensive or overwatch positions. But the most common use is as part of an Infantry Platoon, from the bi-pod, where the firepower and increased effective range of the GPMG can greatly improve a unit's overall ability to deliver suppressive fire against either point or area targets. They are typically chambered for full-sized rifle caliber cartridges (7.62x51mm NATO, 7.62x54mm Rimmed, 7.92x57 Mauser). Modern examples include the M-60, the M-240, and the PK/PKM series of medium machine guns. This is a distinct difference from "Squad Automatic Weapons" (SAW) or "light machine guns" which are normally of the same caliber as the individual Soldiers Assault Rifles (5.56x45-mm NATO, 5.45x39-mm, 7.62x39-mm). Examples of these would be the FN manufactured "MINIMI"/M-249 or the Soviet/Russian RPD, RPK, and RPK-74M.

Specifically, the PK series of Russian GPMGs are chambered for the 7.62x54-mm Rimmed cartridge. This round has been in service since the 1890s when Czarist Russia adopted the Moisin-Nagant bolt action rifle as their standard issue weapon for the Infantry. It is a proven cartridge capable of acceptable accuracy, greater effective range, and the ability to penetrate barriers with greater effect than the 7.62x39-mm or 5.45x39-mm rounds used by the AK series of Assault Rifles or the RPD and RPK series of light machine guns.

Figure 2. Finish Army issue PKM machine gun *Source*: MKVI[2]
Also see TRADOC G2 *Worldwide Equipment Guide*, Volume 1, for PKM data. Chapter 2, p 2-18

The significant points of performance for the PK family of machine guns are as follows:

- Rate of fire (cyclic): 650 rounds per minute.
- Practical or combat rate of fire: 200-250 rounds per minute.
- Effective range: 1,000 meters (point targets); 1,500 meters (area targets).
- Weight: PK 19.84lbs; PKM 16.53lbs; PKP 19lbs.

- Feed system: Belt feed from right side, from detachable box containing 100, 200, or 250 linked rounds. ***Note***: Soviet/Russian machine guns typically feed from the right hand side and eject on the left hand side of the receiver.
- Gas operated: 3-position gas regulator, rotary bolt system, fires from open bolt position.
- Chrome plated bore.
- Air cooled: Quick change capable barrel (PK and PKM basic issue items include a spare barrel). ***Note:*** the quick change feature of the PK series of machine guns is not as efficient or fast as those of Western nation GPMGs.

By 1965, an improved variant had been tested, approved, and issued to the Soviet Army. The PKM (the "M" meaning "Modernized") featured product improvements that primarily lowered the weight from almost 20 pounds to 16.5 pounds (PK to PKM). This was done by replacing some machined steel parts with stamped parts, and by replacing the PK's heavier fluted barrel with a lighter, non-fluted barrel on the PKM. Otherwise, performance remains identical in both weapons. This weapon remains in current service with Russian Army, Naval Infantry, and Airborne forces.

As with the PK machine gun, the PKM can be mounted on a tripod, mounted on a pintle mount for use up top on tanks, Infantry Fighting Vehicles (IFV), Recon Vehicles, and rotary wing aircraft (when fitted with spade grips) for use as door guns. It is also used as a coaxial machine gun on Russian MBTs and IFVs (when fitted with an electrical solenoid).

Brought into service in 1999, the most recent variation on the basic PK/PKM them is the PKP or "Pecheneg." This variant is also the result of product improvements that, in this case, were driven by Soviet Army experiences in Afghanistan, and later in the Caucasus.

Figure 3. PKP (Pecheneg) machine gun *Source:* Vitaly Kuzman[3]

Also see TRADOC G2 *Worldwide Equipment Guide*, Volume 1, for PKM data. Chapter 2, p 2-18

Primarily used by SPETSNAZ and other elite Russian military or Ministry of the Interior forces, the PKP's performance points are basically the same as the PK and PKM. In terms of weight, it comes in at 19 pounds, as it is equipped with a heavier barrel that is manufactured from higher quality ordnance steel.

This totally eliminates the need for a quick change barrel capability, and an extra barrel and tripod are not included with issued PKPs. Its only role is to provide heavy, sustained firepower to squad/team level, without the need to change barrels. In theory, the PKP is capable of firing up to 600 rounds per minute (basically sustained cyclic fire) without overheating the barrel. This is considerably more than the 200-250 rounds per minute of practical or combat rate of fire for the PK/PKM.

Besides the heavier, high quality ordnance steel barrel, the PKP features radial cooling fins machined onto the barrel's surface and it is surrounded by steel jacket, which provides forced air cooling. In theory, air enters the jacket through cuts at the rear of the barrel close to the receiver, and exits the jacket where it terminates, midway down the length of the barrel, just before the gas port. Additionally, a fixed carrying handle is attached to the top of the barrel jacket, and the PKP has sling swivels that allow the gunner to move forward and fire the weapon from the assault position (slung,

and fired from the hip) if necessary. The PKP also has a mount on the left side of the receiver for attaching optical and night vision devices.

One additional modification over the PK/PKM is the location of the bipod. The PKP bipod is located just behind the muzzle of the weapon, which provides a steadier firing platform than the PK/PKM bipod, located on the gas tube. The only disadvantage offered by the PKP's bipod, is that it is too far forward for the gunner to grasp when standing/advancing, and firing from the hip.

The PK series has also been sold directly to many nations around the world, or licenses were granted for rights to manufacture. It is estimated that in excess of 50 nations currently use the PK/PKM or their domestically manufactured copy as their issued GPMG. The weapon's reliability and performance are such that some former Warsaw Pact members (Poland, for example), now manufacture a PKM clones that are chambered in 7.62x51mm NATO.

This level of distribution clearly indicates that like the AK-47/AK-74M and other Soviet era/Russian Federation weapons systems, the potential for future threats and their allies to be equipped and armed the PK/PKM/PKP is very, very high. Knowing and understanding its capabilities is essential for every tactical leader in the US Army.

Figure Credits

[1] PK machine gun. Source: Cpl. Adam Johnston, Photo ID: 2007442010, Submitting Unit: 2nd Marine Division.
[2] Finish Army PKM machine gun. Source: MKFI.
[3] Russian PKP (Pecheneg) machine gun. Source: Vitaly Kuzmin.

OPERATIONAL ENVIRONMENT THREAT TTP: KIDNAPPING AT KATSINA

by Laura Deatrick, OE Assessment Team (CGI CTR)

During the night of 19-20 December 2012, several gunmen simultaneously attacked the police station and a residence in Rimi town, Katsina State, Nigeria. Some of the attackers killed two Nigerians, wounded a third, and kidnapped a French engineer at the residence. The others bombed the police station, which was destroyed in the resulting fire. The OEA Team Threat Report, *Kidnapping in Katsina*, examines the details of the attack and possible training implications.

The nineteenth of December, 2012 started out as a typical evening in Rimi town, Katsina State, Nigeria. Francis Collomp, a French national, had settled into his residence for the night. An engineer by trade, Collomp had agreed to do one last mission for Vergnet S.A., a French company that was contracted by the Nigerian government to build the nearby wind farm. He had elected to be in country over the holidays so his fellow engineers could spend the time at home with their families. The night watchman and a local policeman were on guard duty, and a neighbor had come over to visit the watchman and charge his cell phone (see figure 1).

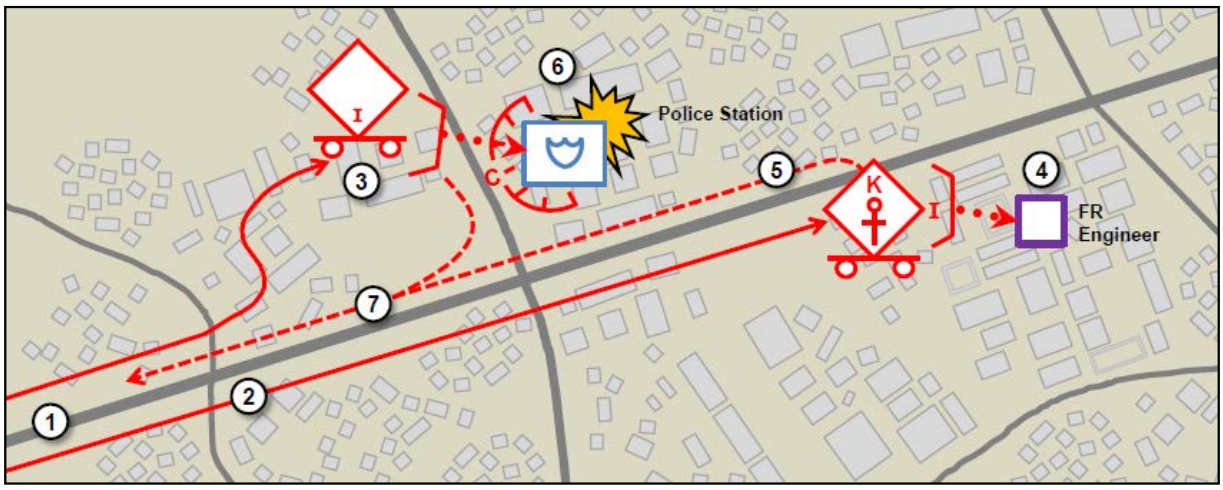
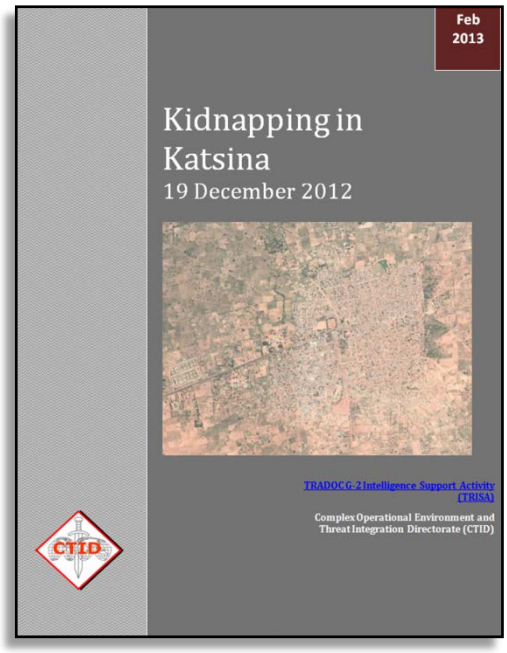


Figure 1. Kidnapping sequence at Katsina

Attack and Kidnapping Sequence (see figure 1)

1. Attackers enter town
2. Group splits into two
3. First element attacks police station
4. Second element attacks residence
5. Second element exfiltrates to vicinity of police station
6. First element bombs police station
7. Re-formed group exfiltrates



Late in the evening, around 30 armed men in three vehicles drove into town from the direction of the Katsina-Kano highway. Breaking into two groups, one element began to attack the local police station with small arms fire. The other proceeded to the residence where the engineers stayed when in-country. Storming the compound, the attackers shot and killed the night watchman and the visiting neighbor, and wounded the policeman

They kidnapped Mr. Collomp and then headed back toward the police station. At the reappearance of their colleagues, the first group threw an explosive device at the station, which detonated and set the building on fire. The re-formed group then drove from the urban area toward the highway.

Several aspects of this event will make it of interest to trainers and scenario writers. First, it is an excellent scenario of MI and MP units. It would be easy to mimic in the home-training environment, and the small number of attackers allows for efficient use of role-players. Finally, additional complexity is added due to the two-pronged attack, the foreign national target, and the possible insider angle.

The *Kidnapping in Katsina* Threat Report provides information to the Army training community on the December attack. In addition to an event review and accompanying diagram, the report considers the likely actors and their motives, provides an analyst assessment of the attack, and examines training implications.

It is important to recognize that during the design of an exercise a trainer or modeler may seek a specific strength percentage or number to use in describing the overall posture for an attacking or defending force. The desired strength percentage becomes even more difficult as a trainer employs a force that is not only representative of a composite of tactics, techniques, and procedures (TTP) found worldwide, but is hybrid in nature as well. Table 2, Hybrid Threats Unit Combat Effectiveness presents a series of strength percentages (developed by TRISA-Threats) to use during the design of an exercise employing a hybrid threats force. Table 1 also provides a summary of actions that may be employed by a hybrid threat commander as the strength percentage decreases. A discussion of the tactics that a hybrid threats force may employ can be found in the TC 7-100 series of publications.

THE THREAT OF FIRE-PRODUCING TTP AND WEAPONS

by Jennifer Dunn, Threat Assessment Team (DAC)

Fire-producing weapons have a long history on the battlefield. From flaming arrows that date back to ancient and medieval periods to the emergence of the first modern flamethrower system during World War I, the threat has utilized tactics, techniques, and procedures (TTP); weapons; and munitions to produce fires in order to destroy materiel and personnel.[1] Despite this long history, TRISA's Complex Operational Environment and Threat Integration Directorate (CTID) has come across recent products from the homeland defense community that indicate a general consensus of fire being an often overlooked threat on the battlefield.[2] Many of these products were created in response to recent articles published by al-Qaeda's *Inspire* propaganda magazine that espouses the benefits of fire as a tactic and teaches readers how to conduct attacks using fire-producing TTP.

Contrary to the concern found in these products that fire is an overlooked threat, Army soldiers are training against these types of TTP and weapon systems.[3] As part of CTID's mission to ensure that the hybrid threat is a representative composite of the threat, CTID has ensured that all OPFOR doctrine sets the proper conditions for effective training. As a result, many, if not most, CTID hybrid threat products and force structures include fire-producing weapons and TTP.[4]

The aggregate effect of these products from the homeland defense community implies that the various departments and agencies responsible for homeland defense are dismissing the threat of fire-producing weapons and TTP. As noted, from the Army training community standpoint, this implication is invalid. It did however cause CTID analysts to conduct further research to ensure current OPFOR doctrine still remains relevant. The result of this research is that the threat of fire-producing TTP and weapon systems is more relevant than ever. Not only are fire-producing TTP being actively used on the battlefield, but the threat is increasingly gaining access to fire-producing weapon systems through arms proliferation. Below are real-world, recent vignettes of representative elements of the hybrid threat (irregular forces, regular forces, and criminal elements) utilizing fire-producing TTP and/or weapon systems.

Irregular Forces

Irregular forces are using fire-producing TTP around the world. The most recent example of this is the attack on the US consulate in Benghazi, Libya on 11 September 2012. In the evening of 11 September, approximately 150-200 armed irregular forces attacked the consulate compound. In addition to carrying RPGs, grenades, AK-47s, mortars, and mounted heavy machine guns, these armed men also carried diesel fuel containers.[5] The purpose of the diesel was to set the compound ablaze. After blockading the main streets leading to the compound, the attackers assaulted firing heavy machine guns, RPGs, and grenades. Reportedly after fifteen minutes, the attackers gained access and immediately began setting the compound on fire.[6] Four Americans died during this attack.

What's relevant for this article is that despite the compound being under attack from a multitude of weapon systems, two of the four deaths were caused by the fire (smoke inhalation), not by the wide ranging weapon systems at the

disposal of the attackers. This incident demonstrates that fire plays a significant, dangerous role on the battlefield even when the typically more lethal weapons of machine guns, mortars, grenades, and RPGs are involved. This tactic is of particular concern because it is an extremely cheap, easy tactic that causes significant damage and destruction of personnel and materiel. For more information on how the OPFOR can exploit fire-producing TTP, see the Worldwide Equipment Guide (WEG) 2012, Volume 1 Ground Systems, Chapter 13 "Obscurants and Flame."

Regular Forces

During February and March of 2013, the Eastern Military District of Russia conducted a live-fire exercise of the TOS-1, a heavy flamethrower system, for the first time.[7] The TOS-1 is a Russian multiple rocket launcher mounted on a T-72 chassis that fires 220 millimeter rockets. This is an extremely significant exercise because while the TOS-1 has been tested in the past, it has never before been used in a live-fire exercise.

Figure 1. TOS-1 heavy flamethrower system[3]

The rockets fired by a TOS-1 carry a fuel-air explosive, or thermobaric, warhead. This type of warhead releases a cloud of flammable gas and causes extremely large explosions. The warhead creates a massive overpressure in the target area for which there is no practical defense, making dismounted units particularly vulnerable.[8] In the exercise conducted by the Russian unit, there was no blast or shrapnel upon impact of the rockets, rather a 300 square meter area of absolute destruction caused by the extremely high pressure and temperature. The TOS-1 can range its destructive fire up to about 3,500 meters. More information on this system can be found in the 2013 edition of the WEG, scheduled to be published later this year.

This exercise of the Russian military is not the only recent example of regular forces using fire-producing weapon systems. In 2012, the Syrian military escalated fighting by implementing the use of a barrel bomb, an incendiary bomb that contains flammable materials.[9] Barrel bombs are in essence improvised explosive devices.

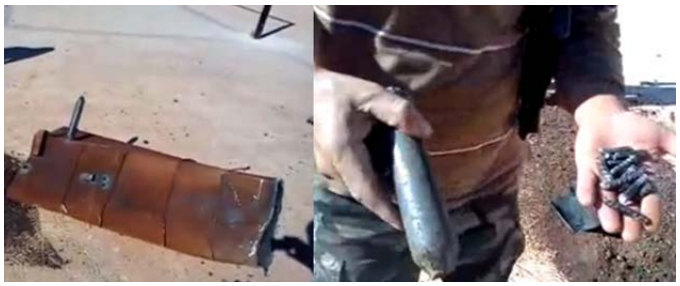


Figure 2. Suspected military barrel bomb and shrapnel[2]

They are constructed from a cylindrical object like a used artillery shell or oil drum and filled with explosive material, oil, and shrapnel. The weapon is loaded into helicopters and pushed out of the helicopter over the designated target area. Syria has been reportedly using these improvised incendiary devices since August of 2012. Videos of this new tactic and weapon being used by the Syrian military can be found anywhere on the Internet.[10]

Criminal Elements

Criminal elements have favored various forms of fire-producing TTP and weapons over history, but the most commonly used seems to be the Molotov cocktail. Molotov cocktail is a generic name that refers to an improvised fire-producing weapon made from a breakable glass bottle containing a flammable substance and a source of ignition like a cloth wick. For use in an attack, the wick is lit and the bottle is thrown at a target. The intent of using this weapon is more about the fire than about the destruction. Criminal elements typically use this type of weapon to make a statement more than to actually cause lethal effects. Recent examples of Molotov cocktails include use by protestors in Turkey, Egypt, and Tunisia and extremists in Palestine.

Proliferation

Fire-producing TTP can proliferate very easily because these TTP are simple, cheap, and extremely effective.

Additionally, terrorist organizations like al-Qaeda use their propaganda machines to ensure that these TTP reach the widest audiences possible. While it is more difficult to proliferate fire-producing weapon systems, there is strong evidence that it is occurring. In 2011, Kazakhstan received a number of the TOS-1 systems from Russia.[11] While Kazakhstan is believed to be the first export customer of this system, there is potential for Russia to arrange sales with other interested states.

While proliferation of the TOS-1 system is limited, there is a smaller manportable flamethrower system, the RPO-A, that is actively being sold by Russia. The Shmel RPO-A, aka 'bumblebee,' is a Russian made infantry rocket-propelled incendiary projectile launcher. The standard projectile fired is thermobaric. On impact, the fuel from the projectile is dispersed, mixed with oxygen from the air, and ignited, which results in high pressure and temperatures. The RPO-A can range up to 1,000 meters and can affect a target area of several meters in diameter. More information on this system can be found in the *WEG* 2012, Volume I Ground Systems, Chapter 2 Infantry Weapons.

Figure 3. RPO-A infantry flamethrower system[3]

In 2012, Lebanese forces seized an arms shipment headed to Libya from Russia. This shipment contained the RPO-A flamethrower system.[12] Given Russia's history of weapons sales, it is extremely likely that this trend will continue and that at some point US forces may be faced with a threat that is equipped with this system. The proliferation of this system presents a significant threat because it can proliferate to both state and non-state actors as opposed to the TOS-1 system, which will likely only proliferate to other state actors.

Training Implications

- New fire-producing TTP and weapon systems will continue to appear as globalization and technological advancements continue.
- The entire spectrum of the hybrid threat – irregular forces, regular forces, and criminal elements – has access to fire-producing TTP and weapon systems.
- Proliferation of fire-producing weapon systems is increasing, ensuring that US soldiers will encounter these systems on the battlefield.

For more information on fire-producing TTP and weapon systems, please contact the CTID Threat Assessment Team at 913-684-7962.

Notes

[1] While this article focuses on the *lethal* effects of fire, fire and smoke are commonly used by the threat for other purposes such as its psychological effects and obscurant properties. See Chapter 13 of the Worldwide Equipment Guide on "Obscurants and Flame" for more information.

[2] See: Scott Stewart, "Fire the Overlooked Threat," *Stratfor Security Weekly,* 28 February 2013; California State Threat Assessment Joint Bulletin, 1 June 2012; Department of Homeland Security Note, 31 May 2012; FBI Situational Information Report, 7 May 2012.

[3] Staff Sgt. Cody Harding, "525th BfSB prepares for unique mission in Kosovo," www.army.mil, 23 May 2013. This unit used simulated Molotov cocktails in their training.

[4] See TC 7-100.2, Opposing Force Tactics, December 2011.

[5] "US 'had no actionable intelligence' over Benghazi attack," *The Telegraph*, 10 October 2012.

[6] Paul Schemm and Maggie Michael, "Libyan Witnesses Recount Organized Benghazi Attack," Associated Press, 27 October 2012.

[7] Robert Beckhusen, "So Russia Has an Upgraded Flamethrower Tank Now," *Wired*, 05 April 2013.

[8] "GUP TOS-1 220 mm (30-round) rocket system," *IHS Jane's*, 6 March 2012.

[9] "Syrian Army Using Missiles, Barrel Bombs," *News 24*, 12 December, 2012; "Improvised Syrian 'Barrel Bombs'," *RAPID*, 10 December 2012; Rick Francona, "The Syrian 'Barrel Bomb' – A Terror Weapon," *Middle East Perspectives*, 27 October 2012; Damien McElroy, "Syrian Regime Deploys Deadly New Weapons on Rebels," *The Telegraph*, 31 August 2012.

[10] See: Al-Arabiya Video: http://www.youtube.com/watch?v=M95ta3_mZBA&feature=player_embedded
Video Pictures are derived from:
http://www.youtube.com/watch?feature=player_embedded&v=Bn57Id00nDI
Inside a barrel bomb: http://www.youtube.com/watch?v=Wv7-cPLmfjM&feature=player_embedded
Shrapnel from barrel bomb: http://www.youtube.com/watch?feature=player_embedded&v=cLwtxvDxjDg
Bomb dropped from helo: http://www.youtube.com/watch?v=YtOPwm9JTTA&feature=player_embedded

[11] "Kazakhstan," *IHS Jane's,* 23 May 2013.

[12] Jeremy Binnie, "Igla-S missiles found in Libyan arms shipment," *IHS Jane's*, 18 April 2013.

Figure Credits

[1] **TOS-1 heavy flamethrower system**
[2] **Suspected military barrel bomb and shrapnel**
[3] **RPO-A infantry flamethrower system**

IED ATTACKS IN PATTANI

by H. David Pendleton, OE Assessment Team (CGI Ctr)

Within a 20-hour period on 16-17 February 2013, insurgents against the ruling Thai national government attempted 11 improvised explosive device (IED) attacks in Pattani, Thailand—possibly as retaliation against the government for the death of 16 of their fellow Islamist insurgents the week before elsewhere in Pattani Province. Less than half of the IEDs exploded due to the insurgents' poor bomb making skills, the vigilance of several civilians, and the skill of government explosive ordnance disposal (EOD) teams to deactivate the IEDs before they detonated. The Threat Report, *Series of IED Attacks in Pattani, Thailand* (FOUO), provides a summary of each of the 11 IEDs that exploded or the EOD teams made safe. Due to the photographs and details of the IED attacks, this Threat Report has been labeled For Official Use Only (FOUO).

The city of Pattani is located about 1,044 kilometers (km) south of Bangkok in a province of the same name. Pattani is one of Thailand's three southernmost provinces where the Islamist separatist movement is most active. Since 2004, over 5,000 people have died due to the insurgency, most of them innocent civilians.

From about 1640 hours local time on 16 February 2013 when the first IED exploded until about 1300 hours the following day when the final bomb was found, first responders—police officers, firemen, and EOD experts—stayed extremely busy with at least 11 documented incidents. EOD personnel disarmed six of the IEDs while five exploded, but not always with as much force and damage the insurgents expected.

The damage would have been much greater without the audacity of several local civilians. Two shopkeepers, who found IEDs in their businesses, courageously picked up the IEDs without regard to their own safety and carried them outside to avoid the blast and fire damage to their stores. One proprietor placed the IED in the middle of the street in front of his shop and the other positioned the IED in a local park across from a police station. EOD personnel disabled both bombs before they were detonated. A third business owner put out a fire caused by an IED explosion in his store, but before the fire could spread to do much damage.

Figure 1 for the sites of several of the IED incidents and explosions in Pattani noted in the Threat Report.

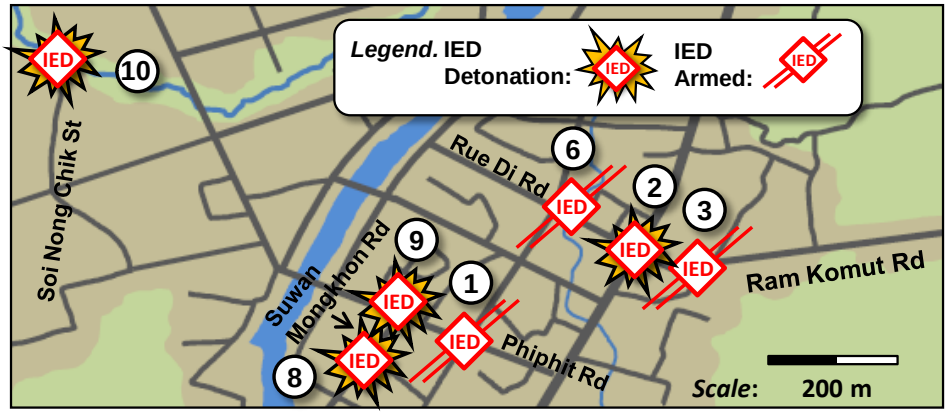


Figure 1. Multiple IED employment

Other businesses targeted by the insurgents suffered significant damage. An IED hidden in a toothpaste box exploded in the Diana Mini Mart and destroyed the entire three-story department store. Another explosion burned down a four-story electrical appliance store. The largest and most deadly of the explosions occurred at about noon on 17 February near the clock tower circle in downtown Pattani. This blast, where only half the explosives actually ignited, killed three volunteer security personnel and heavily damaged a coffee shop/restaurant on the other side of the roundabout.

Two of the incidents in Pattani involved dual bombs at the same location, but the EOD teams disabled the second bomb before it could explode, possibly killing the first responders or additional civilians who came to see the damage from the original bomb. See TRISA G2 Handbook No. 1.07 C3, *A Soldier's Primer to Terrorism TTP in Complex Operational*

Environments, for tactics, techniques, and procedures (TTP) on the use of multiple bombs or a decoy/primary bomb at a single location. The following diagram shows how a double IED could target a restaurant with outdoor seating similar to the attack that occurred at the karaoke bar in Pattani on 16 February 2013.

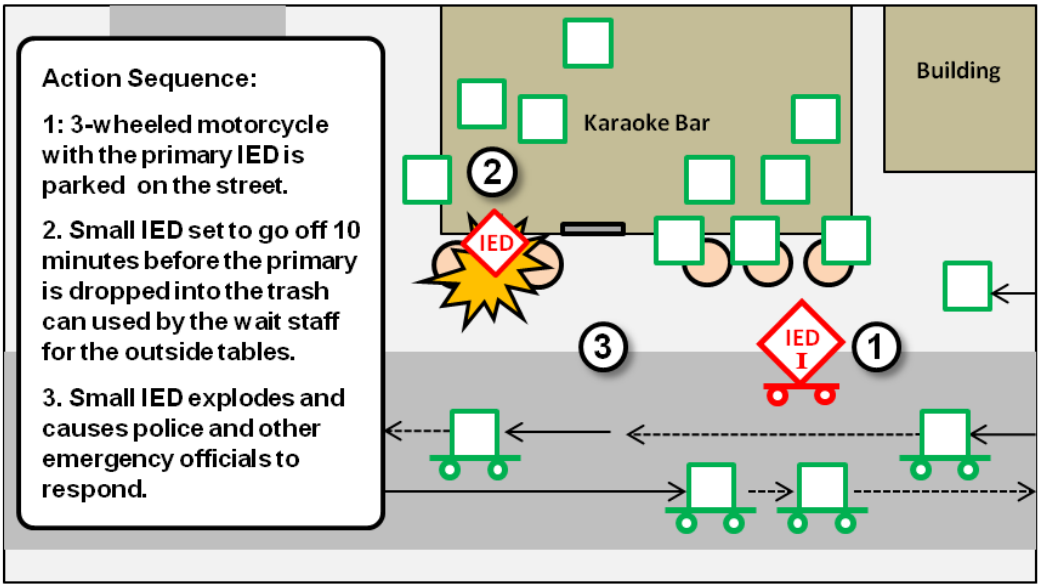


Figure 2. General Sequence of Threat Direct Actions: Initial IED

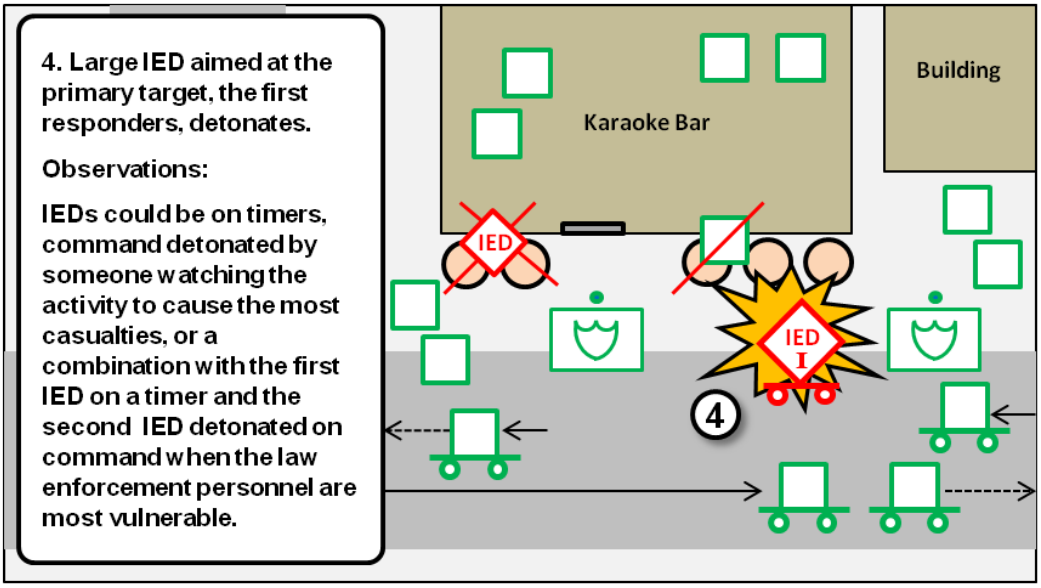


Figure 3. General Sequence of Threat Direct Actions

After the fact, police discovered closed circuit television (CCTV) footage that filmed the insurgents as they traveled by motorcycle around the city planting the 11 bombs in a four square mile area in downtown Pattani. Each motorcycle carried a team of two with the passenger sometimes dressed as a female, but possibly male. Tape showed the team as they dismounted the motorcycle to enter shops appearing as interested customers before leaving their IED behind when they departed. The CCTVs also picked up the movement of a motorized tricycle with a large box on the back for movement of goods around the city, but in actuality had a 30 kg IED hidden between the gasoline tank and the box on the back. The insurgents left the motorized tricycle as the second and larger bomb outside the karaoke bar in an attempt to possibly hit the first responders to the initial explosion hidden in the trash can outside the bar earlier. Alert bar

patrons, however, pointed out the motorized tricycle to the police and the EOD team managed to defuse the device before it exploded. Experts contended that between the bomb and the gasoline contained in the box on the back of the motorized tricycle that the blast would have destroyed at least 20 houses in the vicinity before firefighters could have controlled the blaze.

While the local police attempted to downplay any connection between the series of IED attacks on 16-17 February 2013 and the death of 16 Islamist insurgents the week before in Pattani Province, others are not fully convinced. Insurgents continue to target government workers including first responders, the military, and civilians with other IED attacks in Pattani Province. In one 24-hour period around 24 February 2013, insurgents conducted 30 minor attacks that injured ten people. In another 24-hour period on the night of 11-12 April 2013, insurgents attempted to explode 36 IEDs including an attack against a police unit in rural Pattani Province that killed two soldiers and wounded six others.

The size of the IEDS ranged from 2 kg hidden in a toothpaste box to 50 kg hidden in a pair of fire extinguishers. Many of the items used to assemble the IED were common products easily obtainable. While the harm caused by the series of IEDs in Pattani was substantial and several people were killed, the damage and casualties could have been far worse if all the IEDs had detonated as planned. The vigilance of several civilians, the ineptness of some of the bomb makers, and the rapid response of the first responders all played major roles in the mitigation of the potential damage from the Islamist insurgents' IED spree on 16-17 February 2013.

by Mike Sullivan, TRISA-WETED Red Team

The Wargame, Experimentation, and Threat Emulation Directorate (WETED) of the TRADOC Intelligence Support Activity (TRISA) maintained a significant 2013 schedule of events in support of Army readiness. For example, this past summer WETED continued support at the Advanced Situational Awareness Training facility (see the August *Red Diamond* article on ASAT) at Fort Benning, Georgia; provided subject matter experts (SME) and Red Force "command and control" at three major exercises and experiments; and recruited and trained dozens of new, highly qualified SMEs as role players and threat emulators. These SME supported ASAT and the Network Integration Evaluation (NIE) series at Fort Bliss/White Sands Missile Range (WSMR). WETED also provided support to both Title 10 and US Air Force exercises in CONUS and Germany.

Of particular value to the Army was WETED SME support to the Future Integration Army 2020 (FIATT) series of events at Fort Leavenworth's Mission Command Battle Lab (MCBL). Over a period of eight months culminating in July and early August, the WETED Red Team assisted in assessing the likelihood of success for an reconnaissance and surveillance brigade combat team (R&S BCT) formed around an armor brigade combat team (ABCT) in an extended MCO (Major Combat Operation) against a fully modernized, well armed, sizable enemy force defending its homeland against the attack. The event was broadly intended to simultaneously examine the overall design of current and projected BCTs and EAB (Echelons above Brigade) assets.

Several useful insights emerged from the effort with the most notable being that unmanned aerial system (UAS) warfare is likely to be a major challenge for deploying forces by 2020 and beyond. The proliferation of relatively inexpensive but highly capable UASs with intelligence, reconnaissance, and surveillance (ISR) sensors and/or lethal laser guided

munitions will complicate airspace command and control and threaten US forces and their cyber and sustainment assets as vulnerable to detection and attack by a persistent enemy UAS threat.

The Red Force at FIATT was also effective in using a swarm tactic. In this case, a layered attack of swarming employed UASs, cruise missiles, cyber and electronic warfare (EW) to set conditions for direct action and artillery by destroying Patriot radars and disrupting command and control. Passive use of cyber capabilities as an intelligence gathering asset instead of as a denial mechanism was highly effective and helped keep Red Force cyber operating in the fight longer.

Note. Terms such as "Redfor" and "BluFor" are not in TC 7-100.2, *Opposing Force Tactics*, but are used by WETED in particular events to identify some of the actors among the many participants in an exercise, experiment, or other event that may be from organizations other than the US Army.

Another proven Red Team practice, one of WETED's "Dirty Dozen" principles discussed in the April *Red Diamond*, was highly effective in confounding Blue Force success. By focusing RED force capabilities on the Blue Force rear area and being willing to accept the bypass of Red main force tactical units by Blue maneuver units, the Red force could disrupt and deny Blue logistics flow along MSRs and deny food, fuel, and ammunition to Blue forces in contact deeper in Red territory. Blue forward movement was effectively stopped in many cases. The stresses imposed on the Blue Force brigades were precisely what the Red Force was to present in complex conditions as the Army refines its approach to building the Force for 2020 and beyond. FIATT was effective in indicating or revealing "seams and possible gaps" in the force structure concept. It should be noted here that TRISA and WETED were formed to provide that sort of stress in wargame experimentation, testing, and evaluation venues.

WETED "Dirty Dozen"

1. NEVER cede access to BLUFOR units. Contest every inch of ground if only by ensuring friendly civilian populations are complicating use of routes and "ports." A little counter-mobility goes a long way in halting BLUFOR momentum before it gets started.

2. Consider MSRs, LOCs, and FOBs as opportunities for selective application of fires and other effects. The "Disruption Zone" fight is a constant.

3. NEVER let BLUFOR dictate where and when main forces do battle.

4. Use decoys, spoofing, deception, civilian masking, humanitarian activities, and protected sites for every advantage.

5. Use highly decentralized command and control (C2) mechanisms to ensure continuity of operations and to confound BLUFOR ISR.

6. Develop and selectively apply "swarms" of relatively low tech, high impact weapons, tactics, and fires at BLUFOR high value C2 and logistics targets.

7. Use information operations to every advantage. If BLUFOR claims success in any dimension, find ways to turn it into a "lie or delusion."

8. If available (it almost always is available in some form!) maintain the "WMD option" at all costs.

9. Target soft BLUFOR and BLUFOR Coalition homeland targets relentlessly.

10. Use NGOs and international organizations as "sympathetic" targets for information operations.

11. UASs and UAVs are increasingly available to Red Forces. They are easily procured, very effective as ISR tools, and turn BLUFOR air superiority into a myth. They can also be used as in the attacking swarms described in #6 above.

12. The BLUFOR is casualty averse. Every dead member of the BLUFOR is "Headline News." A BLUFOR strike that kills sympathetic Red civilians is "Breaking News."

WETED

Unified Quest 2013 encompassed a series of events at Carlisle Barracks. Unified Quest is the Army Chief of Staff's annual wargame and exercise aimed at examining issues that will influence how the Army of, in this case, 2030 will be recruited, trained, equipped, deployed, sustained, and led as the Nation's primary land force. More specifically, UQ 2013 looked at how technological advancement and proliferation are accelerating the speed of international events while reducing the time military forces might have in being able to prevent catastrophic outcomes. These conditions, as the Chairman and the Army Chief of Staff have recently argued, will likely demand a more agile and responsive Army. UQ 2013, as has been true in many exercises in recent years, had the Army take a hard look at its capacity to find, seize, control, move, and dispose of weapons of

mass destruction that "in the wrong hands" can threaten entire regions and even the CONUS. The Red Team role was to make examination of these issues as challenging as possible and both groups formed from the team did exactly that.

The most effective tools the Red Teams used in confounding BluFor objectives were really pretty primitive—time, space, and numbers. Both took full advantage of extended BluFor LOCs, limited maneuver space along potential attack axes, sizable Red regular, militia, and special operations forces. Easily hidden and readily transportable WMD devices add to complexity that can make BluFor mission accomplishment literally "a bridge too far."

Finally, the Red Team participated in a very ambitious counter-UAS (CUAS) experiment based at the Fires Battle Lab at Fort Sill, Oklahoma with supporting activities at Fort Rucker, Alabama and Fort Leavenworth, Kansas. Among the Red Team's challenges with FIATT, UQ, and CUAS were the opportunities associated with using simulations as the foundation for engagement by the opposing forces (OPFOR). In FIATT, One Semi-Automated Force (ONESAF) was the centerpiece of a federation of simulations to allow all of the assigned weapons and sensors to be in action as the contesting forces clashed. CUAS used Fire Support Simulation (FIRESIM) as the foundation for analytics with the Advanced Tactical Combat Model (ATCOM) as the contributor of data on aircraft and UAS performance. UQ has, in many cases, been largely a Map Exercise (MAPEX) whose battle outcomes were decided by adjudication panels.

This year the UQ tactical and some operational level engagements were put into a system called Integrated Gaming System, a product of the Virginia Modeling, Analysis and Simulation Center at Old Dominion University. This operation was a very labor intensive effort to get the fidelity and realism desired by the game direction staff. TRISA, TRISA's OE Laboratory, and WETED have been an effective "sanity check" on the utility of simulations. The TRISA team worked closely and effectively with the Army Capabilities Integration Center (ARCIC) and the Community of Practice throughout the summer of 2013 to enhance these capabilities toward more realistic and effective operational environment (OE) depiction. These insights emerged from the collective series of 2013 events: a clear consensus exists on the necessity for the Army to leverage the Air Sea Battle discussions to ensure it can get to where the Nation needs it to go and to be able to protect forces once they are deployed, and any technological advantage a US force might have as it arrives in hostile territory is not likely to last very long.

Meanwhile, TRISA WETED is utilizing a new scenario, road to war, and objective order of battle (OOB) for the Army Expeditionary Warrior series of experiments designed to explore the utility of short turnaround procurements of technology and equipment to help the soldier and leaders on the current battlefield. Spiral G, the 7th layer of assessments in the AEW effort, is in planning stages. WETED SMEs and cadre will lead Threat Emulators (Live) throughout this important experiment work. In the near future, WETED will support initiatives in Army experiments specifically focused on the future of UAS effects in the spectrum of conflict.

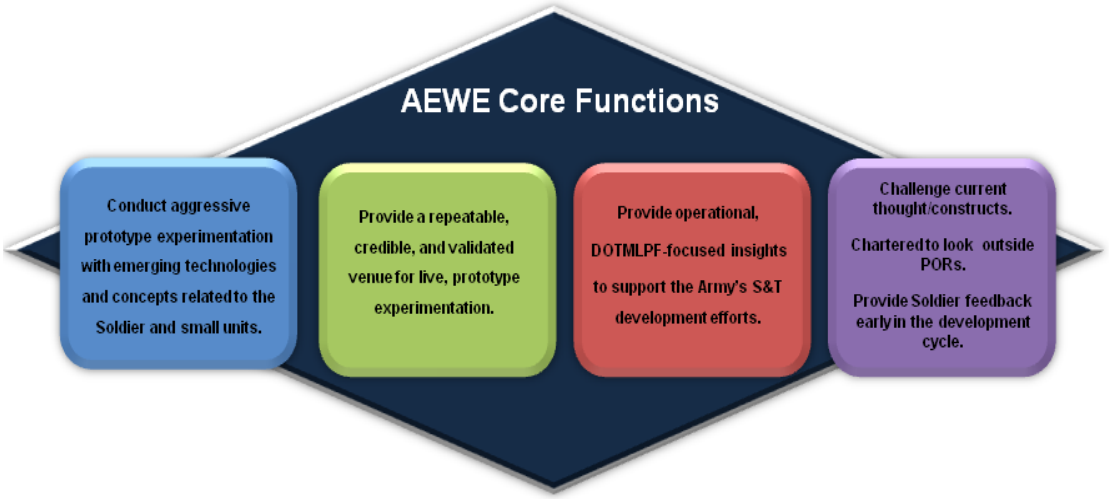


Figure 1. Core functions of Army Expeditionary Warrior Experiments

INSURGENT DISMOUNTED RAID ON A TANK PLATOON

by Jon H. Moilanen, CTID Operations and Threats Terrorism Team (BMA Ctr)

A *raid* is an attack against a stationary target for the purposes of its capture or destruction that concludes with the withdrawal of the raiding force to safe territory. US Army Training Circular 7-100.2, *Opposing Force Tactics*, states that a raid can also be used to secure information and/or deceive the enemy. Keys to successful accomplishment of a raid include—

- Surprise.
- Massed firepower.
- Violent conduct.

Raid objectives can include—

- Destroy or damage key enemy systems or facilities.
- Deny critical information to the enemy.
- Disrupt enemy operations and/or support.
- Distract enemy attention from other threat actions.
- Secure hostages or prisoners.
- Seize critical weapon systems and/or materiel.
- Support the threat information warfare (INFOWAR) plan.

Command and Control of a Raid

A raid can be conducted by threat elements that are autonomous in an OE but are typically associated and/or affiliated with a higher regular or irregular force unit or organization. Although a raid can be supported with operational assets, raids are primarily conducted by task-organized units, cells, or organizations at the tactical level of operations.

Figure 1. Insurgent video surveillance of enemy tank platoon position

Functional Organization for a Raid

Reconnaissance and surveillance provide the foundation for planning and conducting a raid. Resources may be as sophisticated as unmanned aerial vehicles (UAV) or satellite imagery to the simplicity of posting observers at critical points in an operational environment (OE). See the enclosed set of three figures for an example of sequential and concurrent tasks in conduct of a raid.

The size of the raiding force depends upon its mission, the nature and location of the target, and the enemy situation. The raiding force may vary in size and capability from a large mechanized task-organized force such as a threat brigade tactical group (BTG) to a small irregular force of insurgents. Regardless of unit, cell, or organization size, a raiding force typically consists of three elements: raiding, security, and support. It may involve other functional elements such as a breaching element or a fixing element (see TC 7-100.2, para. 3-174 to 3-192).

Raiding Element(s)

The raiding element executes the main task that ensures success of a raid in the destruction or seizure of the target in the raid. This element accomplishes its task through direct actions in a rapid and violent manner. Surprise is critical to mission success.

Security Element(s)

The primary threat to all elements of a raid is being discovered and defeated by enemy forces prior to execution of the raid. The security element within a raid focuses primarily on fixing enemy security and response forces or containing the enemy's escape from the objective area. The security element is equipped and organized to detect enemy forces and prevent or disrupt them from contacting other enemy forces that might influence the raid.

Security elements deploy to locations where they can disrupt the enemy freedom of movement along ground or air avenues of approach and delay reinforcement of the enemy on the objective. The security element operating within a small insurgent cell, regular force, or guerrilla unit mission may be only capable of providing early warning to the raiding and support elements. The security element also covers the withdrawal of the raiding element, and when necessary, acts as a rear guard for the raiding force. The size of the security element depends upon the size of the enemy's capability to intervene and disrupt the raid.

Support Element(s)

The support element has several enabling functions and assists in setting the conditions for the success of the raid. The support element provides fire support, logistics support, and/or reinforcement to the raiding and security elements. TC 7-100.2 states that a commander or leader of a raid typically controls a raid from within the support element. However, the commander or leader determines where to locate for best command and control (C2) the raid.

If needed, support elements may assist the raiding element(s) in reaching the objective and/or target of the mission. They can execute one or more complementary tasks such as—

- Eliminating enemy guards.
- Breaching and removing obstacles to and/or at the objective.
- Conducting diversionary or holding actions.
- Canalizing enemy forces.
- Providing fire support.

Tactical Example: Raid

The following example of a raid is based on a recent tactical action in Syria by insurgent forces on the regular forces of their enemy. Some tactical aspects have been amplified or modified to emphasize tactical principles.

Movement to the Assault Position

① See figure 2. Insurgent reconnaissance and surveillance observe an enemy tank platoon since it occupied a defensive position along an avenue of approach in farmland area near an urban center. Berms are prepared as a hasty circular perimeter with several gaps to allow vehicle movement in and out of the position. The only vehicular traffic for several days is a periodic arrival of a small cargo truck that appears to deliver rations and containers of water. Surprisingly, no other obstacles are constructed and no attempt has been initiated to improve the platoon defenses. Several tents and manmade shelters within the position indicate that the platoon-size force will remain in the area.

② Active supporters of the insurgent cell report on concealed approaches to the enemy position through severe ravines caused by erosion. Site reconnaissance and rehearsals confirm the infiltration routes for small groups of insurgents and where the insurgents will rendezvous near the enemy position. Insurgent observers report that the enemy has conducted no patrolling outside their perimeter and security measures are lax. Enemy soldiers walk individually or in pairs with no weapons, no load bearing equipment, and wear a mixed dress of military and civilian clothing. They appear to be casually talking rather than paying attention to or observing from the immediate perimeter.

No regular preventive maintenance has been performed on the tanks in the past days, turret-mounted machine guns remain under canvas, and all tanks have remained in the same position since their arrival.

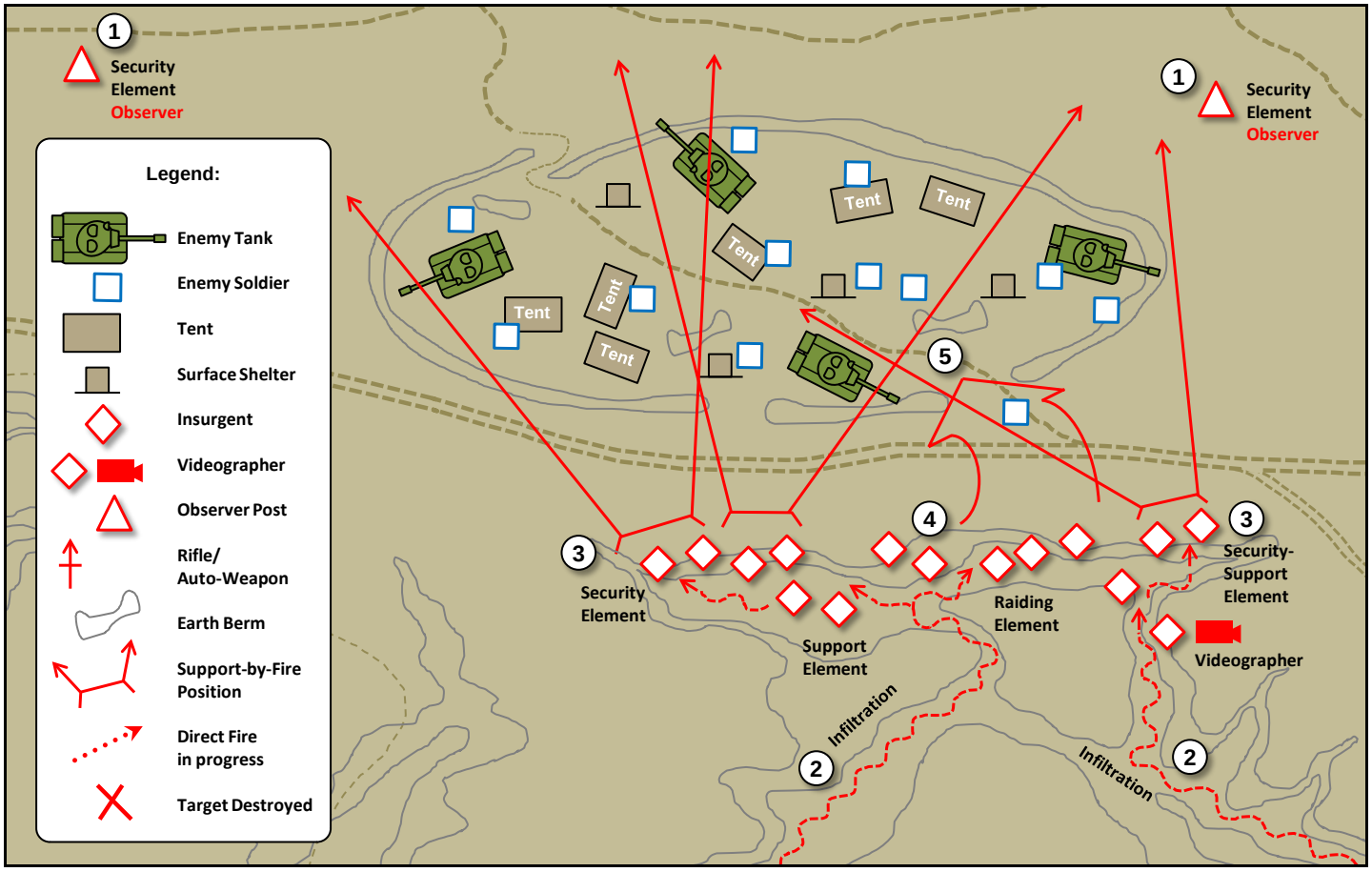


Figure 2. Insurgent plan for raid on tank platoon in defensive position

③ Insurgent support elements move to the flanks and occupy support-by-fire positions while some insurgents also perform a security element function. The right flank support element will initiate the assault on order of the cell leader by killing any enemy soldiers at or near the gap in the berm selected for the assault penetration. The left flank support element prepares to provide support-by-fire small arms fire (SAF) to suppress or contain any enemy soldiers in the western half of the defensive position.

Figure 3. Insurgents infiltrating into their raid assault position

④ The initial raiding element positions on-line just below the crest of the ravine wall and close to the gap in the berm. The insurgent cell leader confirms final preparations and cell readiness. Specific tanks, tents, shelters, and designated

areas have been assigned to insurgents with the task to quickly seize the tanks and kill any enemy soldiers. The insurgent cell is prepared to assault on-line and rush through the gap in the berm.

⑤ Insurgent observers report no enemy activity along the roadway east or west of the tank platoon. An insurgent in the right flank security element sees only one soldier without a weapon at the penetration point. The insurgent leader gives the signal to assault.

Assault

⑥ See figure 3. The right flank security element immediately shoots two soldiers at or near the gap in the berm as the initial raiding element of six to eight insurgents rushes the gap from the ravine. Surprise is complete.

⑦ The left flank support element covers its designated sectors with SAF and contains several enemy soldiers attempting to emerge from their tents or shelters. The SAF also keeps individual soldiers in tanks down inside the turrets. No soldiers attempt to operate individual or crew-served weapons in the tanks and any SAF from enemy soldiers on the ground is sporadic and ineffective. The speed of the assault and massed direct fires of the insurgents is achieving its intended purpose.

⑧ As the initial raiding element races through the gap in the berm and down the center path, insurgents quickly fan out left and right of the path to seize the two nearest tanks. They also quickly yet methodically clear each tent or shelter with SAF. Small arms fire from the enemy is nil.

⑨ The left flank support element shifts its SAF to the western part of the tank platoon position as the lead raiding element continues to assault through the position. The insurgent leader directs the support element to join the assault as these insurgents follow through the gap in the berm.

⑩ The insurgent cell seizes the tank platoon position within several minutes. Each support element designates one insurgent to act as security to the west and east along the main trail as early warning. The insurgent observers also report from their vantage points farther to the north.

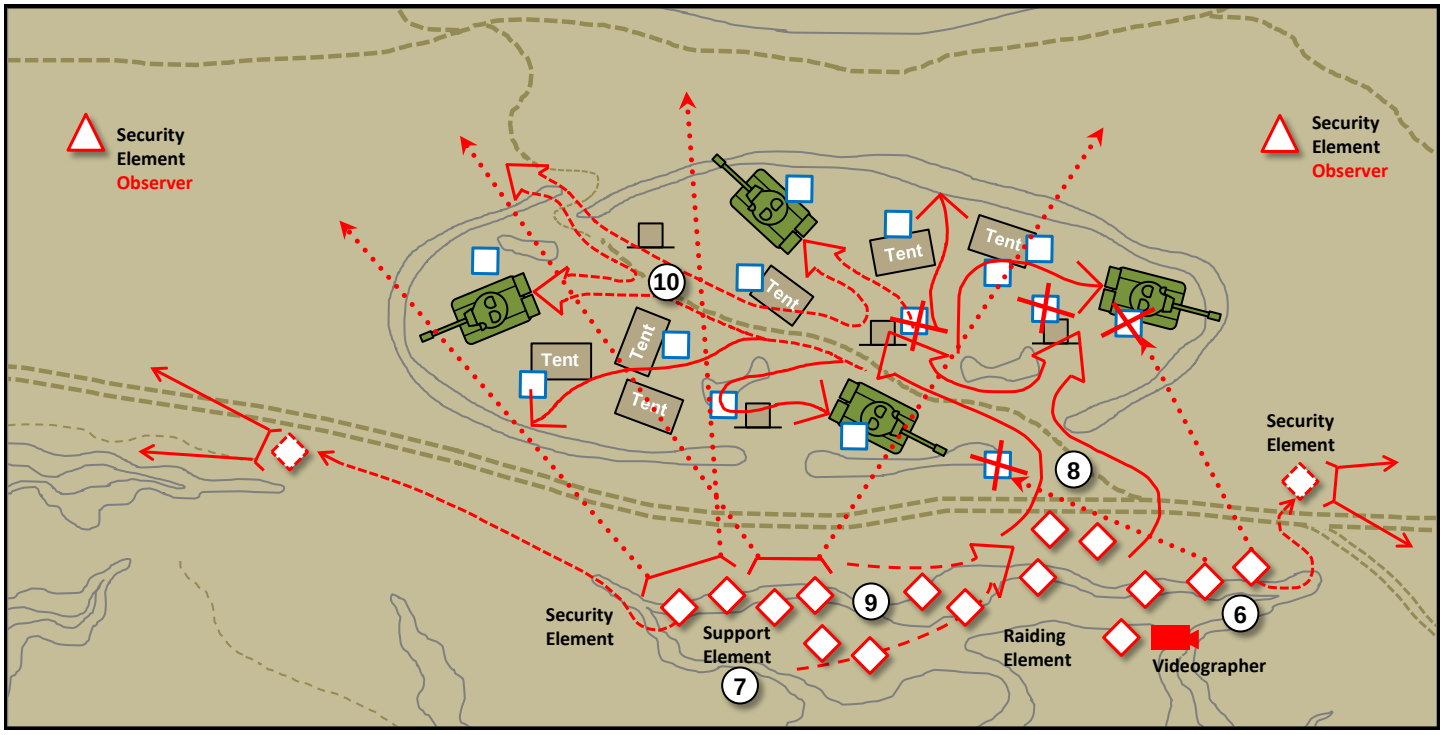


Figure 4. Insurgent conduct of raid on tank platoon in defensive position

Reorganization and Exfiltration

⑪ The insurgent leader directs that each tank is manned immediately and prepared for movement out of the berm position. Other reorganization tasks are limited to verifying the status of all insurgents and reallocating small arms

ammunition. Casualties are limited to two insurgents with minor gunshot wounds. Meanwhile, insurgents gather several enemy weapons and distribute equipment as they organize for their exfiltration.

Figure 5. Insurgents seize a tank platoon defensive position in a raid

⑫ The videographer has recorded scenes during the entire raid and takes particular interest in how unprepared the tank platoon was in its defensive position. He walks among the insurgents and films the destruction of equipment, tanks being prepared for movement, and enemy dead to be abandoned in the position.

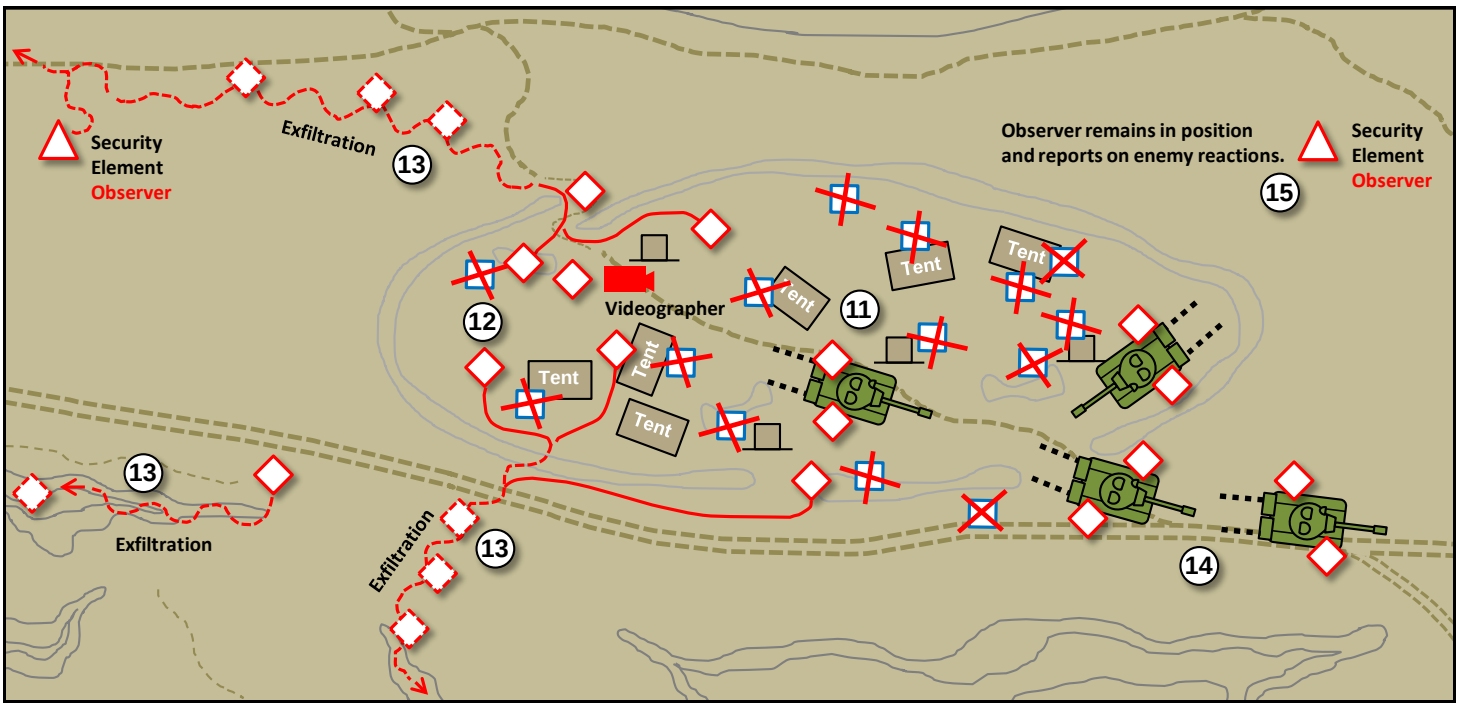


Figure 6. Insurgents moving captured tanks to urban hide positions

⑬ Insurgent groups start to exit the position and exfiltrate on routes different from the routes used for infiltration. The ravines to the south provide excellent concealment and soon the insurgents disappear as the last insurgent descends into the ravines.

Several insurgents exfiltrate to the northwest, link up with one of the observers, and move to an urban complex battle position (CBP). In the west, an insurgent exfiltrates parallel to the main trail and continues to report to the insurgent leader who is on one of the tanks.

⑭ All four tanks are operational and are ordered by the insurgent leader to move east. During rehearsals, the insurgent cell leader identified hide positions near probable ambush sites in the restrictive network of urban streets. The local insurgent organization had already prepared multiple routes and ambush positions for use of tank main guns for flank or rear shots into enemy armored vehicles.

⑮ One insurgent observer remains concealed in a position to the northeast. He continues to send periodic reports to the local insurgent organization leader on how the enemy response forces act when they arrive hours later at the bermed position. Enemy soldier remains were removed and the site was not reoccupied by enemy forces.

Note. Once the insurgent cell has arrived at its urban safe haven, the videotape and audiotape coverage of the raid is provided to an intermediary who transfers the recordings to local-regional media outlets and an INFOWAR cell of the local insurgent organization. The video and audio recordings are publicized on the Internet within hours of the raid and exploited to demonstrate enemy weaknesses in morale, lack of tactical discipline, and absence of force protection measures. The insurgent organization uses the same video and audio recordings as a training aid in orienting recruits on how to successfully conduct tactical operations.

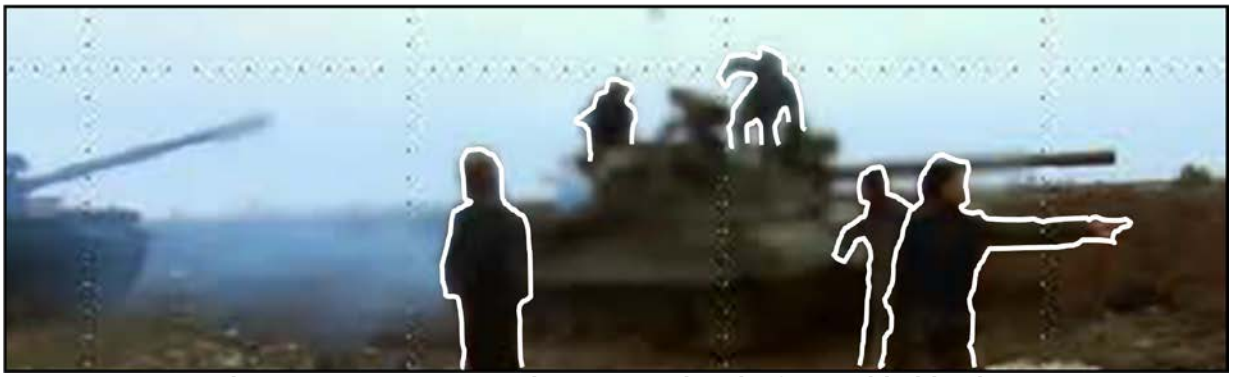


Figure 7. Insurgents moving captured tanks from raid objective

Support of a Raid

A raid typically requires several types of support. These capabilities can include reconnaissance, armor, fire support, air defense, engineer, logistics, and INFOWAR. The primary reconnaissance task in a raid is to locate and monitor the target of the raid until the raiding element is in contact. Reconnaissance also monitors possible or probable enemy responses to a raid.

In the tactical example of this article, no armor vehicles are available to the insurgent organization. No indirect fires are in support of the raid. Air defense is prepared to use a threat *all-arms air defense* tactic (see TC 7-100.2, para. 11-72 to 11-78) with available small arms and automatic weapons.

A detailed reconnaissance of the enemy position determines that no physical breaching element is required for the assault. All logistics for this raid are carried with the insurgents in their infiltration to the attack position.

INFOWAR is a regular–and typically constant–support task to military operations such as a raid. INFOWAR can support a raid by concealing the intended action through deception and perception management. The videographer in the tactical example of this article records the movement and maneuver of the insurgent cell as it—

- Infiltrates from a tactical assembly area.
- Coordinates elements for the raid in an assault position.
- Conducts the assault through a gap in the enemy berms.
- Seizes the enemy platoon position.
- Secures the enemy main battle tanks and equipment.
- Reorganizes for tactical movement.
- Exfiltrates dismounted insurgents on multiple routes.
- Moves captured main battle tanks to urban hide positions.

Observations for Training Readiness

This real-world example of a raid spotlights the importance of reconnaissance and surveillance to find and confirm enemy critical weaknesses. When enemy security measures are lacking and enemy soldier and leader discipline is not observable, a dismounted infantry-like insurgent cell *can* plan and conduct an assault to defeat and/or destroy a

stationary enemy force of main battle tanks in a platoon-size defensive position. For more visual details on what was recorded by an insurgent videographer in an insurgent raid on an armor platoon defensive position in Syria, see Dismounted Raid on a Tank Platoon.

No indirect fire support or heavy weapons were available for the raid. Rehearsals and coordinated teamwork among the insurgent elements emphasized surprise and violent execution of the assault. Using only small arms and automatic weapons, an insurgent cell of twelve to twenty insurgents raids an enemy armor platoon in a defensive position, kills all enemy soldiers, and seizes four main battle tanks for insurgent urban operations against a corrupt governing authority.

Worldwide Threat Assessment of the US Intelligence Community 2013 (U)

Syria and the Nusrah Front

Almost two years into the unrest in Syria, we assess that the erosion of the Syrian regime's capabilities is accelerating. Although the Asad regime has prevented insurgents from seizing key cities—such as Damascus, Aleppo, and Homs—it has been unable to dislodge them from these areas…prolonged instability is also allowing al-Qa'ida's Nusrah Front to establish a presence within Syria.

Honorable James R. Clapper
Director of National Intelligence (12 March 2013)

CORRECTION TO BOOT-HEEL OR ACHILLES HEEL? TURKEY'S HATAY PROVINCE

by CTID Operations

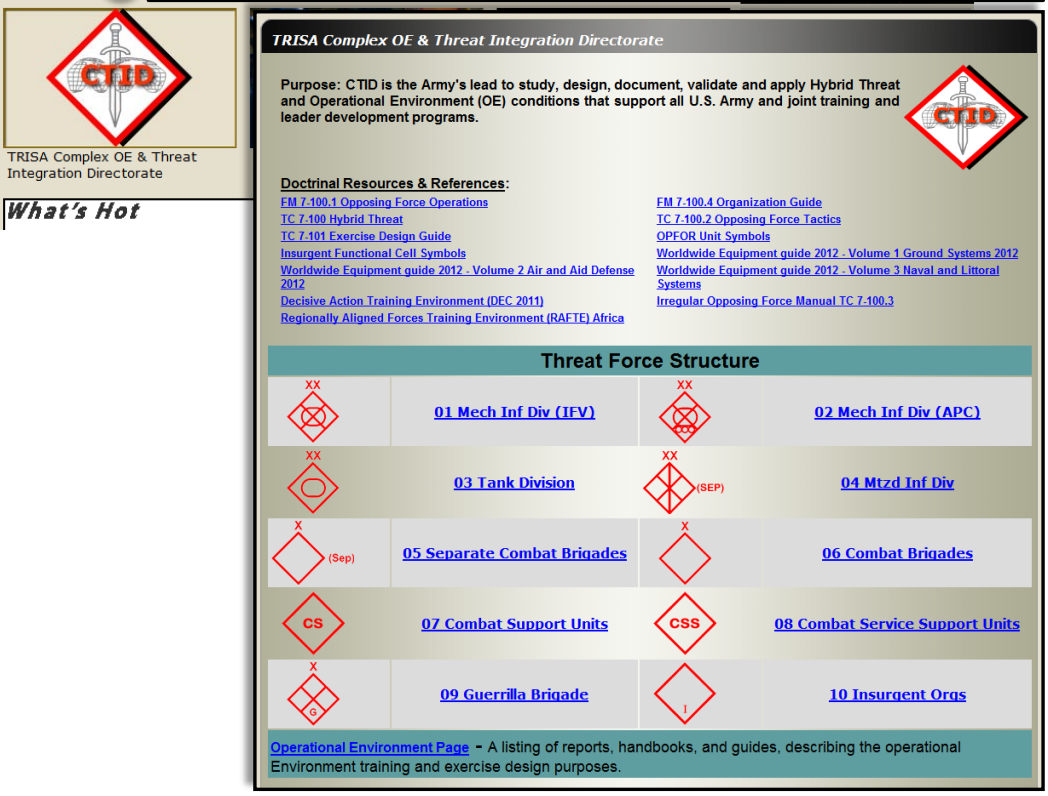
In the November 2013 *Red Diamond*, CTID Operations did not include the complete list of references cited by Jim Bird in his article "Boot-Heel or Achilles Heel? Turkey's Hatay Province." The complete list of endnotes is included below.

[1] Hugh Eakin, "Will Syria's Revolt Disrupt the Turkish Borderlands?" *New York Review of Books,* 24 June 2011.
[2] "Turkey Detains Nine Over Deadly Bombings," *RAPID Weekly News Update* (FOUO, vol. 3 no.20), 17 May 2013.
[3] "Syrian Village Gives Up Secrets After Massacre," Muslim Village.com, 29 May 2013.
[4] Aydin Albayrak, "Mihrac Ural, A Man with a Long History of Terrorism," *Today's Zaman,* 14 May 2013
[5] "Pro-Regime Militant Speaks of 'Cleansing' Banias," *NOW,* 6 May 2013; Stephen Starr, "The Renewed Threat of Terrorism to Turkey," *Combating Terrorism Center at West Point (CTC) Sentinel,* June 2013.
[6] "Report of the Independent International Commission of Inquiry on the Syrian Arab Republic," *United Nations Human Rights Council,* 16 August 2013.
[7] "Assad's Plan B is 'Ethnic Cleansing' Says Turkish FM," *Alarabia.net English,* 8 May 2013; Alexander Christie-Miller Yayladagi, "Assad Massacres Are An Ethnic Cleansing Strategy, Says Turkey," *Times of London, Middle East,* 10 May 2013; Clare Morgana Gillis, "In Turkey, Anger As Syrian Conflict Spills Over," *Ashville Citizen-Times,* 19 May 2013.
[8] Stephen Starr, "The Renewed Threat of Terrorism to Turkey," *Combatting Terrorism Center at West Point (CTC) Sentinel,* June 2013.
[9] Aydin Albayrak, "Mihrac Ural, A Man with a Long History of Terrorism," *Today's Zaman,* 14 May 2013.
[10] Abdullah Bozkurt, "Role of Iran and Syria in THKP/C Terrorism Against Turkey," *Today's Zaman,* 21 September 2012.
[11] Sinem Cengiz, "Turkey Should Take Assad's Retaliation Remarks Seriously," *Today's Zaman,* 15 September 2013
[12] Ely Karmon, "Time to Put An Alawite State on the Map," *Haaretz.com,* 20 March 2013.
[13] William Booth, "In Turkey, Alawite Sect Sides With Syria's Assad," *Washington Post,* 14 September 2012.
[14] Anna Mulrine, "Pentagon's Top Three Threats in the 'Deep Future,'" *Christian Science Monitor,* 24 October 2013.
[15] Gary Grappo, "Syria's Act III: A Religious War in the Middle East," *Fikra Forum,* 26 June 2013
[16] Gary Grappo, "Syria's Act III: A Religious War in the Middle East," *Fikra Forum,* 26 June 2013.
[17] "Blurring the Borders: Syrian Spillover Risks for Turkey," *International Crisis Group,* 30 April 2013.

Go to Army Training Network

1 **Go to https://atn.army.mil/ with DOD-Approved Login =** *Only 2 Clicks!*

2 **Click CTID icon =** *You are at the CTID Products!*



Hybrid Threat – The diverse and dynamic combination of regular forces, irregular forces, terrorist forces, and/or criminal elements unified to achieve mutually benefitting effects. (ADRP 3-0)

PRODUCTS FOR COMPLEX ENVIRONMENTS

by CTID Operations

Sampler of Products:

TC 7-100, *Hybrid Threat*
TC 7-101, *Exercise Design*
TC 7-100.2, *Opposing Force Tactics*
DATE v. 2.0, *Decisive Action Training Environment*

RAFTE-Africa *Regionally Aligned Forces Training Environment*

***Horn of Africa OEA* 2013 (Revised with seven states in HOA OE 2013)**

COMING SOON!

TC 7-100.3, *Irregular Opposing Forces*

***Worldwide Equipment Guide* (WEG) 2013**

For documents produced by TRISA's Complex Operational Environment and Threat Integration Directorate (CTID) of US Army TRADOC G2, with DOD-Approved Certificate login access, see **https://atn.army.mil/**. Look for the CTID logo.

Q: Do you need a copy of TC 7-100, *Hybrid Threat*?

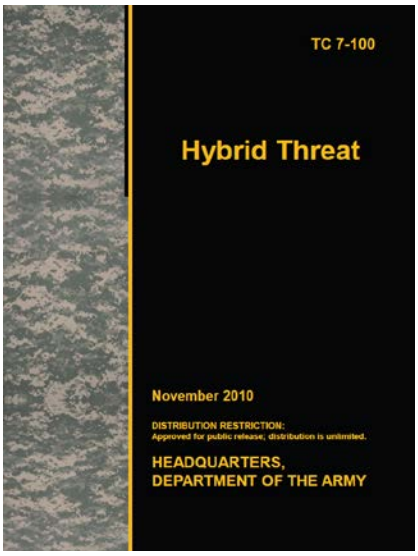
A: Go to ***ATN*** *access,* **https://atn.mil.army**. **Click CTID logo.**

Q: Where else can I go to retrieve TC 7-100, *Hybrid Threat*?

A: *With AKO access, see—*
https://www.us.army.mil/suite/doc/25952049

Q: *Do you have an issue on a threat or opposing force (OPFOR) issue?*

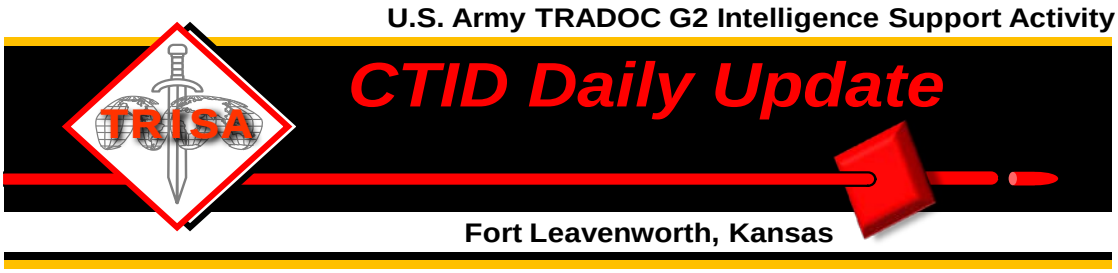
A: *CTID can assist you in identifying a solution. Send TRISA-CTID a request for information (RFI). See POCs on last page of this newsletter.*



THREATS TO KNOW—*CTID DAILY UPDATE* REVIEW

by Marc Williams, Training, Education, and Leader Development Team/JRTC LNO (CGI Ctr)

CTID analysts produce a daily *CTID Daily Update* to help our readers focus on key current events and developments across the Army training community. Available on AKO, each *Daily Update* is organized across the Combatant Commands (COCOMs). This list highlights key updates during the month.



02 December: **Missile defense:** Iran announces development of ballistic missile technology

Nigeria: Boko Haram attack **Maiduguri** International Airport and the Composite Group Air Force Base, at least 20 Soldiers killed

04 December: **Mexico:** Thieves in **Tepojaco** stole a truck of 'extremely dangerous' radioactive material that could be used as a dirty bomb

Lebanon: Hezbollah commander assassinated in **Beirut** by unknown group

06 December: **Al-Qaeda:** AQAP launches suicide assault on **Yemeni** defense ministry complex

Argentina: One dead, 100 wounded in looting after police strike in **Córdoba**

09 December: **Al-Qaeda:** Al-Qaeda in **Syria** has sarin: Russia ready to deal with Syrian al-Qaeda plot against Sochi Olympics

Japan: Chinese trespass first time territorial seas since Beijing set ADIZ

11 December: **Arctic:** Putin vows to beef up Arctic military presence

Central African Republic: Statement on additional US support to France and the African Union in the Central African Republic

13 December: **US:** Man arrested in planned suicide bombing at **Wichita, Kansas** airport

Syria: Pro-West Syrian rebels decimated by Islamist attacks; top general flees to Turkey

16 December: **Central African Republic:** CAR humanitarian situation worsens

US: US boosts naval security aid to Southeast Asia. Taking aim at China?

18 December: **Syria:** Syria barrel bomb raids on **Aleppo** kill 135

South Sudan: State Department to evacuate Americans for South Sudan after failed coup

20 December: **Al-Qaeda:** Latest Treasury designation targets al-Qaeda's fundraising network

South Sudan: US deploys 45 troops to South Sudan amid intense fighting

Red Diamond Index 2013 (Volume 4, Issues 1-12)

Click on each Issue to link to the newsletter on the Army Training Network (ATN). Article titles and authors are listed below each issue. Authors are from TRISA-CTID unless otherwise stated.

01-January 2013 *Red Diamond*

- Operational Environments and the Future by CTID
- Describing a Regionally Aligned Forces Training Environment by CTID Operations
- OE Threat Assessments Overview by H. David Pendleton
- Insurgent Assault on a Coalition Traffic Control Post by Jon H. Moilanen
- Aircraft Threats by Marc Williams
- Iran's "Thunder" SAM by Steffany Trofino
- Maimana Mosque Bombing by Laura Deatrick
- OE Threat Assessment: Kuwait by H. David Pendleton
- OE Threat Assessment: Egypt by Laura Deatrick
- Assassins Target Imams in Dagestan by H. David Pendleton
- Director's Corner: DATE and DATE Implementation by Jon Cleaves
- Threats to Know-CTID Daily Update Review by Marc Williams

02-February 2013 *Red Diamond*

- Regionally Aligned Forces and Army Strategic Planning Guidance 2013 by CTID Operations
- Director's Corner: OPFOR Terms by Jon Cleaves
- Operational Environment Threat Assessment: Saudi Arabia by Laura Deatrick
- Bacha Khan Airport Attack by Rick Burns
- Replacement for the AK-47: Reality or Wishful Thinking? by Mike Spight
- OE Threat Assessment: Jordan by Jim Bird
- Threat Tactical Deception and Decoy Doctrine by Kristin Lechowicz
- Decoys in a Threat Defense TTP by Jon H. Moilanen
- Common Cyber Threats and Indicators by Jerry England
- Iranian Ballistic Missiles by LTC Terry Howard
- Threats to Know-CTID Daily Update Review by Marc Williams

03-March 2013 *Red Diamond*

- FM 5-02, *Operational Environment* Coming in 2013 by Penny Mellies
- Director's Corner: TC 7-100 Series by Jon Cleaves

- Operational Environment Threat TTP: Kidnapping at Katsina by Laura Deatrick
- Irregular Forces: Kachin Independence Army by Marc Williams
- Space/Counterspace Area of Interest in Development for WEG by Jennifer Dunn and Steffany Trofino
- Threat TTP: Suicide Vehicle Borne Improvised Explosive Device by Jim Bird
- Iran's Sea-Skimming Cruise Missile: Noor by Steffany Trofino
- Hybrid Threats and the Art of Reconstitution of the Force by Walter L. Williams
- How to Understand and Use a WEG Sheet by John Cantin
- Irregular Force Symbols: How to Portray the Irregular Threat by Jon H. Moilanen
- Threats to Know-CTID Daily Update Review by Marc Williams

04-April 2013 *Red Diamond*

- *Regionally Aligned Forces Training Environment (RAFTE)* – Coming in June 2013! by Angela Wilkins
- Director's Corner: RAFTE-Africa by Jon Cleaves
- The Long Reach of TRISA-WETED by Mike Sullivan (TRISA-WETED Red Team)
- Kachin Independence Army's Ambush TTP by H. David Pendleton
- Submarine Fiber Optic Cables by Penny Mellies
- OE Threat Assessment Series: Focus on Yemen by Laura Deatrick
- In Amenas, Algeria Gas Plant Attack by Rick Burns
- Hybrid Threats on the Army Training Network by Jerry England
- History and Proliferation of the Hind Helicopter by LTC Terry Howard
- The Puma Infantry Fighting Vehicle by John Cantin
- The PK Series of General Purpose Machine Guns by Mike Spight
- Insurgent Dismounted Raid on a Tank Platoon by Jon H. Moilanen
- Threats to Know-CTID Daily Update Review by Marc Williams

05-May 2013 *Red Diamond*

- Hybrid Threat and Opposing Force: New on ATN! by Jerry England
- Director's Corner: Teaching Threat Tactics by Jon Cleaves
- The WETED "Playing Fields" by Mike Sullivan (TRISA-WETED Red Team)
- Old Ghosts from the Cold War: The Ankara Embassy Bombing by Jim Bird
- Horn of Africa OEA: Djibouti Military Variable Preview by H. David Pendleton
- Russian's Aerospace Defense Forces Satellite System: Kondor by Steffany A. Trofino
- Air Defense Systems: A Fight for Airspace Control by LTC (P) Thomas Georges
- Boat Operations – Nigeria and Somalia by Marc Williams
- Jabhat Al-Nusra: Aleppo Suicide Attack by Rick Burns
- Irregular OPFOR Defense of a Complex Battle Position (CBP) by Jon H. Moilanen
- Threats to Know-CTID Daily Update Review by Marc Williams

06-June 2013 *Red Diamond*

- *Irregular Opposing Forces* Coming Soon! TC 7-100.3 by Jon H. Moilanen
- Director's Corner: Hybrid Threat Train-the-Trainer September 2013 by Jon Cleaves
- WETED Red Team Anti-Access Operations by Mike Sullivan (TRISA-WETED Red Team)
- IED Attacks in Pattani by H. David Pendleton
- Student Text 7-100 *OPFOR Battle Book for the Operational Environment* by Walter L. Williams
- The Threat of Fire-Producing TTP and Weapons by Jennifer Dunn
- The Criminal Elements within the Hybrid Threat and Training Integration by Kristin Lechowicz
- OE Threat Assessment: Iraq by Rick Burns

- RAFTE-Africa Published by TRADOC G1-TRISA by Angela Wilkins
- Hybrid Threat Snipers (Part 1) by Mike Spight
- Irregular Opposing Forces (Coming Soon! Look for Army TC 7-100.3) by Jon H. Moilanen
- Threats to Know-CTID Daily Update Review by Marc Williams

07-July 2013 *Red Diamond*

- Hybrid Threat Train-the-Trainer at CTID – Sep 2013 by Jon H. Moilanen
- Director's Corner: CTID Products and Personnel are Here to Help by Jon Cleaves
- The Perfect "Swarm:" An Effective Red Team "Game Changer" in Exercises, Experiments, and Wargames by Mike Sullivan (TRISA-WETED Red Team)
- Irregular Opposing Forces in Persistent Conflict: Part 1; Understanding an OPFOR Insurgency Rationale by Jon H. Moilanen
- Horn of Africa OEA: Eritrea Military Variable Preview by H. David Pendleton
- Hybrid Threat Marksmen and Snipers: Equipment and Organization (Part 2) by Mike Spight
- Taliban Raid Observation Post by Rick Burns
- Tactical Decisions for Training Leaders: Dutch Army and OPFOR TTP by Jon H. Moilanen
- The Russian S-300 Surface-to-Air Missile System by John Cantin
- Boat Operations Part 2: Liberation Tigers of Tamil Eelam (LTTE) or "Tamil Tigers" by Marc Williams
- Threats to Know-CTID Daily Update Review by Marc Williams

08-August 2013 *Red Diamond*

- *Horn of Africa – Operational Environment Assessment* by Angela Wilkins
- Director's Corner: DATE and Linked Training/How to Request Changes by Jon Cleaves
- TC 7-102, OE Considerations for Training and Education Development by Walter L. Williams
- Advanced Situational Awareness Training: Saving Lives One Vignette at a Time by Mike Sullivan (TRISA-WETED Red Team)
- Shaping the North Korean EMP Threat by Steffany A. Trofino
- Operational Environment Conditions of the Ferghana Valley by Jennifer Dunn
- How Will the Syrian Civil War Affect Jordanian Stability? by Mr. Art McKinney and Dr. Robert Arp (TRISA Modeling & Simulation Directorate and Operational Environment Laboratory)
- Hybrid Threat Train-the-Trainer (HT3) Class – March 2014 by Pat Madden
- *Barisian Revolusi Nasional* in Thailand by H. David Pendleton
- Irregular Opposing Forces in Persistent Conflict: Part 2; Understanding an OPFOR Insurgency Rationale by Jon H. Moilanen
- Threats to Know-CTID Daily Update Review by Marc Williams

09-September 2013 *Red Diamond*

- Hybrid Threat Train-the-Trainer: 23-27 September 2013 by CTID Operations
- Director's Corner: CTC, HST, and CoE Trainers Can Contact CTID for Support by Jon Cleaves
- Noncombatants in Complex Operational Environments: Training – Who is Friend or Foe? by Jon H. Moilanen
- Horn of Africa: Ethiopia Military Variable Preview by H. David Pendleton
- Human Domain and the Hybrid Threat Factor by CPT Ari Fisher
- War Comes to Reyhanli: Terrorist Attack of 11 May 2013 by Jim Bird
- Menagh Airbase Siege: Menagh, Syria by Rick Burns
- Case Study: Mexican Drug Cartel IED Attack on Law Enforcement by Kris Lechowicz
- Reconnaissance and the Threat Cyber Attack Life Cycle by Jerry England
- Threats to Know-CTID Daily Update Review by Marc Williams

10-October 2013 *Red Diamond*

- Operational Environment Assessment: Horn of Africa by Angela Wilkins
- Director's Corner: Decisive Action Events/Moving beyond the Cold War by Jon Cleaves
- Guerrilla and Insurgent: Describing Threats in Complex Environments by Jon H. Moilanen
- Integrating Crime and Criminal Elements into Training by CPT Ari Fisher
- *Atropia Covenant* from the Red Side: JRTC 13-09 by Marc Williams
- Camp Bastion Attack: Update 2013 by H. David Pendleton
- Infiltration and the Cyber Attack Cycle by Jerry England
- Al Shabaab Attack on the Westgate Mall: Nairobi, Kenya by Rick Burns
- Threats to Know-CTID Daily Update Review by Marc Williams

11-November 2013 *Red Diamond*

- Irregular Opposing Forces for Training: TC 7-100.3 Coming Soon by Jon H. Moilanen
- Director's Corner: DATE (Conditions) by Jon Cleaves
- The Cyber Attack Life Cycle: Establishing Command and Control by Jerry England
- Boot-Heel of Achilles Heel? Turkey's Hatay Province by Jim Bird
- Libya: Proliferation of Capabilities by Steffany Trofino
- Boats Part 3. Criminals: OPFPR TTP for Maritime and Littoral Operations by Marc Williams
- Somalia: Military Variable Highlights by H. David Pendleton
- RPG-29 Urban Ambush on an Enemy Tank Platoon by Jon H. Moilanen
- Threats to Know-CTID Daily Update Review by Marc Williams

12-December 2013 *Red Diamond*

- Red Diamond: Best of 2013 by Jon H. Moilanen
- Best of 2013 Introduction: Red Diamond in Review by CTID Operations
- Menagh Airbase Siege: Menagh, Syria by Rick Burns
- Integrating Crime and Criminal Elements into Training by CPT Ari Fisher
- Decoys and Deception TTP in a Defense by Kris Lechowicz
- Aircraft Threats by Marc Williams
- Threat TTP: Suicide Vehicle Borne Improvised Explosive Device by Jim Bird
- Hybrid Threats and the Art of Reconstitution of the Force by Walter L. Williams
- The PK Series of General Purpose Machine Guns by Mike Spight
- Operational Environment Threat TTP: Kidnapping at Katsina by Laura Deatrick
- The Threat of Fire-Producing TTP and Weapons by Jennifer Dunn
- IED Attacks in Pattani by H. David Pendleton
- Wargaming, Experimentation, and Threat Emulation Directorate: Challenging Capabilities and Concepts by Mike Sullivan (TRISA-WETED Red Team)
- Insurgent Dismounted Raid on a Tank Platoon by Jon H. Moilanen
- Threats to Know-CTID Daily Update Review by Marc Williams

CTID Points of Contact

Director, CTID Mr Jon Cleaves DSN: 552
jon.s.cleaves.civ@mail.mil **913.684.7975**

Deputy Director, CTID Ms Penny Mellies
penny.l.mellies.civ@mail.mil **684.7920**

Liaison Officer (UK)
[pending arrival]

Operations -CTID Dr Jon Moilanen
jon.h.moilanen.ctr@mail.mil BMA **684.7928**

Threat Assessment Team Lead DAC 684.7960
Mr Jerry England jerry.j.england.civ@mail.mil

Threat Assessment Team Ms Steffany Trofino
steffany.a.trofino.civ@mail.mil **684.7960**

Threat Assessment Team Mrs Jennifer Dunn
jennifer.v.dunn.civ@mail.mil **684.7962**

Threat Assessment Team Mr Kris Lechowicz
kristin.d.lechowicz.civ@mail.mil **684.7922**

Worldwide Equipment Guide Mr John Cantin
john.m.cantin.ctr@mail.mil BMA **684.7952**

Train-Edu-Ldr Dev Team Lead DAC 684.7923
Mr Walt Williams walter.l.williams112.civ@mail.mil

TELD Team/NTC LNO LTC Shane Lee
shane.e.lee.mil@mail.mil **684.7907**

TELD Team/RAF LNO CPT Ari Fisher
ari.d.fisher.mil@mail.mil **684.7939**

TELD Team/JRTC LNO Mr Marc Williams CGI
james.m.williams257.ctr@mail.mil **684.7943**

TELD Team/JMRC LNO Mr Mike Spight
michael.g.spight.ctr@mail.mil CGI **684.7974**

TELD/MCTP LNO Mr Pat Madden BMA
patrick.m.madden16.ctr@mail.mil **684.7997**

OE Assessment Tm Lead BMA **684.7929**
Mrs Angela Wilkins angela.m.wilkins7.ctr@mail.mil

OE Assessment Team Mrs Laura Deatrick
laura.m.deatrick.ctr@mail.mil CGI **684.7925**

OE Assessment Team Mr H. David Pendleton
henry.d.pendleton.ctr@mail.mil CGI **684.7946**

OE Assessment Team Mr Rick Burns
richard.b.burns4.ctr@mail.mil BMA **684.7897**

OE Assessment Team Dr Jim Bird
james.r.bird.ctr@mail.mil Overwatch **684.7919**

CTID Mission

CTID is the TRADOC G2 lead to study, design, document, validate, and apply hybrid threat in complex operational environment CONDITIONS that support all US Army and joint training and leader development programs.

What We Do for YOU

- **Determine threat and OE conditions.**
- **Develop and publish threat methods.**
- **Develop and maintain threat doctrine.**
- **Assess hybrid threat tactics, techniques, and procedures (TTP).**
- **Develop and maintain the Decisive Action Training Environment (DATE).**
- **Develop and maintain the Regionally Aligned Forces Training Environment (RAFTE).**
- **Support terrorism-antiterrorism awareness.**
- **Publish OE Assessments (OEAs).**
- **Support threat exercise design.**
- **Support Combat Training Center (CTC) threat accreditation.**
- **Conduct "Advanced Hybrid Threat Tactics" Train-the-Trainer course.**
- **Conduct Hybrid Threat resident and MTT COE Train-the-Trainer course.**
- **Provide distance learning (DL) COE Train-the-Trainer course.**
- **Respond to requests for information (RFI) on threats and threat issues.**

YOUR Easy e-Access Resource

With AKO access--CTID products at:
www.us.army.mil/suite/files/11318389