U.S. ARMY TRADOC G2 Intelligence Support Activity

TRISA

Red Diamond

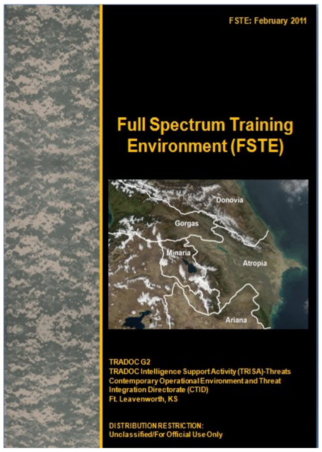
Contemporary Operational Environment and Threat Integration Directorate (CTID)

Fort Leavenworth, Kansas Volume 2, Issue 2 FEB 2011

Full Spectrum Training Environment (FSTE)

INSIDE THIS ISSUE:

Just Published Training Document



FSTE: February 2011

Full Spectrum Training Environment (FSTE)

TRADOC G2
TRADOC Intelligence Support Activity (TRISA)-Threats
Contemporary Operational Environment and Threat Integration Directorate (CTID)
Ft. Leavenworth, KS

DISTRIBUTION RESTRICTION:
Unclassified/For Official Use Only

Based upon guidance from the Chief of Staff of the Army (CSA) and feedback from all Combat Training Center (CTC) Commanders, the TRADOC G-2 was tasked in September 2010 to develop a document to support full spectrum operations (FSO) training environments across all CTCs. The purpose of the FSTE is to provide one document from which to develop exercises and training events. The FSTE is not a scenario. It presents a detailed discussion of all the conditions and characteristics necessary for trainers to build an FSO training environment to include all supporting scenarios.

The FSTE is an unclassified document that defines the conditions of the operational environment (OE) used to build training scenarios and exercises. In this case, the OE consists of four fictional countries (Ariana, Atropia, Gorgas, and Minaria). The FSTE provides a detailed description of the OE across all four countries, and presents an Events list linked to Blue METL. The document also provides and a presentation of TC 7-100-compliant orders of battle for the region.

All comments and suggestions are welcome. Customers at the CTCs are especially encouraged to provide feedback. The FSTE is a dynamic document and will be updated as necessary to support the Army training community. The FSTE is posted on the AKO. For comments or questions regarding this document, contact Penny Mellies at DSN 552-7920, commercial (913) 684-7920, email: penny.mellies@us.army.mil.

All CTID products can be found on AKO. Check out all of our products at:
https://www.us.army.mil/suite/files/11318389

NEWSLETTER DISTRIBUTION UNLIMITED

Suicide Attacks: Afghanistan

by Raines Warford

Suicide bombings are a prominent and continuing threat in Afghanistan. More than 600 suicide bombings occurred between June 2003 and 31 January 2010. Though the attack incidents were initially infrequent, they have remained at over 100 bombings per year for the last five years.

Recognizing the probability of an increase in suicide bombings, in October 2005 the Operational Environment Assessment Team (OEA) Team began collecting open-source information regarding suicide bombings in Afghanistan in an effort to identify TTP and trends. This effort developed into an OEA Team threat report titled *Suicide Attacks: Afghanistan*.

Methodology

The information used in the Threat Report derives from unclassified sources, such as news reports, studies, and papers produced by government and nongovernmental organizations. The research and data analysis is at times challenging. For example, details on suicide bombings vary dramatically across sources. Sources will directly contradict each other. In some cases, the same suicide bombing may be reported with varying casualty numbers by several sources. Part of this is due to different criteria and methodologies employed by various analysts in determining statistics.

Divergence in attack categorization is also a factor. In some cases, suicide bombings may be lumped in with other types of attacks and there is no raw data available from the source. One reads, “200 suicide and IED attacks” but it is not possible to determine from the source how many of these attacks were suicide bombings and how many were IEDs. Obviously, there is potential for a range of disparity in statistics reported in such a manner. Due to difficulties in determining the precise details of individual attacks and the overall statistics, the OEA Team chose a methodology which provides consistency and fulfills the original intent of identifying TTP and trends.

In the threat report, all suicide attacks are placed in one of two categories, either body-borne attacks or suicide vehicle-borne improvised device (SVBIED) attacks. Body-borne attacks are characterized by the bomber carrying the explosives on their person (most often wearing a suicide vest) while approaching their targets on foot. In SVBIED attacks, the explosives are transported in a vehicle of some type and/or the attacker approaches the targets using some form of transportation other than their feet. SVBIED attacks include bombers on motorcycles or bicycles, wearing suicide vests.

In the *Suicide Attacks: Afghanistan* threat report, multiple suicide attackers at the same location are counted as one suicide attack, unless the attackers utilized different delivery methods or the bombings were separated by a significant amount of time or distance. For example, if an SVBIED was detonated and two suicide bombers wearing explosive vests then attacked the same location, it would be counted as two suicide attacks in this presentation (one SVBIED and one body-borne attack). Multiple attackers wearing suicide vests attacking separate buildings in the same general vicinity at the same time would be considered one complex attack. A team of five suicide bombers assaulting a police station is one attack, not five suicide bombings.

Results

An examination of the data reveals some interesting TTP and trends. For instance, suicide attacks were originally concentrated in Kabul, with all attacks in 2003 and 2004 occurring in that province. By the following year, suicide bombings were occurring outside of Kabul province. Attacks began to occur across Kabul, Kandahar, Herat, and Balkh provinces.

OEA Team

Since 2005, suicide attacks have occurred in almost every province of Afghanistan, with the majority happening in provinces bordering Pakistan.

From 2005 through 2010, Kabul was the scene of about 13% of suicide attacks in Afghanistan annually. There were 79 suicide attacks in Kabul during the period from 01 January 2003 through 31 January 2010. Of these attacks, 48 were vehicle-borne (61%) and 31 were body-borne (39%). From 01 January 2003 through 31 January 2010 in Kabul, there were a total of nine bombings in each of the months of January, August, and October. For the month of April, there were only two attacks in Kabul during the eight-year period.

As of 28 February 2011, 3 of 10 suicide bombings (30%) occurred in Kabul in 2011. One of these was a bomber on a motorcycle (SVBIED) while the remaining two were body-borne. This is consistent with the previous eight years' suicide attack trends in Kabul.

Who are the perpetrators of these attacks? Though the typical response to this question is the Taliban, that is an overly simplistic answer. According to *The Long War Journal*, the Kabul Attack Network (consisting of members of the Taliban, the Haqqani Network, and Hizb-i-Islami Gulbuddin) is working in cooperation with Lashkar-e-Taiba and al-Qaeda to conduct attacks in Kabul. Additionally, in a news conference on 10 February 2011, a representative of Afghanistan's intelligence service, the National Directorate of Security, stated Taliban commander Talib Jan has led a suicide bombing network for the past three years. Interestingly, Talib Jan was in Pul-i-Charkhi prison in Kabul during the time he was said to be coordinating suicide bombings. "From inside the Pul-i-Charkhi prison he was appointing people and giving them targets and instructions,'" said a National Directorate of Security spokesman, Lutfullah Mashal. "Most of the terrorist and suicide attacks in Kabul were planned from inside this prison by this man," he said.

The *Suicide Attacks: Afghanistan* threat report, while not a finished intelligence product, provides information to deploying units, scenario developers, and trainers regarding the threat from suicide attacks in Afghanistan. The report provides information including data, trends, and details of attacks such as in the examples for Kabul discussed in this article, along with additional information about suicide attacks throughout Afghanistan.

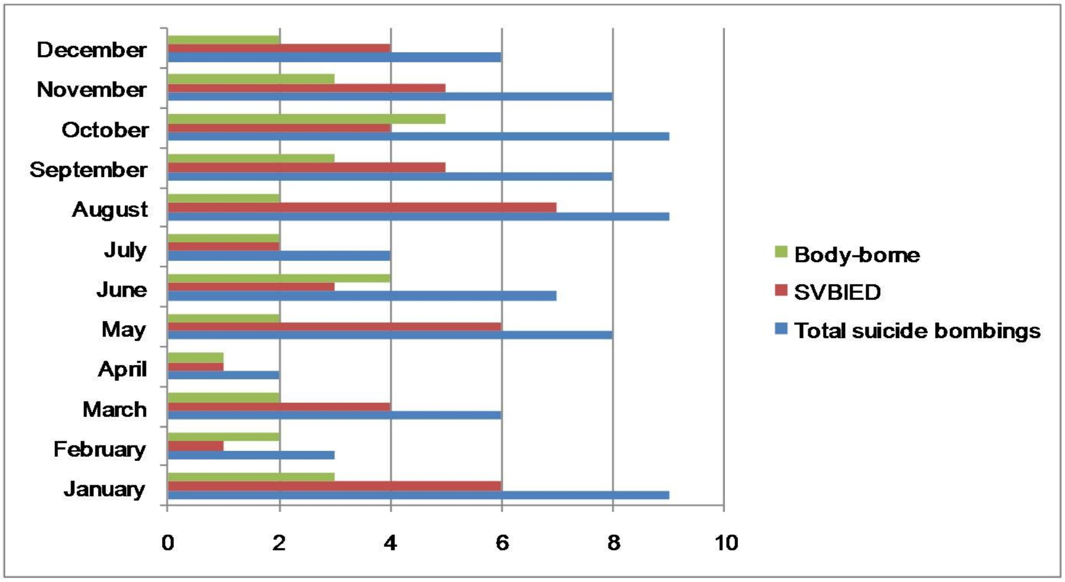


Chart 1: Kabul Suicide Attack Totals by Month and Type (2003-2010).

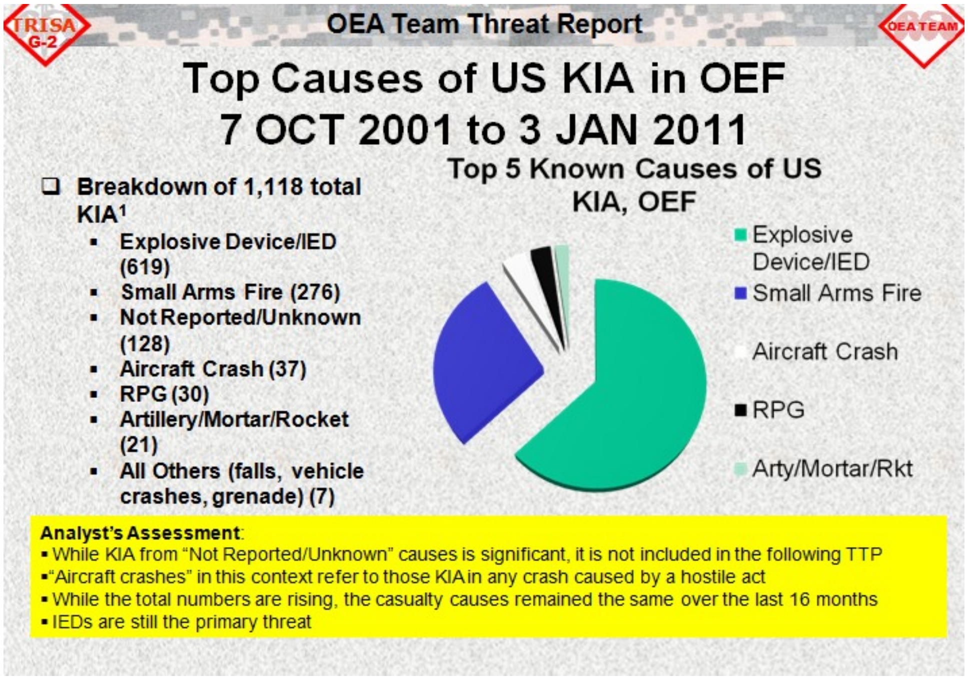
OEA Team

Taliban Top 5 Most Deadly TTP

by Justin Lawlor

The Operational Environment Analysis (OEA) Team continues to monitor the Top 5 casualty causing mechanisms in Afghanistan. As combat operations continue in Afghanistan, it is critical to understand the likely employment of Taliban tactics and techniques in theater. The *Taliban Top 5 Most Deadly TTP* threat report seeks to highlight the Taliban tactics, give an insight into their prevalence and danger, and provide tactical examples usable for training and other pre-deployment evolutions.

The casualties produced by the Top 5 since the beginning of Operation Enduring Freedom (OEF) illustrate the nature of the threat faced by deployed forces. **Improvised explosive devices (IEDs)** account for over 600 of the 1,118 personnel killed in action (KIA) between October 2001 and January 2011. **Small arms fire** is responsible for 276 US killed in action. **Aircraft crashes** due to enemy action represent 37 US KIA. The effects of **rocket-propelled grenade (RPG) fire** have killed US service members, while **rockets, mortars, and artillery** account for 21. Service members wounded in action stand at almost ten thousand, with the cause of those wounds paralleling the cause of those killed in action, by percentage.



OEA Team Threat Report

Top Causes of US KIA in OEF
7 OCT 2001 to 3 JAN 2011

❑ Breakdown of 1,118 total KIA[1]

- Explosive Device/IED (619)
- Small Arms Fire (276)
- Not Reported/Unknown (128)
- Aircraft Crash (37)
- RPG (30)
- Artillery/Mortar/Rocket (21)
- All Others (falls, vehicle crashes, grenade) (7)

Top 5 Known Causes of US KIA, OEF

Analyst's Assessment:
- While KIA from "Not Reported/Unknown" causes is significant, it is not included in the following TTP
- "Aircraft crashes" in this context refer to those KIA in any crash caused by a hostile act
- While the total numbers are rising, the casualty causes remained the same over the last 16 months
- IEDs are still the primary threat

Graphic 1: Top 5 Casualty Causing TTP in Afghanistan.

The IED remains the largest producer of US KIA and wounded in action (WIA) within Afghanistan. While Iraq and Afghanistan share little in common, the importance of the IED as a threat is the exception. While IED mitigation strategies, equipment and, most importantly, awareness are having a positive effect on lowering the rate with which IEDs successfully engage US forces, it is also unlikely the Taliban will abandon IEDs as their primary weapon. IEDs, instead, will probably become larger and more sophisticated in a concerted effort to defeat protective efforts by combination of brute force and technological work-around, as the IED remains responsible for over half of all US casualties.

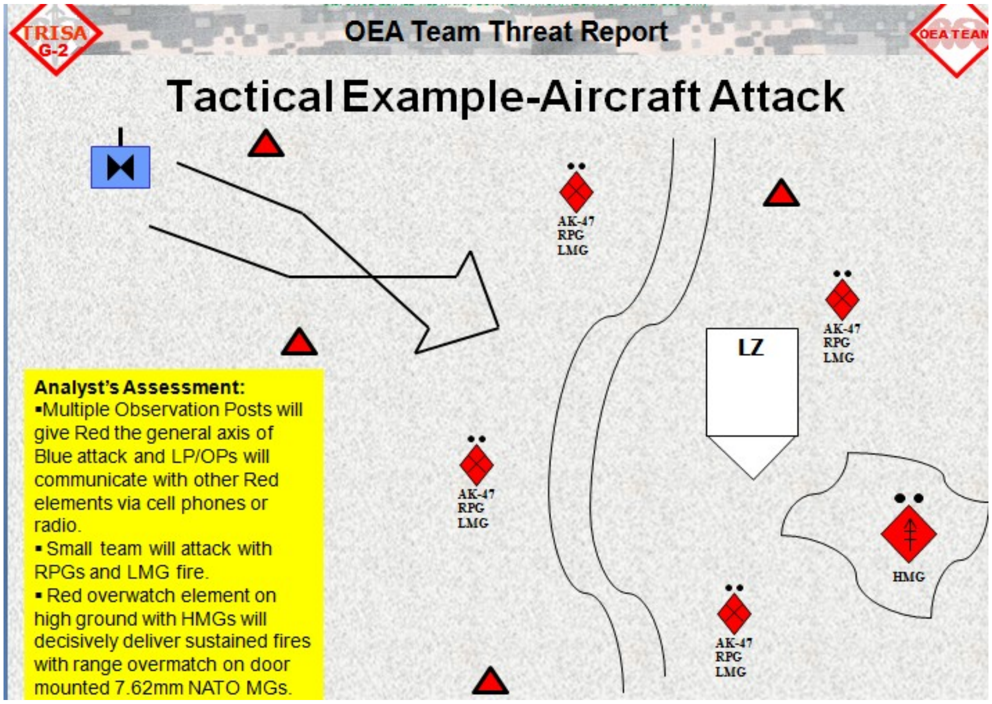
The IED must also be assessed inside two major larger frameworks, that of information operations and operational space. The IED, as an information operations tool, is the most visible means for the Taliban to spread their perception management messages of Taliban power and central government impotence and indifference. Successful attacks also allow for continued international fund-raising as the filming and dissemination of effective attacks aid in this effort. At the more immediate level of operations in Afghanistan, Joint IED Defeat Office (JIEDDO) has assessed the importance of the IED in providing local Taliban commanders the operational space to conduct fundraising and recruitment efforts.

OEA Team

The fundraising aids the protection of the opium crop, and the conversion of the opium into heroin for continued support of the insurgency.

Tactically, the IED will often be used to commence attacks with RPGs and small arms fire, or be staged to attack IED mitigation personnel or other first-responders. RPGs and small arms remain the ubiquitous threat, and are responsible for more than a quarter of US casualties. The likely impossibility of interdicting small arms and RPGs will make this an enduring threat.

Taliban attacks on transiting air assets and indirect fire round out the top five causes of US casualties. The Taliban remain committed to successfully targeting US aircraft as it is a symbol of US power. Rockets and mortars are the prime indirect fire threats. The RPG ambush, combined with crew served machine guns, are the most likely Taliban threats to air operations.



OEA Team Threat Report

Tactical Example-Aircraft Attack

Analyst's Assessment:

- Multiple Observation Posts will give Red the general axis of Blue attack and LP/OPs will communicate with other Red elements via cell phones or radio.
- Small team will attack with RPGs and LMG fire.
- Red overwatch element on high ground with HMGs will decisively deliver sustained fires with range overmatch on door mounted 7.62mm NATO MGs.

Graphic 2: The Taliban Top 5 Most Deadly TTP has multiple tactical diagrams to aid in training design.

All Taliban attacks are likely to be staged attacks, focused on maintaining economy of force. Often tactically warned by far-flung OP/LPs, the Taliban will attempt to ambush Coalition units along logical movement corridors or likely objectives. Starting with an IED or RPG, the Taliban will press the advantage if able, and withdraw using their superior mobility if tactically pressed. Taliban will attempt to use Coalition units' lower mobility to choose the time and place for contact.

The most dangerous Taliban course of action is the massed attack against isolated outposts, as was seen at combat outpost (COP) Kahler, Wanat. Nonetheless, the most likely Taliban course of action remains the IED, especially when used in conjunction with baited ambushes and/or small and indirect weapons fire. It is also possible that the Taliban would wish to emulate the Pakistani Taliban's success at high profile and out-of-area operations. Additionally, reports of state aid to the Taliban remain a troubling prospect for the ability of the Taliban to increase and refine their operations.

Training and Education

Insurgents and Guerrillas—the Heart of the Hybrid Threat

by Michael Spight

What is a hybrid threat? What does it typically consist of and what are its capabilities? According the *TC 7-100: Hybrid Threat,* a hybrid threat is the diverse and dynamic combination of regular forces, irregular forces, and/or criminal elements all unified to achieve mutually benefitting effects. A hybrid threat consists of at least two of the following five elements:

1.) A **conventional regular force**

2.) A **professional military force** or a force comprised of a professional cadre and conscripts

3.) A **paramilitary forces** (state police, internal security troops, border protection forces, etc.)

4.) **Criminal elements**

5.) And **insurgent groups** (typically rely on subversion and violent acts [terrorism] to force political change) and **guerrilla units** (irregular, homegrown forces operating in occupied territory, they may or may not be uniformed, organized, and equipped like a regular force)

In addition, TC 7-100 Hybrid Threat also defines insurgents and guerrillas:

Insurgents: An insurgency is “the organized use of subversion and violence by a group or movement that seeks to overthrow or force change of a governing authority” (JP 3-24).

Guerrillas: A guerrilla is “a combat participant in guerrilla warfare” (JP 1-02). Guerrilla warfare is “military and paramilitary operations conducted in enemy-held or hostile territory by irregular, predominantly indigenous forces” (JP 3.05.1).

History is replete with examples of active hybrid threats, and some of the more notable are:

- ♦ The American Revolution: Continental Army, various militias and guerrilla units vs. the British Army and mercenaries.
- ♦ 1754 to 1763: regular British and French forces fought each other amidst irregular Colonialists fighting for the British and American Indians fighting for both sides.
- ♦ The American Civil War: Bloody Kansas (Quantrill and “Bloody Bill” Anderson).
- ♦ 1814: Peninsula War ended after the combination of regular and irregular allied forces from Britain, Portugal, and Spain prevented France from controlling the Iberian Peninsula.
- ♦ World War II: On the Eastern Front, Soviet partisans tied down approximately 10 Wehrmacht and Waffen SS divisions in the invading German Army’s rear areas. These units later took part in the Red Army’s counter offensive by supporting Red Army in conventional formations.
- ♦ 1954 to 1976: Viet Cong and People’s Army of Vietnam combined irregular and regular forces in fighting the French and US forces. Viet Cong would organize into conventional and unconventional units.
- ♦ 2006: Hezbollah mixed conventional capabilities (such as anti-armor weapons, rockets, and command and control networks) with irregular tactics (including information warfare, non-uniformed combatants, and civilian shielding). The result was a tactical stalemate and strategic setback for Israel.

And the trend continues in Iran, North Korea, and China with each possessing robust conventional capabilities with a significant irregular capability.

Training and Education

We can expect any future adversary to be aware of the successes the hybrid threat, particularly irregular forces, have had against US forces of the past 10 years. When competently led, irregular forces add an amazing level of complexity to the tactical problems BLUFOR must plan for and respond to on the battlefield.

This article will focus on insurgents and guerrillas (irregular forces as part of the OPFOR) and how Combat Training Centers (CTCs) can best replicate their capabilities against Rotational Training Unit (RTUs-BLUFOR) in a manner that supports conventional OPFOR formations and provides a real challenge for the RTU during a Full Spectrum Exercise (FSX).

Tactics

Although the hybrid threat may conduct strategic and operational level planning and operations, this article will focus on the tactical level and its practical application within scenario planning and execution at a CTC.

INFOWAR: INFOWAR is a key weapon system that will be used with great skill by irregular force elements. Specifically, they will seek to degrade/deny BLUFOR communications capabilities and use specific incidents (injuries/deaths of civilians) to their advantage by leveraging the Internet, local, and international media sources. Additionally, capabilities to interfere with BLUFOR GPS based systems or their IT systems are not outside the bounds of reality, and BLUFOR must be prepared for such attacks, as OPFOR's irregular forces and conventional forces must be set to act if an opportunity presents itself.

Systems Warfare: Irregular forces will attempt to locate, identify, isolate, attack and degrade/destroy BLUFOR critical systems. Critical systems consist of the primary system and associated sub-systems; it may be possible to degrade/destroy the ENTIRE critical system by merely attacking a key sub-systems rather than the system in its entirety. C4I, logistical nodes, and critical infrastructure being used by BLUFOR and/or the indigenous population, are examples of potential targets for irregular force elements.

Functional Tactics (Action Functions vs. Enabling Functions): The hybrid threat will utilize specific assets/capabilities it assesses as most capable of accomplishing a given mission against the BLUFOR. That asset or assets are known as the Action Element. If the mission is to conduct an attack, then the mission is performed by the attack element. If the mission is to conduct the main defensive effort, that mission would be performed by the main defense element. But, a force that supports the action element by conducting a separate operation in support of the action element is the enabling element. An example of this could be conduct of an operation in an area designed to draw the BLUFOR away to respond, thus leaving the area (the OPFOR's actual objective) vulnerable to an OPFOR action element attack. Simultaneous (Enabling) functions by irregular forces—attacks on BLUFOR critical nodes, particularly logistical, C4I or indirect fire capabilities—will enable the hybrid threat's conventional force as it conducts combat operations against BLUFOR infantry and armor units.

How can insurgents and guerrillas be most effectively replicated on a CTC? Focus on INFOWAR—this is a critical piece to ensuring OPFOR success, as seen in recent initial full spectrum operations (FSO) exercises at CTCs. The ability to leverage information to OPFOR or BLUFOR advantage, and to do so quickly and efficiently, thus forcing your opponent to react to the information you release is critical, and the importance cannot be overemphasized.

Attack Key Systems (Logistics Nodes, MSRs, RSTA elements, C4I nodes): All of these are important targets than can be very vulnerable to irregular force attack, and not necessarily direct action by the element that locates and identifies the node. The irregular force element can pass information about the node back to OPFOR UAV and/or targeting assets for more detailed examination via UAV or a quick attack by OPFOR indirect fire or CAS assets.

Conclusion

Creative, aggressive use of OPFOR assets in the roles of guerrilla and insurgent elements during FSX CTC rotations will provide rigor, and a challenge to RTUs in an environment that is envisioned as being very, very different than the COIN environment in which we have been operating over the past 10 years. Next time, the contributions that paramilitary forces and criminal elements can make as part of the HT/OPFOR to realistic, challenging FSX training will be examined. All personnel, particularly those assigned to CTC OPFOR units and Ops Groups, are encouraged to refer to TC 7-100: *Hybrid Threat* and TRADOC G2 Handbook No. 1.08: *Irregular Forces* for further detail and discussion.

Hybrid Threats Train the Trainer Course of Instruction (COI)

TRADOC G2 TRISA will host its annual Hybrid Threats, formerly known as Contemporary Operational Environment (COE), "Train the Trainer" Course of Instruction (COI) at Fort Leavenworth, Kansas, **25-29 April 2011**. The course covers Hybrid Threats and associated OPFOR application as depicted in the TC 7-100 series of field manuals (organization, doctrine, tactics, techniques, and procedures). The training will consist of a 40-hour block of instruction including lecture and practical exercises designed to train the trainer. The class continues to be five full days in length with participatory practical exercises comprising one or more days.

The class content has been updated with information from the new TC 7-100 *Hybrid Threat*, TC 7-101 *Exercise Design*, and the recently released Distributive Learning COE Interactive Multimedia Instruction Courseware.

The intent of this COI is to train a limited number of personnel who will return to their installation and/or command to present the material to others. Attendees should have a minimum of one year remaining longevity and the ability to present this COI instruction to the rest of their organization.

For further information, please contact patrick.madden@us.army.mil.

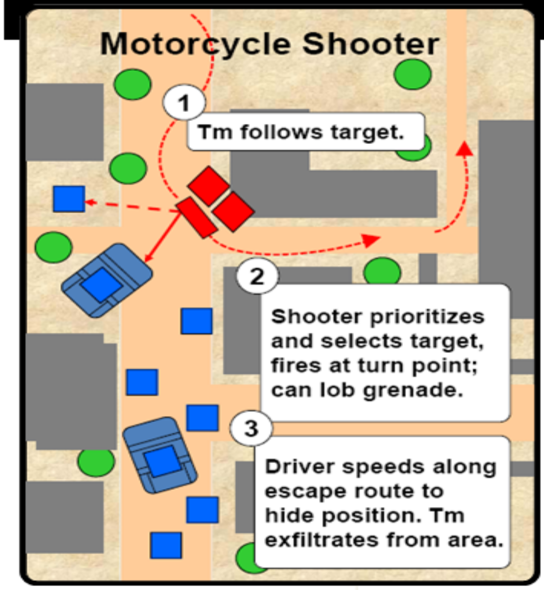
Requests for Information

- ***Your source for information on all OPFOR and Threat issues***
- ***See SME list on page 12 for key POCs***

Tactics, Techniques, and Procedures (TTP)

Threat Bullets

Terrorism TTP -- Keep it Simple...
Threats Terrorism Team (T3)
Know the Threat – Know the Enemy



Motorcycle Shooter

1 Tm follows target.

2 Shooter prioritizes and selects target, fires at turn point; can lob grenade.

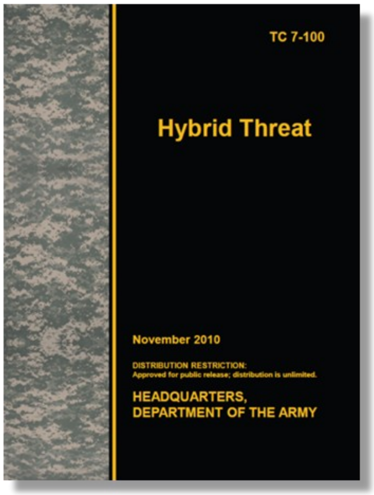
3 Driver speeds along escape route to hide position. Tm exfiltrates from area.

Small Arms Fire (SAF): Motorcycle Moving Shooter

Driver **sees** target and approaches firing point. Shooter **selects** aim point and **fires as motorcycle speeds past target.** Attack team uses preselected **escape** route to a safe haven. Variants can include **hand grenade** into target or group as motorcycle **passes**.

Attack can use multiple vehicles.

Training Circulars 7-100 Hybrid Threat and 7-101 Exercise Design are official!



TC 7-100

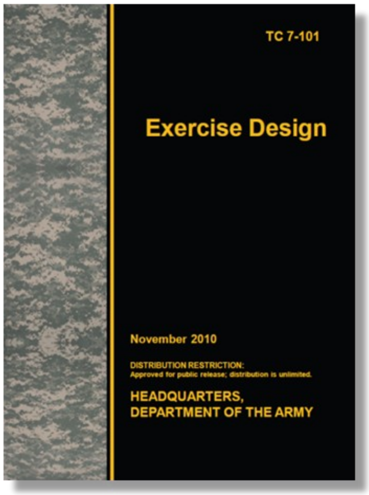
Hybrid Threat

November 2010

DISTRIBUTION RESTRICTION:
Approved for public release; distribution is unlimited.

HEADQUARTERS,
DEPARTMENT OF THE ARMY

TC 7-100 *Hybrid Threat* and TC 7-101 *Exercise Design* have been officially approved and are posted on Reimer Digital Library. The TC 7-100 supersedes FM 7-100, *Opposing Force Doctrinal Framework and Strategy*, 1 May 2003.



TC 7-101

Exercise Design

November 2010

DISTRIBUTION RESTRICTION:
Approved for public release; distribution is unlimited.

HEADQUARTERS,
DEPARTMENT OF THE ARMY

Article of Interest

Introduction to Theater Ballistic Missiles

by Kristin Lechowicz

Globally, many countries are in the midst of developing, or have some sort of theater ballistic missile (TBM) programs. TBMs are an expanding threat to US personnel, allies, and interests in regions where military forces are deployed, such as South Korea, Japan, Iraq, or Afghanistan. The trend among military forces for acquisition of theater missiles has expanded along with the growth of regional rivalries and the strategy of using long-range strike capability to gain regional leverage. TBMs provide an adversary the ability to strike a target 3,000km (1,864mi) away with a nuclear warhead or with an array of conventional warheads.

This article provides a basic introduction to TBMs and addresses the categories, payloads, countermeasures, characteristics, and emerging trends. Although not ballistic, cruise missiles also fall into the category of theater missiles. Cruise missiles are not included in this article and will be addressed in a future issue of the *Red Diamond*.

Categories

TBMs fall into the categories of **short**- and **medium-range** ballistic missiles. These missiles provide a deep strike capability extending well beyond that of the close battle and are categorized by their maximum possible range from launch platform to target (*see table 1*).

Picture 1: Iranian TBM mobile erector-launcher Shahab-3.

Payloads

The warhead is the munition and is selected for a particular strike mission. Modern warhead developments include nuclear and chemical warheads, separating warheads, and multiple warheads. TBMs can also deliver a wide variety of conventional munitions. Some examples are high explosive, anti-radiation, fuel air explosive, dual purpose improved conventional munitions, improved conventional munitions, cluster munitions, electronic warhead and electromagnetic pulse fills, warhead buses (varied sub munitions), and precision navigating and homing warheads (such as IR homing).

Countermeasures

Countermeasures, including separating and maneuvering warheads, penaids, and other technical measures will further challenge the capability of theater missile defense assets to prevent strikes against priority targets.

Characteristics

These missiles employ a high-atmospheric or exo-atmospheric ballistic trajectory to reach the target. Most TBMs follow a set course that cannot be altered after the missile has burned its fuel. However, some have the capability for non-ballistic trajectories and precision maneuver. The majority of TBMs are able to launch from the ground or from naval assets. Missile ground launch platforms vary from fixed launchers, trailer launchers, mobile launch complexes (numerous vehicles), and transporter erector launchers.

Ballistic missiles have three categories of propellant for engines, which are liquid, hybrid, or solid, all of which affect the distance a missile can travel and the circular error probable (CEP), or accuracy. Accuracy ranges from approximately 300m to 500m CEP for older systems, to less than 50m CEP for some advanced systems.

Article of Interest

Updates to both launch platforms and missiles systems are allowing the threat to become increasingly mobile and accurate. The extended range of both missiles and their mobile platforms create a dangerous combination providing a potential adversary the ability to launch missiles and strike well beyond preconceived ranges.

Short-range ballistic missile (SRBM)	Medium-range ballistic missile (MRBM)
0-1,000km (0-621 miles) (Straight line distance from Fresno, CA to Portland, OR)	1,001-3,000km (621 to 1864 miles) (From New York, NY to Topeka, KS)

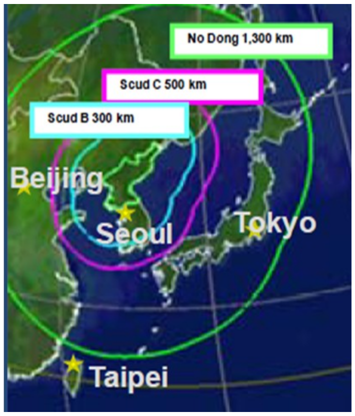
Table 1. Theater ballistic missile ranges.

Trends

The 2010 *Ballistic Missile Review* noted that in the upcoming decade, ballistic missiles and missile delivery systems will proliferate and evolve considerably. Technological advancement in the field of ballistic missiles has created an increase in flexibility, mobility, survivability, and reliability in both missiles and missile platforms.

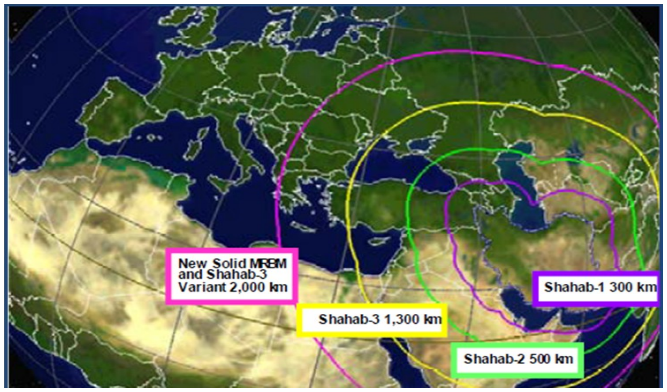
Potential threat countries such as Iran and North Korea are working towards extending missile ranges and are also in various stages of developing nuclear capabilities. The extended range not only changes the regional, but impacts strategic dynamics. As seen in picture 2, North Korea's TBM capability reaches South Korea and the No Dong 1 can potentially target Japan. The Iranian Shahab-3 has a range of 2,000km, well within the range of Israel and US forces in Saudi Arabia and Iraq.

Emerging missile technology is often viewed as a status symbol supporting countries like North Korea's and Iran's (*see picture 3*) belief that they should be viewed as powerbrokers. This is based in their concept that TBMs equate to symbols of national might with the ability to have regional and possibly strategic impact.



Picture 2: TBM ranges from North Korea.

The reasons for the rapid evolution and proliferation of TBM are considerable. Technological developments are increasing the range and accuracy of the missile systems, while platforms are becoming more agile, mobile, and harder to detect. There also remains the continuing threat that new technological developments in ballistic missile systems and nuclear capability by state actors could be acquired by non-state threat actors. TBMs will remain an ever increasing threat to overseas US interests, military forces, and allies.



Picture 3: TBM ranges from Iran.

YOUR Subject Matter Experts

Director, CTID DSN: 552
Mr Jon Cleaves FAX: 2397
jon.cleaves@us.army.mil 913.684.7975

OE & OPFOR Doctrine & Training Lit.
Senior Analyst CTID: Dr Don Madill 684.7926
donald.madill@us.army.mil

OPFOR Doctrine Team
SME: Mr Rick McCall 684.7960
rick.mccall@us.army.mil

Intelligence Specialist
SME: Mr Kris Lechowicz 684.7992
kristin.lechowicz@us.army.mil

Intelligence Specialist
SME: Mr Jerry England 684.7934
jerry.england1@us.army.mil

Worldwide Equipment Guide (WEG)
SME: Mr Tom Redman BAE 684.7925
tom.redman@us.army.mil

Threats Terrorism Team (T3)
SME: Mr Jon Moilanen L3 MPRI 684.7928
jon.moilanen@us.army.mil

Operational Environment Analysis
SME: Ms Penny Mellies 684.7920
penny.mellies@us.army.mil
SME: Ms Angela Wilkins L3MPRI 684.7929
angela.m.wilkins.ctr@us.army.mil

Training-Education-Leader Development
SME: Mr Walt Williams 684.7923
walter.williams@us.army.mil

National Training Center - OPFOR
SME: MAJ Terry Howard USAR 684.7939
terry.d.howard@us.army.mil

Joint Readiness Training Ctr - OPFOR
SME: Mr Marc Williams BAE 684.7943
james.marc.williams@us.army.mil

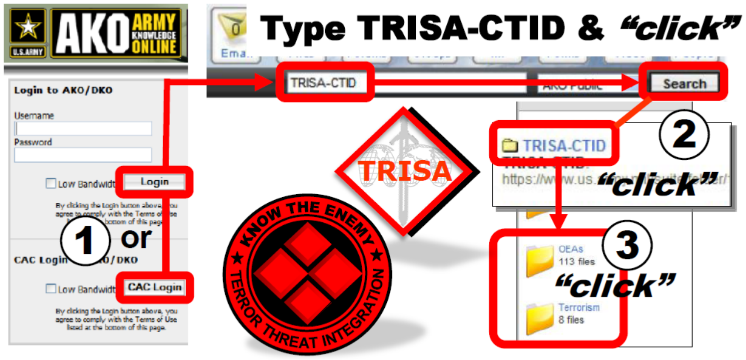
Joint Maneuver Readiness Ctr - OPFOR
SME: Mr Mike Spight BAE 684.7974
michael.spight@us.army.mil

Battle Command Training Program - OPFOR
SME: Mr Pat Madden S3 Inc 684.7997
patrick.madden@us.army.mil

Threats Website-Support Operations
SME: Mr Charles Christianson 684.7984
charles.christianson@us.army.mil

YOUR Easy e-Access Resource

AKO *Three "Click"* Drill-Down



By clicking the Login button above, you agree to comply with the Terms of Use listed at the bottom of this page.

Find Your Topic – Do Your Research

What We Do for YOU

- Determine OE Conditions
- Publish OE Threats in FSO
- Publish Army OPFOR Doctrine
- Assess Threat-Enemy & TTP
- Support Terrorism Awareness
- Publish OE Assessments

Director's Corner: *Looking Ahead --*

The hot new item is the Full Spectrum Training Environment (FSTE). Designed to provide the CTCs with a one-stop integrated shop for scenario development, I suspect its applications will be in demand for classroom instruction as well. If you're a trainer, this is going to impact your future one way or another and I would strongly recommend you take a good look at it, especially the events section. We welcome all your comments so we can make this the right product for you.

- Jon Cleaves