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 8 August 2011

Tools of the Trade: OPFOR and Related Publications

by Don Madill

AR 350-2, which establishes policies and procedures for the Army's Opposing Force (OPFOR) Program, defines ***opposing force*** as "a plausible, flexible military and/or paramilitary force representing a composite of varying capabilities of actual worldwide forces, used in lieu of a specific threat force for training and developing U.S. forces." As a training tool, the OPFOR must be a challenging, uncooperative sparring partner, capable of stressing any or all warfighting functions and mission-essential tasks of the U.S. force.

AR 350-2 designates the TRADOC G-2 as "the responsible official for the development, management, administration, integration, and approval functions of the OPFOR Program across the Army." That AR also tasked the TRADOC G-2 with producing the FM 7-100 series manuals and related materials to support the use of OPFOR and realistic and relevant operational environments (OEs) in training Army wide.

Within the TRADOC G-2 organization, TRISA-CTID now provides a comprehensive array of tools (see figure 1) for designing the appropriate OPFOR and other conditions for a training exercise. The Training Circular (TC) 7-100 series (formerly the FM 7-100 series) describes the doctrine, organizations, and equipment of such an OPFOR and how to combine it with other operational variables to portray the qualities of a full range of conditions appropriate to Army training environments.

TC 7-101, *Exercise Design*, is meant to be used in conjunction with the 7-100 series as well as the other publications listed in figure 1. These tools can be found on the TRISA-CTID AKO. Together, these tools outline an OPFOR than can cover the full spectrum of military and paramilitary capabilities against which the Army must train to ensure success in the types of OEs it can expect to encounter now and in the clearly foreseeable future.

NEWSLETTER DISTRIBUTION UNLIMITED

INSIDE THIS ISSUE:

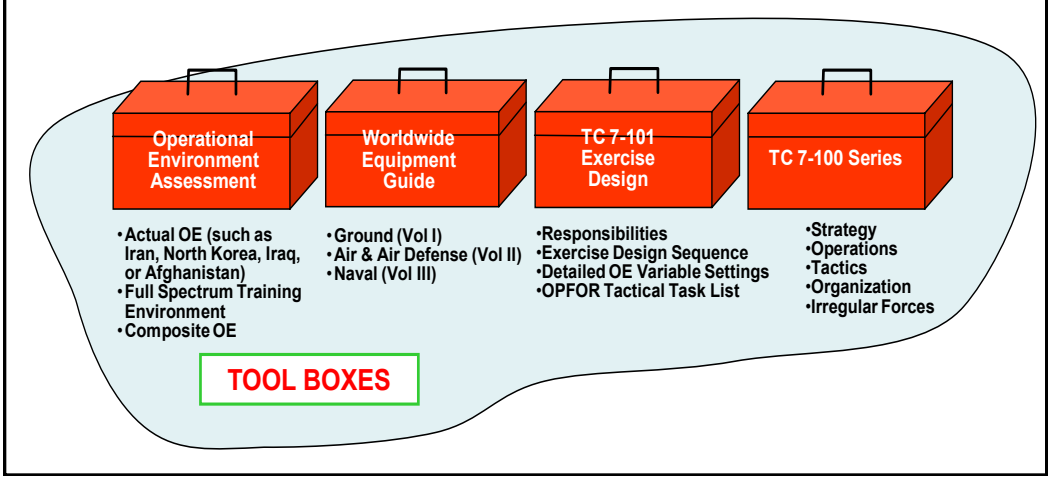


Figure 1: Exercise design tools

All TRISA-CTID products are on AKO.

TC 7-100 Series

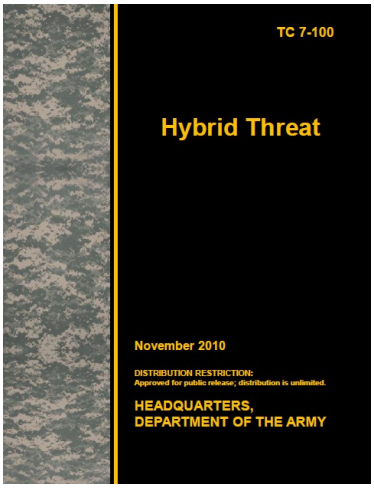
This series (formerly the FM 7-100 series) describes the OPFOR that reflects the characteristics of military and paramilitary forces that may be present in contemporary OEs. Like those real-world threats, the OPFOR will continue to present new and different challenges for U.S. forces. The most current versions of publications in this series are posted in the **Hybrid Threat Doctrine folder** on AKO.

A ***hybrid threat*** is the diverse and dynamic combination of regular forces, irregular forces, and/or criminal elements all unified to achieve mutually beneficial effects (TC 7-100 and FM 3-0). The Hybrid Threat (HT) for training is a realistic and relevant composite of actual hybrid threats. This composite constitutes the enemy, adversary, or threat whose military and/or paramilitary forces are represented as the OPFOR in training exercises. HT doctrine is presented in a series of TCs that describes the OPFOR for training U.S. Army commanders, staffs, and units. Together, the TC 7-100 series outlines an OPFOR that can cover the entire spectrum of military and paramilitary capabilities against which the Army must train to ensure success in any future conflict.

Applications for this series of publications include field training, training simulations, and classroom instruction throughout the Army. These publications apply to the Active Army, the Army National Guard (ARNG)/Army National Guard of the United States (ARNGUS), and the United States Army Reserve (USAR). All Army training venues should use an OPFOR based on these publications, except when mission rehearsal or contingency training requires maximum fidelity to a specific real-world threat. Even in the latter case, trainers should use appropriate parts of the OPFOR publications to fill information gaps in a manner consistent with what they do know about a specific threat.

OPFOR Doctrine Team

TC 7-100, *Hybrid Threat* (26 November 2010). This TC superseded FM 7-100, *Opposing Force Doctrinal Framework and Strategy* (1 May 2003) as the capstone of the 7-100 series.



The purpose of this TC is to describe hybrid threats and summarize the manner in which such threats may operationally organize to fight U.S. forces. It also outlines the strategy, operations, tactics, and organization of the HT that represents a composite of actual threat forces as an OPFOR for training exercises. In exercise design (see TC 7-101), the type(s) of forces making up the OPFOR will depend on the conditions determined to be appropriate for accomplishing training objectives. In some cases, the OPFOR may only need to reflect the nature and capabilities of a regular military force, an irregular force, or a criminal organization. However, in order to be representative of the types of threats the Army is likely to encounter in actual OEs, the OPFOR will often need to represent the capabilities of a hybrid threat.

FM 7-100.1, *Opposing Force Operations* (27 December 2004). By 30 January 2012, this FM will be converted into TC 7-100.1, with a new cover but no change in content.

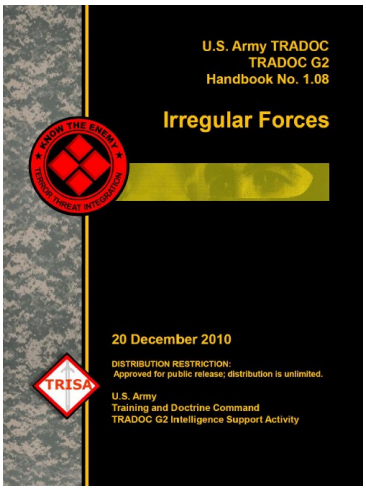
This FM describes the operational-level doctrine of the OPFOR that represents the Armed Forces of a fictitious state. This OPFOR is a representative composite of the capabilities of real-world forces. Although not specifically stated in the original FM, the regular military forces of this nation-state can also be part of the HT for training.

TC-7-100.2, *Opposing Force Tactics* (final draft 15 July 2011).

Currently posted on the TRISA-CTID AKO site is the final draft of individual chapters, minus the index. CTID is currently preparing the index and will submit the final electronic file to the Army Publishing Directorate (APD) before the end of August 2011. Final publication (electronic only) will probably occur 2 or 3 months later, depending on the APD workload.

The OPFOR tactics described in TC 7-100.2 are appropriate for use by an OPFOR that consists either entirely or partly of regular military forces. Some of these tactics, particularly those carried out by smaller organizations, can also be used by irregular forces or even by criminal elements. Even those tactics carried out primarily by regular military forces may involve other components of the HT acting in some capacity. When either acting alone or in concert with other components of the HT, irregular forces and/or criminal elements can also use other tactics, which are outlined in TC 7-100.3.

TC 7-100.3, *Irregular Opposing Force* (to be published in FY 12).



CTID is currently working on an author's draft of this TC. In the interim, refer to TRADOC G-2 Handbook 1.08, *Irregular Forces* (20 December 2010), available at https://www.us.army.mil/suite/doc/25984933,which reflects research on real-world irregular forces (insurgents and guerrillas) that provided the basis for the Irregular OPFOR for training.

OPFOR Doctrine Team

FM 7-100.4, *Opposing Force Organization Guide* (3 May 2007). By 30 January 2012, this FM will be converted into TC 7-100.4, with a new cover but no change in content.

This manual describes the baseline OPFOR organizations to be used in designing the appropriate OPFOR order of battle (OB) for U.S. Army training exercises. This manual differs from others in the series in that it includes both OPFOR doctrine regarding organization (administrative force structure and task-organized fighting force structure) and training-related issues from a U.S. viewpoint. This organization guide also differs from other FMs in the fact that it is linked to online organizational directories. TRISA-CTID maintains these directories and updates them, as necessary, to represent contemporary and emerging capabilities. In order to provide a comprehensive menu of the numerous types of OPFOR organizations in the detail required for the Army's live, virtual, and constructive training environments, these directories exceed the scope and size that can be accommodated within a traditional FM format. The directories contain over 10,000 pages detailing OPFOR organizations. From this menu, users can select and download just those parts needed to build the appropriate OPFOR for a particular exercise. Task-organizing an exercise OB also requires that users have the ability to use downloaded organizations in an interactive manner. For these reasons, it is necessary for this FM to be linked to organizational diagrams and associated equipment inventories made available in electronic form that users can download and manipulate as necessary in order to create task organizations capable of fighting in adaptive ways.

Once exercise planners determine the mission-essential tasks on which the U.S. unit is to be trained, they would begin determining the appropriate type and size of OPFOR unit(s) capable of performing the necessary OPFOR countertasks. The type of OPFOR unit is determined by the type of capability required for each OPFOR countertask. The size of the OPFOR organization is determined by the type of capability required and the size of the U.S. unit(s) being trained.

At this point, exercise planners review the OPFOR administrative force structure (AFS) organizational directories, which provide example equipment plus personnel types and the numbers of each type typically found in specific organizations. The AFS is to be used as the basis for OPFOR organization in all Army training exercises, except real-world-oriented mission rehearsal exercises (MRXs). Within the AFS, tactical-level commands have standard organizational structures. The purpose of the AFS is to give trainers and exercise planners a general idea of what an OPFOR structure should look like. A complete list of AFS organizational directories can be found at the TRISA-CTID AKO site under FM 7-100.4, in the subfolder Admin Force Structure, which is broken down into four volumes:

- Volume I, Divisions (Mechanized Infantry, Motorized Infantry, and Tank Division)
- Volume II, Nondivisional Units (Echelons above Division)
- Volume III, Paramilitary and Nonmilitary Organizations (Insurgent, Guerrilla, Unarmed Combatants, and Noncombatants)
- Volume IV, Other (Combatants, Noncombatants, and Other Nondivisional Units)

Note. The AFS organizational directories are online files linked to FM 7-100.4. FM 7-100.4 provides detailed step-by-step instructions on how to construct a task organization and how to select equipment options.

From the AFS menu, exercise planners determine which standard OPFOR unit(s) most closely match the type and size of units required for performing OPFOR countertasks. In most cases, the organizations found in the AFS will require task-organizing in order to construct an OPFOR OB appropriate for the exercise.

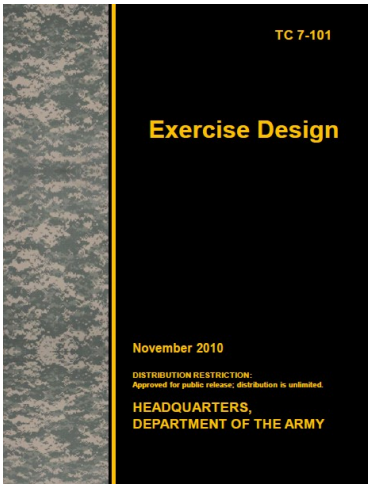
Graphics Library

The graphics library is a compendium of PowerPoint objects used in the creation of graphics in TC 7-100.2. It is posted on the TRISA-CTID AKO cite, in the Hybrid Threat Doctrine folder, for the convenience of readers who need to create their own graphics for a particular exercise event.

OPFOR Doctrine Team

RELATED PUBLICATIONS

TC 7-101, *Exercise Design* (26 November 2010), also found in the Hybrid Threat Doctrine folder.

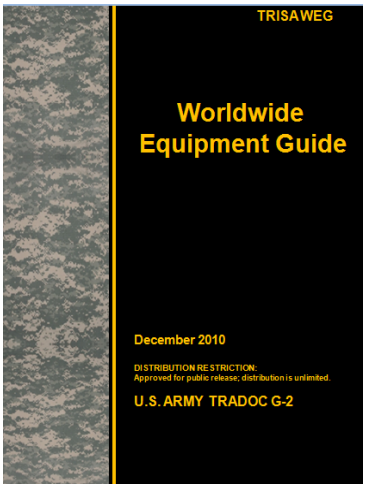


This TC is a planning and design tool that significantly enhances an exercise planner's ability to produce an OE that achieves desired unit training objectives while fielding a challenging OPFOR consistent with Hybrid Threat OPFOR doctrine as described in the TC 7-100 series. By using the political, military, economic, social, information, infrastructure, physical environment, and time (PMESII-PT) operational variables and incorporating them into every aspect of the scenario, the training unit will experience a realistic and challenging exercise every time. The bottom line is that this TC gives planners the tools to provide the correct exercise conditions for the training unit's training objectives, resulting in effective training.

The processes described in this TC are applicable to any number of exercise venues to include field training exercises, command post exercises, and simulations. They can also be used in the development of MRXs. The operational variables and the settings for their subvariables and sub-subvariables can be used to develop OEs for exercises or for describing actual OEs portrayed in MRXs.

For an MRX, the characteristics of the OE would be based on an operational environment assessment (OEA) of the actual OE in the area of planned deployment. For full spectrum exercises at Army combat training centers (CTCs), TRISA-CTID has developed the Full Spectrum Training Environment (FSTE: see next page). For exercises that do not require fidelity to an actual OE or the use of the FSTE, exercise planners can modify an existing OEA (for an actual operation or for an existing training scenario) or design their own composite OE by selecting the appropriate subvariable or sub-subvariable settings.

Worldwide Equipment Guide (WEG) Folder



During the task-organizing process, adjustments in equipment may be necessary in order to modify the strength and capability of the OPFOR unit. If a particular piece of equipment shown in the AFS organizational directories is not appropriate for a specific scenario, exercise planners may substitute another system according to the guidelines in the WEG. The WEG is organized into online directories consisting of three volumes:

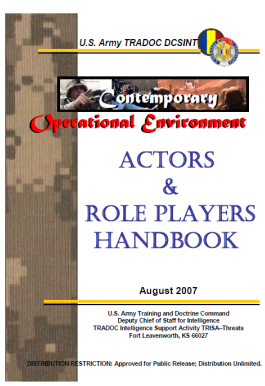
- Volume I, Ground Systems
- Volume II, Airspace and Air Defense
- Volume III, Naval and Littoral Systems

The WEG is maintained and continuously updated, as necessary, by TRISA-CTID. It is important to note that even the baseline OPFOR organizations are subject to change over time. The equipment found in those organizations can also change. Therefore, planners should always consult the online AFS directories and the WEG for the latest, most up-to-date versions of organizational and equipment data.

The WEG contains equipment data, tier tables, and substitution matrices for the various categories of equipment found in OPFOR organizations. Exercise planners should exercise caution in modifying equipment holdings, since this impacts on an OPFOR unit's organizational integrity and combat capabilities.

OPFOR Doctrine Team

COE Actors & Role Players Handbook (August 2007).



This handbook is a supplement to the FM/TC 7-100 series of OPFOR documents. It is an unclassified primer and reference guide for trainers and role-players. It supports operational missions, institutional training, initial entry training, and professional military education for U.S. military forces. The integration of the various actors in the training environment improves the readiness of U.S. military forces. As a living document, this handbook will be updated as necessary to ensure it remains a current and relevant resource.

This handbook exists primarily for U.S. military forces. However, other applicable groups include interagency, intergovernmental, civilian contractor, nongovernmental, private voluntary, and humanitarian relief organizations. Compiled from open source material, this handbook promotes a perspective of the various actors existing within a real-world environment.

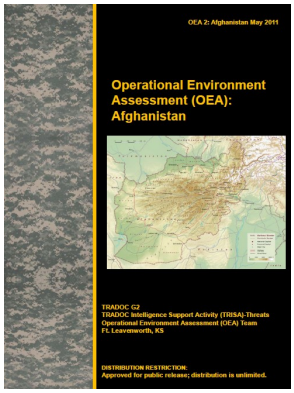
Full Spectrum Training Environment (FSTE) (Feb 2011).

The purpose of this FSTE document is to provide the U.S. Army training community with a detailed description of the conditions of the OE in the South Caucasus region; specifically the fictitious countries of Ariana, Atropia, Gorgas, and Minaria. The country of Donovia will be added in the December 2011 version. It presents trainers with a tool to assist in the construction of scenarios for specific training events, but does not provide a complete scenario. The FSTE offers discussions of OE conditions through the PMESII-PT variables. This FSTE applies to all U.S. Army units (Active Army, Army National Guard, and Army Reserve) that participate in an Army or joint training exercise.

This FSTE will incorporate some real-world data and some artificial data in order to set the conditions for a wide range of training events, to include full spectrum operations, to occur. Section 2: Variables of the OE provides the bulk of these details. The variable discussion explores the complex and ever-changing combination of conditions, circumstances, and influences that could affect military operations within a given OE. The PMESII-PT variables elicit understanding of each country's independent, dynamic, and multidimensional environment. By defining these variables' makeup and interoperability as they relate to a specific country, a picture of the environment's nature and characteristics emerges.

Operational Environment Assessment (OEA) Folder

The purpose of an OEA is twofold. First, an assessment provides a detailed description and analysis of an OE; second, it presents a methodology for the application of the OE framework to any real-world OE. The OEA framework is an analytical construct developed to explore the complex and ever-changing combination of conditions, circumstances, and influences that affect real-world military operations within a given OE. The framework provides a method to describe the conditions of military operations and capabilities, and is applicable across leader development, education, and training environments as well as real-world contingency planning or predeployment exercises. OEAs are intended to support the Army training community in the development and execution of MRXs, training exercises/events, and general cultural awareness training.



Each OEA discusses the PMESII-PT variables and their related effects, as well as exploring potential trends across the specific OE being analyzed. An OEA helps define the OE's nature and characteristics and seeks to present an understanding of the variables and their impact across the OE. The analysis presented in each OEA is based upon open-source research, and all information contained therein is unclassified. Products currently available in the OEA folder include OEAs for Afghanistan, Azerbaijan, the Horn of Africa, Iran, Iraq, North Korea, and Pakistan.

OEA Team

Motorcycle Improvised Explosive Devices

by H. David Pendleton

Terrorists and other radical groups do not confine their use of improvised explosive devices (IEDs) delivered by a motorcycle to a particular part of the world, one particular type of non-four wheeled vehicle, or to any one particular delivery method. Instead, the perpetrators use motorcycles and other non-four wheeled vehicles to approach targets where a truck or car bomb might not reach. While the news often highlights motorcycle IED explosions that occur in the Middle East or Central Asia, such IED attacks took place in at least ten separate countries on four different continents over the past five years. The OEA Team threat report, ***Motorcycle IEDs*** (August 2011), describes in detail motorcycle IED attacks from 2007 through 2011 around the world.

Motorcycle IED attacks possess several advantages over the use of truck or car bombs with few disadvantages for the individual or group that plants the bomb. First, the bomber needs significantly less explosives and shrapnel to make a motorcycle bomb than a car or truck bomb. The motorcycle contains much less room for the explosive charge and can contain less shrapnel since the IED must fit into the motorcycle itself (such as the gas tank), a box or parcel strapped to the motorcycle, or in the motorcycle's own storage container. The bomb maker needs to obtain fewer explosives or purchase smaller quantities of the bomb precursors so the individual or group reduces the likelihood of detection by law enforcement forces (LEF) or raising the suspicion of business owners.

Second, the motorcycle's smaller size makes it easier to maneuver in crowded cities where many bombers attack with IEDs. The motorcycle can move around stalled traffic without raising suspicion since motorcycles do this continuously in many urban centers worldwide. Due to its maneuverability, the motorcycle can also often move around many of the defensive mechanisms set up to stop car or truck bombers.

In most of the world's busy urban centers, workers often use motorcycles and motor scooters for their daily commute which enhances the motorcycle IED bomber's ability to blend in with his or her urban surroundings. In many cities, motorcycles parked in non-standard locations remain the norm and not the exception. One additional motorcycle in areas where motorcycles often park usually raises no suspicions from either LEF or civilians. Thus, the motorcycle IED bomber can often park his motorcycle next to the target without attracting attention. Many businesses in large urban areas receive deliveries by motorcycles, and big boxes on the back of a two-wheeled vehicle are a frequent sight in large cities.

Terrorists can use a motorcycle in various attack methods and two-wheeled vehicles serve as an excellent getaway vehicle. Terrorists can park their motorcycle next to or near their target and set the IED off by a timer or remote control, often in the form of a cell phone call. Other methods include suicide bombers who ram their motorcycle into their intended target, use motorcycle sell and swap sites to deliver a bomb to the target area often in busy downtown plaza areas, or even get off and go on foot to toss the bomb at their target. In the latter method, the bomber can escape on his motorcycle, and in the other attack methods, an accomplice on another motorcycle can pick up the bomber so he can make his escape.

The negative aspects of motorcycle IEDs do not outweigh the positives for the terrorists who wish to set off a homemade bomb. First, even though motorcycle IEDs may carry fewer explosives than larger car or truck bombs, the motorcycle bombs can still create high casualty counts and cause much structural damage. In a motorcycle attack in February 2010 in Karbala, Iraq, a parked motorcycle IED killed over 20 people and injured 108. In another motorcycle IED attack in Yakaghund, Pakistan in July 2010, the bomb created a five-foot deep crater and damaged over seventy shops, two hotels, six houses, and one prison wall. While motorcycle IEDs often cause less death and damage than larger truck or car bombs, the psychological effects can still reverberate just as much.

OEA Team

Another negative for the perpetrators in their use of motorcycle IEDs comes from the inability to completely direct the bomb's explosion in the intended direction. Due to the limited spaces to place explosives within the motorcycle itself or in a box attached to the motorcycle, an explosion within a confined space goes in the direction of the weakest barrier. A motorcycle bomb will often explode in the direction it wants instead of the direction a bomb maker, especially those without much experience, wants the bomb to go.

Lastly and likely the largest negative for the bombers is that the motorcycle offers little protection for the bomber before, during, or after an attack. If detected, LEF may shoot the bomber before he reaches his target or during his attempted escape after the attack. Unless the motorcycle IED bomber wants to become a martyr to his cause, the lack of protection remains an especially hazardous limitation to the rider.

Motorcycle IED attacks do not limit themselves to only the use of two-wheeled vehicles, but include the use of three-wheeled vehicles (rickshaws) and even bicycles. In Helmand Province, Afghanistan in March 2010, a rickshaw loaded with explosives attempted to ram an Afghan National Army (ANA) convoy while it crossed a bridge. The three-wheeled vehicle missed the convoy and went over the embankment where it killed ten civilians and injured another seven people, all native Afghan picnickers celebrating the Zoastrian New Year. In March 2008, in New York City, a bicyclist with a backpack dismounted and set off a bomb at the door of the US Army recruiting station in Times Square before he made his escape on the bicycle.

Some motorcycle IED bombers target specific individuals or groups as seen in attacks in Batasanga Pambansa, Philippines in 2007; on a nuclear scientist in Tehran, Iran in early 2010; or on a group of tribal elders in Yakaghund, Pakistan in 2010. In November 2007, Muslim rebels targeted a Philippine congressman for revenge as their former colleague then supported military action against the guerrillas. In Iran in January 2010, unknown people assassinated a physics professor as he left his home for work. In Pakistan in July of the same year, Tehrik-e Taliban Pakistan (TTP) rebels claimed credit for an attack against tribal elders friendly to the Pakistani government who wanted to raise a *lashgar* (tribal force) to fight the Taliban.

Other motorcycle IED attackers do not possess specific targets, but just want to create as much death, destruction, and panic as possible. In Karachi, Pakistan in January 2008, a motorcycle bomb exploded outside a textile factory where it killed 11 people and injured between 30 and 60 more, most poor laborers. In Jolo, Philippines in July 2009, a motorcycle bomb exploded just after mass let out in a nearby Catholic church; six people were killed and 30 were wounded. Authorities could not discover any specific targets in either attack.

Sometimes the motorcycle IED attacks involve religious issues, especially between Sunni and Shi'ite Muslims. In Karbala, Iraq in February 2010, a motorcycle bomb killed over 20 Shi'ite pilgrims on the way to a festival and injured another 108. In Karachi, Pakistan in the same month, a 20-pound bomb planted on a motorcycle killed 12 and wounded 40 Shi'ite mourners headed to participate in a religious procession. Sunni extremists appear as the likely culprit in both attacks.

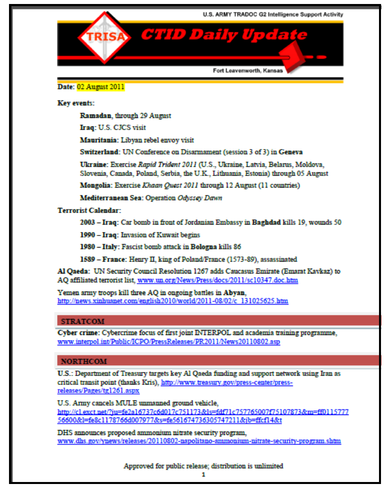
Despite the knowledge that terrorists often use non-four wheeled vehicles to make IED attacks, the motorcycle IED will likely remain a major terrorist tactic in the Middle East and throughout the world. Reports indicate that in 2008, Iran trained hundreds of Shi'ite insurgents known as "Special Groups" to construct bombs and equipped them with motorcycles to carry the IEDs for use in Iraq. So far, it appears that these Special Groups did not significantly elevate the number of IED attacks over the past three years in Iraq, but the potential for increased motorcycle IEDs still remains. Terrorist and other groups around the world will continue to use motorcycle IEDs to carry out their bomb attacks due to the two-wheeled vehicle's maneuverability, its omnipresence in most large cities, and the smaller logistics required to carry out an attack against any group they wish to target.

Training and Education Team

Daily Updates and How to Use Them

by Marc Williams

What is the TRISA CTID *Daily Update*? It is a listing of articles and papers which focus on threats (manmade and natural) and emerging capabilities of interest to combat Soldiers, intelligence operators, and homeland security specialists. It differs from the Early Bird and Intellist in that it is more tightly focused, and yet is broader than most STRATFOR products. Originally developed as a tool for the TRISA combat training center support team, it grew in popularity and people from multiple agencies and units began requesting a subscription. These articles include threats such as terrorism, revolutions, assassinations, regional conflicts, drug/human trafficking, pandemic diseases, deadly weather, and large earthquakes (6.0 or higher). Also included are articles concerning new technologies with military or law enforcement applications and changes in regional or strategic alliances.



U.S. ARMY TRADOC G2 Intelligence Support Activity

TRISA **CTID Daily Update**

Fort Leavenworth, Kansas

Date: 02 August 2011

Key events:

Ramadan, through 29 August

Iraq: U.S. CJCS visit

Mauritania: Libyan rebel envoy visit

Switzerland: UN Conference on Disarmament (session 3 of 3) in **Geneva**

Ukraine: Exercise *Rapid Trident 2011* (U.S., Ukraine, Latvia, Belarus, Moldova, Slovenia, Canada, Poland, Serbia, the U.K., Lithuania, Estonia) through 05 August

Mongolia: Exercise *Khaan Quest 2011* through 12 August (11 countries)

Mediterranean Sea: Operation *Odyssey Dawn*

Terrorist Calendar:

2003 – Iraq: Car bomb in front of Jordanian Embassy in **Baghdad** kills 19, wounds 50

1990 – Iraq: Invasion of Kuwait begins

1980 – Italy: Fascist bomb attack in **Bologna** kills 86

1589 – France: Henry II, king of Poland/France (1573-89), assassinated

Al Qaeda: UN Security Council Resolution 1267 adds Caucasus Emirate (Emarat Kavkaz) to AQ affiliated terrorist list, www.un.org/News/Press/docs/2011/sc10347.doc.htm

Yemen army troops kill three AQ in ongoing battles in **Abyan**, http://news.xinhuanet.com/english2010/world/2011-08/02/c_131025625.htm

STRATCOM

Cyber crime: Cybercrime focus of first joint INTERPOL and academia training programme, www.interpol.int/Public/ICPO/PressReleases/PR2011/News20110802.asp

NORTHCOM

U.S.: Department of Treasury targets key Al Qaeda funding and support network using Iran as critical transit point (thanks Kris), http://www.treasury.gov/press-center/press-releases/Pages/tg1261.aspx

U.S. Army cancels MULE unmanned ground vehicle, http://cl.exct.net/?ju=fe2a16737c6d017c751173&ls=fdf71c757765007f75107873&m=ff011577756600&l=fe8c1178766d007977&s=fe561674736305747211&jb=ffcf14&t

DHS announces proposed ammonium nitrate security program, www.dhs.gov/ynews/releases/20110802-napolitano-ammonium-nitrate-security-program.shtm

Approved for public release; distribution is unlimited

1

Information contained in the *Daily Update* comes from multiple sources, including journalistic websites, wire services, government websites, think-tanks, jihadi forums, and single-interest blogs. Due to multiple viewpoints and different times of reports, the articles may actually contradict each other. The *Daily Update* tends to reinforce the military maxim, “the first report is always wrong.”

Criteria for article inclusion are credible open-sources with no security markings. All updates are marked as “Approved for public release; distribution is unlimited.” CTID will not use FOUO or Law Enforcement Sensitive information. This was a conscious decision to prevent spillage and to allow ease of use. Also, we will not use opinion/editorial pieces and avoid the use of Wikipedia as that source is based on user input and the information is not always vetted for accuracy. Simple criminal activity is not included unless it impacts U.S. national security, such as transnational criminal organizations (TCO) and drug trafficking organizations (DTO). While there are many good articles available, the question to be answered is, does this pose a potential threat to the U.S., its citizens, or its allies?

The articles are organized beginning with major diplomatic and military events, a brief rundown of the terrorist events of that particular day in history, and a specific header for al-Qaeda and its affiliates. The major headings are grouped by combatant command (COCOM) for ease of use and quick scanning. People focused on one COCOM can go there quickly, see what is happening, extract what they need, and discard the rest. Further, since it is all open sources, disposal is painless.

The final page is a “terrorist of the day” (the unofficial name is less than flattering) drawn from U.S. and international databases. Domestic sources include the FBI, U.S. Marshals Service, the Drug Enforcement Agency, Department of Homeland Security, and Department of Treasury. International sources include INTERPOL and national military and law enforcement websites. When a photo or diagram is to be used, nothing is used that is copyrighted. All photos/diagrams are from government sources such as Defense Video and Imagery Distribution System (DVIDS), Department of Defense, Department of Transportation, Department of Justice, and Department of State. When possible, the source and photographer will be cited.

The *Daily Updates* are available through direct e-mailings, or can be downloaded from the Army Professional Forums and Army Knowledge Online (AKO). The location of the Army Professional Forums is in the Warrant Officer Net within the Observations, Insights, and Lessons portion. The web address is https://forums.army.mil/secure/communitybrowser.aspx?id=1337468&lang=en-US and requires either CAC card or AKO credentials. The AKO web address is https://www.us.army.mil/suite/files/25567294.

Training and Education Team

The real "so what" of the *Daily Update* is how to apply the information it contains. Below are some examples:

- Comparison of real world activities to those portrayed in training at home station, schools, and centers. (Answers the challenge of "they wouldn't do that"). Iraq and Afghanistan trends can also be gleaned from open source reports and applied to MRE/MRX training.

- Scenario development, including enemy tactics, techniques, and procedures (TTP) and equipment capabilities. (Answers the challenge of "they wouldn't have that thing/capability").

- Tracking of regional situations and trends. These include USNORTHCOM's interest in Arctic issues and transnational criminal organizations; USPACOM's interest in activities in the South China Sea, pirate activity in the Indian Ocean, and radicalization in south Asia; and USSOUTHCOM's interest in DTOs and revolutionaries.

- Assistance with research. The information in the Daily Update can be used to support research for papers and monographs. It can also be used to track the activities of regional entities such as Gulf Coalition Council (GCC), the African Union (AU), the Shanghai Cooperation Organization (SCO), the Association of Southeast Asia Nations (ASEAN), the North Atlantic Treaty Organization (NATO), and the Brazil-Russia-India-China-South Africa (BRICS) partnership.

- Tracking specific capabilities. Analysts and operators will find new information on unmanned aerial systems, unmanned vehicles, unmanned surface vessels, new aircraft, new ships, new radar, antiaircraft, and missile systems. The *Daily Update* also includes DTO/TCO use of ultralight aircraft and development and implementation of submarines and submersibles to move illegal drugs.

For people needing a quick read, the *Daily Update* provides a snapshot of world events with a focus on threats, both manmade and natural, and new capabilities among the world's militaries. For people needing to track trends of specific regions, the *Daily Update* is organized by COCOM for quick reference and provides unclassified access with no fears of intelligence spillage. Further the *Daily Update* assists trainers with scenario development or refinement to capture real world capabilities and TTP.

Feedback from users is critical to ensure we are remaining relevant and looking at areas of interest. Recommendations for improvement are always appreciated. To be added to the direct mailing list, or to offer suggestions for improvement, simply contact the author at james.marc.williams@conus.army.mil.

OPFOR TTP

Defense of a Complex Battle Position

by Jon Moilanen

This example of a complex battle position (CBP) illustrates the defensive action by an opposing force (OPFOR) guerrilla platoon. The tactical situation is a guerrilla platoon that occupies a CBP and is prepared to defend.

Situational Conditions

An increased tempo of enemy company-size operations in the neighboring valleys resulted in several engagements with significant combat losses in OPFOR guerrilla manning, and blocked freedom of movement to and from safe havens across the international border.

This platoon is one of several platoon-size elements that has been directed by its guerrilla company headquarters to disperse as platoons into rural mountainous terrain in order to refit for future combat operations and train recruits that were recently coerced from villages in the valley farmlands. The platoon leader is not to conduct any local offensive actions without permission of the company commander. Communication between the platoon and its company headquarters is only by courier-messenger. In case of CBP discovery by the enemy, the platoon leader will notify the company headquarters via long-range cordless telephone.

The purpose of an OPFOR CBP must be understood as different from a strongpoint as described in U.S. military tactical doctrine. A ***complex battle position*** is a defensive location designed to employ a combination of complex terrain; camouflage, concealment, cover, and deception (C3D); and engineer effort to protect the unit(s) within them from detection and attack while denying their seizure and occupation by the enemy (TC 7-100.2).

A CBP has the following typical characteristics that distinguishes it from an OPFOR simple battle position (SBP):

- Limited avenues of approach. CBPs are not necessarily tied to an avenue of approach.
- Any existing avenues of approach are easily observable by the defender.
- 360-degree fire coverage and protection from attack. This may be due to the nature of surrounding terrain or engineer activity such as tunneling.
- Engineer effort prioritizing C3D measures; limited countermobility effort that might reveal the CBP location.
- Large logistics caches.
- Sanctuary from which to launch local attacks.

Planning and Preparing the Defense of a CBP

CBPs are designed to protect the units within them from detection and attack while denying their seizure and occupation by the enemy. Commanders occupying CBPs intend to preserve their combat power until conditions permit offensive action. The platoon leader occupies an isolated canyon-ravine far from any dirt roads and accessible on the ground only by trails that generally rise rapidly in elevation from canyon floors. Previous reconnaissance of this ravine confirmed a fresh water source from a seasonal spring. The commander develops his defensive plan on most likely and possible enemy avenues of approach into his defensive position from the east and northeast, and accounts for a possible enemy landing zone (LZ) in the vicinity.

OPFOR TTP

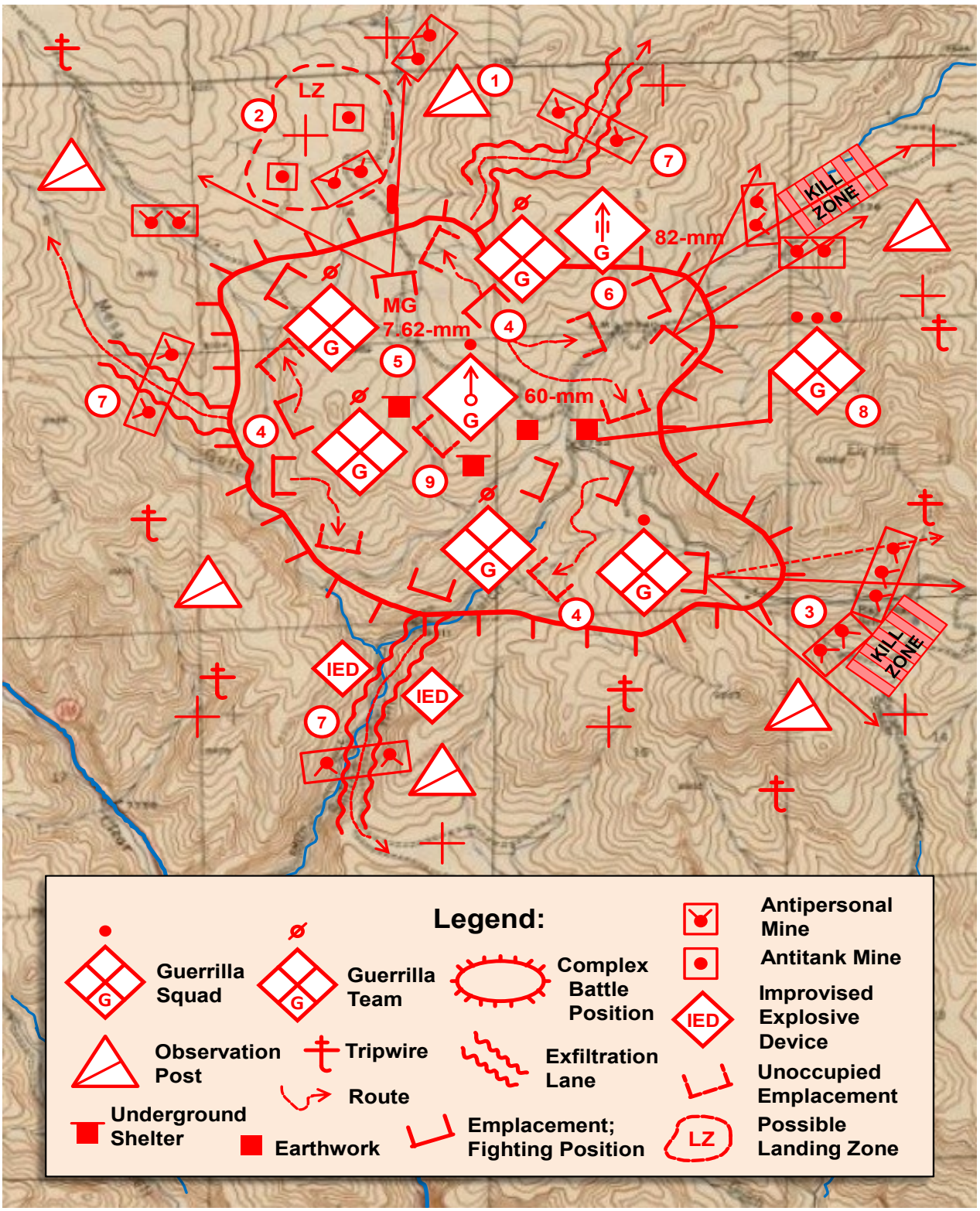
Terrain Appreciation

The platoon remains under strength from its normal manning of about 50 guerrillas, even with eleven coerced recruits. Several of the OPFOR junior noncommissioned officers and guerrillas were killed or captured in recent fighting. The platoon leader has only one PKM remaining in his machinegun section, but does have a 60-mm mortar and 82-mm recoilless gun that were allocated from the company before the company's platoons dispersed into the mountains.

The CBP allows the OPFOR to improve its combat power undetected until conditions permit offensive action. The platoon makes maximum use of C3D, and uses restrictive terrain and engineer countermobility efforts to deny the enemy the ability to identify and attack the position.

Depending on conditions, the platoon leader may order a withdrawal prior to contact with the enemy in order to preserve his unit's combat power. In the case of an attack on the CBP, the platoon will engage only as long as they believe they can defeat the enemy. If the OPFOR in a CBP is about to be decisively overmatched, the platoon leader will order a withdrawal under pressure on designated exfiltration routes.

OPFOR TTP



Guerrilla platoon defense of a CBP

OPFOR TTP

Functional Organization of Elements to Defend a CBP

The platoon leader explains his defensive plan to his platoon using standard OPFOR doctrinal terms and functional purpose. His defense accounts for the platoon's under-strength manning and available weapons. The CBP is organized to defend as follows:

Disruption Element

The disruption element of a CBP is primarily concerned with providing early warning to the defending force. C3D measures are critical to the success of a CBP because the platoon wants to avoid enemy contact.

A series of two-man observation posts (OPs) monitor air and ground routes into the CBP area. Trip wires and antipersonnel (AP) mines are under direct observation by OPs that can call for indirect fires. The OP ① nearest the possible landing zone (LZ) ② emplaces AP mines and antitank (AT) mines as part of an antilanding ambush and defense. Each AT mine has a small camouflage parachute attached to its tilt rod. Previous ambushes have been successful when the prop wash of descending helicopters filled parachutes, bent the tilt rod, and detonated the AT mine. An expedient of rocks and other natural debris covering the AT mines enhances shaped-charge effects.

Main Defense Element

The main defense element of the CBP consists of two- to three-man fighting positions with assigned sectors of fire. The terrain does not allow for interlocking fires along certain portions of the CBP perimeter. However, fighting positions are sited for interlocking fires within teams. Shifting to alternate or supplemental fighting positions within the CBP is on order of the platoon leader. The battle zone is the area in and surrounding the CBP that the defending force can influence with its direct fires.

Fighting positions in a CBP

Two- to three-man fighting positions are created with hand tools and manual labor. Based on the rock core of the ravine and mountainsides, positions have overhead cover and natural concealment. Light discipline is strictly enforced and daytime movement within the CBP is held to a minimum. Communication within the CBP is by messenger or wire telephone.

A squad is assigned the most likely enemy avenue of approach from the east ③ and has the initial priority call for fire from the 60-mm mortar. Two- to three-man guerrilla teams ④ will shift between fighting positions, on order, to reinforce the platoon defense.

OPFOR TTP

The PKM machinegun ⑤ is assigned a primary sector of fire that covers the possible LZ and trails approaching the CBP for the north and northwest. The OPs will conduct calls for fire and assist in adjusting fires for the 60-mm mortar squad.

The 82-mm recoilless gun ⑥ is placed for effective direct fires down a terrain corridor and a likely enemy avenue of approach from the northeast. Prioritized indirect fires will add to kill zone effectiveness. One OP will remain in position to adjust fires and report any approaching follow-on forces. Guerrillas manning OPs at the time of an attack may be directed to remain in place, or may be recalled to fighting positions inside the CBP.

The platoon leader plans to defeat an attacking enemy force in the battle zone, or delay the enemy while the platoon withdraws under pressure. Exfiltration routes from the CBP have been marked, and guides have been assigned for passage through IEDs and AP mine lanes ⑦ that will be closed after guerrillas have passed through the lane. Each guerrilla knows the rally points that are quite distant from the CBP.

Reserve Element

A reserve element provides for tactical flexibility. In this case, the platoon leader has placed squads and teams throughout the CBP without a dedicated reserve. He has rehearsed contingencies of how he will reposition designated teams, on order, to counter penetrations of the CBP, defend against an enemy heliborne landing, or assist platoon elements to break contact and exfiltrate from the immediate area.

Support Element

The platoon leader locates his fighting position and command post ⑧ where he can best control the defense. He chooses a position between the defending squads near the two most likely enemy approaches in the east and northeast. He is also able to directly influence indirect fires from this site. His acting platoon sergeant locates with the northern squad and prioritizes his supervision to defense of the northwest. The platoon leader accepts a degree of risk to the south and southwest with his third squad, but has provided for early warning and reinforced limited AP mines with improvised explosive devices for defense, and if necessary, to delay pursuing enemy if this exfiltration lane is used by the platoon.

The 60-mm mortar squad locates in a small earthwork that allows for 360-degree coverage of the CBP battle zone. Natural foliage placed on a light wood frame provides overhead concealment, and can be removed immediately for fire missions. Target reference points have been plotted. Indirect fires will disrupt attackers along avenues of approach and in LZs, support the defeat of attackers in the battle zone, and assist in covering the withdrawal of guerrillas from the CBP.

Passive air defense is in effect for the CBP. No man-portable air defense system is with the platoon. Massed small-arms fire is the available air defense in case of an attempted heliborne landing or other type of aerial attack on the CBP. Firing on any aircraft is only on the order of the platoon leader.

Supplies and equipment are located in a group of underground shelters ⑨ near the center of the CBP, which in some cases are little more than crevices reinforced with hastily constructed stone walls and scrub trees. Food is prepared in one of the underground shelters near the center of the CBP. Limited supplies were brought with the platoon when occupying the CBP, but pack mules and porters are planned to arrive with additional weapons, ammunition, and basic medical supplies in the coming week. The platoon depends on periodic resupply of food from a clandestine support network from the neighboring valley villages. A large supply cache does not exist in the CBP.

OPFOR TTP

The CBP relies on its own manual resources to improve its C3D. Actions include concealing survivability positions such as entrenchments, mortar pit, entrances to underground shelters, and two-man fighting positions. AP and AT mines and trip wires are concealed from observation. These obstacles are generally intended as protective measures to turn an attacker away from a vulnerable flank, turn an attacker into a kill zone, or protect an exfiltration route.

The platoon leader minimizes his information warfare actions. He maintains a low unit profile while he refits for future combat. Through trusted contacts in the valley villages, he downplays the existence or significance of his CBP, and plants misinformation that directs enemy attention far to the west. Concurrently, the platoon leader uses his contacts to ensure that the villagers receive a recurring message that the guerrillas are intent on fighting and eventually preventing the extortion and presence of corrupt local government officials and internal security forces. The platoon leader uses trusted contacts to remind village elders that any attack on the CBP places the young men and boys recruited from the villages in grave danger.

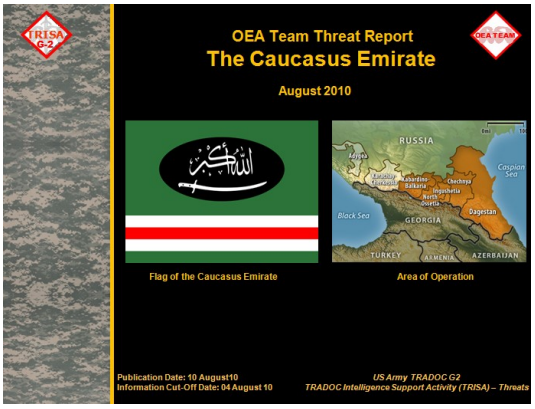
Executing Defense of a CBP

Security and counterreconnaissance will use passive measures unless attack is imminent. Direct and indirect fires will be initiated on order of the platoon leader. The guerrilla platoon will attempt to defeat attacking forces in the battle zone. Should the platoon leader determine that he lacks the capacity to defeat an attack, he may direct a sequence of withdrawals before becoming decisively engaged. If an enemy attack proceeds more quickly than anticipated and an orderly withdrawal is not practical, the platoon leader may direct individual two-man exfiltrations while he conducts a delay with designated elements of his platoon.

Note. For more OPFOR doctrinal information and tactical illustrations, see chapter 4, **Defense of a Complex Battle Position** of TC 7-100.2 *Opposing Force Tactics* (2011).

Product of Interest

On 28 July 2011, the United Nations in accordance with two resolutions,1267 (1999) and 1989 (2011), approved the addition of the Caucasus Emirate group to its “sanctions list of individuals and entities subject to the assets freeze, travel ban, and arms embargo” based on the group’s relationship to al-Qaeda. The UN press release stated that the group is mainly active in Russia, Afghanistan, and Pakistan. For more information on the Caucasus Emirate see the OEA Threat Report The Caucasus Emirate (August 2010) for detail on the group’s origins, leadership structure, and commonly used TTP.



Doctrine Team

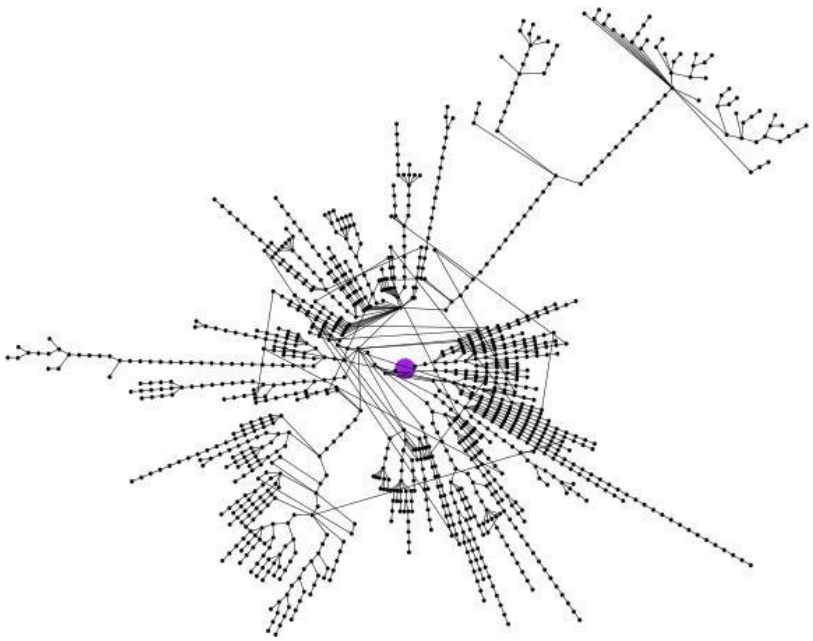
Information Attack

by Jerry England

Information attack (IA) is a critical element of OPFOR information warfare (INFOWAR). This type of action focuses on the intentional disruption or distortion of information in a manner that supports accomplishment of the mission.

The Stuxnet attack is an example of a targeted information attack that is believed to have achieved a significant strategic affect. Described as a virtual guided missile, Stuxnet is a cyber worm designed to attack a system that meets a very specific criteria, namely Supervisory Control Access Data Acquisition (SCADA) systems for nuclear material refineries in Iran.

Some speculate that Iran was not the intended target and that other similar systems in the mining sector were equally valuable. However, over 60% of the infected systems were in Iran and the planning involved in creating the Stuxnet indicated that it was designed for a specific military purpose and was most likely created by a state agency. Officials in Iran confirmed that Stuxnet had infected some computers in the nuclear program and this was corroborated when various virus protection firms were contacted by Iranian officials to help mitigate a serious malware attack.



Stuxnet's propagation mechanisms are all LAN based and thus, the final target must be assumed in close network proximity to the initial seeded targets.

The details of the Stuxnet worm are still being discussed, but it has been described as the most advanced information attack to date and a game changer. How the experience of Stuxnet translates into increased threats to tactical and operational military information systems remains to be seen. But if such closely guarded national programs can be penetrated by an information attack launched anonymously from a remote location, then it is feasible to expect even encrypted military system can be compromised.

Doctrine Team

INFOWAR and Software Defined Radios

by Jerry England

Information warfare (INFOWAR) units engage in a combination of computer warfare, information attack and perception management to establish and maintain information dominance. Integrated within INFOWAR doctrine are the following seven elements:

- Electronic warfare (EW)
- Deception
- Physical destruction
- Protection and security measures
- Perception management
- Computer warfare
- Information attack (IA)

By using both direct and indirect attacks on their adversary's computer networks, INFOWAR units seek to locate and exploit vulnerabilities across the full spectrum of information enabled weapons and battlefield systems. Employing INFOWAR capabilities means bringing to bear the information-oriented elements of national power to decisively defeat the enemy.

THREATS

Not just the military, but government institutions and private citizens as well who are affiliated with the OPFOR cause, will form the base for the collective INFOWAR campaign. It is the pervasive nature of the information age which has increased the risk of attack.

Hobbyists, criminals, scientists, activist groups, and state sponsored actors all have the ability to affect the informational domain and information oriented military operations. Criminal elements have developed their abilities to penetrate secure information systems for illicit gain to such an extent that they are being enlisted by governments to develop weaponized versions of malware designed to attack strategic targets.

From strategic to tactical level operations, the push for the U.S. military is to provide wide band secure communications to the edge of the battle field. This presents a target rich environment for threat actors throughout the operational environment.

SOFTWARE DEFINED RADIOS

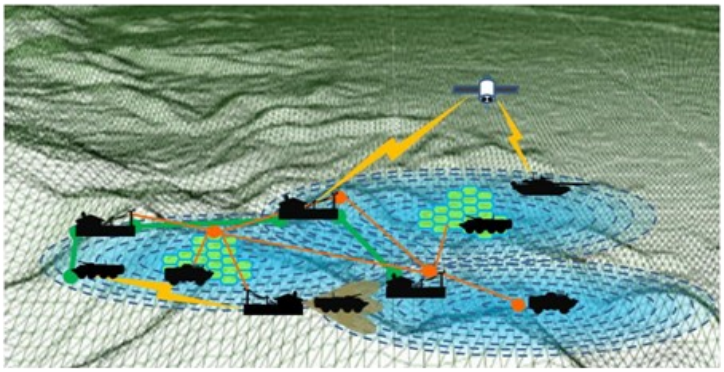
Software defined radios (SDRs) are key enablers to the U.S. military's vision of a fully integrated battlefield information system (IBMS). Similar to traditional tactical communications systems such as handheld radios and combat net radios, SDRs are more like miniature computers with a transmitter attached.

SDRs are the latest command and control systems designed to leverage advances in wireless networking and mobile computing. These radios can create mobile ad hoc networks (MANET) that are self organizing and self healing. SDRs also provide a full range of services from voice to data to real-time imagery. This is possible by converting all transmissions to internet protocol (IP) and using network enterprise architecture for transport.

Doctrine Team

SDRs offer significant benefits such as increased connectivity and higher data rates, which improves situational awareness, but is a benefit that comes with its share of risks.

Devises such as wireless routers, personal data assistants (PDAs), and smart phones are examples of the commercial technology that make up the multifunctional nature of SDRs.



SDRs are a part of the integrated battlefield system

There is a cost to these enhanced capabilities. Wireless technology is vulnerable to attacks and quality of service issues due to a wide range of threats and environmental factors. Using penetration techniques such as packet injections and cross-site request forgeries, an attacker can gain access to wireless tactical information systems through vulnerabilities in the configuration of the network or the hardware itself. The software is widely available to the hacker community and with modifications can become a threat to SDRs.

WIRELESS VULNERABILITIES

Software suites such as Linux Auditor include detectors for wireless networks and packet sniffers and are used by hackers to locate vulnerabilities. They provide the capability to locate a wireless access point, capture the packets needed to authenticate the threat system, and to access a network.

The mobility of wireless handheld devices coupled with the convenience of automatic link establishments (ALE) make SDRs a powerful capability able to provide increasing amounts of data in dynamic operational environments. The use of SDRs provides the flexibility to modify radio propagation (waveforms), encryption and bandwidth to suit the operation. This can mask the content of message traffic and establish communications on the move (COTM) throughout the battlefield. They cannot, however, hide the energy that is being used to transmit these messages.

OPEN SOURCE SOFTWARE

Many open source and commercial capabilities are available and can easily be modified to perform sophisticated INFOWAR missions. Software designed to turn any computer into an SDR is available online and free of charge. If the source code was modified, it also could be used to monitor a wide range of radio frequencies including those used for military operations. Audio files can be created by recording transmissions and emailed for analysis at a later date. Since it is software, all settings and tolerances can be modified to monitor a variety of signals including known military frequencies and waveforms.

Doctrine Team

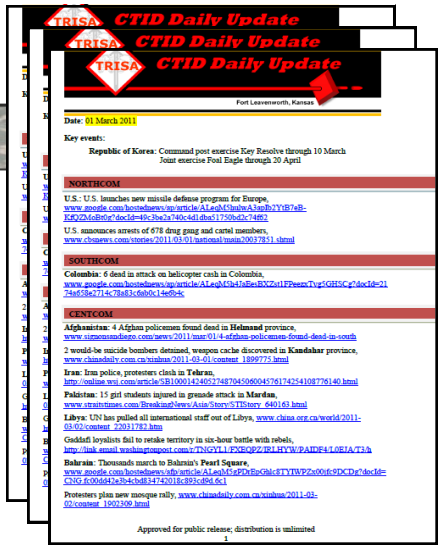
Since the software enables remote monitoring through the Internet, INFOWAR units do not have to be physically located at the receiver and can monitor signal traffic from U.S. SDRs from anywhere simply by logging on to the receiver's web-site. The ability to monitor radio traffic from any computer increases operational security (OPSEC) for the OPFOR by disassociating the operator from the equipment.

Open-source SDR software running on a Linux based operating system

In the near future, it is possible that the U.S. military's reliance on commercial research and development will make any technological overmatch gained by the use of SDRs short lived. Commercial improvements are eventually rendered vulnerable by hackers. In the past the military was late to adopt necessary technology, and procured systems that were either obsolete, incompatible or compromised the day they were fielded.

The tradeoff between access and security always includes risks as more data is pushed to the tactical level. Increased bandwidth expands the need for security which in turn requires more bandwidth. The proliferation of U.S. information systems on the battlefield exposes data and presents the OPFOR with opportunities to conduct an information attack.

Monthly Wrap-Up of CTID Daily Update



CTID analysts produce a *Daily Update* to help focus our readers on key current events and developments which may be of interest across the Army training community. Each *Daily Update* is organized topically across the Combatant Commands (COCOMs). The following list is a highlight of developments in August 2011. CTID does not assume responsibility for the accuracy of each article. The *Daily Update* is a research tool and an article's inclusion in the *Update* does not reflect an official U.S. Government position on the topic. The *CTID Daily Update* is posted daily on AKO.

Aug 1: **North Korea**: DPRK suffers great damage caused by typhoon and heavy rains.

Aug 2: **Argentina**: Argentina eyes nuclear-powered sub project.

Aug 2: **Iraq**: Car bomb near church wounds 19 people in Kirkuk.

Aug 3: **World**: McAfee report outlines global cyber spying.

Aug 3: **Somalia**: U.S. weapons now in Somali terrorists' hands.

Aug 4: **Colombia**: Forces shut down 20 FARC cocaine labs.

Aug 4: **Afghanistan**: IED attacks in Afghanistan hit all-time high.

Aug 5: **Sudan**: UNAMID peacekeeper killed in Darfur ambush.

Aug 8: **Mexico**: Mexican military helicopter lands in Laredo, Texas by mistake.

Aug 9: **Egypt**: Riot in southern Egypt kills three.

Aug 10: **Afghanistan**: Taliban is planning spectacular terrorism attack warns British Army chief in Afghanistan.

Aug 11: **World**: The end of war; nonstate violence is the new norm.

Aug 11: **Afghanistan**: Afghanistan order of battle as of July 2011.

Aug 12: **Social Media**: War, famine and Facebook: Deadly propaganda of Somalia's al-Shabaab terrorists.

Aug 15: **Iraq**: Wave of bombings kills 60.

Aug 15: **China**: Rare series of bombings hit Chinese government buildings.

Aug 16: **China**: The South China Sea is the future conflict.

Aug 17: **Afghanistan**: Motorcycle bomb explodes in market. (***See p. 7 for related OEA Team article***)

Aug 18: **Russia**: 13 fighters killed in Chechnya and 2 in Dagestan.

Aug 19: **Kazakhstan**: Kazakhstan's Islamist Threat?

Aug 22: **Mexico**: DHS shuts down Arizona-Mexico tunnel.

Aug 23: **Arctic Issues**: Denmark moves forward on North Pole claim.

Aug 24: **World**: Department of State releases country reports on Terrorism.

Aug 25: Germany: Germany increasingly a center for terrorism in Europe.

Aug 26: **Nigeria**: Suicide VBIED hits UN building in Abuja, at least 10 dead, Boko Haram responsible.

Aug 29: **Afghanistan**: Inside Afghanistan's deadly copter war.

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: LTC 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

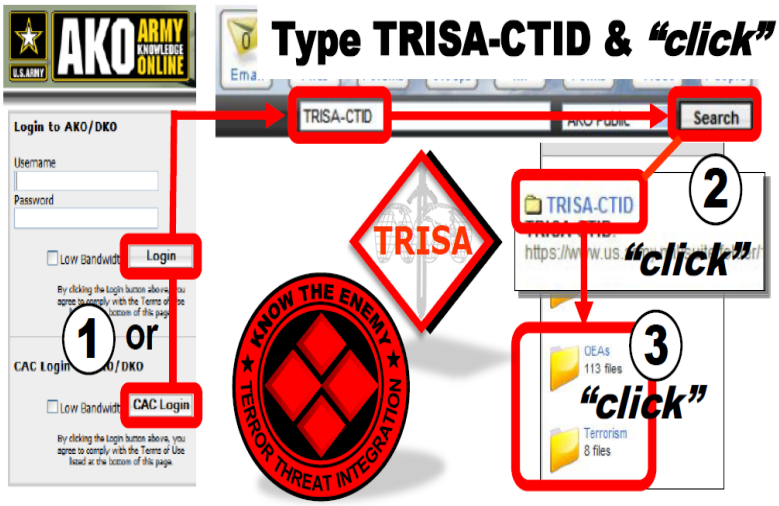
Joint Maneuver Readiness Ctr - OPFOR
SME: Mr Mike Spight BAE 684.7974
michael.spight@us.army.mil

Mission 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



Find Your Topic – Do Your Research

What We Do for YOU

- ***Determine OE Conditions***
- ***Publish Operational Environment Assessments (OEAs)***
- ***Publish OE Threats in FSO***
- ***Publish Army OPFOR Doctrine***
- ***Assess Threat-Enemy & TTP***
- ***Support Terrorism Awareness***

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