U.S. TRADOC G2 Intelligence Support Activity

Red Diamond

Complex Operational Environment and Threat Integration Directorate

Fort Leavenworth, KS Volume 4, Issue 9 SEP 2013

INSIDE THIS ISSUE

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

TRISA *Hybrid Threat Train-the-Trainer* 2013 Update

Hybrid Threat
Train-the-Trainer
23-27 SEPTEMBER 2013
U.S. Army TRADOC G2 Intelligence Support Activity (TRISA)
Complex Operational Environment and Threat Integration Directorate (CTID)

by CTID Operations

The Complex Operational Environment and Threat Integration Directorate (CTID) of TRISA completed a successful resident ***Hybrid Threat Train-the-Trainer*** at Fort Leavenworth, Kansas 23-27 September 2013. The training focused on how to conduct Threat functional analysis and portray a challenging and realistic Hybrid Threat (HT) in Army training, professional education, and leader development venues. Almost 80 military members, Department of the Army Civilians, and contractors represented many of the activities, organizations, and institutions in support of Army readiness: observer-controllers (O/Cs) from the Army's Combat Training Centers (CTCs), scenario developers, staff officers or Threat subject matter experts from Army schools and Centers of Excellence (CoEs), Army Reserve, and Army National Guard. This five-day session emphasized practical exercises and small group discussion to plan and conduct experiences of tactical operations in complex operational environments. Hybrid Threats include diverse and dynamic combinations of regular forces, irregular forces, and/or criminal elements, and often use terrorism as integral to their tactics and techniques.

The next scheduled resident Hybrid Threat Train-the-Trainer course is 10-14 March 2014 at Ft. Leavenworth, Kansas. CTID can also adapt HT training modules for modified sessions less than five days and mobile training teams (MTT). Interested? Plan now. Contact us now.

RED DIAMOND TOPICS OF INTEREST

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

This issue of TRISA ***Red Diamond*** features an article on noncombatants in complex environments and ways to create dynamic conditions in training using armed and unarmed noncombatants. Other opportunities to create complexity are cyber attacks and how such actions can be injected into training situations. The Hybrid Threat (HT) for training includes many perspectives of the human domain and how to shape, influence, or coerce change in a relevant population.

Recent examples of irregular forces conducting operations are an insurgent attack on a Syrian air base that included use of an armored personnel carrier as a vehicle borne improvised explosive device (VBIED), IED use to assassinate a Mexican law enforcement official, and IEDs used in a Turkish urban setting for the psychological impact on a community.

The TRISA-CTID *Horn of Africa (HOA) Operational Environment Assessment* provides a selected preview with a military variable in Ethiopia as one of seven HOA states.

Email your topic recommendations to:

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

CTID *Red Diamond* Disclaimer

The *Red Diamond* presents professional information but the views expressed herein are those of the authors, not the Department of Defense or its elements. The content does not necessarily reflect the official US Army position and does not change or supersede any information in other official US Army publications. Authors are responsible for the accuracy and source documentation of material that they reference. The *Red Diamond* staff reserves the right to edit material. Appearance of external hyperlinks does not constitute endorsement by the US Army for information contained therein.

US ARMY TRADOC
KNOW THE ENEMY
TERROR THREAT INTEGRATION
TRISA
Complex Operational Environment and Threat Integration Directorate
Know the Irregular Force Threat
Know the Enemy
in Complex
Operational
Environments
Insurgents
Guerrillas
Terrorists
Criminals
Affiliates
Adherents
Never Forget
911
We are at War and Combating Terrorism
Training Readiness to Protect and Preserve
TRISA
U.S. Army
TRADOC G2
Intelligence Support Activity
TRISA Combating Terrorism (CbT)
Poster No. 12-13
911 Special
(Photo: U.S. Coast Guard)

Director's Corner:
Thoughts for Training Readiness

by Jon Cleaves, Director, Complex Operational Environment and Threat Integration Directorate

There is no question that a great deal of what goes on in the world of Threats is focused on our Combat Training Centers (CTCs). They have professional opposing forces (OPFOR) and they are the best resourced to create realistic environments for training. However, the CTCs are only one third of our lines of effort. We are just as committed to supporting home station training (HST) and training that takes place in our Centers of Excellence (CoEs).

These training venues need our help as much if not more than the CTCs. If you are a unit trainer or a CoE instructor or training developer, come to us for help in setting realistic challenges for your training audience if you aren't already doing so. We provide a host of products that help create realistic challenges for training (Operational Environment Assessments, Threat Reports and Handbooks, TC 7-100 series, etc.). We are the lead for the Decisive Action Training Environment (DATE). We will review programs of instruction, OPFOR orders and plans, and OE events. We will, when possible, come to your location with a mobile training team and provide threat training customized to your needs.

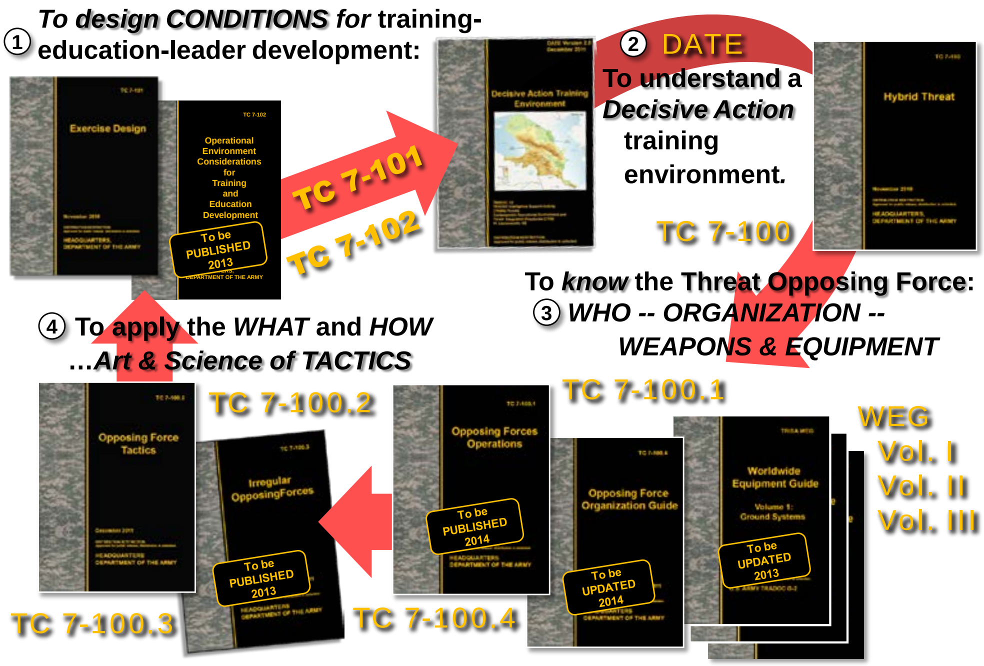
Although it has many manifestations, we only have one job: to help you put realistic OE conditions into your training event. Help us help you.

Jon

jon.s.cleaves.civ@mail.mil

____

Visualizing a Rationale of Threat Opposing Force Literature—Army Readiness



① *To design CONDITIONS for* training-education-leader development:
Exercise Design
Operational Environment Considerations for Training and Education Development
To be PUBLISHED 2013
TC 7-101
TC 7-102
② DATE
To understand a *Decisive Action* training environment.
Decisive Action Training Environment
Hybrid Threat
TC 7-100
To *know* the Threat Opposing Force:
③ *WHO -- ORGANIZATION -- WEAPONS & EQUIPMENT*
④ To *apply* the *WHAT* and *HOW* …*Art & Science of TACTICS*
Opposing Force Tactics
TC 7-100.2
Irregular Opposing Forces
To be PUBLISHED 2013
TC 7-100.3
Opposing Forces Operations
To be PUBLISHED 2014
TC 7-100.1
Opposing Force Organization Guide
To be UPDATED 2014
TC 7-100.4
Worldwide Equipment Guide
Volume 1: Ground Systems
To be UPDATED 2013
WEG
Vol. I
Vol. II
Vol. III

Complex Variables in an Operational Environment (OE)

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

Noncombatants in an operational environment (OE) require an acute awareness and understanding of their possible, probable, or known threat to dynamic and complex conditions in military operations. A host of noncombatants add complexity to any operational environment (OE). The positive and negative impacts of noncombatants in training embed realistic challenges and opportunities in live, virtual, constructive or gaming (LVCG) training context.

Irregular opposing forces (OPFOR) in training attempt to manipulate noncombatants in ways that support its goals and objectives. Many noncombatants are completely innocent of any involvement with the irregular OPFOR. However, irregular OPFOR will seek the advantages of operating within a relevant population of noncombatants whose allegiance or support it can sway in its favor. Aspects of noncombatant support can include clandestine yet willing active support (as combatants or noncombatants), coerced support, support through passive or sympathetic measures, or either unknowing or unwitting support.

General Characteristics

Noncombatants are persons not actively participating in combat or actively supporting any of the forces involved in combat and related direct actions. The definition of what comprises "active support" can require legal analysis and determination to support the conduct of particular military operations. For example, noncombatants can be armed or unarmed. Figure 1 displays examples of these two basic types of noncombatants that can be manipulated by the irregular OPFOR. These examples are not all-inclusive, and some of the example entities can change be either armed or unarmed.

> ***Note.*** From a US viewpoint in training vignettes and exercises, the status of noncombatants can be typically friendly, neutral, or unknown. Comparatively, noncombatants could view US and/or local governing authority forces as friendly or neutral in regard to themselves. Other expectations about noncombatants can exist and evolve depending on the particular training conditions of an OE. For consistency throughout this article for training, an o*pposing force* (OPFOR) refers to the governing authority and associated US or coalition forces as "enemy."

Aside from military and paramilitary forces, the civilian population of a nation or region is often the single most important aspect of an OE. This situation can be further complicated by the presence of other noncombatants who are not indigenous to the country or region and present conditions of very diverse motivations and expectations.

Noncombatant Relationships with the Irregular OPFOR

The irregular OPFOR recognizes that noncombatants living and/or working in an area of conflict can be a significant source of—

- Intelligence collection.
- Reconnaissance and surveillance.
- Technical skills.
- General logistics support.

Therefore, irregular OPFOR actively uses noncombatants within a relevant population to support its goals and objectives. It sees them as a potential multiplier of irregular OPFOR effectiveness. It will also attempt to use the presence of noncombatants to limit the effectiveness of its enemies. A typical technique of the irregular OPFOR is to marshal and conceal its combatant capabilities while hiding among armed and unarmed noncombatants in a geographic location.

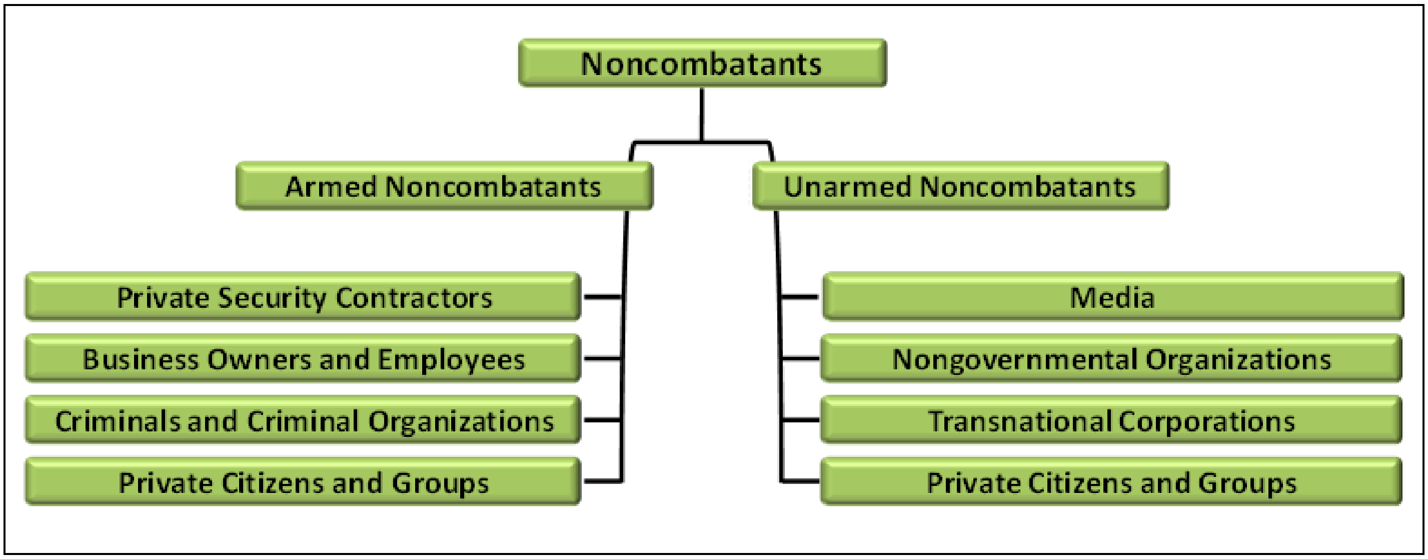

Noncombatants
Armed Noncombatants
Unarmed Noncombatants
Private Security Contractors
Business Owners and Employees
Criminals and Criminal Organizations
Private Citizens and Groups
Media
Nongovernmental Organizations
Transnational Corporations
Private Citizens and Groups

Figure 1. Armed and unarmed noncombatants (examples)
(See CTID Final Approved Draft of TC 7-100.3 *Irregular Opposing Forces*—Pending APD Review)

Changes in an OE and persuasion by irregular OPFOR information warfare (INFOWAR) activities can cause rapid or gradual shifts in allegiance of noncombatants. Any noncombatant is a potential recruit to become a combatant in support of irregular OPFOR. However, irregular OPFOR will also attempt to use those who remain noncombatants to its advantage. It purposely exploits noncombatants to cause doubt or hesitation in an enemy's decision to act. It takes advantage of the difficulties its enemies may have in distinguishing combatants from noncombatants. This uncertainty exists because both types of civilians may or may not be armed and may appear to not be participating in or supporting irregular OPFOR actions.

Irregular OPFOR may use noncombatants for shielding its operations close to and/or within a relevant population. An intentional purpose may be to cause enemy reactions which cause hazard or harm to noncombatants. Incidents such as noncombatant detention and/or casualties can alienate a relevant population from enemy forces with whom the irregular OPFOR is in conflict.

> ***Note.*** The Geneva Conventions state criteria for combatants as individuals who operate under the recognized command and control of an organization, are clearly armed, and do not attempt to disguise their intended actions when deploying for and conducting military-like actions. The irregular OPFOR is not bound by such conventions. The US Army and regulated military forces of other nations consider chaplains, medical doctors, and medics as noncombatants. However, the irregular OPFOR does not necessarily recognize such functional distinctions. In guerrilla OPFOR units, for example, medics are combatants and trained to fight alongside other guerrillas.

Motivations

Irregular OPFOR uses several forms of passive, active, or violent persuasion to motivate and obtain support from noncombatants in a relevant population. Means of persuasion can include—

- INFOWAR activities.
- Social welfare programs.
- Political activism and mobilization.
- Coercion.

When co-opted directly or indirectly by irregular OPFOR, noncombatants are a means to weaken control and legitimacy of a governing authority over its population. The irregular OPFOR attempts to communicate a compelling narrative of its own legitimacy that is accepted by the relevant population. Its visible actions, often localized in perspective, focus on demonstrating its power and authority as an OPFOR.

Irregular OPFOR may appeal to noncombatants based on unresolved grievances of a relevant population. Unresolved grievances, perceived or factual, create conditions where individuals believe they must act to obtain a just and satisfactory solution. The irregular OPFOR can appeal to aspects of ethnicity, geographic claims, and regional history that affect personal and group relationships. These perspectives can also be reflected in social status and networks, lifestyle, employment, religion, and politics. Irregular OPFOR can manipulate at least three areas of grievance by to obtain noncombatant support:

- Personal or social identity and/or social mobility or advancement.
- Religious beliefs and/or persecution.
- Unjust political representation and/or governance.

Motivations to support irregular OPFOR may also vary from religious extremism to pure criminality for personal or organizational profit. Often, the deciding factor may be the desire of a relevant population for local freedom from control by the governing authority and its international supporters.

Types of Support by Noncombatants

A relevant population can willingly provide active or passive support to irregular OPFOR. However, noncombatants can be coerced by irregular OPFOR. Some noncombatants may be aware of irregular OPFOR activities and choose to remain passive and not report information to the governing authority. Noncombatants may be sympathetic to the irregular OPFOR but remain uninvolved in any overt activity. Other noncombatants may unknowingly support irregular OPFOR initiatives such as money donations to charities or apparent humanitarian relief organizations that are actually front organizations for irregular OPFOR financing and/or materiel support. Those members of a local populace who elect to participate in or actively support the irregular OPFOR can in some cases become combatants, even if they do not bear arms. Figure 2 shows various types of support that noncombatants can provide to irregular OPFOR.

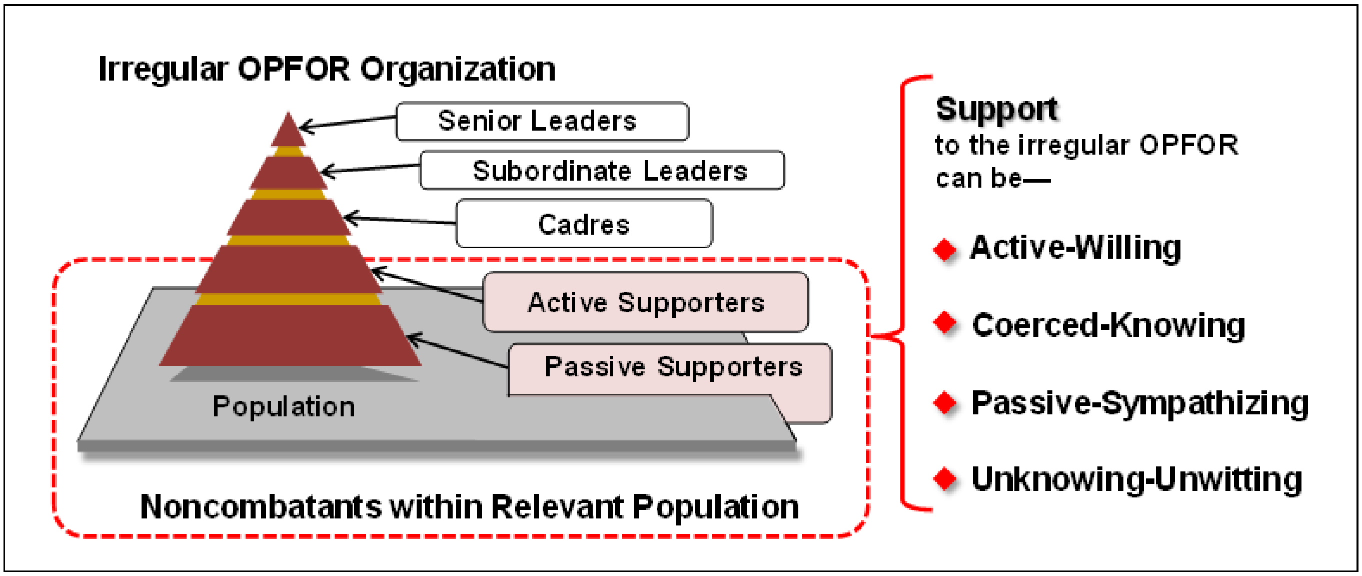


Figure 2. Model of noncombatant support to the irregular OPFOR (examples)

Unarmed Combatants

The local populace contains various types of unarmed nonmilitary personnel who, given accommodating conditions, may decide to purposely support hostilities against the enemy of irregular OPFOR. Such active support or participation may take many forms, not all of which involve possessing weapons.

In an insurgent organization or guerrilla unit, unarmed personnel might conduct recruiting, financing, intelligence-gathering, supply-brokering, transportation, courier, or INFOWAR functions (including videographers and camera operators). Technicians and workers who fabricate improvised explosive devices might not be armed. The same is true for people who provide sanctuary for combatants.

Unarmed religious, political, tribal, or cultural leaders might participate in or actively support irregular OPFOR. Unarmed media or medical personnel may become affiliated with a military or paramilitary organization. Even unarmed individuals coerced into performing or supporting hostile actions, and those who do so unwittingly, can in some cases be categorized as combatants.

> ***Note.*** In training exercises, some governing authorities may consider any armed or unarmed person who engages in hostilities, and/or purposely and materially supports hostilities against the governing authority or its partners, as a combatant.

Other examples include individuals who perform money-laundering or operate front companies for large criminal organizations might not be armed. Individual criminals or small gangs might be affiliated with a paramilitary organization or irregular OPFOR and perform support functions that do not involve weapons.

Armed Combatants

Any OE will have nonmilitary individuals who are armed but are not part of an organized paramilitary or military structure. Nonetheless, such people may be disgruntled and hostile to the governing authority or paramilitary and military forces that support it. Armed noncombatants may represent a large portion of the undecided citizens in a population. Some of these nonaffiliated people may possess weapons legally to protect their families, homes, and/or businesses. Some people may use weapons as part of their occupation (such as hunters, security guards, or local police). Other civilians may be minor criminals who use their weapons for activities such as theft or extortion. Given the fact that they are already armed, it could be easy for such noncombatants to become or be categorized by some organizations as combatants. Concurrently, some criminals may be directly associated with irregular OPFOR. Numerous reasons, including prejudices and grievances, can cause armed noncombatants to choose sides or change sides. They may switch allegiances repeatedly as circumstances evolve.

Some armed noncombatant entities can be completely legitimate enterprises. However, some activities can be criminal under the guise of legitimate business. The irregular OPFOR can embed operatives in legitimate commercial enterprises or criminal activities to obtain information and/or capabilities not otherwise available to it. Actions of such operatives can include sabotage of selected commodities and/or services. They may also co-opt capabilities of a governing authority infrastructure and civil enterprises to support irregular OPFOR operations.

Examples of armed noncombatants commonly operating in an OE are—

- Private security contractor (PSC) organizations.
- Local business owners and employees.
- Private citizens and private groups authorized to carry and use weapons.
- Ad hoc local “militia” or neighborhood security programs.
- Criminals and/or organizations with labels such as cartels, gangs.

Criminals and irregular OPFOR in an OE can be associated and/or affiliated with each other. For example, some insurgents and criminals can form temporary coalitions when it serves their mutual interests. Crime is a lucrative means to—

- Fund operations.
- Coerce and control key leaders and/or a relevant population.
- Erode governmental authority.

Some criminals may oppose irregular OPFOR when its actions jeopardize criminal operations and profits. Criminal organizations may hire PSCs to provide additional security. Larger criminal organizations can employ paramilitary elements and tactics. Some may expand from traditional criminal activities into a pseudo-insurgency and establish de facto governance in areas, regions, and enclaves within an otherwise sovereign territory of the governing authority.

Training Implications

Uncertainty and complexity characterize current OE and will continue to be so for the foreseeable future. Training at all levels from Soldier and leader self-development must include these often rapidly changing conditions into training exercises.

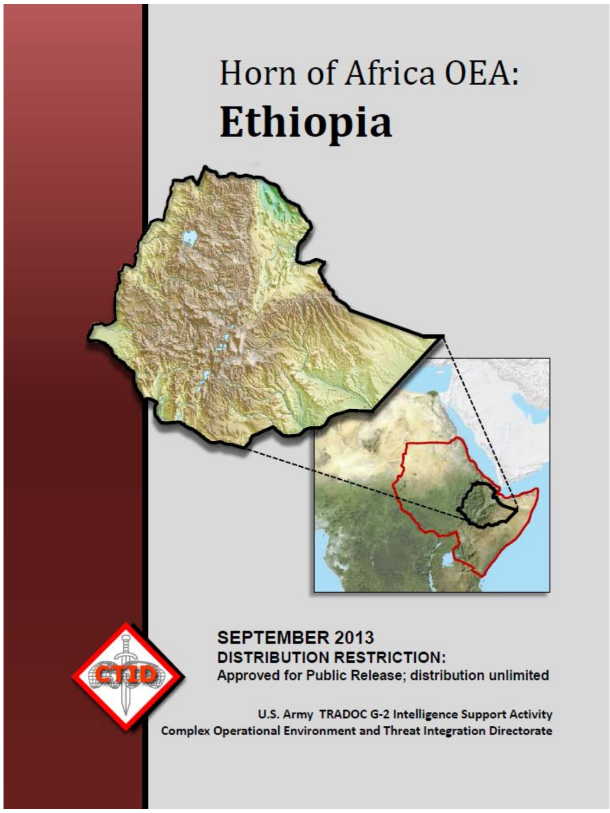
Determining who is a noncombatant from a combatant will often reside in tactical situations that require immediate decisions to act in a particular way. Such decisions, embedded in training and after action reviews at home station events, field exercises, and combat training centers (CTCs) will improve the character and abilities of Soldiers and leaders to make satisfactory decisions in moments of crisis when deployed in operational missions.

Use the US Army opposing force (OPFOR) training materials in the field manual and training circular 7-100 series and related TRADOC G2 TRISA handbooks and resources to create a credible Threat for a particular OE in training. Segments of this article are amplified in the pending publication of Army Training Circular 7-100.3, *Irregular Opposing Forces*.

Horn of Africa: Ethiopia Military Variable Preview

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

This fall, TRISA-CTID will publish the Horn of Africa (HOA) Operational Environment Assessment (OEA) update. So far in 2013, articles on the Djiboutian and Eritrean military variables have been published in the *Red Diamond*, and this article will cover Ethiopia. Throughout the next several months, the other countries in the HOA – Kenya, Somalia, Sudan, and South Sudan – will also receive coverage.



Horn of Africa OEA:
Ethiopia

SEPTEMBER 2013
DISTRIBUTION RESTRICTION:
Approved for Public Release; distribution unlimited

U.S. Army TRADOC G-2 Intelligence Support Activity
Complex Operational Environment and Threat Integration Directorate

Ethiopia is a landlocked country located in northeast Africa. After a 30-year civil war with the Eritrea Liberation Force (ELF) that ended in the creation of a separate country, Ethiopia lost its access to the sea. Due to the poor relations between the two countries, Ethiopia now exports and imports most of its goods through the port in Djibouti. Ethiopia possesses greater potential for development than many of its neighbors, thanks primarily to the Blue Nile River and possible hydroelectric plants that could sell excess electricity to nearby energy-starved countries.

Without access to the ocean, Ethiopia only fields an army and an air force. Since just 2,000 of the 152,000 military personnel serve in the air force, the army dominates the Ethiopian National Defense Force (ENDF). Ethiopia possesses extensive combat experience through years of internal civil war and external conflicts with Eritrea and Somalia. The Ethiopian military uses a combination of Western and non-Western doctrine based on its historical ties, first to Great Britain and then the US in the 1970s. Later, Ethiopia came under the influence of the former Soviet Union before returning to the mentorship of Western powers – including the US – over the last decade.

The ENDF fields a voluntary military, with the shortest enlistment period being two years. While technically volunteers cannot join until they are 18, the lack of accurate birth records makes this policy difficult to enforce. All citizens over the age of 18 are vulnerable to conscription in case of a national emergency, and must comply or face punishment. There have been cases where recruiters have coerced civilians to join military service.

The ENDF national command structure is a straight line from the Prime Minister, who serves as commander-in-chief of the military, to the Minister of Defense (MOD), to the Army Chief of Staff. The Ethiopian Air Force is subordinate to the army, and the air force commander reports directly to the army chief of staff. The Federal Police Commission, a government paramilitary organization, reports through the Minister of Federal Affairs to the Prime Minister.

Due to its guerrilla and conventional war with Eritrea, the ENDF has experience in both counterinsurgency (COIN) and conventional military operations. While the army now numbers a robust 250,000 active duty soldiers and another 100,000 militia members, this is a drop from its 2002 zenith strength, when the ENDF counted 400,000 members. The army operates through four military districts, a strategic reserve, and a special operations force (SOF). Each military district contains a corps headquarters, two infantry divisions, and one mechanized infantry brigade. The strategic reserve consists of six specialized brigades, while the SOF fields one special commando battalion and two commando brigades.

While no US forces are permanently stationed in Ethiopia, members of the Combined Joint Task Force-Horn of Africa (CJTF-HOA) and Soldiers – often from American National Guard units – train the ENDF ground forces to improve their proficiency and professionalism. Despite the recent influence from the West, most of Ethiopia's current inventory of weapons and equipment came from Russia or former Warsaw pact countries. The ENDF operates over 300 main battle tanks and 180 other armored vehicles in its formations. Maintenance issues, however, reduce the vehicles' combat capabilities.

Both the size and quality of the Ethiopian air force have fluctuated over the years. Before May 1991, the air force was fairly robust with a high level of serviceability – mainly due to the presence of Soviet advisors in the country. The air force became a shell of its former self with the fall of the Derg government in Ethiopia, the imprisonment of many of the pilots by the new government, and the collapse of the Soviet Union that ended its role as mentor. Maintenance issues grounded most of the aircraft at that time. Since 1998, the air force has rebounded – quicker than the experts anticipated. Both rotary and fixed wing aircraft helped dramatically in the border war with Eritrea. Since that time, the Ethiopian air force has focused on ground attack airplanes as well as helicopters and transportation aircraft.

The Ethiopian air force operates a squadron-based system with at least two fighter squadrons, three helicopter units, four transportation units, and a training unit. Approximately 2,000 personnel currently serve in the air force, down from a high of 5,000 airmen in 1991. Almost all air assets are based at Debre Zeit, near Addis Ababa, the location of the Ethiopian air force's command center. The air force primarily operates in support of the ground forces, but can conduct some strategic bombing missions. The stated Ethiopian air force mission is to protect the national air space, support the army, and provide assistance in national emergencies. The quality of the pilots has improved since 1991, when a purge removed pilots regarded as politically unreliable. Most aircraft are Russian made, but small numbers manufactured in other countries are part of the air force inventory.

There are two government paramilitary groups in Ethiopia. The Ethiopian Federal Police Force falls under the control of the Federal Police Commission (FPC), with a strength of about 16,700 police officers armed with small arms. The FPC is involved in both internal security throughout Ethiopia and COIN operations through its Anti-Terrorism Task Force. The Customs Service also possesses small arms, but is normally responsible only for customs and tax collection and smuggling prevention, as opposed to conducting combat operations.

There are several non-state paramilitary forces in Ethiopia. The Afar Revolutionary Democratic Union Front (ARDUF) is actually a splinter group that refused to sign the June 2000 peace treaty that ended the border war with Eritrea. The ARDUF splinter group's stated goals are for greater regional autonomy, expanded rights for Afar people in Ethiopia, and a more equitable distribution of revenues generated by the local region's salt industry. The Ethiopian People's Patriotic Front (EPPF) is an ever-shifting alliance of insurgent groups that, while unanimously opposed to the current government, form and break apart as ideological differences surface. The Ogaden National Liberation Front (ONLF) is located in the Ogaden region of eastern Ethiopia and consists primarily of the Ogaden clan. Its stated goals include defending the region from outsiders, protecting natural resources from those who wish to exploit the local people, full human and civil rights for all Ogadens and, most importantly, the right of national self-determination. The Oromo Liberation Front (OLF), founded in July 1973, champions the political and cultural rights of the Oromo people. That al-Qaeda (AQ) also operates in Ethiopia is reflected by the arrest on 2 January 2013 of 15 members of an Eastern African AQ cell in the country.

Ethiopia and the US are allies in the war on terrorism in the HOA region. The CJTF-HOA and other trainers continue to hone the ENDF's conventional and COIN skills to reduce and deter the potential terrorist threat in the HOA. US support of Ethiopia will almost always irritate Eritrea due to the longstanding mutual distrust between the two countries. The US will have to walk the fine political line of supporting an ally in the HOA without antagonizing other countries in the region.

ANTITERRORISM AWARENESS OF SOCIAL MEDIA USE

by CTID Operations—*Supporting the US Army Antiterrorism Strategic Plan: Phase III*

Army 4Q/FY13 Antiterrorism Awareness Theme

USE of SOCIAL MEDIA

U.S. Army Training and Doctrine Command G2
TRADOC G2 Intelligence Support Activity
Antiterrorism - Counterterrorism
Terrorism
Threats Terrorism Team (T3)
T3 Advisory
Social Media and Antiterrorism Awareness
Antiterrorism Awareness in Social Media
Know the Threat
Be aware of social network IMPERSONATIONS.
Be aware of social network LEAKAGE and SEEPAGE.
Beware of how you discuss—
Yourself
Your Family
Your Duty
PROTECT:
People
Information
Property
Facilities
Know the Enemy
ANTITERRORISM Principles:
ASSESS
DETECT
WARN
DEFEND
RECOVER
Do YOU — PROTECT and PRESERVE:
TRISA
JUL 2013 No. 10-13
AUG 2013 No. 11-13
SEP 2013 No. 12-13
JUL 13
AUG 13
SEP 13

Protect the Force

TRADOC G-2 Intelligence Support Activity
Complex Operational Environment and Threat Integration Directorate

Terrorism

The calculated use of unlawful violence or threat of unlawful violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological.

U.S. Department of Defense

HUMAN DOMAIN AND THE HYBRID THREAT FACTOR

Complex Operational Environments and Complex Threats

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

Strategic Landpower; Winning the Clash of Wills, a recent white paper from the Strategic Landpower Task Force, succinctly articulates the strategic importance of the "human domain" in future operations. Fundamental is the understanding that if people are the epicenter of national engagements, then conflict "is also an inherently human endeavor."[1] Independently, force indomitability will not be sufficient therefore, "strategic guidance must have human objectives, defined as actions taken to influence people, be they government and military leaders or groups within a population, as their core strategic focus."[2] As stated, however, much may be left to the imagination leaving more questions than answers. For instance, what is the human domain, how do opposing forces operate within it, and how do we achieve objectives within a domain that is inherently intangible? The human domain encapsulates the elements that influence the human condition which define human terrain "features." This provides friendly forces a map to identify decisive points against a populace's center of gravity, and serves as both friendly and opposing forces' "ways" to a populace's "ends."

Part One – Framing

Admiral William H. McRaven postulates that "the human domain encompasses the totality of the physical, cultural, and social environments that influence human behavior."[3] Although informative, further delineation of the human domain is prudent. Human and land domains overlap along the Range of Military Operations (ROMO). Strategically for both friendly and opposing forces, human domain centric operations occur preceding land domain focused operations.[4] Historically hybrid threat (HT) actors conducting irregular warfare (IW) dominate within the human domain, their preferred arena of conflict. As a result, United States Government agencies are left to "analyze what it takes to win wars among the people" addressing what it means to actually win hearts and minds.[5]

Executing categorical analysis of the human domain is far more difficult. For this reason Maslow's Hierarchy of Needs may prove useful. For the purposes of this article, Maslow's Hierarchy of Needs provides a construct to facilitate further discussion on irregular opposing force actions and a way to leverage operational art. It is not the intention to develop or advocate a comprehensive analytical comparison of human psychological needs within the operating environment (OE).

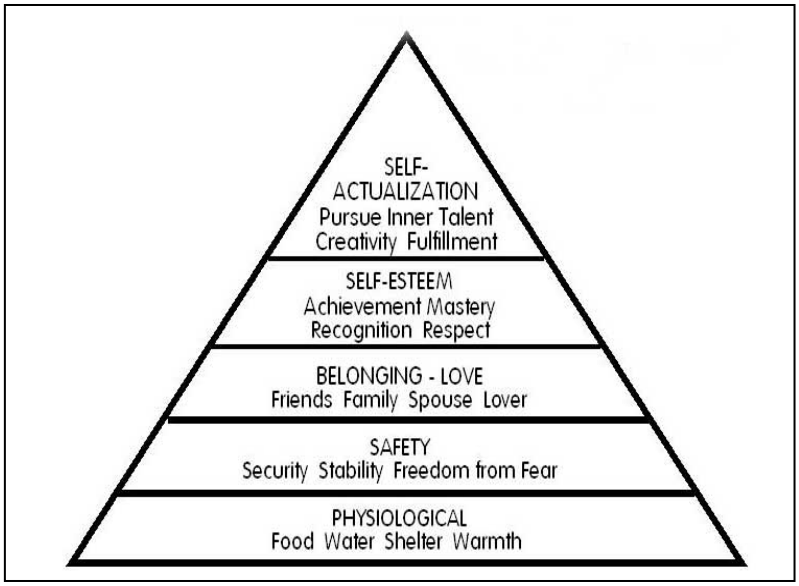


Figure 1. Maslow's Hierarchy of Needs

Maslow believed that people are inherently motivated to achieve a need and once complete they move to another need. Satisfaction of lower order needs is requisite to climbing the hierarchy. In ascending order, the five hierarchies include biological and physiological, safety, social, esteem, and self-actualization. Biological and physiological needs include things like food, water, warmth, sex, and sleep; safety needs include things like protection from the elements, security, law and order, and stability; social needs include things like belongingness, love and affection, family, and work/social groups and relationships; esteem needs include things like self-esteem, achievement, mastery, independence, social status, prestige, and responsibility; and finally, self actualization needs include realizing personal potential, self-fulfillment, seeking personal growth, and peak experiences.[6]

Conscious to Maslow or not, HT actors can be highly effective at executing tasks, operations, or roles to fulfill needs. Foremost, attaining an effective level of authenticity is paramount for any actor seeking longevity as a figure or apparatus of authority granted by the general public. This applies equally to the policeman on the beat and the elected official as it does the insurgent, criminal, or guerrilla. Ultimately, within the human domain, "the irregular [opposing force] seeks to obtain recognition of its legitimacy by a willing populace."[7] Guerrillas and insurgents are largely native. Therefore it is reasonable that their indigenous knowledge of customs, language, concerns, geography, and residents provides both the innate ability to develop relationships and meet hierarchical needs as well as provide a marked advantage over often viewed, or at least portrayed, imperial visitors.[8]

Army doctrine explains that in a complex OE, centers of gravity can be either physical or moral. Where physical centers are easier to identify and singularly affected by military means, moral centers are "intangible and more difficult to influence."[9] Included in the list of examples of a moral center is a "strong willed populace;" therefore, in applying the operational art to the human domain we are well on our way by identifying our center of gravity.[10] Note, identical is our center of gravity to that of the irregular opposing force's desired core of legitimacy. Subsequent effort should go to decision point and line of operations and effort classification.

Part Two – Opposing Force "Ways"

Hybrid threat actors have a multitude of ways to exert control over the populace within the human domain. Ultimately locals may provide either active or passive support to HT actor efforts.[11] Motivations may vary, but generally they can be aligned along a hierarchical need. For instance, the motivation could "be financial (payment or beneficial effects on business profits) or security provided them" meeting some physiological and safety needs or perhaps "based on ethnic or religious issues, to an insurgent or guerrilla organization even if they do not share that organization's political agenda," meeting social needs.[12] Numerous examples exist of the overlap between populace need deficiency and HT actor need fulfillment.

Human biological and physiological needs are vital. Where the state fails to provide basic services, other actors must step up. In the Dominican Republic, churches, community organizations, and non-governmental organizations temporarily filled the gap, but recently, criminal organizations with the funds and resources available fill the vacuum left by repeated state failure.[13] One way to earn money is through resource or commodity sales. In southern Afghanistan the opium trade is rich. The Taliban will offer loans for farmers to grow poppy to meet a production quota helping to satisfy a local need for work that will sustain a family. Known as the salaam system, farmers "pre-sell their crops at planting time at a price that was lower than its market value at harvest," ultimately it "has trapped thousands of poor farm families into a crippling debt cycle."[14] In this case, the Taliban meets a biological need of that farmer to provide minimally for his family while also holding him captive for future exploitation. This is not uncommon and an example of insurgent civic interaction and support of criminal enterprise profiting. Although effective means of control and meeting an essential need, this may not the best means of gaining legitimacy.

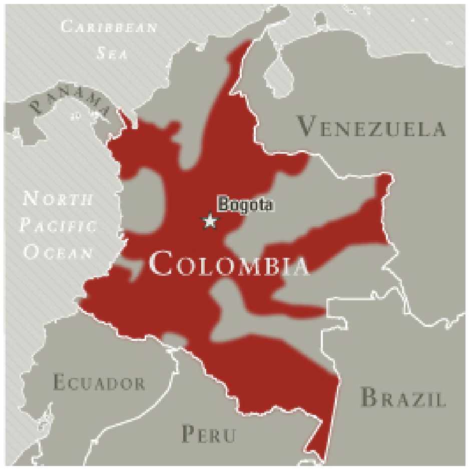


Figure 2. FARC influence: Colombia

Imperative to the human condition is security, law, and stability. For instance, the Revolutionary Armed Forces of Columbia (FARC) are more known for what they are today, a terrorist organization and transnational organized criminal syndicate. However, they "got their start like modern-day Robin Hoods, protecting rural peasants from the excesses of a corrupt government."[15] Protection is only one piece. Far more effective is the establishment of a governing structure to supplant the state. When successful, this garners great populace support. In Afghanistan, Haqqani long served the role of providing shadow organizations to provide minimal state functions such as dispute resolution.[16] They are not alone and are one of "many insurgent and organized crime networks throughout history and around the globe" to serve as security and rule of law provider.[17] Similarly to biological and physiological needs, these examples demonstrate the irregular opposing force in civic interaction. Moreover, Jalaludin Haqqani's network serves as a great example of actions to gain legitimate authority as well as provide for needs across hierarchies.

Social needs are also very important. Jalaludin Haqqani took great effort to maintain good community relations. Rent collection "[provided] vital public services, including religious education and health care."[18] Of note is the religious education system that provides the perfect forum to foster belongingness, family, and relationships. In this case, Jalaludin "founded a *madaris* (plural madrassa) network that played a key role in spreading his jihadist world view."[19] In duality, this demonstration of civic interaction and support serves a populace need and threat actor operations. Of recent development is the use of information technology, social media, and electronic networks for social belonging. This medium enables "people to mobilize and create strategic events at incredible speeds and then dissolve, shift activity or disappear entirely," while "also [creating] second- and third-order ripple effects that can be felt outside the region."[20] For instance, one reporter live tweeted drone strikes from the United States occurring in Yemen garnering quite a following.[21] Also recently, the Syrian president's son, Haffez Assad, or someone claiming to be him, left a Facebook post which was commented on, shared, or liked numerous times also collecting supporters.[22] Regardless of origin, both serve as examples that meet a social need while also supporting OPFOR information warfare efforts by managing populace perceptions.

Esteem needs are more likely to be met by a willing populace that is not only satisfied but pleased with those in power. For example, "a grateful public can provide valuable security and support functions. The local citizenry may willingly provide ample intelligence collection, counterintelligence, and security support."[23] In this case we are assuming that this support is not a product of some form of coercion as it would not meet the need of status, achievement or managerial responsibility. What is interesting to note is that in some instances diverging beliefs help rationalize this active support both to continue fulfillment of esteem needs, but also for profit to fulfill lower order needs, especially biological. Case in point: some Islamic scholars contend that Islam bans any dealings with narcotics. Others argue it is only wrong to consume but, partaking in other aspect of the drug trade are acceptable to earn money and fight the holy war.[24]

Self actualization is far more rare and difficult to target and would most likely occur in isolated instances for select individuals with satisfied esteem needs. Predominately, examples of irregular OPFOR action occur in the lower hierarchies as they are easier to control.

Part Three – Friendly Force Articulation

Implementing concepts and executing upon objectives within the human domain is important to achieve strategic success. Subsequent discussion serves only to stimulate further discourse and is a way to approach operational implementation. Considering the identification of a shared center of gravity or core of legitimacy with irregular opposing forces, Maslow's Hierarchy of Needs, and examples of HT actor engagements, we move forward using operational art and looking at a paradigm of an interoperable and interdependent structure designed to achieve success in the human domain.

The human domain in itself may not be a line of effort (LOE). However, consider developing decisive points relative the human domain using Maslow's Hierarchy. Decisive points can seek to fulfill populace needs or an operational effect upon the irregular OPFOR's ability to fulfill populace needs. Subsequently plot the aforementioned decisive points along LOEs. The resulting picture, made more clear by listing LOEs in ascending order (i.e.: Restore/Develop Essential Services, Security, Governance, Infrastructure Development), should align with Maslow's hierarchical levels. Failure or success to progress along our LOEs uniformly as well as identify, depict, and achieve decisive points can then provide insight to our effectiveness answering "are we doing the right things" and avoid us asking, "how did we do so much and achieve so little?"

Arguably, military action in the human domain may be a proactive effort rather than use as a final instrument of national power. For instance, Special Operations Forces (SOF) advocates for a Seventh Warfighting Function (WfF) to attend to "the related tasks and systems that influence the behaviors of a people (friendly, neutral, [and] adversary), security forces and governments and enables the prioritization and synchronization of efforts to achieve strategic effects."[25] The assertion is this allows the Army to leverage its recent wartime experience. In many cases, leveraging this experience could occur in missions such as unconventional warfare, foreign internal defense, stability operations, and security force assistance. In a recent article published by the Army News Service, COL Robert Simpson, acting director, Concepts Development & Learning Directorate, TRADOC, commented that in a proactive capacity, "we have the ability not only to compel, but to persuade people in a positive way."[26] Preventing conflict is always preferred, but proactive involvement will also reduce the likelihood of experiencing strategic surprise, aggressor miscalculation of our resolve or capability, and an increased responsiveness to crises.[27]

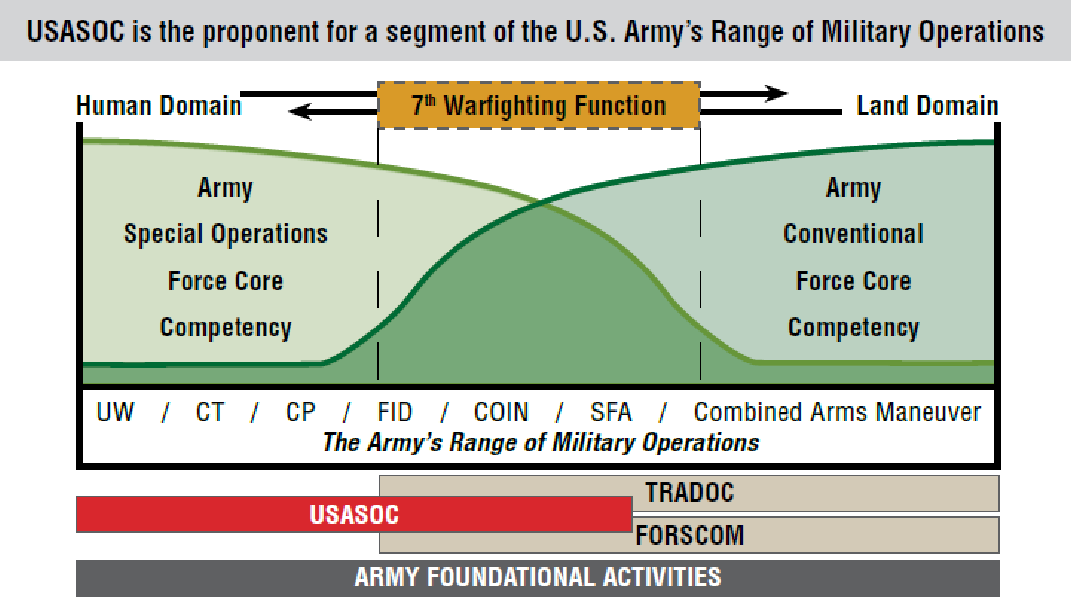

USASOC is the proponent for a segment of the U.S. Army's Range of Military Operations
Human Domain
7th Warfighting Function
Land Domain
Army
Special Operations
Force Core
Competency
Army
Conventional
Force Core
Competency
UW / CT / CP / FID / COIN / SFA / Combined Arms Maneuver
The Army's Range of Military Operations
TRADOC
USASOC
FORSCOM
ARMY FOUNDATIONAL ACTIVITIES

Figure 2. Seventh Warfighting Function and Human Domain/Land Domain along range of military operations

Successful engagement in the human domain includes strategies that are both interoperable and interdependent. The Strategic Landpower White Paper asserts "interdependent teams of conventional and special operations forces can build local forces capable of handling many situations that previously called for direct US intervention."[28] An example is a recently developed concept at the Joint Readiness Training Center Rotation 13-09. Leaders and subject matter experts from the United States Army Special Forces Command (Airborne) [USASFC(A)] and the United States Army Military Police (MP) Corps convened to develop a concept that would build a Provost Martial Cell within USASFC(A) and construct small interoperable deployable teams. Utilizing shared security force assistance experience and branch specific knowledge, skills, and abilities, their main effort would focus on assessing and developing national and strategic policing capability in a culturally attuned manner to support mission objectives as well as build partner nation capacity for security, governance, and rule of law. Capability and capacity growth could include, but is not limited to, police management, emergency response, public safety, and anti-corruption. This example of interoperability highlights two interesting notes. First, in regard to operational art, the suturing of SOF and MPs provides a unique means to achieve success in decision points along multiple LOEs in multiple phases of operation. Second, in regard to proactive engagement and a Seventh WfF, deployable combined SOF and MP teams with the aforementioned mission is applicable throughout the ROMO and is probably most effective early.

Diligent and careful extrapolation to derive specificity in our approach of the human domain is surely forthcoming. However there are certain truths that we can accept. First, we must understand that "when we have formally studied the lessons of our wars and anticipated the demands of the new order that historically follows those wars, we have been successful in subsequent conflicts."[29] Critical and creative thinking are essential. In this case, the Maslow's Hierarchy of Needs and the Operational Art serve as ways to frame and visually model a way to view the human domain. Second, whether by populace-supported legitimacy or coercion, irregular opposing forces are consistently dominating within the human domain as their operations often align with the most basic of human needs. Looking forward, we should expect further complexity of the strategic environment by "the rising velocity of human interaction (e.g., through the Internet, Twitter, Facebook, and other social media), multiplied by the ever increasing numbers of people in constant close association (urbanization)."[30] Third, leaning forward, the joint force is already working to develop concepts, such as articulating a Seventh WfF as well as interoperable and interdependent teams capable of producing successes in multiple forms, to better engage in a complex operating environment. Ultimately we must truly believe that "thinking is free."[31] To that end we must be exhaustive, inventive, and aggressive as surely our adversaries are and will continue to be.

Notes

[1] Strategic Landpower Task Force, “*Strategic Landpower; Winning the Clash of Will,*” www.arcic.army.mil, 3 September 2013.
[2] Strategic Landpower Task Force, “*Strategic Landpower; Winning the Clash of Will,*” www.arcic.army.mil, 3 September 2013.
[3] Claudette Roulo, McRaven, “*Success in Human Domain Fundamental to Special Ops,”* American Forces Press Services, 5 June 2013.
[4] United States Army Special Operations Command, *“Army Special Operations Forces 2022,”* Headquarters, Department of the Army.
[5] United States Army Special Operations Command, *“Army Special Operations Forces 2022,”* Headquarters, Department of the Army.
[6] Sam McLeod, “*Maslow’s Hierarchy of Needs*,” Simply Psychology, 2007, Updated 2013.
[7] United States Army TRADOC G2 Intelligence Support Activity Complex Operational Environment Threat Integration Division, *Irregular Opposing Forces – TC 7-100.3*, July 2013.
[8] United States Army TRADOC G2 Intelligence Support Activity Complex Operational Environment Threat Integration Division, *Irregular Opposing Forces – TC 7-100.3*, July 2013.
[9] Department of the Army, “*ADRP 3-0 Unified Land Operations,*” Headquarters, Department of the Army, May 2012.
[10] Department of the Army, “*ADRP 3-0 Unified Land Operations,*” Headquarters, Department of the Army, May 2012.
[11] United States Army TRADOC G2 Intelligence Support Activity Complex Operational Environment Threat Integration Division, *Irregular Opposing Forces – TC 7-100.3*, July 2013.
[12]United States Army TRADOC G2 Intelligence Support Activity Complex Operational Environment Threat Integration Division, *Irregular Opposing Forces – TC 7-100.3*, July 2013.
[13] Lillian Bobea, *“How Caribbean State Crime is Replacing the State*,” InSigntCrime, 24 July 2013
[14] Gretchen Peters, “*Seeds of Terror: How Heroin Is Bankrolling the Taliban and Al Qaida,*” (New York: St. Martin’s Press) 2009.
[15] Gretchen Peters, “*Seeds of Terror: How Heroin Is Bankrolling the Taliban and Al Qaida.*” (New York: St. Martin’s Press) 2009.
[6]Gretchen Peters, “*Haqqani Network Financing: The Evolution of an Industry,*” Combating Terrorism Center at West Point, July 2012.
[17] Gretchen Peters, “*Haqqani Network Financing: The Evolution of an Industry,*” Combating Terrorism Center at West Point, July 2012.
[18] Gretchen Peters, “*Haqqani Network Financing: The Evolution of an Industry,*” Combating Terrorism Center at West Point, July 2012.
[19] Gretchen Peters, “*Haqqani Network Financing: The Evolution of an Industry,*” Combating Terrorism Center at West Point, July 2012.
[20] David Vergun, “*Influencing Narative, Human Behavior Key to National Security,*” Army News Service, 28 August 2013.
[21] Spencer Ackerman, “*Yemeni Tells Senators About ‘Fear and Terror’ Caused by US Drones*,” Wired Online, 23 April 2013.
[22] Liam Stack, *“Facebook Post Said to Be by Assad’s Son Dares Americans to Attack*,” New York Times Online, Blogs, 29 August 2013.
[23] United States Army TRADOC G2 Intelligence Support Activity Complex Operational Environment Threat Integration Division, *Irregular Opposing Forces – TC 7-100.3*, July 2013.
[24] Gretchen Peters, “*Seeds of Terror: How Heroin Is Bankrolling the Taliban and Al Qaida.*” (New York: St. Martin’s Press) 2009.
[25] United States Army Special Operations Command, *“Army Special Operations Forces 2022,”* Headquarters, Department of the Army.
[26] David Vergun, “*Influencing Narative, Human Behavior Key to National Security.*” Army News Service, 28 August 2013.
[27] Strategic Landpower Task Force, “*Strategic Landpower; Winning the Clash of Will,*” www.arcic.army.mil, 3 September 2013.
[28] Strategic Landpower Task Force, “*Strategic Landpower; Winning the Clash of Will,*” www.arcic.army.mil, 3 September 2013.
[29] Strategic Landpower Task Force, “*Strategic Landpower; Winning the Clash of Will,*” www.arcic.army.mil, 3 September 2013.
[30] Strategic Landpower Task Force, “*Strategic Landpower; Winning the Clash of Will,*” www.arcic.army.mil, 3 September 2013.
[31] Strategic Landpower Task Force, “*Strategic Landpower; Winning the Clash of Will,*” www.arcic.army.mil, 3 September 2013

War Comes to Reyhanli: Terrorist Attack of 11 May 2013

Complex Operational Environments and Terrorism

by Jim Bird, OE Assessment Team (Overwatch Ctr)

On 11 May 2013, the eve of Mother’s Day, the Syrian civil war violently intruded upon the daily lives of peaceful Turkish citizens. Early that Saturday afternoon, the border city of Reyhanli suffered what one local observer called a huge “Middle Eastern-style civilian massacre,” when insurgents almost simultaneously detonated two large car bombs that had been pre-positioned at the city center.[1] In the aftermath of the twin explosions, there were neither sufficient coffins to keep up with the sudden surge in demand, nor enough Islamic clergymen available to accommodate the funerals occasioned by the incident.

The blasts devastated four city blocks, leaving more than 50 people dead (including 36 Turkish citizens), and more than 100 wounded. Property damage extended to eight public buildings, 732 businesses, 120 houses, and 62 vehicles. Casualty figures set a new record for the number of Turkish lives lost in a single terrorist incident, as well as for the number of civilians killed.

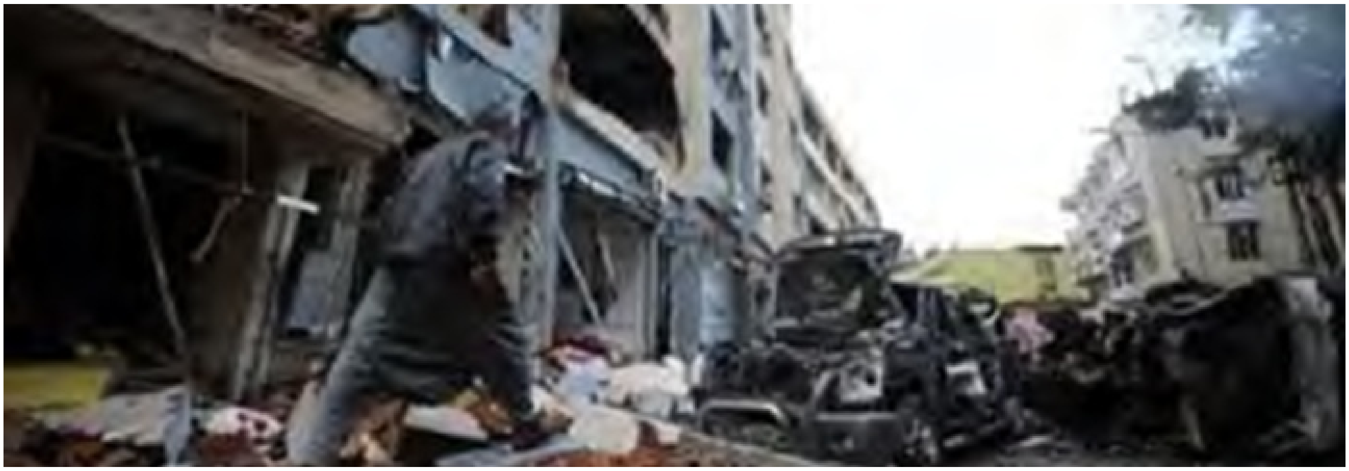


Figure 1: Street view of Reyhanli bombing aftermath, *RAPID* Weekly News Update, 17 May 2013

Tempting Target of Strategic Significance

Reyhanli's importance as a target for terrorists derives from its proximity to the Syrian border, which lies about three miles east of the city. Most Syrian customs agents have fled their country, loathe to enforce the draconian tactics of Bashar al Assad's regime or fearing the violence unleashed by its rebel opponents. Accordingly, the Cilvegözü border crossing, regarded as Turkey's main gateway to the Middle East, is only lightly manned, with virtually no official presence on the Syrian side. In short order, the administrative and security vacuum created by this absence of visible customs authority creates a steady stream of people and goods that continuously flows back and forth between villages near Reyhanli and similar counterpart communities on the Syrian side of the international boundary. Some of these cross-border ties involve shared ethnic and tribal relationships.

It is hardly surprising, then, that an undetermined proportion of Reyhanli's residents rely on smuggling for a livelihood. Inside the city, the streets are typically crowded with people wearing a variety of Syrian uniforms. A visiting stranger would have difficulty distinguishing the city from a Syrian village. As one observer noted, "an outsider may think that Turkey and Syria have merged or Reyhanli has been occupied by the Syrian army."[2] Sooner or later, a prospective terrorist was bound to take notice of the confused mass of humanity freely intermingling on Reyhanli's streets. This, in conjunction with the unrestrained cross-border traffic moving through the Cilvegözü checkpoint – or bypassing it altogether – inevitably offered an array of tempting targets to any threat actor bent on either harming or embarrassing the Turkish government.

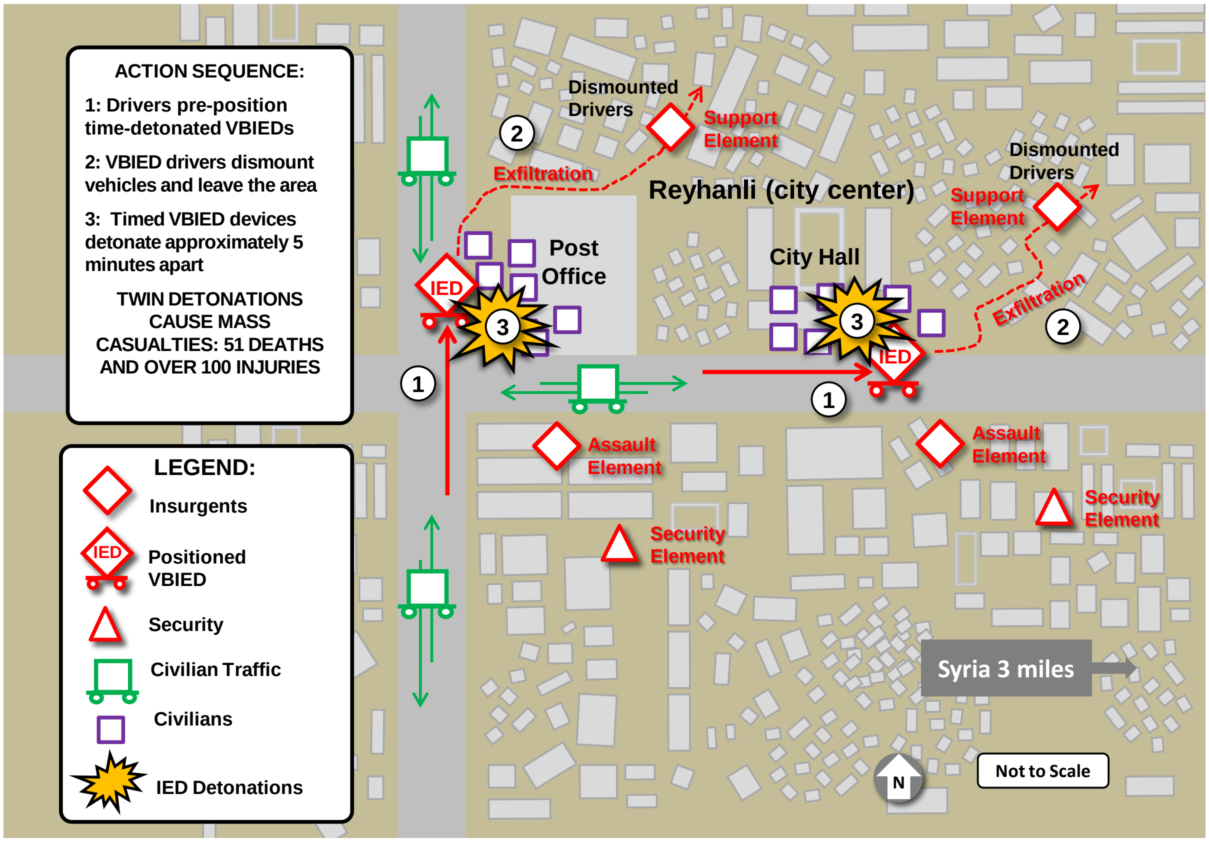
Incident Details

The potential for a terrorist attack materialized into tragic reality at approximately 1300 hours local time on 11 May 2013. Sometime in advance of the actual event, insurgents parked two vehicles, each packed with approximately a half-ton of "factory made" explosives, near the post office and city hall, both located at the center of downtown Reyhanli.[3] The drivers then dismounted their vehicles and, undetected, successfully exfiltrated the municipal complex. At the time and date indicated, between five and fifteen minutes apart, insurgents detonated both vehicle-borne improvised explosive devices (VBIEDs), inflicting the mass casualties described above.

Assigning Blame and Analyzing Tactics, Techniques, and Procedures (TTP)

Although no group claimed responsibility for the terrorist attack, Turkish authorities were quick to point an accusing finger at the Syrian government. Prime Minister Erdogan charged that "the incident is certainly linked to the Syrian regime."[4] A Syrian government spokesman vehemently denied the allegation, and countered by calling Turkey's ruling Justice and Development Party "al-Qaeda's political branch."[5] In the aftermath of the Reyhanli bombings, Turkish authorities rounded up 13 suspects, all leftists with alleged connections to Syrian intelligence.

Analysts differed in their opinions regarding the purpose of the attack and the group behind it. Some argued that the bombings reflected a level of sophistication that exceeded the capabilities of al-Qaeda (AQ) and Jabhat al Nusra, two radical Islamist elements currently fighting in league with the Free Syrian Army (FSA). These experts associated the professional know-how, logistical planning, and bomb-making materials used in the Reyhanli incident with skill-sets possessed by the current Syrian military establishment. Another group of analysts insisted that car bombs capable of inflicting mass casualties are an AQ weapon of choice, and suggested that various rebel groups allied with the FSA had a vested interest in provoking Turkish and/or international intervention in the Syrian civil war.



ACTION SEQUENCE:

1: Drivers pre-position time-detonated VBIEDs

2: VBIED drivers dismount vehicles and leave the area

3: Timed VBIED devices detonate approximately 5 minutes apart

TWIN DETONATIONS CAUSE MASS CASUALTIES: 51 DEATHS AND OVER 100 INJURIES

Figure 2: Reyhanli, Turkey car bombings, TRISA, 2013

If analysts disagreed over threat actors and motives behind the Reyhanli car bombings, convincing evidence led to a general consensus on at least one note: mass-casualty producing VBIED events in the Middle East spiked dramatically in the first four months of 2013 (to 62), compared with the number of such attacks perpetrated during the same period in 2012 (16). This drastic increase suggests that Syria's internal chaos acts as a drawing card for state-sponsored terrorists as well as non-state actors, all with their own set of reasons for affecting the course of events. An analyst from the American Enterprise Institute observed, "car bombs become a symbol of expertise flowing into the country that isn't homegrown."[6] Although his statement referred to events unfolding in Syria, on 11 May 2013 the same dynamic leached across the international boundary to play out in Turkey. Whoever carried out the attack, little doubt exists that the bombmakers had access to resources that were anything but homegrown. Syria's civil war had come to Turkey.

Aftermath and Ramifications

The Reyhanli attack blurred the distinction between local, national, and international politics. Locally, with the possible exception of the actual casualties and their friends and relatives, the city's Syrian residents (the largest concentration of refugees in Turkey) suffered most. The all too human tendency to blame the victim assumed the guise of local rage directed against Syrians for bringing the neighboring civil war to Turkey's doorstep. Some refugees suffered beatings or saw their property vandalized. Other Syrians, afraid to leave their homes or send their children to school, removed Syrian license plates from their cars. "The bombs attempted to destroy the bonds between the Reyhanli people and the Syrian refugees," said one observer. "And the terrorists achieved what they were pursuing."[7]

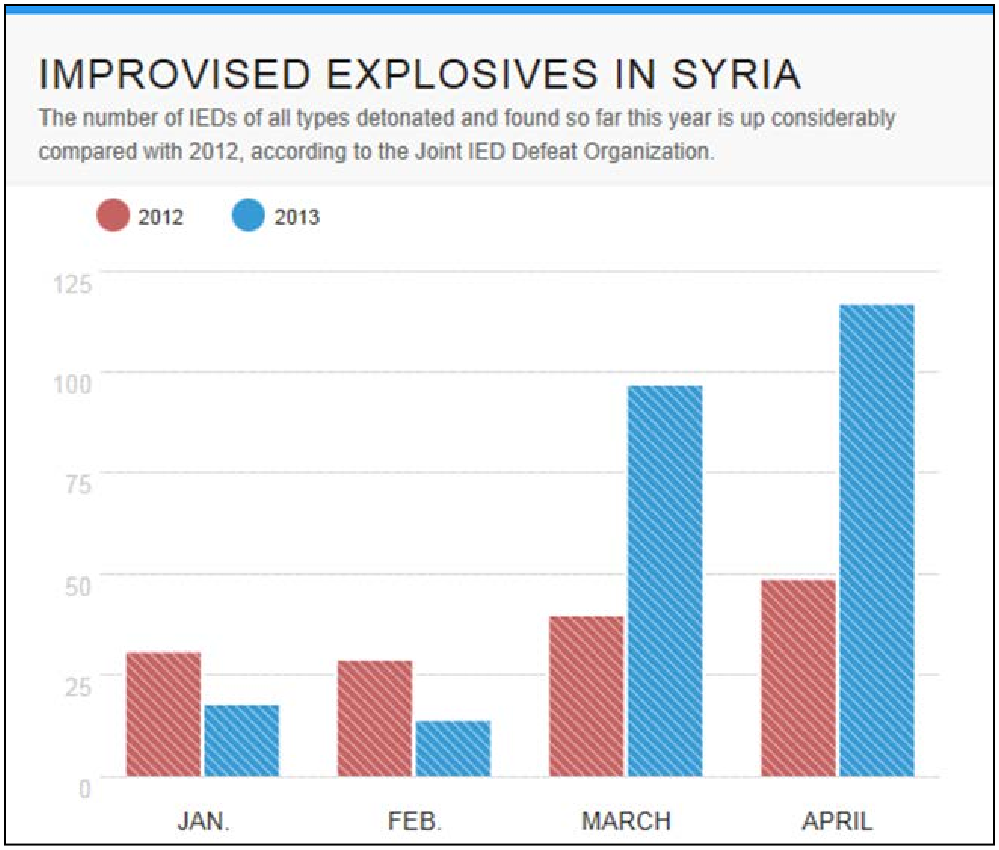


Figure 3: 2012-2013 graph of IEDs in Syria, *RAPID* Trend Report, 10 June 2013

The bombings on the eve of Mother's Day struck at an awkward moment for the Turkish Prime Minister, who was scheduled to confer with US President Barack Obama at the White House during the week of 13-17 May. Prime Minister Erdogan's Justice and Development Party (AKP), after recently celebrating 10 years in power, will face local and presidential elections in 2014 and general parliamentary elections the following year. The Reyhanli bombing incident embarrassed the AKP and underscored a potential stumbling block to its success in the coming elections. Opposition parties manipulated the incident to focus attention on growing public concern over Turkey's strident foreign policy stance toward Syria. While deploring the abuses Syrian President al Assad has heaped on his own people since the advent of the Arab Spring, most Turkish citizens retain a healthy respect for Syria's national sovereignty and fear that too much interference in its domestic affairs could drag them into a war, exacting a high price in blood and national treasure.

Shortly after the Reyhanli bombings, a local court took the unusual measure of imposing a reporting ban on the incident. A court order directed radio, television, and print media to refrain from covering the attack, whether in the context of its details, its implications and significance, or anything related to its victims. In effect, the media ban amounted to an extraordinary government-driven censorship decree. Turkish journalists and political opposition leaders were quick to allege that the root cause of the clampdown was a government desire to use the tragedy as a pretext for shutting down legitimate public debate over the AKP's increasingly unpopular foreign policy.

American media outlets, preoccupied with a lingering national focus on the previous month's Boston Marathon bombing, paid relatively little attention to the terrorist attack in Turkey. Reyhanli nevertheless surfaced as a subject of interest during a 14 May 2013 joint press conference held by President Obama and Prime Minister Erdogan in the White House Rose Garden. The president conveyed the condolences of the American people as he decried "the outrageous bombings that took place in Reyhanli."[8] Between NATO allies, the ramifications of twin VBIEDs detonated in a remote border town unknown to most Americans that had attained a stature of strategic international significance.

The events of 11 May 2013 proved to be a milestone in downward-spiraling Turkish-Syrian relations, and as noted earlier, a major embarrassment to Turkey's ruling Justice and Development Party. Until then, although an occasional artillery shell or relatively minor IED event disturbed the peace along Turkey's 559-mile border with Syria, most of Turkey's citizenry had been spared the horrors of the civil war that afflicted its neighbor to the south. Not that long ago relations between Turkey and Syria had been friendly. Indeed, shortly after coming to power in November 2002, Prime Minister Erdogan announced plans to pursue a "zero problems with neighbors" policy.[9] Yet the upheavals of 2011's Arab Spring brought consequences no one had foreseen. Once Erdogan openly called for the ouster of Syrian President Bashar al Asad for outrages committed against his own people, the two countries charted mutually hostile courses that may or may not lead to some future collision, but certainly promise to complicate the challenges US officials face in shaping American foreign policy in support of a stalwart NATO ally.

Figure 4. President Obama with Prime Minister Erdogan, whitehouse.gov, 16 May 2016

Notes

[1] Hasan Kanbolat, "Analyzing Reyhanli as a Reyhanli Resident," *Today's Zaman,* 16 May 2013.

[2] Hasa Kanbolat, "Looking At Syria From Hatay-Reyhanli," *Today's Zaman,* 22 July 2012.

[3] "Global IED Monthly Summary Report" (FOUO), *Joint Improvised Explosive Device Defeat Organization/Counter-IED Operations/Intelligence Integration Center,* May 2013.

[4] Glen Johnson and Patrick J. McDonnell, "Turkey Bombings Prompt Outcry Over Support for Syria," *Los Angeles Times,* 13 May 2013.

[5] Glen Johnson and Patrick J. McDonnell, "Turkey Bombings Prompt Outcry Over Support for Syria," *Los Angeles Times,* 13 May 2013.

[6] Jim Michaels, "Large Car Bombs Increasing in Syria," *USA Today,* 9 June 2013.

[7] Hasa Kanbolat, "Analyzing Reyhanli as a Reyhanli Resident," *Today's Zaman,* 16 May 2013.

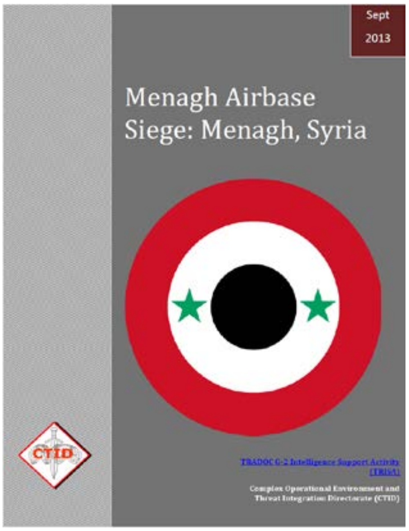
[8] "Joint Press Conference by President Obama and Prime Minister Erdogan of Turkey," *Office of the Press Secretary, The White House,* 16 May 2013.

[9] Andrew Finkel, "Viewpoint: What Now For Turkey's Ruling Party?" *BBC News, Europe,* 31 October 2012.

Menagh Airbase Siege: Menagh, Syria

Tactics and Techniques in Complex Operational Environments

by Rick Burns, OE Assessment Team (BMA Ctr)



Sept 2013

Menagh Airbase Siege: Menagh, Syria

CTID

TRADOC G-2 Intelligence Support Activity (TRISA)

Complex Operational Environment and Threat Integration Directorate (CTID)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

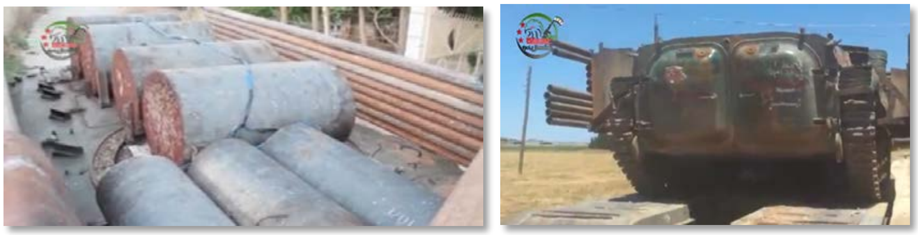


Figure 1. Specially-outfitted BMP VBIED loaded with explosive containers

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

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

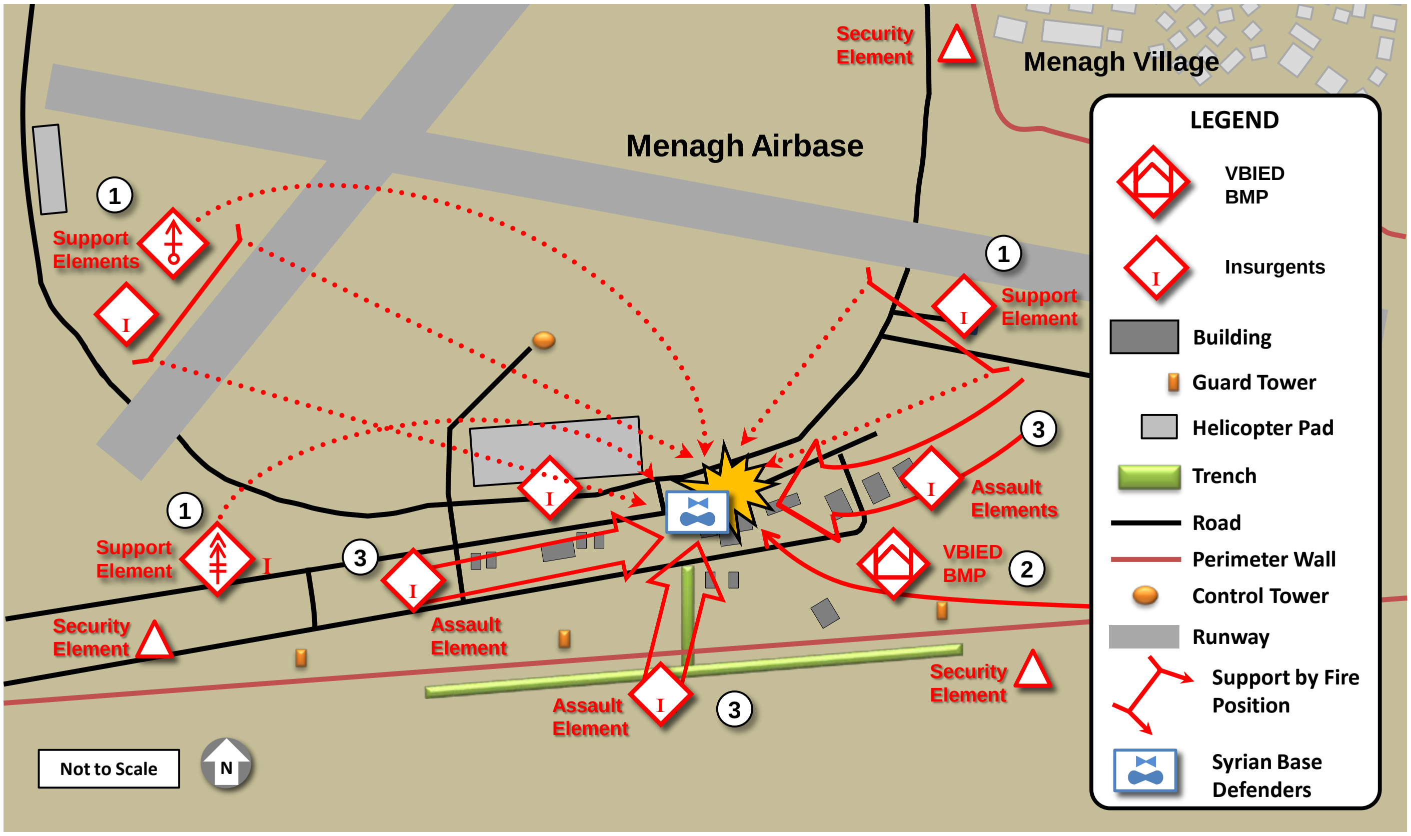


Figure 2. 5 August 2013 Menagh Airbase Attack, TRISA, 2013

ISIL reportedly formed the vanguard of the attack, with other units supporting. Nine brigades participated in the final attack on Menagh Airbase. The exact number of insurgents, however, is not known, as insurgent unit manning does not correlate with conventional organizational constructs. A brigade, for example, may not be more than a company-size element. It is certain that the number of insurgents outnumbered the small contingent left to defend what had become a barebones Menagh Airbase outpost.

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

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

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

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

CASE STUDY: MEXICAN DRUG CARTEL IED ATTACK ON LAW ENFORCEMENT

by Kris Lechowicz, Threat Assessment Team (DAC)

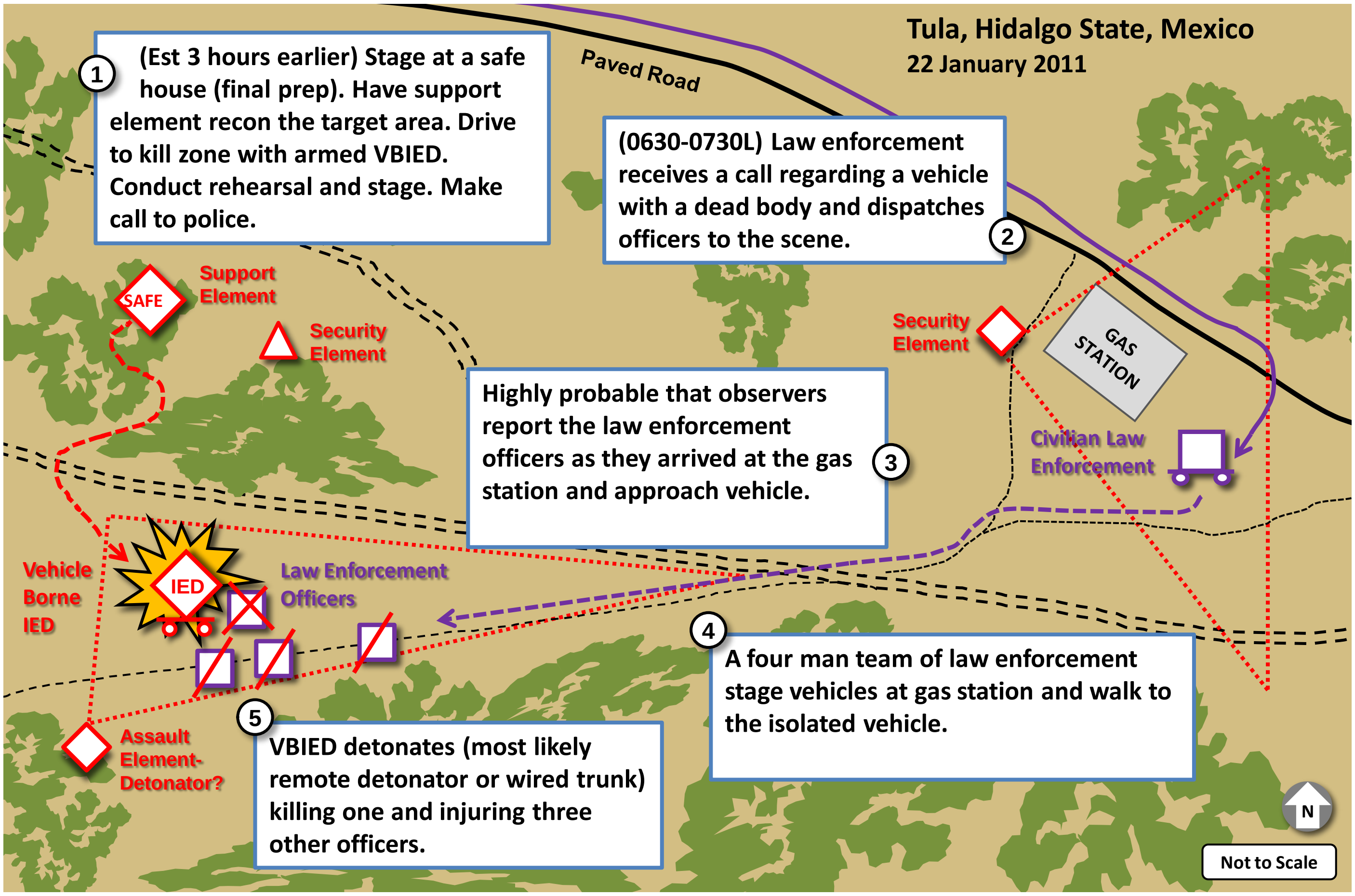
The Complex Operational Environment Threat Integration Directorate has the responsibility of creating complex operational environments (OEs) and dynamic hybrid threats (HT) that stress the capabilities of the US Army's training community. One example of real world threat integration can be found in one of CTID's current projects, *The Global IED Study,* which supports TRADOC's Counter-IED plan. [*The Global IED Study* is in progress and will be published in winter 2013.] This project focuses on IED tactics employed throughout US Army Combatant Commands (COCOMs). The IED threat is not a new concept for the US Army in persistent conflict; however, the following example from Mexico exhibits particular techniques in planning and conduct of an IED execution. This article illustrates a case study and doctrine that can be used for scenario developers as a composite example for integration into the US Army's training community.

The case study examines an IED attack that took place in Tula, Hidalgo State, Mexico on 22 January 2011. It provides powerful insight into a tactic that could occur during current or future US military operations. This tactic can be replicated by the opposing force (OPFOR) within the training environment. Attack analysis uses current training principles from the soon-to-be published *TC 7-100.3 (Irregular Opposing Forces)* and illustrates a particular technique. This case study indicates the role that criminal elements such as cartels can provide as a lethal threat to US military, law enforcement, or coalition forces in a complex OE.

Background on IED Attack Case Study (Mexico)

On 22 January 2011, Mexican police received an anonymous phone call regarding a dead body in a trunk of an abandoned car in Tula, Hidalgo State, Mexico. This is not the first time a body has been the bait for an IED ambush on first responders in Mexico. The authorities responded accordingly with four officers being dispatched. The officers, upon investigation, found a white Volkswagen Bora in the vicinity of a convenient store parking lot. Reporting differs at this point. However, the IED detonated when the officers were either moving toward the vehicle or upon examining the trunk. All four officers were wounded by the explosion. This action indicates that the IED was either command detonated or victim-initiated with a mechanism linked to the trunk. The commander of the unit later died of his wounds at a nearby medical facility. Reporting indicates that *Los Zetas* drug cartel was responsible for the attack.

Los Zetas are a feared and infamous drug trafficking organization (DTO) within Mexico. *Los Zetas* original members were former elite Mexican Military Special Forces. The group is highly trained and actively recruits from other military sources including Guatemalan Special Forces, law enforcement agencies, and street gangs. The *Zetas* are familiar with law enforcement/military procedures, skilled at intelligence collection, and trained in unconventional warfare. The US Armed Forces could face this type of highly trained criminal organization in multiple OEs worldwide. The diagram below demonstrates the analyst's interpretation of the events leading to the IED attack that could be used for the training community and future training scenarios.



Tula, Hidalgo State, Mexico

22 January 2011

1 (Est 3 hours earlier) Stage at a safe house (final prep). Have support element recon the target area. Drive to kill zone with armed VBIED. Conduct rehearsal and stage. Make call to police.

2 (0630-0730L) Law enforcement receives a call regarding a vehicle with a dead body and dispatches officers to the scene.

3 Highly probable that observers report the law enforcement officers as they arrived at the gas station and approach vehicle.

4 A four man team of law enforcement stage vehicles at gas station and walk to the isolated vehicle.

5 VBIED detonates (most likely remote detonator or wired trunk) killing one and injuring three other officers.

Figure 1. DTO IED attack Hidalgo Mexico 22 January 2011, TRISA, June 2013

Analysis of the IED Attack

In the past, that law enforcement unit engaged and targeted the *Los Zetas* cartel. The death of the commander may have been an unexpected coincidence but that premise is unlikely. The *Zetas* may have merely wanted to make an example of the law enforcement agency. They did specifically place the call to that particular unit; however, the *Zetas* most likely selected the commander as the primary target and conducted surveillance to identify how the unit responded to similar calls and noted their tactics. The *Zetas* hypothetically could have gathered intelligence about the team's tactics, techniques, and procedures (TTP) and work schedules, and planned the ambush which is consistent with the cartel's military background of conducting reconnaissance in support of military operations.

The IED was placed in a remote area and the blast was relatively small (though deadly) and precise. The *Zetas* (despite their reputation for extreme violence) appear to have planned for limited collateral damage. This could be due to *Los Zetas'* lessons learned from the Colombian cartels' large-scale bombing in the late 1980s which ultimately was one of the organizational downfalls, and ironically, began the rise of the Mexican cartels. This small-scale attack still sent a clear warning to law enforcement that would attempt to hinder Los Zetas' criminal operations.

The possibility of this IED TTP migration to United States is low to medium. The small, pinpoint, no collateral damage IED ambush could be a useful TTP for gang members associated with the cartels to eliminate key rival gang members or suspected informants. It is highly unlikely that either organization would want to draw the attention of attacking US law enforcement. Any use of an IED would increase the organizational signature of the cartel and would draw unwanted attention from US Federal Agencies. However, many cartels see the gangs as expendable foot soldiers and if the target was important enough would go to extreme measures. Nonetheless, this incident provides a good case study for scenario developers to create for the training community. The following diagram shows how CTID uses real-world examples in the building of doctrine that translates to the training community.

Characteristics from TRISA's TC 7-100.3 and Similarities to the Attack Analysis in Mexico:

- Discourage enemy activity in certain areas. (The IED attack was a warning to keep law enforcement from disrupting cartel operations.)
- Demoralize personnel of the enemy force, members of the enemy leadership, or the general populace. (The death of the commander was a targeted message for the law enforcement.)
- Discredit enemy leadership and degrade its legitimacy. (Attacks such as these affect the legitimacy of law enforcement's perceived ability to combat cartel elements.)
- Destroy enemy leadership, command and control, and/or cohesion (Common tactics and techniques include assassination and kidnapping).

Comparing TC 7-100.3 and the Analysis of the Attack in Hidalgo

TC 7-100.3 states that an assassination is a deliberate action to kill political leaders or people designated as a very important person (VIP). The terrorist group, or in this case the drug cartel, assassinates or murders individuals it cannot intimidate or who have some symbolic significance for the enemy. This is the case with the attack at Hidalgo, Mexico. The attack was a likely a warning to law enforcement as well as a means to demonstrate that the law enforcement were powerless to protect themselves, much less the community.

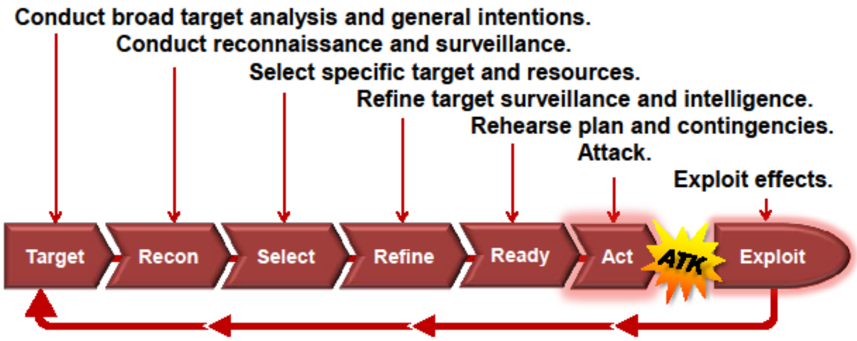

Conduct broad target analysis and general intentions.
Conduct reconnaissance and surveillance.
Select specific target and resources.
Refine target surveillance and intelligence.
Rehearse plan and contingencies.
Attack.
Exploit effects.
Target
Recon
Select
Refine
Ready
Act
ATK
Exploit

Figure 2. Model of a Planning Cycle and Learning Continuum

Terrorist groups sometimes refer to these killings as "punishment." *Los Zetas* likely could have viewed this attack as punishment for past law enforcement operations conducted by that unit.

Many targets of assassination are symbolic and often have a great psychological impact on the "enemy" as in this case of law enforcement). This type of attack can demoralize not only law enforcement but also the community in general, and *Los Zetas* gains power and influence through fear and intimidation. TC 7-100.3 states that assassination methods include remotely-detonated bombing, the use of firearms, and poisoning. A target's vulnerabilities often determine the method of assassination. The *Los Zetas* targeted and conducted surveillance to find the best method of eliminating the threat while making a violent demonstration to the community.

Case studies like the IED attack that took place in Tula, Hidalgo State, Mexico are significant examples that can be included in training to enhance realistic scenarios. This article shows the potential role that criminal elements such as drug cartels provide as a lethal threat to US military, law enforcement, or future coalition forces in a complex OE.

TC 7-100.3 has captured many of the basic concepts of irregular force threats that would empower scenario developers in creating a realistic training environment. Doctrine embeds the lessons learned from real-world threats in order to create complex and composite conditions that challenge the warfighter and improve US Army performance in its missions.

RECONNAISSANCE AND THE THREAT CYBER ATTACK LIFE CYCLE

Complex Cyber Threats in an Operational Environment

by Jerry England, Threat Assessment Team Leader (DAC)

The future of military operations will include an increased reliance on information and communications technology (ICT) on all sides of a potential conflict. Much of the concern for this new reality is the exposure of advanced military systems and information resources to cyber attack.[1] According to a report on the US Cert Website, at least 18 countries currently engage in one or more types of cyber operations.[2] This does not account for the many countries that are the sources for malicious attacks of which 10 are responsible for 66% of the attacks in 2012.[3] For this reason, understanding the techniques and tactics of cyber attacks is a useful approach to addressing the emerging element of the hybrid threat.

Cyber Attack Life-Cycle

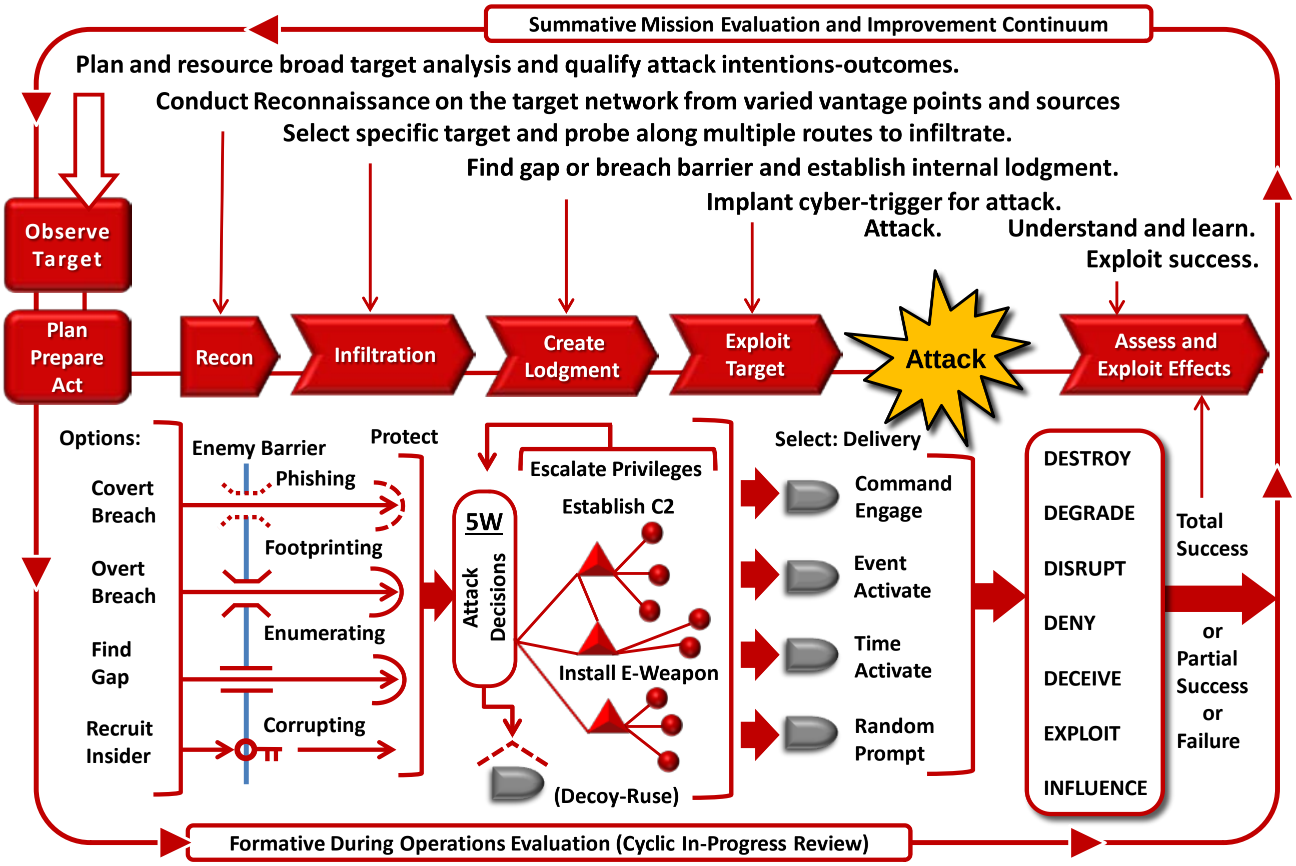


Figure 1. Threat Cyber Attack Life Cycle, TRISA

The Threat Cyber Attack Life Cycle is a composite product based on various "anatomy of an attack" articles from computer security firms and computer security sites.

A part of this understanding is devising a framework for the threat cyber attack based on threat tactics and terminology. The discussion below is intended to propose a model for the threat cyber attack lifecycle that is based on analysis of threat terms, technology, tactics, and empirical events. Additionally, a discussion on the first step of the life cycle – reconnaissance – is included as the first part of a series of articles on the Threat Cyber Attack Life Cycle.

Threat Cyber Attack Life Cycle

The Threat conducts cyber attacks through a six-step process designated the threat cyber attack life cycle (T-CALC). The six steps, however, do not occur sequentially and the Threat can skip or repeat steps as appropriate. The steps in the T-CALC are as follows:

- Reconnaissance.
- Infiltration.
- Create Lodgment.
- Exploit Target.
- Deliver Attack.
- Assess and Exploit Effects.

Reconnaissance

Reconnaissance in the T-CALC is a type of computer exploitation operation designed to identify and select targets within the information space. Examples include locating individuals' online personas, diagramming the networks in high value systems and organizations, and harvesting information in order to build a list of actionable targets and information requirements for high value/high priority targets. The objective is to document as much of the technical specifications of the target as possible. The software, the architecture of the network, the battle rhythm of users, and the public/private, infrastructure, are all examples legitimate cyber reconnaissance nodes, links, and relationships that require attention. The reconnaissance phase of the T-CALC relies on mainly open source research to locate those organizations and formations of interest that the Threat deems necessary for cyber attack operations to achieve its objective.[4] Potential Threat methods that might be used to exploit a network include the following—

- Footprinting the network using publically available information to diagram publicly accessible information on target network.
- Port scanning with tools for unsecured devices and websites helps locate unsecured access points to targeted networks.
- Analyzing social networks/media to determine official and unofficial relations between high value targets and named area of interest.
- Enumerating hosts, applications, and users applies a systematic approach to predicting how users are identified and how systems are configured.
- Locating devices that are connected to the Internet which are not actual computers but receive commands remotely.

Threat reconnaissance efforts will establish the priorities for future cyber operations, and initiate the T-CALC process. The reconnaissance phase builds a picture of the target infrastructure, weapons, and resources within the information space through online pattern of life analysis and vulnerability exploitation.[5] To maintain the initiative and the ability to strike first, a cyber threat uses software and other analytical tools to improve its cyber reconnaissance efforts. Delays can give the Threat's enemies an opportunity to develop defenses that would stop the cyber attack or limit its effects.

A cyber reconnaissance table [see page 29] can assist the Threat to manage its collection effort by helping to designate priorities, determine available assets against prospective targets, and to assist in identifying vulnerabilities in enemy infrastructure, weapons systems, informational resources, and any other potential targets within the information space. The Threat takes proper security measures and uses a variety of cyber tools including malware attached to phishing emails to map the enemy's network and locate vulnerabilities anonymously.[6]

The Threat may also recruit external resources during the reconnaissance phase for its cyber activities. Recruited individuals that can access a targeted network are of particular interest as the insiders can provide an anonymous route into the network with a low probability of detection by the enemy. The hacktivist group Anonymous used this phase of the attack lifecycle to recruit individuals to use its “Low Orbit Ion Cannon” (LOIC) DDOS tool to attack a variety of organizations.[7] The Threat may also leverage criminal elements that have already developed tools to breach secure information systems for financial gain when the Threat does not possess the current technical skills or when anonymity is of utmost importance. The Russian cyber criminal gang known as the Russian Business Network (RBN) is believed by many cyber experts to have assisted the Russian government to launch cyber offensive operations against Georgia.[8] The recruiting of individual citizens using patriotic themes and messages can allow the Threat to expand their operational capacity potentially to include online users. For roughly 10 years, China has been recruiting IT personnel from business and academia to serve as information warfare militias in order to increase coordination between military and civilian efforts to conduct cyber operations.[9]

Reconnaissance Table

Target NAI	Priority	Time Frame	Social Media	Spoof Signal	Footprint	Enumerate
Govt. Official	1		x		x	x
Sensors	2			x	x	x
Electrical Grid	3		x		x	x
Telecom Networks	4		x	x	x	x
Pol. Blogs	5		x		x	x

Figure 2. Reconnaissance Table, TRISA

The Threat may test perception management themes and messages during the reconnaissance phase. This enables the Threat to determine the best method to construct their information warfare campaign and use other products in order to generate interest and to facilitate the compromise of designated targets. Understanding the target’s interests in certain topics may help the Threat facilitate phishing operations as current events and sensitive subject matter is used to spark interest in emails and other forms of communications used as attack vectors. Sophisticated spear phishing techniques requiring advanced profiling of potential targets, and analysis of social media networks indicate a common Threat capability.[10]

Proxies are information warfare resources that can obscure successful attribution of an attack. The use of proxy servers to mask the source of reconnaissance efforts is a common practice among hackers and anyone who wishes to remain anonymous on the Internet.[11] Other organizational proxies include criminal groups, online activists, and in some cases business personnel and students who exploit and share information for patriotic purposes. Informational resources are designed to distribute malware and compromise ICT without the knowledge of the enemy user.

Implications for Training

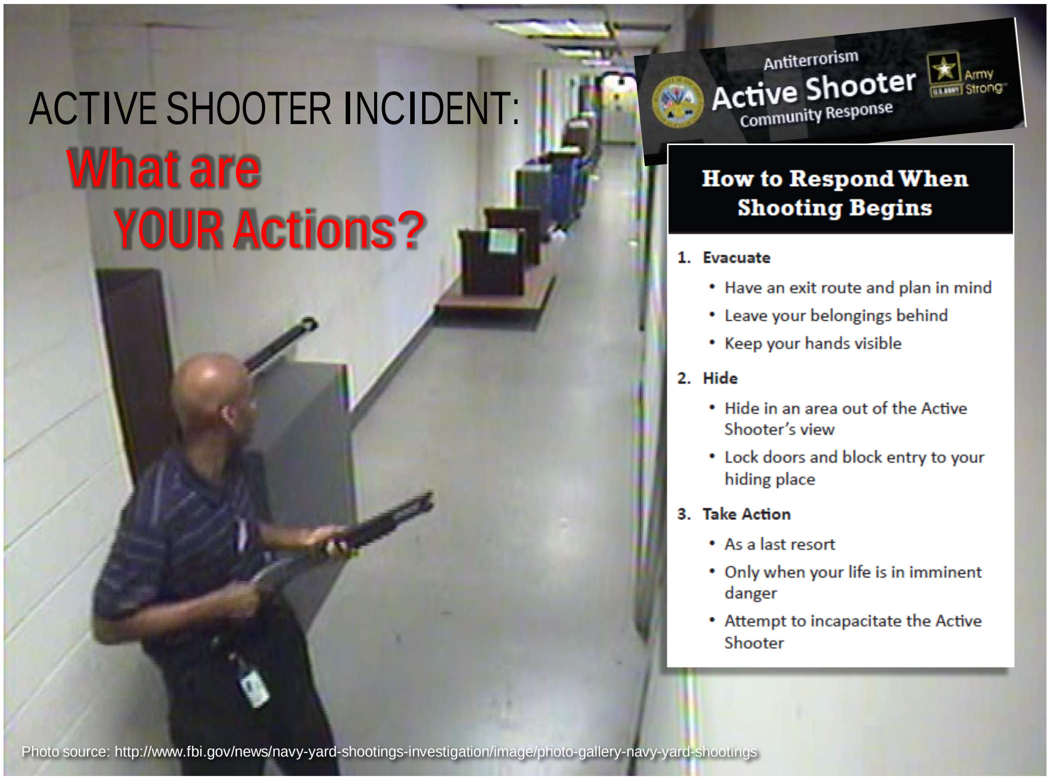
By applying the T-CALC in situations of a possible or likely cyber attack, or when the Threat has demonstrated the ability to achieve cyber effects, analysts can establish a model from which to base logical analysis in these types of situations. Although the T-CALC is presented sequentially it should be noted that the Threat is adaptive enough to apply those steps most necessary to the current situation and may skip steps or repeat certain activities as needed. For example, the launch of a denial of service attack could be deception measure to mask an in depth reconnaissance effort. Even in this situation an analyst could apply the model to investigate the root of the attack and possibly how the system was initially breached, thus possibly preventing a similar attack. Even when the attack is well known, US analysts should have a concept of how it was developed and the process involved in launching the cyber attack by applying the T-CALC. Implications for consideration of the T-CALC as the model for OPFOR cyber operations are as follows:

- Hacker groups are proving that a small group of experts can be the cause of significant strategic-level effects, thus a method for analyzing their activities can be used to determine both capabilities and intentions of potential adversaries.
- The Threat will disregard traditional notions of national sovereignty with regard to borders, networks and infrastructure, and attacking targets both locally and abroad. By understanding the attack life cycle, analysts may begin to infer the purpose and attribute the source of cyber attacks.
- The Threat will use a combination of existing offensive cyber methodologies, newly discovered vulnerabilities, and customized exploits in an effort to achieve scalable effects on targeted systems. The attack lifecycle will allow analysts to determine how to categorize the sophistication of the attackers.
- Cyber reconnaissance is the first step in the Threat Cyber Attack Life Cycle and can present insight into the enemy's intelligence requirements.

Notes

[1] DoD Defense Science Board, Task Force Report: Resilient Military Systems and the Advanced Cyber Threat, January 2013, p 1.
[2] Julie Mehan, Are We Really in a Cyberwar? The Dangers of Hype, slide 38.
[3] Symantec, Internet Security Report Appendix 2013, Figure A.7, p 11.
[4] Symantec, Internet Security Threat Report 2013, p 21.
[5] Symantec, Internet Security Threat Report 2013, p 21.
[6] Mandiant, APT1 Exposing One of China's Cyber Espionage Units, p 28; Imperva, Hacker Intelligence Summary Report, Anatomy of an Anonymous Attack, p 12.
[7] Imperva, Hacker Intelligence Summary Report, Anatomy of an Anonymous Attack, p 2.
[8] Khatuna Mshvidobadze, Analysis: Is Russia on the Wrong Side of the Net?, Jane's Defence Weekly, 28 February 2011.
[9] Northrop Grumann, Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation, prepared for the US-China Economic and Security Review Commission, 9 October 2009.
[10] Symantec, Internet Security Threat Report 2013, p 36.
[11] Imperva, Hacker Intelligence Summary Report, Anatomy of an Anonymous Attack, p 12.

TRISA-CTID Combating Terrorism with Awareness: HQDA "Evacuate-Hide-Take Action" Guide



How to Respond When Shooting Begins

1. **Evacuate**
   - Have an exit route and plan in mind
   - Leave your belongings behind
   - Keep your hands visible
2. **Hide**
   - Hide in an area out of the Active Shooter's view
   - Lock doors and block entry to your hiding place
3. **Take Action**
   - As a last resort
   - Only when your life is in imminent danger
   - Attempt to incapacitate the Active Shooter

Photo source: http://www.fbi.gov/news/navy-yard-shootings-investigation/image/photo-gallery-navy-yard-shootings

THREAT PRODUCTS FOR COMPLEX ENVIRONMENTS

by CTID Operations

A Sampler of TRISA-CTID Products & Processes
Complex OE and Threat Integration Directorate 2013
TRISA
TRADOC G2 Intelligence Support Activity
Fort Leavenworth, Kansas
Hybrid Threat
Exercise Design
Opposing Force Tactics
Irregular Opposing Forces
Decisive Action Training Environment
Worldwide Equipment Guide
Hybrid
EXD
Terror
OE
TTP
DATE
WEG
Training
Enemy
OEA
Threat
Know the THREAT — Know the ENEMY

Sampler of Products:

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

RAFTE-Africa
Regionally Aligned Forces
Training Environment

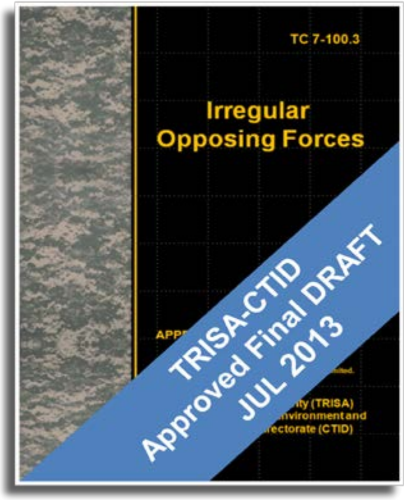
COMING in 2013:

TC 7-100.3
Irregular Opposing Forces

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

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

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



Q: Do you need a copy of Irregular Opposing Forces?

A: AKO access, see* CTID *Approved Final Draft TC 7-100.3
https://www.us.army.mil/suite/doc/40913959

Q: When will TC 7-100.3 be published by HQDA?

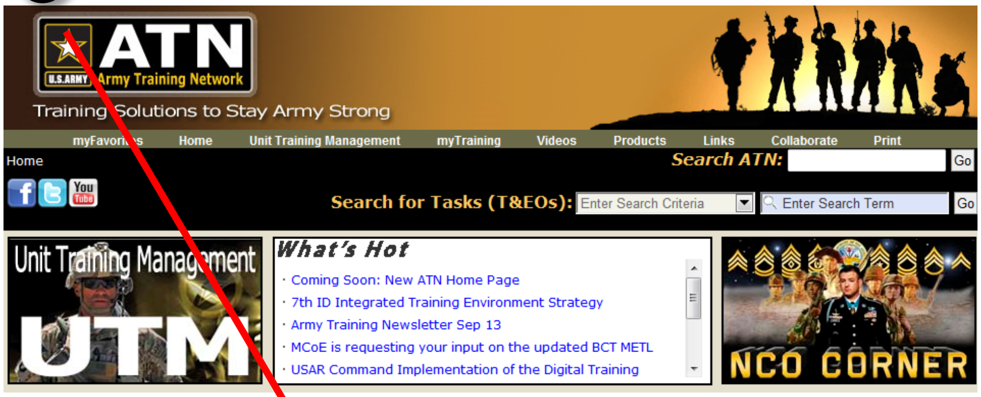
A: TC 7-100.3 is at the Army Publishing Directorate (APD) for review and approval. Publication is planned for 2013.

Q: Do you have a question on a Threat or Opposing Force (OPFOR) issue that CTID can assist you with in identifying a solution?

A: Send us a request for information (RFI).

Go to Army Training Network

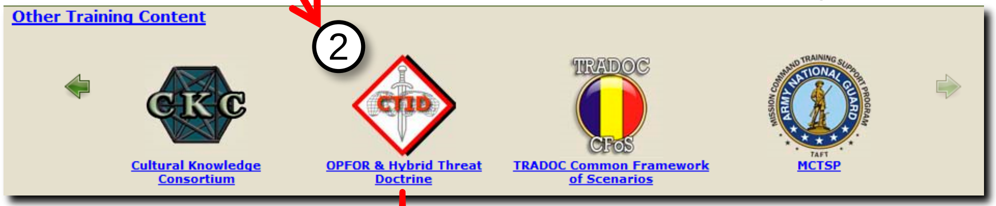
1 Go to https://atn.army.mil/ with DOD-Approved Login



What's Hot

- Coming Soon: New ATN Home Page
- 7th ID Integrated Training Environment Strategy
- Army Training Newsletter Sep 13
- MCoE is requesting your input on the updated BCT METL
- USAR Command Implementation of the Digital Training

Scroll to CTID "Red Diamond" logo & "*click*"



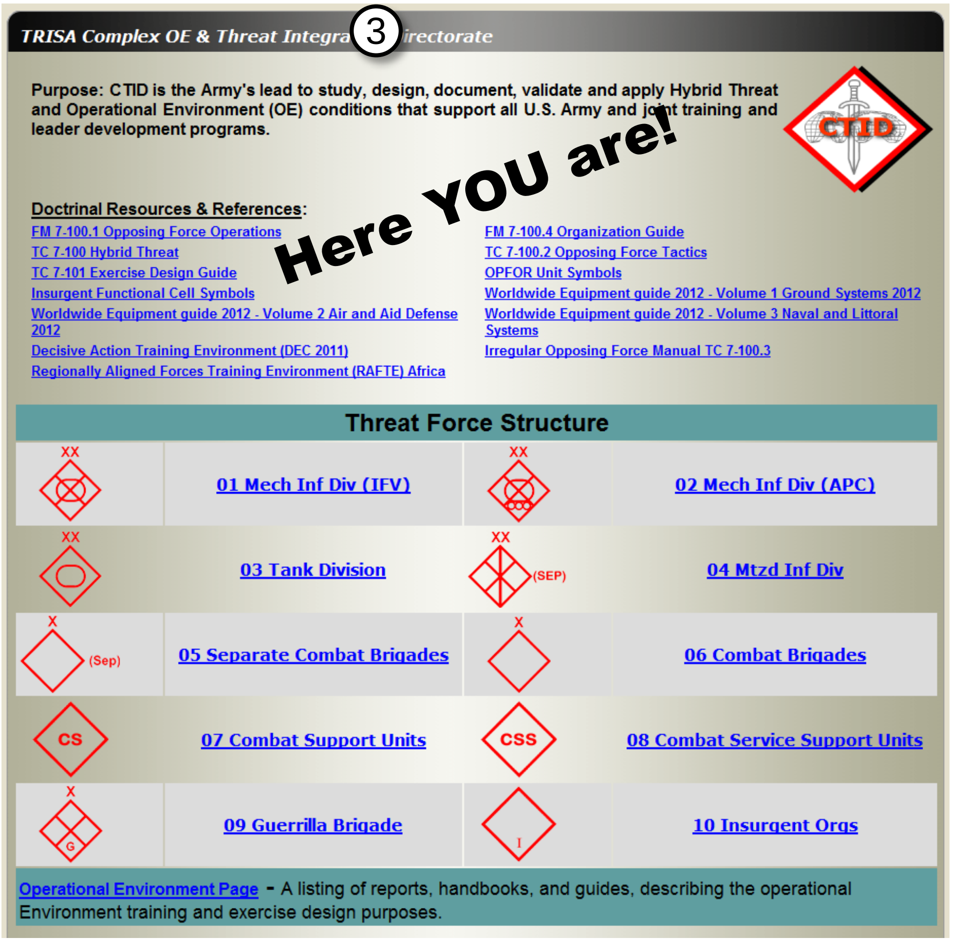
Other Training Content

Cultural Knowledge Consortium

OPFOR & Hybrid Threat Doctrine

TRADOC Common Framework of Scenarios

MCTSP



TRISA Complex OE & Threat Integra[3]irectorate

Purpose: CTID is the Army's lead to study, design, document, validate and apply Hybrid Threat and Operational Environment (OE) conditions that support all U.S. Army and joint training and leader development programs.

Doctrinal Resources & References:

- FM 7-100.1 Opposing Force Operations
- TC 7-100 Hybrid Threat
- TC 7-101 Exercise Design Guide
- Insurgent Functional Cell Symbols
- Worldwide Equipment guide 2012 - Volume 2 Air and Aid Defense 2012
- Decisive Action Training Environment (DEC 2011)
- Regionally Aligned Forces Training Environment (RAFTE) Africa
- FM 7-100.4 Organization Guide
- TC 7-100.2 Opposing Force Tactics
- OPFOR Unit Symbols
- Worldwide Equipment guide 2012 - Volume 1 Ground Systems 2012
- Worldwide Equipment guide 2012 - Volume 3 Naval and Littoral Systems
- Irregular Opposing Force Manual TC 7-100.3

Threat Force Structure			
XX	01 Mech Inf Div (IFV)	XX	02 Mech Inf Div (APC)
XX	03 Tank Division	XX (SEP)	04 Mtzd Inf Div
X (Sep)	05 Separate Combat Brigades	X	06 Combat Brigades
CS	07 Combat Support Units	CSS	08 Combat Service Support Units
X G	09 Guerrilla Brigade	I	10 Insurgent Orgs

Operational Environment Page - A listing of reports, handbooks, and guides, describing the operational Environment training and exercise design purposes.

Threats to Know—*CTID Daily Update* Review

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

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

U.S. Army TRADOC G2 Intelligence Support Activity

TRISA

CTID Daily Update

Fort Leavenworth, Kansas

4 September. HACKER WAR: Anonymous takes down Syrian Electronic Army

Syria: Syrian Army crushes US-backed rebel assault from Jordan

6 September. Al-Qaeda: Al-Qaeda group killed MSF doctor in **Syria**, NGO says

Pakistan: US drones kill 4 Haqqani Network fighters in **North Waziristan** strike

9 September. Philippines: Moro National Liberation Front (MNLF) fighters attack **Zamboanga**, take hostages

Cyprus: Syrian warplanes flee after testing defenses at British air base in Cyprus

11 September. Libya: Explosion damages Libya's Foreign Ministry in **Benghazi** on anniversary of 9/11 attack on US Consulate

Central African Republic: Toll from CAR fighting nears 100

13 September. Al-Qaeda: Al-Qaeda chief calls for attacks on US in 9/11 speech to followers

US: Floods in **Boulder, Colorado** kill three, force thousands to flee

18 September. US: Victims of Washington Navy Yard massacre identified

Afghanistan: US drone strike kills six Taliban in **Kunar** province

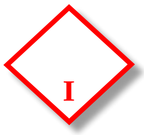
20 September. Al-Qaeda: AQAP kills 56 Soldiers, policemen in southern **Yemen**

Syria: Thousands of Syrians caught in border shelling

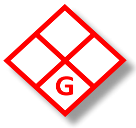
30 September. Al-Qaeda: Free Syrian Army units ally with al-Qaeda, reject Syrian National Coalition, and call for sharia

Sudan: At least 140 killed in Sudan unrest

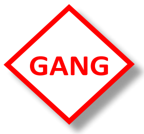
Know *Irregular Opposing Force* Symbols:TRISA-CTID



Insurgent



Guerrilla



Criminal

CTID Points of Contact

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

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

Liaison Officer (UK)
[pending arrival]

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

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

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

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

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

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

Train-Educ-Ldr Dev Team Leader 684.7923
Mr Walt Williams walter.l.williams112.civ@mail.mil

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

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

TELD Team/NTC-JMRC LNO Mr Mike Spight
michael.g.spight.ctr@mail.mil ISC 684.7974

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

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

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

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

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

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

CTID Mission

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

What We Do for YOU

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

YOUR Easy e-Access Resource

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