U.S. TRADOC G2 Intelligence Support Activity

TRISA

Red Diamond

Complex Operational Environment
and Threat Integration Directorate

Fort Leavenworth, KS Volume 4, Issue 10 OCT 2013

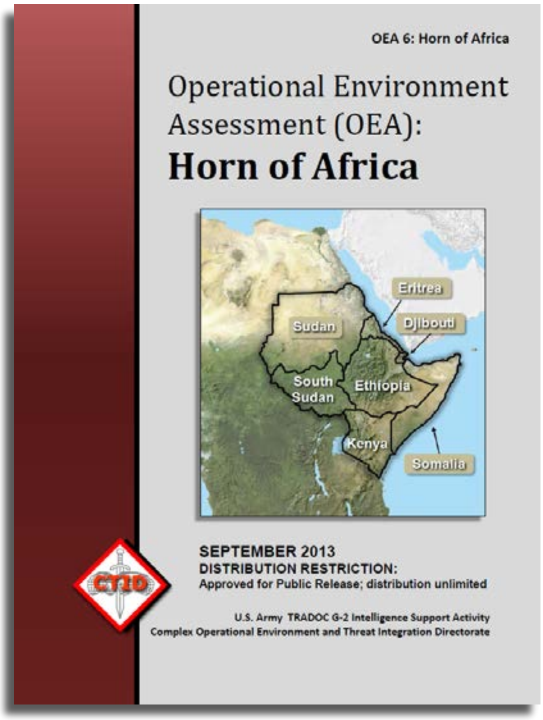
INSIDE THIS ISSUE

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

OPERATIONAL ENVIRONMENT ASSESSMENT: HORN OF AFRICA

by Angela Wilkins, OE Assessment Team Lead (BMA Ctr)

The *Horn of Africa Operational Environment Assessment* (OEA) is now available for download from AKO and ATN. TRISA-CTID first produced this OEA in 2008. The new version reflects the Horn of Africa's current state according to PMESII-PT variables. The Horn of Africa (HOA) includes seven countries now that Sudan split: Djibouti, Eritrea, Ethiopia, Kenya, Somalia, Sudan, and South Sudan.


OEA 6: Horn of Africa

Operational Environment Assessment (OEA):
Horn of Africa

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

While certain conditions have not changed significantly in terms of culture and economics, the effects of ongoing conflict (such as between Eritrea and Ethiopia) and the continued presence of threat groups (al Shabaab in Somalia, for example) negatively shape the HOA operational environment (OE). In addition to significant terrorist group presence, the HOA OE houses repressive governments, impoverished and only moderately literate populations on average, significant health issues, displacement of citizens, human rights violations, violence, and newly emerging information and technology capabilities. Existing and potential humanitarian, security, and antiterrorism missions are abundant in the Horn of Africa.

Operational Environment Assessments (OEAs) are comprehensive documents detailing conditions of an operational environment (OE) based on the PMESII-PT [Political, Military, Economic, Social, Information, Infrastructure, Physical Environment, and Time] variables.

RED DIAMOND TOPICS OF INTEREST

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

This issue of TRISA ***Red Diamond*** spotlights the *Horn of Africa Operational Environment Assessment* (2013). This document is a major update on seven states in the HOA. For training, another document published in June by TRISA-CTID is the *Regionally Aligned Forces Training Environment (RAFTE)-Africa*.

Updated information since the publication of the Threat Report on the Camp Bastion Attack in Afghanistan reveals recently released details of what occurred in the attack on the airfield. Another Threat Report assesses the insurgent attack on a shopping mall in Nairobi, Kenya.

Entities such as guerrillas and insurgents are examples that appear to lack concise definition. To know a threat and know an enemy, an article offers considerations to describe and understand these threats in training.

Criminality in the context of a Hybrid Threat (HT) for training addresses how to integrate criminal activities in training exercises. Dynamic changes and capabilities of an Opposing Force (OPFOR) in a Combat Training Center (CTC) rotation present the complexities encountered in a persistent conflict environment.

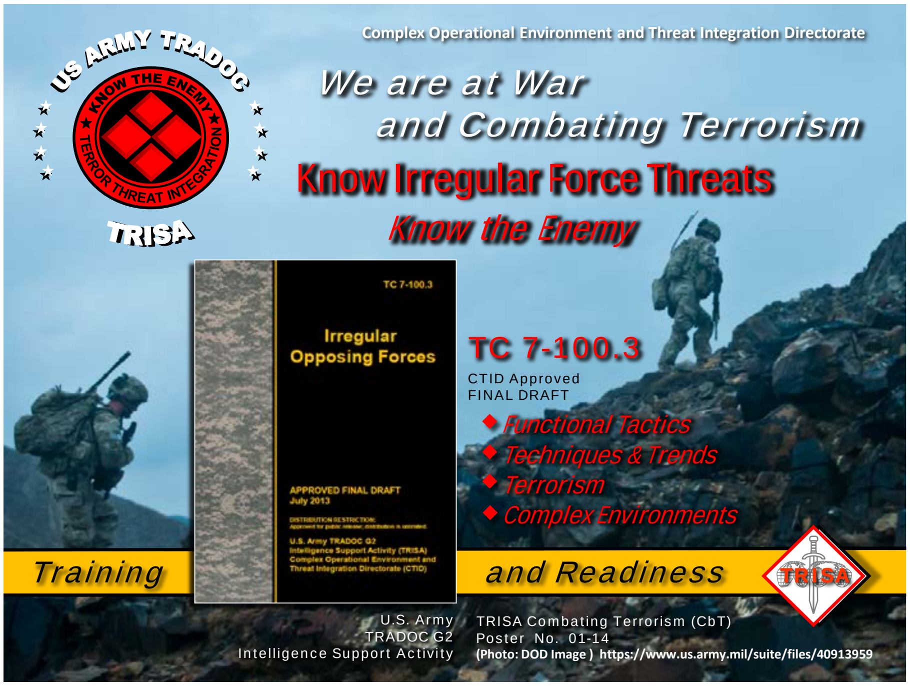
The cyber threat and electronic infiltration tactics and techniques are the focus of an article on capabilities and effects of computer warfare and information attack.

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.



(Photo: DOD Image) https://www.us.army.mil/suite/files/40913959

Director’s Corner:
Thoughts for Training Readiness

by Jon Cleaves, Director, Complex Operational Environment and Threat Integration Directorate (TRISA-CTID)

The conditions we have put, and will continue to put, into training at our CTCs, units, and schools are neither Afghanistan nor the Cold War.

If someone wonders why decisive action events at a CTC do not look like Afghanistan, it is because that is not where we will deploy next.

Maybe the next thing we do looks somewhat like Afghanistan and has a heavy COIN component. Even if that is true, it will not be Afghanistan – the manifestations of the operational variables will all be different to one degree or another. Just in the infrastructure variable alone there pretty much have to be major differences, as Afghanistan is without significant industrial processes, which would provide many other potential OEs with dangerous capabilities.

Maybe the next thing we do is deploy to enforce a Zone of Separation between two states with significant military hardware, possibly even tactical nuclear weapons. The fact of a large number of shoulder-launched ATGMs, or the presence of an artillery piece, does not make that battlefield the “Cold War.”

Amateurs, or even worse, professionals with agendas, are observing your training and saying some pretty inappropriate things about it. Our Army has been and will continue to be called upon to do a very wide variety of missions in highly divergent OEs. The Threats program does not make conditions to fight the last war; it makes conditions that realistically challenge your training objectives. We would not suggest that you fight a tank battle in a clear space devoid of urban terrain or civil populations. That does not mean that rocket batteries, UAVs, and electronic warfare are not going to be present just because they are not a major characteristic of our fights today.

Decisive action training is training for task proficiency without the benefit of knowing exactly where one is going or in what OE one will be operating. Our program provides you realistic threats taken from those available in likely OEs of today and the near future.

Help us educate those around us about what this means and how important it is to our Army. Start with anyone using the words “Cold War” in a declarative statement.

Jon
jon.s.cleaves.civ@mail.mil

Army Readiness and the Future

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

Guerrilla and Insurgent: Describing Threats in Complex Environments

Complex Variables in an Operational Environment (OE)

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

Knowing the threat and knowing the enemy is a fundamental aspect of military plans and operations. Consistent with the concept of "knowing" is the ability to clearly describe a particular threat and/or enemy and ensure a common understanding among tactical participants. As cogent as this statement appears, some significant categories of irregular forces lack a commonly accepted US Army definition. Neither the Army Doctrine Reference Publication (ADRP) 1-02, *Terms and Military Symbols* (2013) nor the US Department of Defense (DOD) *Dictionary of Military and Associated Terms* states a definition for *guerrilla* or *insurgent*.[1] This absence of definition poses an adverse impact on Army training readiness.

When no DOD definition exists for a term, the Army doctrinal norm is to use a general-use dictionary definition. However, lack of a concise definition for these two terms hampers effective assessment and analysis of similarities and differences in motivations, purpose and intent, and organizational capabilities and limitations. In principle, a succinct definition of each term enhances situational awareness and situational understanding of how guerrillas and insurgents may operate as separate and independent organizations, or may cooperate as associated, affiliated, or integrated organizations and units. In the cases of a guerrilla and an insurgent, definitions differ among several respected dictionaries and suggest that the Army requires definitions to enhance an accurate description of a guerrilla and an insurgent.

A casual Internet search of dictionaries confirms the diversity of "common" definitions for *guerrilla* and *insurgent*. Examples demonstrate that some similarities but differences exist and may be acceptable for common discussion but may not provide the precision required when attempting to identify a threat or enemy in complex military operations. Three examples of dictionary definitions for *insurgent* follow:

- A person who fights against an established government or authority; a person who revolts against civil authority or an established government; especially**:** a rebel not recognized as a belligerent; one who acts contrary to the policies and decisions of one's own political party.[2]
- A person who is a member of a group that is fighting against the government of their country.[3]
- One who is insurgent; [as an adjective] rising in revolt against established authority, especially a government; rebelling against the leadership of a political party.[4]

Three dictionary definitions for *guerrilla* are similar in variance. Differences are identifiable in examples as follows:

- A member of a usually small group of soldiers who do not belong to a regular army and who fight in a war as an independent unit; a person who engages in irregular warfare especially as a member of an independent unit carrying out harassment and sabotage.[5]
- A member of an unofficial military group that is trying to change the government by making sudden, unexpected attacks on the official army forces: guerrilla warfare.[6]

- A member of an irregular, usually indigenous military or paramilitary unit operating in small bands in occupied territory to harass and undermine the enemy, as by surprise raids.[7]

Describing Irregular Threats in Complex Environments

Current complex operational environments (OE) in contemporary military operations indicate that guerrillas and insurgents are a norm in the dynamic conditions of the foreseeable future. Another reality is that the US Army will be involved in persistent conflict confronting many types of threats as a norm in that foreseeable future. One of the overarching perspectives of persistent conflict recognizes that hybrid threats will continue to operate adaptively and attempt to counter US Army operations. The Army's definition of *hybrid threat* describes the complexity of threat actors that can include various combinations regular forces, irregular forces such as guerrilla units and insurgent organizations, criminal organizations, and terrorists.[8] To accent these dangers, the Chief of Staff of the US Army emphasizes an extremely complex environment "that has varied threats: conventional threats, unconventional threats, terrorism and criminality, all in an environment of instantaneous movement of communications."[9]

Hybrid Threat
The diverse and dynamic combination of regular forces, irregular forces, terrorist forces, and/or criminal elements unified to achieve mutually benefitting effects.
***Unified Land Operations*, ADRP 3-0, May 2012**

Narrowing the focus to irregular forces as a grouping of threats that include guerrillas and insurgents, the Army definition of *irregular forces* is "armed individuals or groups who are not members of the regular armed forces, police, or other internal security forces.[10] The term *irregular warfare* provides additional description to consider in a definition of a guerrilla or an insurgent. Irregular warfare is "a violent struggle among state and non-state actors for legitimacy and influence over the relevant population(s). Irregular warfare favors indirect and asymmetric approaches, though it may employ the full range of military and other capacities, in order to erode an adversary's power, influences, and will."[11]

Characteristics of "Irregular" Conflict

Isolating key phrases in the definition of *irregular warfare* suggests the motivations and actions of individuals participating in this form of persistent conflict. Discernible elements include the following—

- "Violent struggle."
- "Among state and non-state actors."
- "For legitimacy and influence over the relevant population(s)."
- "Favors indirect and asymmetric approaches."
- "May employ the full range of military and other capacities…to erode an adversary's power, influences and will."

Within this context, approved DOD terms related most closely to an insurgent and a guerrilla are *insurgency*, *guerrilla force*, *guerrilla warfare*. Analyzing the definition of each of these terms reveals aspects that can more clearly identify the description of an insurgent and a guerrilla.

An *insurgency* is "the organized use of subversion and violence by a group or movement that seeks to overthrow or force change of a governing authority. Insurgency can also refer to the group itself."[12] There are other factors that can augment the description of an insurgency in a complex OE context—

- Transition between subversion and violence dependent on specific conditions.
- Undermine the confidence gradually of a relevant population.
- Achieve insurgent aims without violence but this non-violence is not the norm.
- May conduct operations in combination with regular military forces of a state in conflict with the governing authority the insurgents oppose.

A *guerrilla force* is "a group of irregular, predominantly indigenous personnel organized along military lines to conduct military and paramilitary operations in enemy-held, hostile, or denied territory.[13] The term *guerrilla warfare* is defined as “military and paramilitary operations conducted in enemy-held or hostile territory by irregular, predominantly indigenous forces.[14] A way to bracket key aspects of a participant in guerrilla warfare includes these phrases—

- “predominantly indigenous individuals.”
- “structured similar to regular military forces.”
- “use military-like tactics and techniques.”
- “normally operate in areas occupied by an enemy or denied to the guerrilla by a hostile actor that jeopardizes the guerrilla’s intended purpose and objectives.”

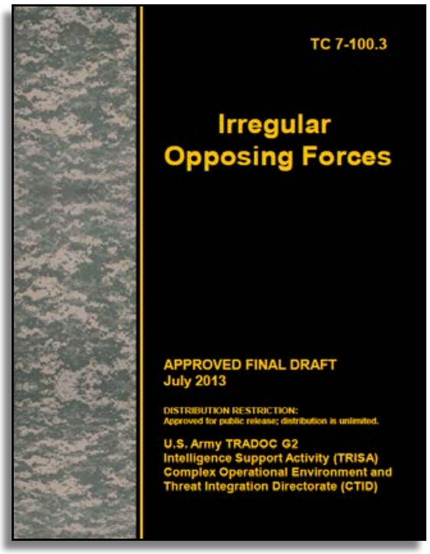
The term *unconventional warfare* is often associated with irregular warfare and guerrilla warfare, and describes “activities conducted to enable a resistance movement or insurgency to coerce, disrupt, or overthrow a government or occupying power by operating through or with an underground, auxiliary, and guerrilla force in a denied area.”[15] Although the irregular OPFOR does not use words such as underground and auxiliary to describe its support activities, the organizational intention of irregular OPFOR is to acquire willing, coerced, or unknowing support from within a relevant population, as well as from other state and non-state actors with objectives aligned to an insurgency or guerrilla force.

Describing Guerrillas and Insurgents of an Irregular OPFOR

Guerrillas and insurgents are recurring irregular OPFOR conditions in Army training events. For irregular OPFOR in US Army training, a baseline training publication that describes the guerrilla and insurgent is Army Training Circular 7-100.3, *Irregular Opposing Forces*. As of fall 2013, this publication is at the Army Publishing Directorate (APD) for review prior to formal publication. The proponent for TC 7-100.3 is the Complex Operational Environment and Threat Integration Directorate (CTID) of the TRADOC G2 Intelligence Support Activity (TRISA). The CTID final approved draft of this training circular is available at https://www.us.army.mil/suite/files/40913959 with Common Access Card (CAC) access. TC 7-100.3 is one document in a family of threat publications that supports the Army’s *Opposing Force Program.*[16]

Irregular OPFOR for Training

Training Circular 7-100.3 presents three basic types of forces that can be part of or combined as an irregular OPFOR. The distinctions among insurgents, guerrillas, and criminals are often blurred in actions and intent. Motivations and purpose of each group may have much in common or be very diverse. Complexity and dynamic change is a norm. Numerous insurgents, guerrillas, and criminal organizations can be operating concurrently in the same area and may involve sub-groups and/or splinter groupings with different aims, tactics, techniques, and objectives. Criminal organizations and noncombatants are in any OE but are outside the scope of this article. Nonetheless, from the viewpoint of an existing governing authority and ally or partner armed forces in conflict with guerrillas or insurgents, irregular OPFOR activities are embedded within a complex relevant population. Conflict outcomes such as a successful attack or defensive action are often overshadowed by the psychological effects of an incident on the relevant population.


TC 7-100.3

Irregular Opposing Forces

APPROVED FINAL DRAFT
July 2013

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

U.S. Army TRADOC G2
Intelligence Support Activity (TRISA)
Complex Operational Environment and
Threat Integration Directorate (CTID)

Persistent Conflict and Irregular OPFOR

An OPFOR insurgent organization expands its capabilities and organizational infrastructure along multiple functions. Insurgent cells often remain covert or clandestine but can also acquire public and/or legitimate recognition in political, social, economic, and information promotional programs. Depending on local or regional conditions, some insurgent organizations or guerrilla units may be affiliated with or subordinate to regular forces, or they may operate independently of such organizations. Other elements of the organization can emerge into a more hierarchical military-like structure for specified, paramilitary, or guerrilla operations. In some situations, OPFOR direct action and functional cells within an insurgent organization may combine capabilities to form guerrilla-like teams, squads, and platoons. Other specialized cells of an insurgent organization can evolve into or associate as—

- Functional supporting action or sustainment elements of a guerrilla unit.
- Staff elements of a guerrilla company, battalion, or brigade.

Guerrillas of an irregular OPFOR operate as paramilitary units in or near areas occupied by an enemy or where a hostile actor threatens the guerrilla's intended purpose and objectives. Guerrilla leaders adapt to circumstances and available resources in order to sustain or improve their combat power and influence on a relevant population and decisionmakers. Guerrillas engage increasingly in the scope and scale of military-like operations as an insurgency develops extensive popular and logistics support. Some guerrilla units may be fully integrated as a subordinate force of an insurgency while other guerrilla units may operate independently with their own agenda.

When insurgent leaders believe that appropriate conditions are set, the insurgent organization may generate conventional military forces from its guerrilla units that can directly confront regular forces of an existing governing authority with whom the insurgency is in conflict. In advanced phases of an insurgency, guerrilla units can even be integrated into a regular military OPFOR. Insurgents and guerrillas do not necessarily comply with international law or conventions on the conduct of armed conflict between and among declared belligerents. Irregular OPFOR actions are typically described in one of three general categories—

- Military-like functional tactics.
- Criminal activities.
- Terrorism.

Actions and appearance can mask the distinction between irregular OPFOR and regular OPFOR military units. Both types of forces use the same functional tactics in OPFOR mission tasks such as reconnaissance and counter-reconnaissance, assault, ambush, raid, defend, breach, and information warfare (INFOWAR). Insurgents and guerrillas can act separately from other groups, organizations, and/or activities in conflict with the same enemy, or can act in conjunction to pursue common objectives.

Regular forces can provide overt and covert support to insurgent and guerrilla operations including the expertise of advisors, liaison teams, and special purpose forces (SPF). Regular OPFOR and SPF may use terrorism tactics similar to those conducted at times by irregular OPFOR. Since SPF serving as trainers, liaisons, or advisors alongside guerrillas or insurgents may not be in a military uniform, distinguishing SPF from irregular OPFOR insurgents or guerrillas can be difficult.

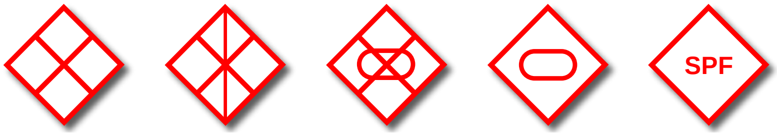


Figure 1. Regular forces and special purpose forces provide advisor-liaison-training expertise

Affiliates are actors, units, or organizations that have aligned temporarily to another organization by mutual agreement in order to achieve a common purpose. *Affiliated* organizations are those operating in another unit's AOR that the unit may be able to sufficiently influence or act in concert for a limited time. No command relationship exists between an affiliated organization and the unit in whose AOR it operates. Affiliated organizations are typically nonmilitary or paramilitary groups such as criminal cartels or insurgent organizations.[17] A guerrilla organization that is affiliated with or subordinate to an insurgent organization may also be affiliated with SPF, other regular military forces, and/or criminal elements. *Adherents* are individuals who have formed collaborative relationship with, act on behalf of, or are otherwise inspired to take action to further the goals of an irregular OPFOR unit or organization.

Guerrillas and insurgents can be part of the hybrid threat (HT). The HT can be any combination of two or more of the following components: regular forces, irregular forces (such as guerrillas and/or insurgents), and/or criminal elements. Possible HT combinations can include insurgents or guerrillas operating openly with regular military forces, criminal organizations, or varied forms of covert or clandestine cooperation. See TC 7-100, *Hybrid Threat*, (2010) for a detailed discussion of the HT for training. Possible affiliations with insurgent, guerrilla, criminal, or regular military OPFOR may also be associated with supportive civilians such as networks acting with a facade such as a charitable organization, co-opted nongovernmental organization (NGO), or coerced transnational corporation. The assistance to irregular OPFOR provided by civilians and activities can include willing, coerced, passive support by people sympathetic, and unknowing support.

Guerrilla: An OPFOR Description

Guerrilla OPFOR use a military-like organizational structure for command and control (C2) and conduct of operations. The basic building block of a guerrilla organization is the squad consisting of two fire teams. Squads are the basis for building guerrilla platoons, companies, battalions, and brigades. However, guerrilla commanders can task-organize these units for specific actions. Prior to specific direct actions, entire guerrilla companies may already be restructured (task-organized) as hunter-killer (HK) companies, made up HK groups, HK sections and HK teams.

Note. The OPFOR guerrilla use the diamond-shape with the infantry functional icon and a unit echelon designator.

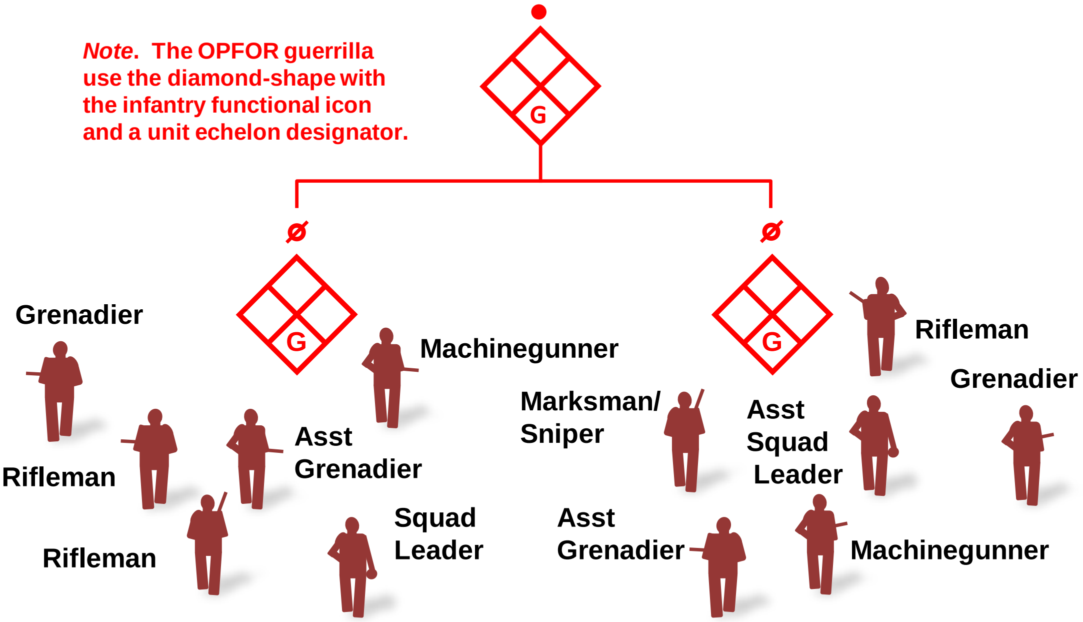


Figure 2. OPFOR guerrilla squad basic structure per FM 7-100.4 (example)

Insurgent: An OPFOR Description

Insurgent OPFOR are armed and/or unarmed individuals or groups who promote a movement's agenda that seeks to overthrow or force change of a governing authority. Insurgent organizations typically configure as a network with the cell as its basic organizational structure. An insurgent OPFOR organization does not have a fixed structure. The mission, environment, geography, goals, and objectives determine the composition and evolution of an insurgent OPFOR organization.

Note. The OPFOR insurgent use an "I" text modifier inside the diamond-shape frame with no internal icon or echelon-size, as a norm.

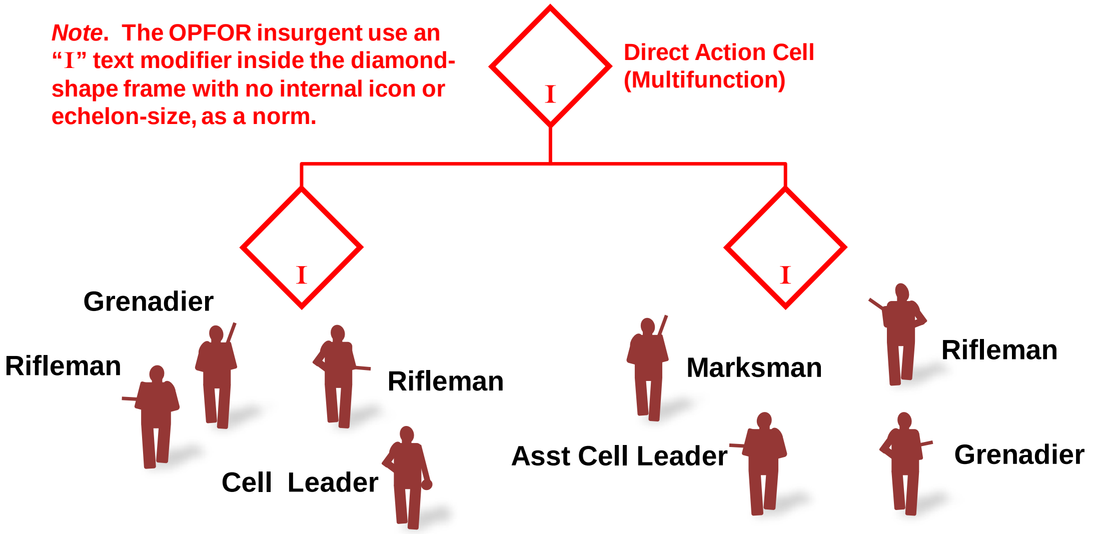


Figure 3. OPFOR insurgent cell (multifunction) basic structure per FM 7-100.4 (example)

Insurgents transition between subversion, threat of violence, and violence dependent on specific conditions. These types of actions intend to disrupt a governing authority with whom the insurgency is in conflict. Insurgents gradually undermine the confidence of a relevant population in its governing authority's ability to provide and justly administer civil law, order, and stability. Insurgents can achieve their aims without violence, but this experience is not the norm.

Defining a Threat

The description at Table 1 is a concept of how to present a common definition of an OPFOR guerrilla and an insurgent. Both individuals may have changing allegiances, purposes, capabilities, limitations, and constraints. However, the ability to accurately describe each threat is fundamental to understanding an enemy as one of the critical conditions in any operational environment.

Table1. Defining an OPFOR Threat: Guerrilla and Insurgent

	Defining a Threat	
	Guerrilla	**Insurgent**
Who:	A ***guerrilla*** is an armed or unarmed member of a guerrilla unit, typically indigenous to a region,	An ***insurgent*** is an armed or unarmed member of an insurgent organization
What:	distinct from but resembling a regular armed force in organization, equipment, training, or mission	organized as a movement
How:	that conducts paramilitary tactical direct action and supportive operations	that conducts comprehensive direct, clandestine, and covert actions in subversion, threat of violence, or violence
Where:	in an area occupied, hostile, or denied to the guerrilla force by an enemy	in an area occupied, hostile, or denied to the insurgent organization by an enemy
When:	during a period of persistent conflict	during a period of persistent conflict
Why:	in order to achieve specified tactical tasks and objectives.	in order to influence or seize political governance of a relevant population.

Training Implications

The OPFOR structure, personnel, equipment, and weapons configuration for a guerrilla unit or an insurgent organization—from an ad hoc guerrilla team to a sophisticated higher insurgent organization network—depend on specific training requirements of a supported US Army unit commander. The commander's decisions on training requirements establish the size, number, and type of irregular OPFOR needed to set challenging yet realistic conditions for specified missions in an OE.

So, how does the Army trainer, educator, and leader define *guerrilla* and *insurgent*? What other descriptions exist for an OPFOR guerrilla or insurgent that support Army training and readiness? Submit your ideas to TRISA-CTID: jon.h.moilanen.ctr@mail.mil. Selected submissions related to an OPFOR will be compared and contrasted in a future issue of the TRISA *Red Diamond*.

Note. Use Army Training Network (ATN) www.https://atn.army.mil with Army Knowledge Online (AKO) access. Additional details of a local insurgent organization and its direct action and supporting functional cells are at Appendix C of FM 7-100.4, *Opposing Force Organization Guide*. The base organization of a guerrilla company task-organized as a guerrilla hunter/killer company is at Appendix E of FM 7-100.4. To find these details on the Army Training Network: With a Common Access Card (CAC), go to the ATN website and click the CTID red diamond logo. Find the "FM 7-100.4 Organization Guide" banner and click. The organization and unit diagrams are a baseline that trainers can modify to provide the appropriate conditional capabilities or limitations to tailor an OPFOR for a particular training exercise and/or training task. FM 7-100.4 provides detailed step-by-step instructions on how to construct a task organization based on training requirements and objectives. FM 7-100.4 also describes how to select equipment options. See also TC 7-101, *Exercise Design*, for guidance on creating an appropriate OPFOR order of battle or tailored OPFOR organizations in an OE during an exercise design process.

See FM 7-100.4, Opposing Force Organization Guide (2004).

See TC 7-100.2, Opposing Force Tactics (2011).

Notes

[1] Department of Defense, Joint Publication (JP) 1-02, *Dictionary of Military and Associated Terms*, 08 November 2010, as amended through 15 September 2013.

[2] Insurgent. (n.d.) In *Merriam-Webster's Online Dictionary*, Retrieved 9 October 2013.

[3] Insurgent. (n.d.) In *Cambridge Dictionaries Online*, Retrieved 9 October 2013.

[4] Insurgent. (n.d.) In *The Free Dictionary*, Retrieved 9 October 2013.

[5] Guerrilla. (n.d.) In *Merriam-Webster's Online Dictionary*, Retrieved 9 October 2013.

[6] Guerrilla (n.d.) In *Cambridge Dictionaries Online*, Retrieved 9 October 2013.

[7] Guerrilla. (n.d.) In *The Free Dictionary*, Retrieved 9 October 2013.

[8] Hybrid threat. In Headquarters of the Army, Army Doctrine Reference Publication (ADRP) 1-02, *Terms and Military Symbols* (ADRP 1-02), 24 September 2013, chapter 1.

[9] Raymond T. Odierno. "CSA draws blueprint for complex global environment," *Army Homepage* www.army.mil, 23 October 2012.

[10] Irregular forces. In Headquarters of the Army, Army Doctrine Reference Publication (ADRP) 1-02, *Terms and Military Symbols* (ADRP 1-02), 24 September 2013, chapter1.

[11] Irregular warfare. Ibid.

[12]Insurgency. Ibid.

[13] Guerrilla force. Ibid.

[14]Guerrilla warfare. In Department of Defense, Joint Publication (JP) 1-02, *Dictionary of Military and Associated Terms*, 08 November 2010, as amended through 15 September 2013.

[15] Unconventional warfare. In Headquarters of the Army, Army Doctrine Reference Publication (ADRP) 1-02, *Terms and Military Symbols* (ADRP 1-02), 24 September 2013, chapter 1.

[16] Headquarters of the Army, Army Regulation (AR) 350-2, *Opposing Force (OPFOR) Program*, 10 May 2004.

[17] Headquarters of the Army, Army Training Circular (TC) 7-100.2, *Opposing Force Tactics*, 9 December 2011, para. 2-9.

INTEGRATING CRIME AND CRIMINAL ELEMENTS INTO TRAINING

Complex OPFOR Threats and Criminality

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

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

Themes

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

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

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

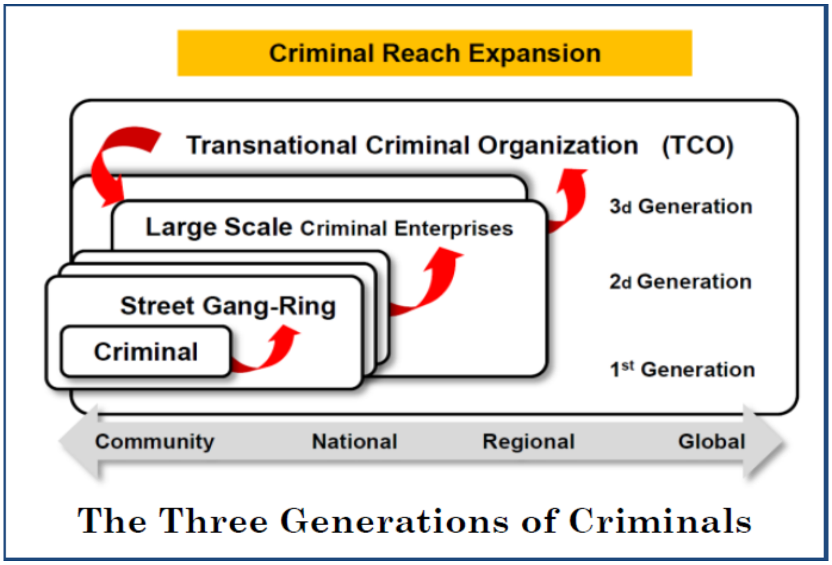


Figure 1. Three generations of criminals (example)

Integrating Crime

This first example integrates only criminal activity: Create a police or government official that is also a guerrilla company commander. He or a close associate may also be the owner, possibly in name only, of a private business. For the sake of argument, let's say that business is a fuel distribution point or some other resource that holds significant value. To protect that resource, our corrupt official employs a guerrilla platoon that doubles as private security. There are many ways to further complicate this scenario. For instance, indicate that the fuel distribution point or resource mining site frequently siphons product to smuggle it to other regions, charges at an inflated rate, and possibly launders money with proceeds that benefit and directly sustain guerrilla or other threat operations. Finally, consider the treatment of business employees by the owner or guerrilla security element that can be further integrated into the storyline and facilitate or drive other reporting or action. For instance, do they pay well and take care of families or are they abusive and commit atrocities?

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

Integrating One Criminal Organization

This second example integrates both criminal activity and at least one criminal organization: Consider in this case that the criminal organization is classified as a transnational criminal organization (TCO) and takes on a primary roll of trafficking. With significant earnings, TCOs are capable of owning or controlling vast resources such as shipping companies and assets and have access to governmental officials who can provide official documentation authorizing commodity trading and transfer.

To build upon the previous example, this TCO ensures the trafficking of fuel or other resources out while the same assets and logistics lines traffic arms, personnel, or other sustainment back to threat actors. The criminal organization benefits in at least two ways. The first is of course the money earned during the transfer of goods. The second is the link to a government official who can guarantee official documents. This gives the TCO's transportation fleet and front companies the appearance of legitimacy and facilitates regional operations.

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

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

Integrating Multiple Threat Organizations

This third example links multiple threat organizations together: Expanding upon the prior two examples, we introduce a third organization that provides mediation, another commodity required to complete the trafficking chain, or to serve a specific function. Our guerrillas were successful in securing the fuel or resource to the TCO, but the TCO cannot or does not use that commodity. Therefore they provide it to a third organization, perhaps a gang they exert control over that is able to sell it on the streets in another region. The money earned goes back to the TCO allowing it to grow as a regional player. To add further complexity, consider the size and breadth of this organization.

Perhaps this TCO physically controls multiple trafficking routes within a region and is also profiting from everything else that travels along those routes regardless of their personally supported operations. Now any organization transporting even licit material in this region must account for additional fees or tolls extorted by the TCO along the route. Also consider how that gang interacts or seeks to control the local populace. What other crimes are they committing to support the main effort of drug sales?

Again the FARC serves as a real-world example. They reportedly enjoy a relationship with al-Qaeda in the Islamic Maghreb (AQIM). AQIM agrees to secure cocaine shipments through Mali to users in Spain for approximately $2,000 per kilogram. In at least one instance, the Malian military found an abandoned aircraft capable of lifting 20 tons of cocaine; the flight originated in Venezuela.[4] Also, in Afghanistan the Haqqani organization is familiar with criminal activity, specifically extortion. Haqqani controls areas in Loya Paktia on both sides of the Durand line. Transport trucks carrying supplies, including those contracted by coalition forces, pay fees along the way that vary depending upon the cargo.[5] Finally, consider Mara Salvatrucha (MS-13) as an example of gang activity. MS-13 has links with Los Zetas Cartel managing human trafficking routes north through Central America. Similarly, gangs of the like serve as a source of personnel which often results in armed factions that, in addition to committing less lucrative crimes, assist larger groups' wage conflict to gain power.[6]

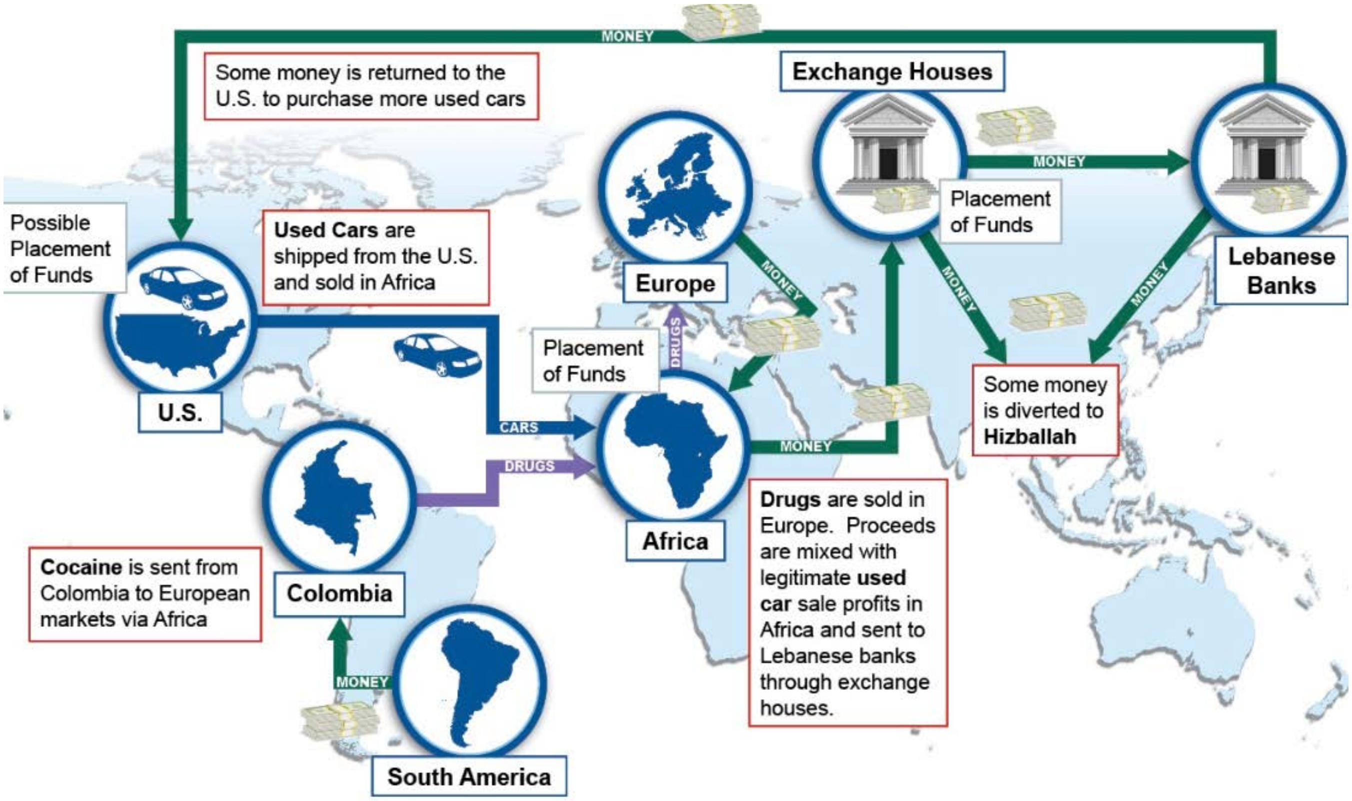

MONEY
Some money is returned to the U.S. to purchase more used cars
Exchange Houses
MONEY
Placement of Funds
Lebanese Banks
Possible Placement of Funds
Used Cars are shipped from the U.S. and sold in Africa
Europe
MONEY
MONEY
MONEY
DRUGS
Placement of Funds
Some money is diverted to Hizballah
U.S.
CARS
MONEY
DRUGS
Africa
Drugs are sold in Europe. Proceeds are mixed with legitimate used car sale profits in Africa and sent to Lebanese banks through exchange houses.
Cocaine is sent from Colombia to European markets via Africa
Colombia
MONEY
South America

Figure 2: Hezbollah crime to fund operations (example)
Source: Financial Crimes Enforcement Network, US Department of Treasury, 4 April 2013

Exercise Design Considerations

The subsequent discussion only serves to highlight certain considerations within the exercise design process to facilitate the use of crime and criminal organizations. When developing detail within operational variables, crime fits very well into the economic variable, but can also be prevalent within the political and social variables. Understandably, the amount of actual "play" time may limit the extent and breadth of criminal operations.

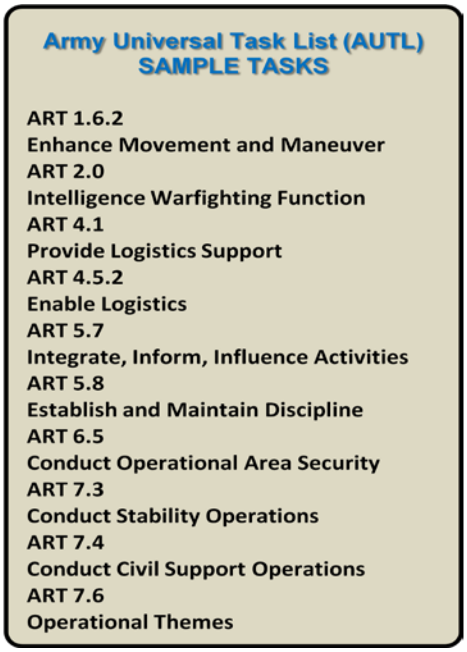
Consider building additional detail into the road to war especially in regard to their current relationships, alliances, and control or pervasiveness within the populace. Knowing the criminal element's primary motivation of profit, developing great detail early will not restrict follow on play as these elements readily shift alliances to best posture themselves for future earnings and power gain.

Crime and criminal organizations may only seem pertinent when conducting stability operations. However, like any threat actor, training units must consider second- and third-order consequences of the operational effect they seek to achieve. For instance, consider how the construction of combat roads and trails, the development of traffic control plans, enforcement of highway regulations, or area security during offensive or defensive operations purposefully or inadvertently impact criminal operations and what could be threat responses.

A cursory review of the Army Universal Task List (AUTL) reveals several tasks in which leveraging crime and criminal organizations against may prove useful. These tasks, and some of their subordinate tasks include but are not limited to those tasks in Figure 3.

Integrating crime and criminal organizations into scenarios will yield a more complex and realistic scenario. The aforementioned examples build upon trafficking successes demonstrated at one CTC, which is also important due to its prevalent practice. However, integrating other forms of crime, many of which can be found in TC 7-100.3, *Irregular Opposing Forces*, and showing their support to each other or even criminal civic action is also effective.

Build the threat as it best suits the training unit's objectives and task list, but do not feel the pressure to build additional force structure to do so as integrating crime is just as important. Ultimately, making a great dinner doesn't always mean using everything in the pantry.



Army Universal Task List (AUTL)
SAMPLE TASKS

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

Figure 3. AUTL tasks (example)

Notes

[1] Douglas Farah, "Fixers, Super Fixers and Shadow Facilitators: How Networks Connect," International Assessment and Strategy Center, 20 April 2012.

[2] Douglas Farah, "Fixers, Super Fixers and Shadow Facilitators: How Networks Connect," International Assessment and Strategy Center, 20 April 2012.

[3] Douglas Farah, "Terrorist-Criminal Pipelines and Criminalized States: Emerging Alliances," 1 June 2011.

[4] Douglas Farah, "Terrorist-Criminal Pipelines and Criminalized States: Emerging Alliances," 1 June 2011.

[5] Gretchen Peters, "Haqqani Network Financing: The Evolution of an Industry," July 2012.

[6] Patrick Corcoran, "How Street Gangs Have Complicated Mexico Security," 10 September 2013.

ATROPIA COVENANT FROM THE RED SIDE: JRTC 13-09

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

Joint Readiness Training Center (JRTC) rotation 13-09 (*Atropia Covenant*) was a Decisive Action Training Environment (DATE)-based rotation that featured new levels of complexity to challenge the rotational training unit (RTU). This was achieved by requiring the RTU to conduct a non-combatant evacuation operation (NEO), interagency and intergovernmental operations, a coordination of missions with US special operations forces (SOF), security missions (including internally displaced persons [IDP]), and counterinsurgency missions (COIN) simultaneously. These were done while also monitoring a UN-mandated zone of separation (ZOS) between two warring nations. Civilians on the battlefield (COB) were portrayed by 200 role players provided by Forces Command (FORSCOM).

Atropia Covenant featured a robust hybrid threat to the RTU. The irregular threat to the RTU was an aggressive insurgency, a dedicated terrorist group with a suicide-bomber cell, a powerful crime family undeterred by international boundaries, and special purpose forces (SPF) from a hostile country. The conventional threat was an armor/mechanized force with powerful indirect fire capability and coordinated air defense systems. The scenario was further complicated with considerable chemical and biological threats from chemical weapons, chemical factories, a biological warfare laboratory, an oil pipeline, and associated pump stations. Finally, information warfare (INFOWAR) capabilities existed down to the battalion level and included information operations and computer network attacks. Electronic warfare capabilities included Global Positioning System (GPS) jamming.

The responsibility of presenting these threats accurately fell on the 1st Battalion, 509th Parachute Infantry Regiment (1-509 PIR) with a battalion task force from the 11th Armored Cavalry Regiment (11 ACR). Enablers attached to this team came from the 18th Fires Brigade; 1st Information Operations (IO) Command; 20th Chemical, Biological, Radiological, Nuclear, Explosives (20 CBRNE) Command; 1st Maneuver Enhancement Brigade (1 MEB); a US Navy Aerostar team; and a US Air Force advanced gunnery training system (AGTS) team.

RTU

The RTU for 13-09 was the 3rd Brigade Combat Team, 82nd Airborne Division (3/82 ABN). They were augmented by Stryker units from 7th Infantry Division (7ID), armor units from 4th Infantry Division (4ID), the 1st Battalion 31st Airborne Field Artillery Regiment (1-31 AFAR), and the 1st Battalion (Reconnaissance), 82nd Combat Aviation Brigade (1-82 ARB). Additionally, 3/82 ABN worked jointly with multiple special operations forces (SOF) and US Air Force airlift, reconnaissance and attack aircraft. Airlift/airdrop aircraft also came from the Royal Canadian Air Force and the Royal New Zealand Air Force.

Scenario

The strategic setting for this exercise included the following disposition of countries in the region.

Table 1. Exercise countries in the region (exercise example)

REPUBLIC OF ATROPIA (ROA-Friendly to the US)	Dictatorship using dynastic approach to governance
People's Democratic Republic of Atropia (PDRA-Hostile to the US)	Aggressive, capable, and intent on creating an ethnic Persian State
ARIANA (Hostile to the US)	Aggressive, capable, revolutionary, and intent of spreading it's version of Islam. State sponsor of the PDRA.
GORGAS (Friendly to the US)	- Emerging representative democracy - Relies on Western support to make democracy work
MINARIA: (Neutral)	Autocracy with goal of survival and advancement of Minaria People
DONOVIA: (Neutral)	Resurgent nation that lost dominance in the region in early 1990's

The exercise scenario was based in Atropia. Atropia was split with Republic of Atropia (ROA) in the east and People's Democratic Republic of Atropia (PDRA) in the west with a UN-brokered ZOS between them. ROA had significant oil assets with numerous American citizens (AMCITs) throughout the country needing to be evacuated and chemical sites that needed to be secured.

US SOF were inserted to work with the ROA military followed by the 3/82 ABN parachute insertion on D-Day. 3/82 ABN had security and defense missions the first half of the exercise and a deliberate attack the second half. Throughout the entire exercise they had to contend with an active insurgency conducting harassing and spoiling attacks. The defense phase culminated with an armor/mechanized attack across the ZOS by the PDRA army which 3/82 ABN had to repel. The offense phase culminated with a brigade attack across the ZOS to destroy PDRA forces and seize a chemical weapons site in the village of Sangari.

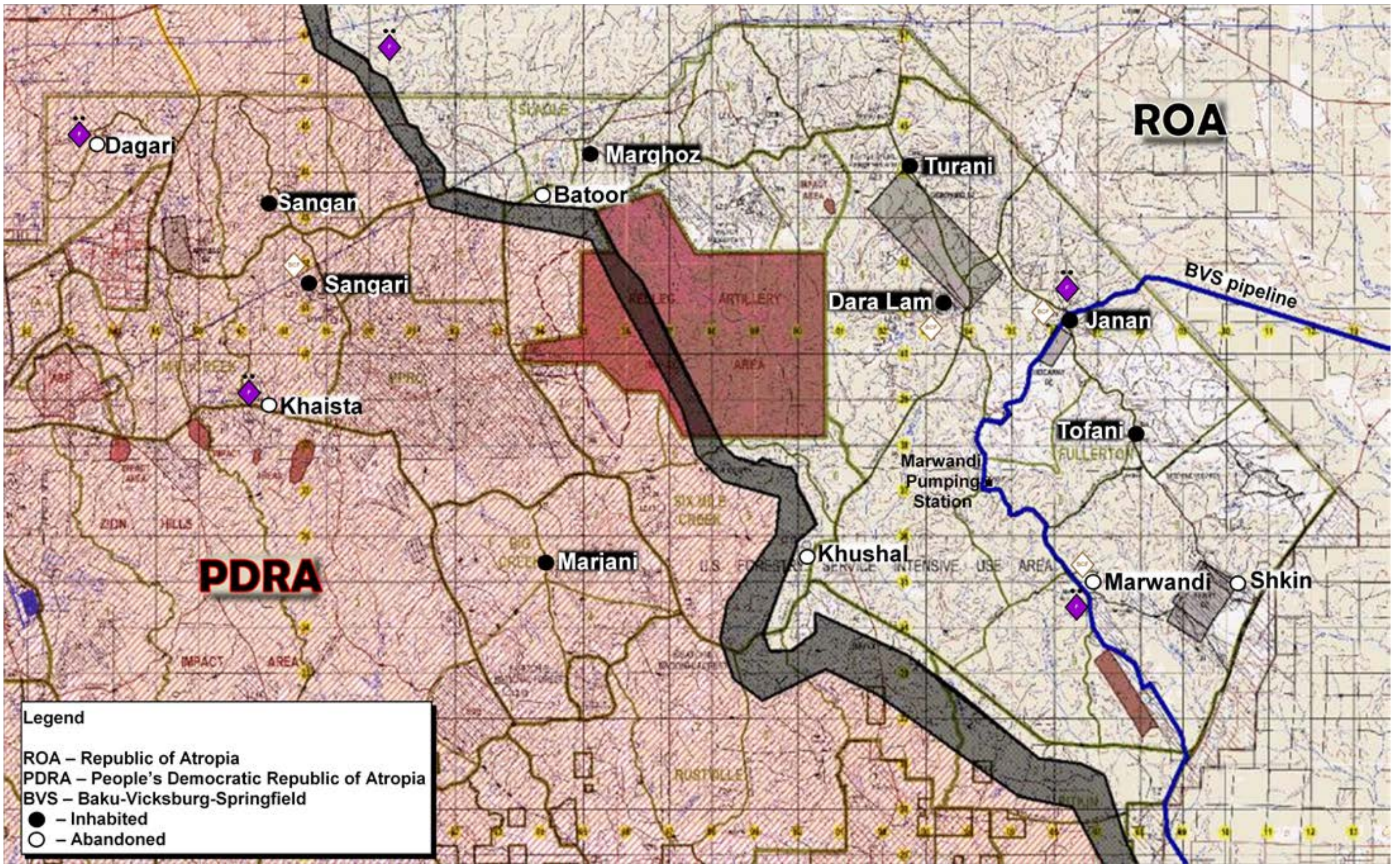


Figure 1. PDRA/ROA map (exercise example)

Opposing Forces (OPFOR) in ROA

Arianian Special Purpose Forces (SPF). SPF units are a real challenge for the RTU. Seldom operating in the open or on direct action missions, SPF teams operate behind the scenes, training, resourcing, and sometimes leading insurgent, guerrilla, or criminal elements.

Insurgents. Insurgents in this conflict were portrayed by the State-sponsored South Atropia People's Army (SAPA) and the non-State sponsored Faqih and the Godly Martyrs Brigade (GMB).

The SAPA motivation was to continue the rejectionist insurgency within ROA to expand their influence and gain control of the oil pipeline. SAPA was dependent on the SPF for training and access to chemical and biological weapons. This was a decentralized element in platoon and company elements that operated independently using technical vehicles, light and heavy machineguns, 60mm mortars for indirect fire (IDF), RPG-27s, with limited surface-to-air capability. Their tactics included guerrilla warfare, indirect fire, mass casualty attacks, ethnic cleansing, sabotage, entry denial and disruption, intimidation, kidnappings, extortion, hostage taking, assassinations, maiming, and torture.

The Faqih and GMB were a jihadist insurgent/terrorist group operating across the ROA and the PDRA. This organization followed a Salafist theo-ideology with the objective of establishing a Caucasus Emirate/Caliphate. Although formed into multi-functional teams in a decentralized network addressing primarily local concerns, it would be wrong to view them as driven solely by these concerns and lacking a central control or hierarchy. The Faqih were dismounted and primarily conducted operations using small arms, RPG, and limited IDF (60mm mortars). GMB provided suicide vehicle borne improvised explosive device (SVBIED) and suicide vest (SVEST) capability. The combined strength of these groups ranged between 150-200 people; Faqih maintained a strength between 9 and 10 teams at 3-20 people, and the GMB 9-10 teams at 3-5 people. Collectively, these groups enjoyed internal support from like-minded Sunni fundamentalist and external support for training, advice and operational planning and execution from al-Qaeda and Islamic charities. In this exercise, the SVEST attacks by females were particularly effective

Criminals. The Baqquani Crime Family (BCF) was an independent organization with no alliances or affiliations other than some economic ones with SPF. This was not a local gang. The BCF was a sophisticated, third-generation transnational criminal organization (TCO) with an ambitious economic and political agenda. BCF was peopled by bandits, gangs, organized crime factions, and corrupt government officials. The BCF used intimidation to gain influence and was a major driver of instability in ROA. Motivated by money and not politics, the BCF began the exercise working independently of the other OPFOR elements.

They were a neutral entity until the 3/82 ABN angered them within 24 hours of arrival. They then offered their services to the PDRA (for a fee) and began working against the US. Throughout the exercise, the BCF would approach US forces attempting to earn money or favors, even offering information on the OPFOR, but were always rebuffed. They would then turn to the PDRA or SAPA. They also proved that by day seven of the exercise, US traffic control guards could be bribed with M&Ms to let them through.

OPFOR in PDRA

Conventional near-peer force. The People's Democratic Army (PDA) portrayed a conventional near-peer force with a mixed light and mechanized infantry force supported by Ariana with SPF support. The PDA's stated goal was to seize all remaining ethnic enclaves within ROA and absorb them into the PDRA.

Order of battle. The PDA was organized into four major commands: Northern Command, Central Command, and Southern/Capital Command, and a separate SPF Command. In *Atropia Covenant*, the RTU faced the Central Command with SPF support.

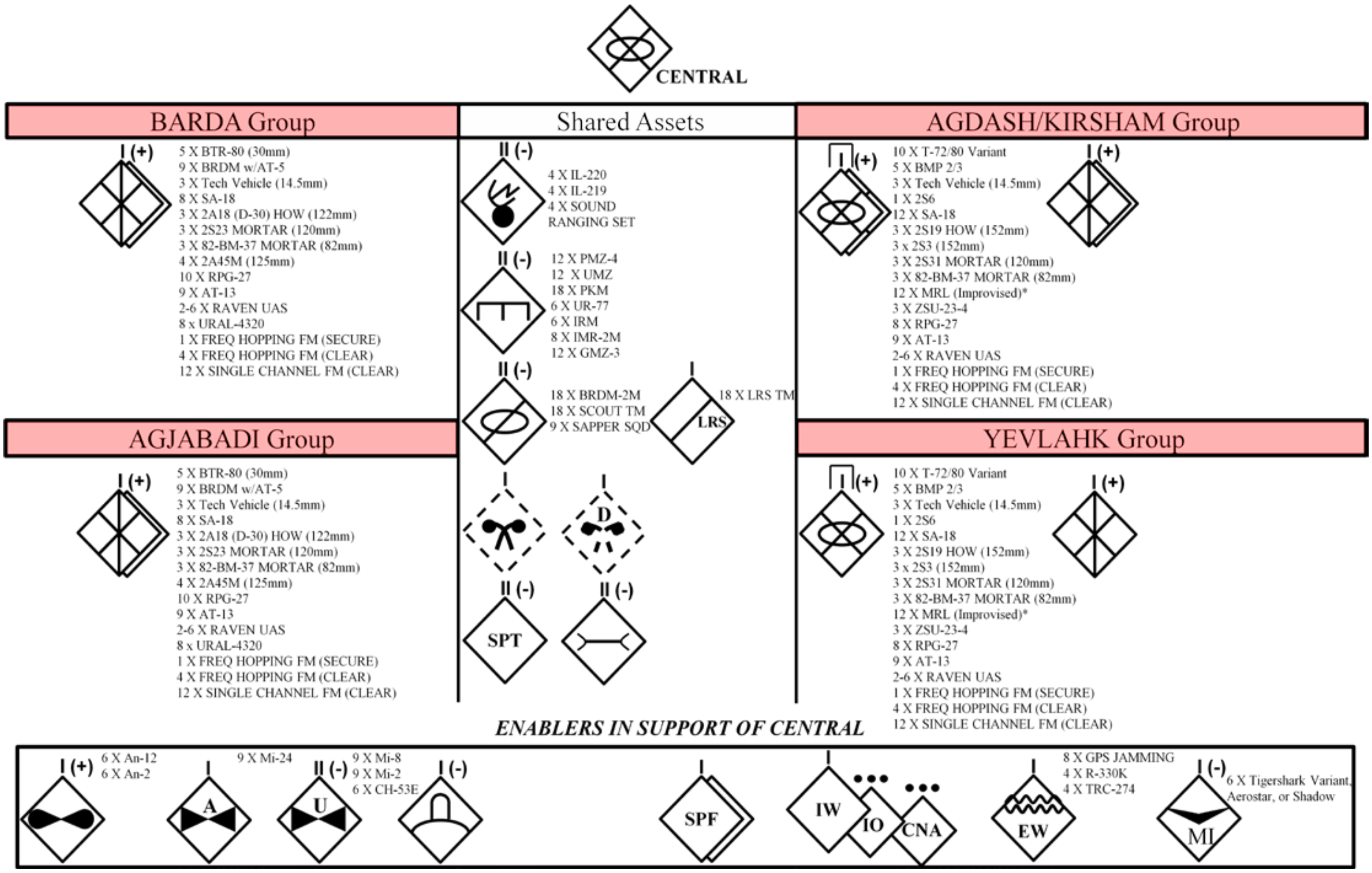


Figure 2. Central command of the PDA (exercise example)

Capabilities. The PDA Central forces were primarily mechanized infantry with organic IDF assets, and therefore, a major challenge to a light force such as the 3/82 ABN. Long range surveillance (LRS) teams and SPF units provided "eyes on" in the ROA. PDA capabilities included powerful INFOWAR assets. This capability allowed the OPFOR to conduct data mining on RTU networks, open source intelligence collection, and computer network attacks (CNA). Other enablers with the Central Command included air defense systems, rotary- and fixed-wing assets, unmanned aircraft systems (UAS), chemical warfare and decontamination units, and electronic warfare systems for GPS jamming. Finally, there was an integrated air defense system along the ZOS which did not allow a permissive flying environment for RTU aircraft, as they learned the first day in the box.

Major weapons systems. Surface vehicles replicated included T-72/80 variant main battle tanks, BRDMs, BTR-80s, and BMP-2/3s. IDF was provided by 122mm Howitzers, 120mm mortars, 82mm mortars, and locally manufactured multiple rocket launchers (MRL). Anti-armor systems included the 2A45M anti-tank gun, RPG-27s, and AT-13s. Anti-aircraft systems included the ZSU 23-4, SA-18, SA-6, and SA-2.

Scripted Versus Freeplay

The majority of this exercise was freeplay with some scripted events injected to meet particular training requirements. Scripted actions included assassinations of local and national leaders and some specific IED incidents. However, freeplay was the signature of *Atropia Covenant* as the OPFOR were allowed to develop situations as they appeared and to adapt tactics as needed. The OPFOR commander designated main efforts (including INFOWAR), placed priorities on targets, and shifted forces as needed without direction from the Operations Group.

An example of this would be when the OPFOR commander was unhappy with the battle damage assessment (BDA) he was getting from indirect fire. So, he shifted the effort from hitting equipment with artillery and mortars to actually stealing the 3/82 ABN vehicles. These were then either used against the RTU or taken out of play.

Another example was on D+2, the OPFOR commander was unhappy with the BDA he was getting from remote-controlled IEDs (RCIED). He then had his staff coordinate with the Operations Group to switch to victim-operated IEDS (VOIED) and explosively formed penetrators (EFP). This matched OPFOR doctrine of a “thinking enemy” that can adapt to changes on the battlefield.

The OPFOR emphasis throughout the exercise was synchronization of effort. The command group reminded elements daily that this was a unit fight, not an individual fight. This allowed all elements of combat power (direct fire, indirect fire, INFOWAR, etc.) to be focused on primary and secondary objectives, and not just activity in the box.

OPFOR Effectiveness

Throughout *Atropia Covenant*, the OPFOR demonstrated resiliency, adaptability, and persistence. Success was reinforced, and failures resulted in a quick assessment followed by a change of tactics. The result was, on many occasions, a smaller force being able to defeat or delay a larger force.

In one battle, 18 SAPA personnel with dispersed mortar tubes took one village and held off attacks from three companies for over 24 hours. RTU reconnaissance units were routinely targeted and removed from the fight. Lax security procedures allowed SAPA teams to infiltrate into the RTU areas and steal vehicles and take prisoners. Troops posting photos on unsecure websites allowed OPFOR INFOWAR teams to identify personnel, units, and locations, and then to exploit that intelligence. This was not an easy rotation for any RTU element.

> **“We always want the Soldiers’ worst days to be here and not overseas.”**
> **MAJ Gabriel Ramirez-JRTC Public Affairs Officer**

Recurring observations and training impacts. This was the fourth DATE rotation to be observed at JRTC by TRISA personnel. Some observations among RTU units are identical and could be used as training events/lanes.

- **Not dismounting vehicles when in contact, or moving off the road into the wood line when forced to stop.** Routinely we see units mounted in trucks get hit with IDF, direct fire, or stopped by an IED or an obstacle, and no one dismounts. The OPFOR covers its obstacles with either IDF or direct fire, so being stopped makes for targets. The OPFOR covers obstacles with UAS, and a line of stopped vehicles makes for a tempting target.

- **Lax security in the brigade support area or between battle positions.** This results in high value targets being identified and destroyed, or vehicles being stolen and Soldiers taken prisoner. It also assists the OPFOR command in developing future attack plans.
- **Operating in immature areas.** Some units are struggling with unplugging their digital systems and then being deployed to immature areas; i.e. no forward operating bases (FOBs). Many units are struggling with field craft having to deal with extended combat operations with no FOB.
- **Not zeroing radios on capture.** Captured secure radios with current fills are a wonderful source of intelligence for the OPFOR. Not only will they monitor all the nets, they will issue false orders to units that do not authenticate properly and cause more confusion for the RTU.
- **Not following the Code of Conduct.** Captured Soldiers are being manipulated by OPFOR interrogators into signing "confessions" while being filmed and answering questions about their unit and missions. This is further exploited through broadcasts of the interrogations and newspaper articles circulated throughout the tactical box.

Training at JRTC is tough. Things to remember about the OPFOR when training for a rotation:

The Opposing Force (OPFOR) are committed to defeat you in TRAINING.

The OPFOR will—

- **ATTACK where your security is lax.**
- **EXPLOIT every opportunity, whether it is talkative Soldiers, open Internet sources, or compromised radio networks.**
- **ADAPT tactics, techniques, and procedures if you are being successful.**
- **"SHOOT DOWN" your aircraft (including UAS).**

  and
- **"HUNT DOWN" your reconnaissance units.**

The OPFOR fight to win every battle.

Army 1Q/FY14 Antiterrorism Awareness Theme

Antiterrorism Risk Management

TRADOC G2 Intelligence Support Activity
Antiterrorism - Counterterrorism
Terrorism
Threats Terrorism Team (T3)
T3 Advisory
Antiterrorism Best Practices & Readiness
Know the Threat
Identify lessons learned & best practices for Antiterrorism Risk Management
Know the Enemy
Hybrid Threat
Train-the-Trainer
OCT 2013
No. 01-14
OCT 2013
Antiterrorism Risk Management
Risk Management
Linking Tactical Execution to Strategic Outcomes
Antiterrorism Strategic Plan
BURNISHING THE STEEL
2013-2016
Protect the Force

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

Camp Bastion Attack

Update 2013

Tactics and Techniques in Complex Operational Environments (OE)

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

In October 2012, The Operational Environment Assessment (OEA) Team published a Threat Report on the Taliban Attack on Camp Bastion in Helmand Province, Afghanistan that took place the night of 14-15 September 2012. Since the original report, additional information about the attack has come to light. The Marine Corps conducted an investigation into the attack, and the Marine Corps Commandant has forced two generals to retire for their failure to take all prudent precautions to ensure the safety of their Marines.

Attack Recap

On the night of 14-15 September 2012, fifteen Taliban members infiltrated Camp Bastion in three groups of five insurgents each, wearing American military uniforms. The first group targeted the Marines' Harrier jets and hangars, the second group's primary target were the helicopters, and the final group was the military personnel in tents around the airfield. The insurgents used F-1 anti-personnel grenades, not the previously reported rocket-propelled grenades (RPGs), to destroy aircraft on the ground, three aviation refueling stations, and several temporary aircraft shelters. Two Marines died in the firefights that ensued. Marines and other coalition forces on the base killed fourteen of the attackers and captured the lone survivor, the leader of the third group.[1]

New Information Invalidates Previous Reports

Initial reports are rarely completely accurate, and that is the case with this attack. The October 2012 Threat Report listed nine other casualties besides the two Marines killed. Officials now report that there were two US personnel killed in action (KIA), eight US personnel wounded in action (WIA), eight United Kingdom (UK) personnel WIA, and one civilian contractor WIA during the attack. The initial report also claimed six Marine AV-8B Harrier jets were destroyed in the attack. The number of Harriers remains the same, but the destruction also included two AV-8B Harrier jets and one C-130E cargo plane severely damaged; one C-12 damaged; and three MV-22Bs and one UK Sea King helicopter with minor damage. The attack also significantly damaged two UK Jackal vehicles; destroyed three fuel bladders and five sun shades; and generated minor damage against four sun shades, concrete structures, and a hangar/maintenance facility[2]

Harrier jet

Other discrepancies between initial reports and the detailed investigation have also emerged. Some of the initial reports made the three security "rings" appear much stronger than they were in reality. While the inner wire fence may have been 30 feet tall with guard towers, it was not a 30-foot concrete blast wall as some reports suggested, but only a chain linked fence. The outer ring consisted of a single row of concertina wire with a ditch and berm between the two fences to stop vehicle penetration. The concertina wire was also not as thick or six feet high as some journalist's stories suggested and the attackers easily passed through with wire cutters. Thus, initial reports asserting that one of the attackers wearing a suicide vest ran up to the outer fence and detonated it proved to be erroneous.[3]

Other New Information

The later investigations into the attack revealed other pieces of information not previously known. The presence of Camp Bastion created a sewage runoff that made part of the desert arable, and Afghans put the well-fertilized soil to good advantage growing crops, especially poppies. The attackers possibly used the presence of the new agricultural workers to disguise themselves as farmers to reconnoiter Camp Bastion. In the months leading up to the attack, several breaches or near breaches of the Camp Bastion complex occurred. In one of these incidents, the security personnel performed their duties properly and the possible intruder immediately retreated.

Figure 1. Surveillance imagery of perimeter intrusion attempt by five individuals (example)
Source: USMC News Release Headquarters, United States Marine Corps, 1 October 2013

Twice, intruders were able to breach the perimeter security and escape detection until seen later when security personnel were looking at tapes from the night before. One intruder entered an empty guard tower and looked around while the other made it as far as the cryogenics lab on the airfield before exiting the same way he entered. A security team member stated that during his time at Camp Bastion, they had identified 24 separate breaches in the chain-linked fence that needed repair from intrusion. The Camp Bastion leadership blamed these incidents on “scrapers” looking for metal to sell or thieves looking for items to steal. From these probes, the Taliban learned at what times certain guard towers were unmanned. That the Taliban achieved excellent intelligence about the entire compound was demonstrated by their drawings, which surfaced in a YouTube video posted after the attack. This video was made several months in advance and did not actually feature the real attackers as several of them had been killed accidently during training. The Taliban delayed the attack from July 2012 to September in order to train a new assault team. Despite the external threat, the Marines were more worried about an attack from inside their compound than from the outside.[4]

Due to the drawdown of American forces from Afghanistan, Marine MG Charles “Mark” Gurganus had to make do with less security personnel than he wanted. Gurganus, the Regional Command Southwest Commander, asked for 205 additional Marines for base security, but higher headquarters in Kabul denied his request.[5] Without the additional Marines, Gurganus cut the number of Marines conducting patrols outside the wire from 325 to 100 just one month before the attack. Since Camp Bastion was formerly a British base, its security belonged to that country’s military. In turn, the British delegated the base security mission to coalition soldiers from the small South Pacific island of Tonga. Several times before the night of the attack, some American Soldiers claimed that Tongan soldiers were sleeping in their guard towers instead of remaining vigilant at their posts. This is probably not the case as the Tongans used the base of the tower where their soldiers could sleep when not on their actual guard shift. Americans running for exercise saw these Tongans sleeping and thought they were not performing their duties.[6]

Tonga had deployed only 55 soldiers to Afghanistan, not nearly enough to man all the towers that surrounded the 36 square miles of Camp Bastion and Camp Leatherneck, the portion of the base occupied by to the American military. Because the guard tower closest to the point of enemy infiltration was not manned on the night of the attack, the adjacent towers could not observe some of the area, creating a dead spot perfect for the Taliban to exploit using a dry river bed. The Taliban attackers used wire cutters to cut a hole two feet by five feet through the inside chain-linked fence as well as the concertina wire strung in the outer defensive layer. There was no 30-foot concrete blast wall to surmount anywhere in the three layer defensive system, but instead some barriers used to protect the planes and other facilities from direct fire coming from outside the compound surrounded the outside edge of the airfield. The attackers also used their wire cutters to cut through concertina wire placed in July 2012 around the most vulnerable areas of the airfield.[7]

The three Taliban teams separated based on their pre-planned objectives. One team went after the Harrier jets and successfully blew up several with F-1 anti-personnel grenades and other incendiary devices they carried. A second team attacked the cryo facility, a lab near the flight line that produced oxygen and nitrogen for the various jet aircraft. Blast barriers sixteen feet high and ten feet wide surrounded the cryo lab, and would later serve the attackers as a defensive bunker when the group came under attack. The final group of five insurgents went after the fuel bladders; all located in the same general vicinity. Due to the distance from the penetration point to the helicopter pad, the group tasked with the mission to destroy the helicopters never got close to their target before coalition forces engaged them.[8]

Due to the distances separating the three groups of attackers, and the darkness, the battle that developed became three individual firefights that took six hours to reach a final conclusion. Once they realized that Camp Bastion was under a ground attack, small groups of Marines, often led by officers and sergeants not in the chain of command, took the initiative to go after the enemy infiltrators. Several Marine aviators got their Cobra helicopters in the air to provide aerial support, despite the minimal distance between friend and foe on the ground. A British quick reaction force arrived near one of the firefights, but refused to get involved until additional British forces arrived. The Marines initially went ahead without the Brits, who eventually showed up with their armored vehicles to assist. Between the Cobra helicopters in the air and the makeshift teams on the ground that eventually numbered about 100 coalition troops, the Marines were able to kill or capture all 15 attackers.[9]

Aftermath

After the attack, Gurganus chose not to conduct a full investigation because Camp Bastion was a British base, not American. Between 16 September 2012 and 21 November 2012, five separate investigations took place by various commands. These included the United Kingdom, 16 September 2012; the Joint Combat Assessment Team (JCAT) Review, 18 September 2012; the Regional Command (RC) Southwest RC(SW), 24 September 2012; the International Security Assistance Force (ISAF) Review, 27 September 2012; and the RC(SW) Supplemental Review, 21 November 2012. The Department of Defense decided to launch a full-scale investigation of the attack in late May 2013 to determine if any senior Marines should be held accountable for Camp Bastion's security failures. The widows of the two Marines killed in the attack, LtCol Christopher K. Raible and Sergeant Bradley Atwell, were both unhappy that it took so long to launch the investigation. The Lieutenant General in charge of the investigation completed his report on 19 August 2013 with a memorandum to the Commander of the United States Central Command. In the middle of September, both widows received a briefing from the Marine Corps after the completion of the investigation.[10]

On 30 September 2013, the Pentagon announced that two Marine generals would be disciplined because of their failures to prevent the attack at Camp Bastion one year earlier. The Marine Corps Commandant, General James F. Amos concluded that MG Gurganus and MG Gregg Sturdevant, the Marine Aviation Wing Commander on the base, did not take adequate security precautions to protect their subordinates. The Pentagon directed both generals to retire. The Marine Corps also rescinded Gurganus' selection for his third star and a position as the third highest ranking officer in the Marines. Sturdevant also received a letter of censure from the Secretary of the Navy for his failure to integrate the security of his aviation squadron into the Camp Bastion security plans. This is a rare instance where senior commanders received disciplinary action for failure in combat.[11]

Analyst Assessment

The security failure at Camp Bastion on 14 September 2012 demonstrates the importance of the smallest detail in military operations. The security personnel who chose to blame the "scrapers" and the military leadership who accepted the analysis chose the easy excuse for the multiple fence penetrations leading up to the attack. The decision not to man certain guard towers created blind spots that could have been covered by electronic means, but this weakness was not discovered until after the attack. With base security in the hands of the British, the American Marine commander, MG Gurganus, decided that he could take a risk when his request for 205 additional Marines for security was turned down. No one in the headquarters that denied the request for additional security, however, received any punishment. Gurganus took even further risk when he reduced the number of Marines conducting security patrols outside the wire. The British compounded the situation by delegating the security of part of the perimeter to soldiers from Tonga. The Marine Aviation Wing Commander, MG Sturdevant, also chose to delegate the security of his personnel and equipment to other forces instead of providing even a minimal amount of internal protection for his unit on Camp Bastion. While each of these decisions seemed small at the time, they culminated in the worst single-day loss of American military aircraft since the Vietnam War, the death of two American Marines, and the wounding of over a dozen coalition troops. The first rule that any officer learns is to always have security out. The Marines failed to even put out a small roving patrol to keep an eye on their aircraft, and therefore relearned this lesson the hard way at Camp Bastion.

Notes

[1] Ernesto Londoño, "Slain Marine commander's actions in Afghanistan called heroic," The Washington Post, 22 September 2012; Dan Lamothe, "Fallen Marine commander up for Silver Star," Marine Times, 19 October 2012; United States Army Forces Command Memorandum, Subject: Army Regulation (AR) 15-6 Investigation of the 14-15 September 2012 Attack on the Camp Bastion, Leatherneck, and Shorabak (BLS) Complex, Helmand Province, Afghanistan, pp 2 and 6.

[2] Matthieu Aikins, "Enemy Inside the Wire: The Untold Story of the Battle of Bastion," GQ Magazine, September 2013; United States Army Forces Command Memorandum, Subject: Army Regulation (AR) 15-6 Investigation of the 14-15 September 2012 Attack on the Camp Bastion, Leatherneck, and Shorabak (BLS) Complex, Helmand Province, Afghanistan, p 2.

[3] Matthieu Aikins, "Enemy Inside the Wire: The Untold Story of the Battle of Bastion," GQ Magazine, September 2013; United States Army Forces Command Memorandum, Subject: Army Regulation (AR) 15-6 Investigation of the 14-15 September 2012 Attack on the Camp Bastion, Leatherneck, and Shorabak (BLS) Complex, Helmand Province, Afghanistan, p 11.

[4] The Marine Times, "Accountability issues raised in Camp Bastion attack," 23 April 2013; Jim Michaels, "Two generals asked to retire in wake of Bastion attack," USA Today, 30 September 2013; Matthieu Aikins, "Enemy Inside the Wire: The Untold Story of the Battle of Bastion," GQ Magazine, September 2013; United States Army Forces Command Memorandum, Subject: Army Regulation (AR) 15-6 Investigation of the 14-15 September 2012 Attack on the Camp Bastion, Leatherneck, and Shorabak (BLS) Complex, Helmand Province, Afghanistan, pp 18-19; Headquarters, Regional Command (Southwest), International Security Assistance Force, Joint Review Board Initial Report of Administrative Inquiry of the 14-15 September 2012 Insurgent Attack on Camp Bastion, pp 1-2.

[5] Jim Michaels, "Two generals asked to retire in wake of Bastion attack," USA Today, 30 September 2013.

[6] The Washington Post, "Reduced security blamed for Taliban attack," 20 April 2013; ; The Marine Times, "Accountability issues raised in Camp Bastion attack," 23 April 2013; Jim Michaels, "Two generals asked to retire in wake of Bastion attack," USA Today, 30 September 2013; Matthieu Aikins, "Enemy Inside the Wire: The Untold Story of the Battle of Bastion," GQ Magazine, September 2013; United States Army Forces Command Memorandum, Subject: Army Regulation (AR) 15-6 Investigation of the 14-15 September 2012 Attack on the Camp Bastion, Leatherneck, and Shorabak (BLS) Complex, Helmand Province, Afghanistan, pp 6.

[7] Ernesto Londoño, "Slain Marine commander's actions in Afghanistan called heroic," The Washington Post, 22 September 2012; Dan Lamothe, "Fallen Marine commander up for Silver Star," Marine Times, 19 October 2012; The Washington Post, "Reduced security blamed for Taliban attack," 20 April 2013; The Marine Times, "Accountability issues raised in Camp Bastion attack," 23 April 2013; Jim Michaels, "Two generals asked to retire in wake of Bastion attack," USA Today, 30 September 2013; Matthieu Aikins, "Enemy Inside the Wire: The Untold Story of the Battle of Bastion," GQ Magazine, September 2013; United States Army Forces Command Memorandum, Subject: Army Regulation (AR) 15-6 Investigation of the 14-15 September 2012 Attack on the Camp Bastion, Leatherneck, and Shorabak (BLS) Complex, Helmand Province, Afghanistan, p 13; Headquarters, Regional Command (Southwest), International security Assistance Force, Memorandum: Supplemental Review of 14-15 September 2012 Insurgent Attack at Camp Bastion Focusing on the Response to the Joint Staff Integrated Vulnerability Assessment (JSIVA), pp 3 and 5.

[8] Ernesto Londoño, "Slain Marine commander's actions in Afghanistan called heroic," The Washington Post, 22 September 2012; Matthieu Aikins, "Enemy Inside the Wire: The Untold Story of the Battle of Bastion," GQ Magazine, September 2013.

[9] Ernesto Londoño, "Slain Marine commander's actions in Afghanistan called heroic," The Washington Post, 22 September 2012; Dan Lamothe, "Fallen Marine commander up for Silver Star," Marine Times, 19 October 2012; ; Gretel C. Kovach, "Camp Bastion Attack Investigation Wraps:

Family of Marines killed Sept. 14, 2012 Being Briefed on Results," U-T San Diego, 14 September 2013; Jim Michaels, "Two generals asked to retire in wake of Bastion attack," USA Today, 30 September 2013; Matthieu Aikins, "Enemy Inside the Wire: The Untold Story of the Battle of Bastion," GQ Magazine, September 2013.

[10] Dan Lamothe, "Military launches investigation into Camp Bastion attack," Marine Times, 30 May 2013; Gretel C. Kovach, "Camp Bastion Attack Investigation Wraps: Family of Marines killed Sept. 14, 2012 Being Briefed on Results," U-T San Diego, 14 September 2013; United States Army Forces Command Memorandum, Subject: Army Regulation (AR) 15-6 Investigation of the 14-15 September 2012 Attack on the Camp Bastion, Leatherneck, and Shorabak (BLS) Complex, Helmand Province, Afghanistan, pp 1-2.

[11] Jim Michaels, "Two generals asked to retire in wake of Bastion attack," USA Today, 30 September 2013.

INFILTRATION AND THE CYBER ATTACK CYCLE

Cyber Attack in Complex Operational Environments

by Jerry England, Threat Assessment Team (DAC)

Military operations rely on information and communications technology (ICT). The exposure of military systems and information resources to cyber attack is a reality as more warfighting functions become integrated with software and computer applications. As countries develop offensive cyber operations, the threat from computer warfare and information attack against friendly capabilities increases.[1] For this reason, understanding the techniques and tactics of cyber attacks is a useful approach to addressing this emerging element of the hybrid threat. Devising a model for threat cyber operations based on current tactics and terminology will assist exercise designers to include threat cyber operations and meet future training objectives. The discussion below is the second part in a series that illustrates a model for describing the threat cyber attack lifecycle that focuses on the second part of the lifecycle: the infiltration stage.

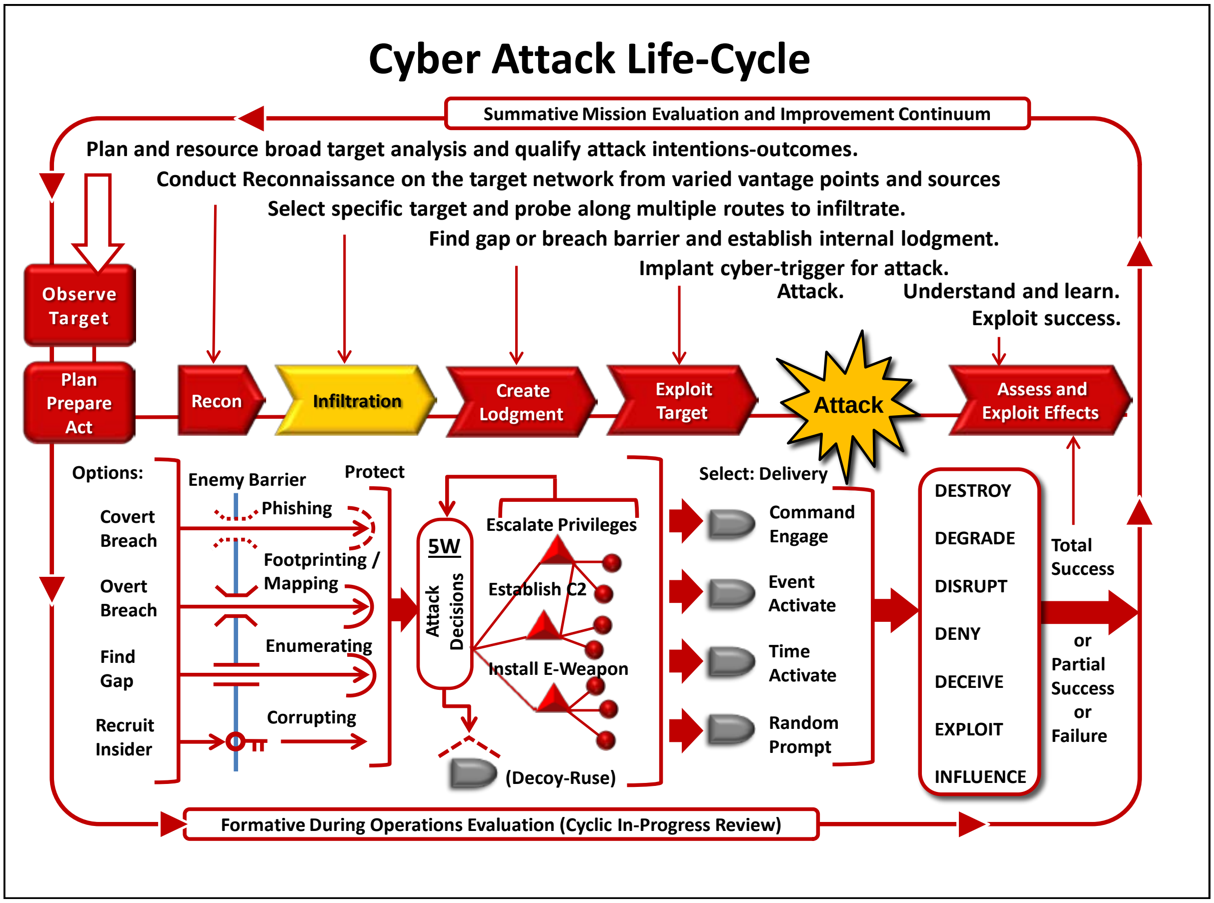


Figure 1. Infiltration in a cyber attack cycle, (TRISA-CTID example)

Cyber Attack Lifecycle (Recap)

The threat conducts cyber attacks through a six-step process designated the cyber attack lifecycle (CALC). The six steps however, do not occur sequentially and the threat can skip or repeat steps as if it is appropriate. The steps in the cyber attack lifecycle are the following —

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

Infiltration

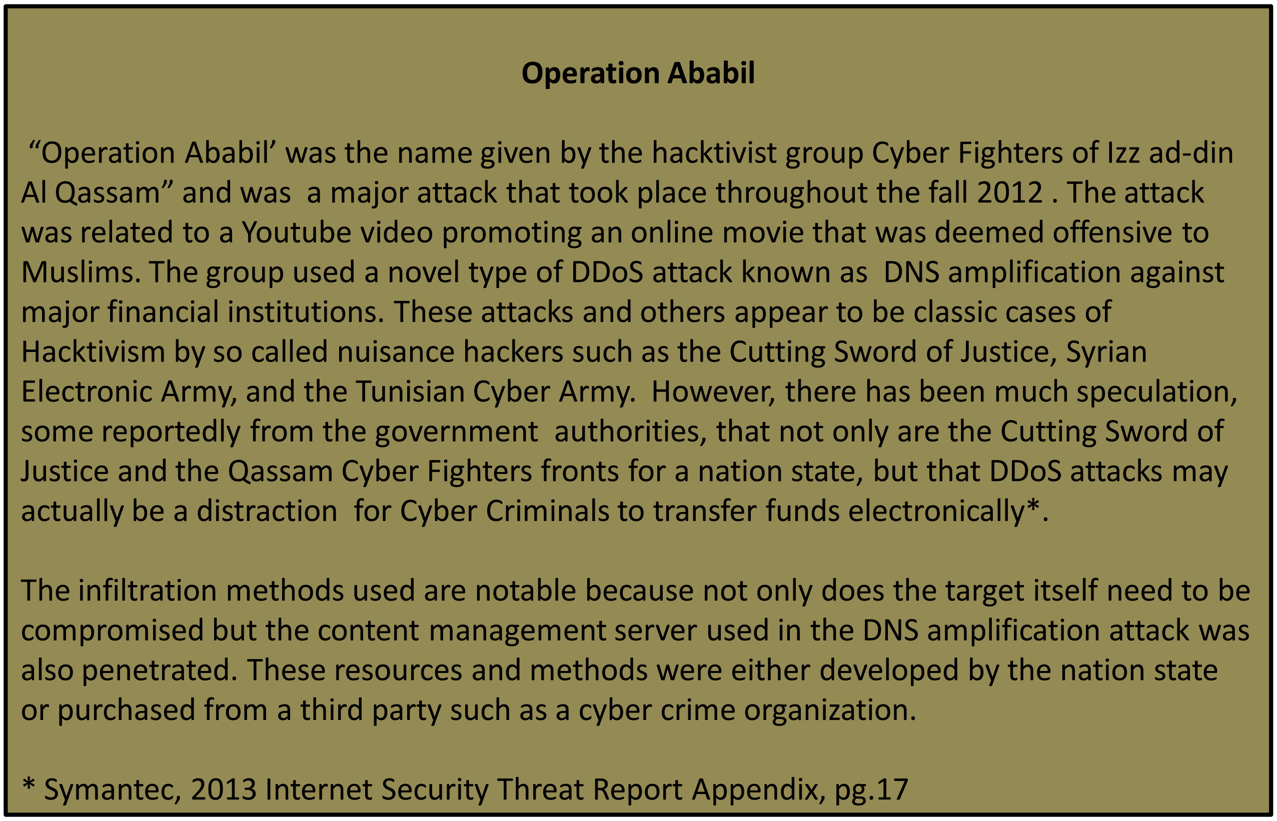
The second step in the cyber attack lifecycle is the infiltration step and includes the penetration of the defenses of an ICT system in order to manipulate, deny, degrade, or destroy the information contained or the system itself.[2] Once the reconnaissance phase is complete, the cyber threat actor will develop a list of targets and access points for use in the next phases of the attack. A map of the targeted network and its associated vulnerabilities provides technical data about the routes, nodes, and software used for the infiltration phase and the initial information for the attack.[3]

By mapping the targeted network, the attacker is able to customize and adapt the attack methodology to predict and circumvent security controls and standard incident response practices for the duration of the cyber attack based on intelligence from the reconnaissance step.[4] The access points, configuration of the target, and the associated vulnerabilities provide the details needed to execute the planned attack whether it is a distributed denial of service (DDOS) attack or a targeted attack. In most cases, known vulnerabilities or "commodity threats" will be used to breach the target system such as common remotely embedded executables known as Trojans or malicious applets and scripts."[5] However, superior cyber threat actors will design new attack methods based on advanced expertise and known weaknesses which may be much more direct in penetrating their intended target. As a point of comparison, a Trojan may be sent to a number of email recipients and require the target to execute the malicious process in order to obtain access, while the exploitation of a known website vulnerability such as an SQL inject or other malicious scripting can be done without any action by the targeted users.

In the infiltration step, the Threat compromises friendly access control measures of the target system through a variety of techniques. The most common method for this is through social engineering techniques such as spear phishing.[6] Emails that target an individual user or organization may include requests for information that can compromise the targeted system or direct the user to a malicious website, a technique known as spoofing. Other methods rely on Trojans that are embedded with malicious code that logs keystrokes or exfiltrate access and authentication credentials automatically. In this situation, the threat will attempt to compromise targets by establishing trust with an enemy user of the targeted system. Once trust is established, the threat uses all available resources to successfully exploit the system.

Attempts to compromise a system through vulnerabilities in the network, the trust management system, or other system design flaws are other forms of infiltration that may occur without users or systems administrators knowing that they have been compromised. The goal of the infiltration phase is to establish access and authorization for the threat within a targeted system without being discovered.[7] Whether the ultimate goal is a targeted attack or an advanced persistent threat or a denial of service attack, it is likely that threat cyber attackers will ensure that they are hidden until the time of execution.

Information and networked systems are usually protected by a variety of security measures and access controls. Infiltration of these advanced systems may require a series of compromises, both in the physical domain as well as the cyber domain. Falsifying credentials in order to obtain access for a particular ICT asset is a form of exploiting holes in the trust management system and may require a variety of methods including physical theft of passwords, compromise of authentication procedures, or fabrication of counterfeit access tools. Another approach may involve the breach of a logical inconsistency in the access control process, as in the case where a third party may have access to an intermediate party which enjoys access to the targeted system and inadvertently allows bypassing control measures.[8]



Operation Ababil

“Operation Ababil’ was the name given by the hacktivist group Cyber Fighters of Izz ad-din Al Qassam” and was a major attack that took place throughout the fall 2012 . The attack was related to a Youtube video promoting an online movie that was deemed offensive to Muslims. The group used a novel type of DDoS attack known as DNS amplification against major financial institutions. These attacks and others appear to be classic cases of Hacktivism by so called nuisance hackers such as the Cutting Sword of Justice, Syrian Electronic Army, and the Tunisian Cyber Army. However, there has been much speculation, some reportedly from the government authorities, that not only are the Cutting Sword of Justice and the Qassam Cyber Fighters fronts for a nation state, but that DDoS attacks may actually be a distraction for Cyber Criminals to transfer funds electronically*.

The infiltration methods used are notable because not only does the target itself need to be compromised but the content management server used in the DNS amplification attack was also penetrated. These resources and methods were either developed by the nation state or purchased from a third party such as a cyber crime organization.

* Symantec, 2013 Internet Security Threat Report Appendix, pg.17

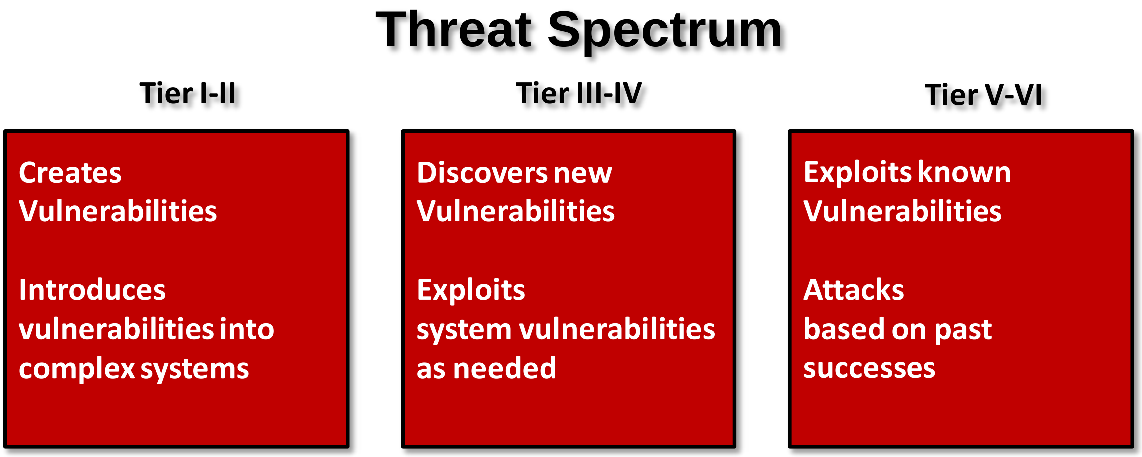
Figure 2. Operation Ababil

Compromising the target and the electronic attack resources is a necessary step to mounting a cyber attack, so the threat is constantly is probing and testing the defenses of targeted information resources. This is mostly accomplished in the reconnaissance phase with the help of malicious software known as scanners and sniffers that probe for security breaches and monitor network traffic. In threat strategic operations, priority is given to known enemy states, military organizations, insurgent groups, and electronic resources such as online phone directories and databases with personally identifiable information. When conflict is evident, as is the case in regional operations, the threat uses its elements of technical overmatch to preclude regional alliances or outside intervention by exploiting systems the threat believes will yield significant intelligence about a high value cyber target.[9]

The breaches most often occur at the end points of an information system with those nodes at the farthest ends of the network most at risk. For example, friendly units will attempt to prevent anti-access and area deniability operations by establishing reliable local resources for their operations requiring access to remote APOD and SPOD locations. The networks established to support this effort may provide for a variety of functions including situational awareness reporting, logistics support, and the transfer of funds to local nationals that support the friendly cause. If not properly monitored and secured, these remote stations will infiltrated through a variety of physical and technological means and compromise the entire mission.

Purely external attacks also known as network attacks usually require a compromise from a system component to be successful. As previously explained, system components that are improperly installed, configured, or secured may offer vulnerabilities unique to the system which have not yet been discovered. This problem does not only apply to command and control (C2) and logistics systems but to various weapons systems as well. For example, early warning systems are vulnerable as they may require analogue inputs from naturally occurring events in order to function. With technical expertise, the threat can exploit this design flaw and conduct cyber attacks. As weapons systems become increasingly dependent on software, computer hardware, and integrated battlefield management systems, the threat of being targeted through cyber means also increases. Active protection systems that rely on inputs from short-range sensors to initiate may have the potential to be spoofed by electronic warfare means into either failing to engage an incoming projectile or firing at a false positive.[10] If the control sequences for the input and output of operational data such as targeting, GPS, and short-range situational awareness systems is compromised, it is possible that a successful infiltration could produce multiple levels of damage from misguiding a platform on its way to an objective to overwriting system controls within the platform.[11]

Tier levels are presented in an ascending order to align with FM/TC 7-100 series conventions. The most capable threat is considered a Tier I threat.


Threat Spectrum
Tier I-II
Tier III-IV
Tier V-VI
Creates Vulnerabilities
Introduces vulnerabilities into complex systems
Discovers new Vulnerabilities
Exploits system vulnerabilities as needed
Exploits known Vulnerabilities
Attacks based on past successes

Insert Figure 3. Threat spectrum and vulnerabilities

Source: *DSB Task Force Report:* Resilient Military Systems and the Advanced Cyber Threat, February 2013

Threat Tier Levels[12]

The ability to create a new vulnerability where one did not exist by developing security breaching code is an example of a tier I-II threat capability. A tier I cyber threat uses both automation and a highly developed targeting process to focus on denying, degrading, disrupting, or destroying secure advanced information systems. The act of maintaining and repeatedly accessing a compromised securing system in order to exploit intelligence surreptitiously is another indicator of a tier I threat known as a targeted attack. Targeted attacks that rely on highly customized intrusion techniques are classified as advanced persistent threats (APT).[13] Generally, the more structured the attack the more evidence of an advanced cyber threat.

Tier III-IV threats discover new vulnerabilities that were previously unknown through a combination of research and electronic reconnaissance. An example might be the discovery of a new zero day vulnerability that is retained by the threat and embedded into a critical industrial control system for use at a later date.

Utilization of known vulnerabilities which may or may not be mitigated by the target system is an example of a tier III-IV cyber threat. These types of attacks are favored mainly by criminal elements that sell and trade known vulnerabilities on message boards and “hacker” forums. These guns for hire may lend their services to governments and/or non-state actors needing cyber warfare capabilities in order to make a profit or to enable some other motivations.

Implications

By understanding the methods by which the threat attempts to infiltrate targeted systems, analysts can establish a model from which to base logical analysis.

In the future, the ability to surreptitiously and quickly steal large volumes of data or to prevent friendly computer network operations on a massive scale represents possible key abilities for future attacks. Most of these advances will be software based and involve advanced encryption and multi-tiered information protection measures. Weaponized computer hardware will be lightweight and durable and bring advanced processing power to the tactical battlefield. These devices, when attached to a local network, will easily locate and analyze vulnerabilities on a targeted network and automatically offer a range of attack options. The result will be advanced cyber capabilities for the local commander that can be launched with minimal involvement from higher levels of command. Once access and authorization have been established, the threat will seek to exploit as much of the system as possible either locally or remotely depending on the complexity and the security of the targeted system.

Although the infiltration step is presented as the second step in the cyber attack lifecycle, 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. In each step there are indications that may aid cyber defenders in discovering the threat intentions. See Red Diamond Volume 4, Issue 2 FEB 2013 article, "Common Cyber Threats and Indicators."

Notes

[1] TRISA, TC 7-100.2, Opposing Force Tactics, Chapter 7 Information Warfare, pp 7-15, 2011.
[2] Lionel D. Alford Jr., Cyber Warfare: The Threat to Weapons Systems, The WSTIAC Quarterly, Volume 9, Number 4, p 4, April 2010.
[3] Amit Sharma,Cyber Wars: A Paradigm Shift from Means to Ends p 8 , August 2009.
[4] Dell SecureWorks Counter Threat Unit TM (CTUTM) Research Team, 2012 Threatscape Report, p 15, May 2013.
[5] Dell SecureWorks Counter Threat Unit TM (CTUTM) Research Team, 2012 Threatscape Report, pp 2-3, May 2013.
[6] Bill Sweetman, Breaching Defense Contractor Data, Aviation Week, p3, September 2012.
[7] Symantec, 2013 Internet Security Threat Report Appendix, p52, April 2013.
[8] Qijun Gu, Peng Liu, and Chao-Hsien Chu, Hacking Techniques in Wired Networks, Pennsylvania State University, p 7, May 2004.
[9] TRISA, FM 7-100.1 Opposing Force Operations, Chapter 1, Strategic Framework, pp 1-10, December 2004.
[10] Thomas Withington, Code of Mass Disruption, Armada International, October/November 2012, p 35.
[11]Lionel D Alford, Jr., Cyber Warfare: The Threat to Weapons Systems, The WSTIAC Quarterly, Volume 9, Number 4, p 6, April 2010.
[12] DSB TASK FORCE REPORT, Resilient Military Systems and the Advanced Cyber Threat, p 10, February 2013.
[13] Symantec, 2013 Internet Security Threat Report Appendix, p 20, April 2013.

AL SHABAAB ATTACK ON THE WESTGATE MALL: NAIROBI, KENYA

Tactics and Techniques in Complex Operational Environments

by Rick Burns, Operational Environment Assessment Team, (BMA Ctr)

Purporting to punish Kenya for its military participation in the African Union Mission in Somalia (AMISOM), on Saturday 21 September 2013 al Shabaab, a Somalia-based militant organization, began a four-day siege and massacre of non-Muslim patrons of the Westgate Mall in Nairobi, Kenya. Planned and reconnoitered over months from the safety of a business setup inside the mall, al Shabaab attacked a place where most Kenyans and foreigners felt safe. The Westgate Mall is a popular place to shop, particularly with foreigners living in Nairobi, and viewed as a secure place with shops, a large supermarket, banks, a theater, a food court, etc. The attack on the Westgate Mall by al Shabaab militants also guaranteed international media attention, with large numbers of foreign patrons in the mall on a busy Saturday.

The attack also represents a significant evolution in al Shabaab's capabilities and will attract foreign fighters to its cause. From the safety of the business it had setup in the mall, al Shabaab operatives spent months pre-positioning weapons and conducting reconnaissance of the mall. Al Shabaab has easy access to safe havens within the prosperous Eastleigh neighborhood, among thousands of Somali refugees that have flooded to Kenya, and in other parts of Kenya where ethnic Somalis live. The Westgate Mall attack has raised the security stakes in Kenya and the region.

Al Shabaab is a militant Islamist group formed and operating primarily in Somalia. AMISOM has had significant success against al Shabaab, pushing its operations into the more rural areas of southern and central Somalia. The organization was formed in 2002 by a small group of Somali veterans of the jihadist training camps in Afghanistan. Between 2004 and 2006 it operated as a militia affiliated with the Union of Islamic Courts (UIC). The UIC, previously a confederation of clanbased court militias, developed into a collective of formerly independent jihadist groups like al Shabaab. Within the new organization, al Shabaab leaders held a number of important positions, to include the General Secretary of the Executive (led by Ahmad Abdi Aw Muhammad Godane) and overall command of the newly combined militia (led by Aden Hashi Farah Ayro).

After the Ethiopian intervention in Somalia and the defeat of the UIC in December 2006, al Shabaab carved out an independent ideological position and established itself as the leading insurgent organization operating in Somalia. Since the formation of the Somalia Transitional Federal Government (TFG) in Nairobi, Kenya in 2004, al Shabaab has dedicated itself to overthrowing the TFG and establishing an Islamic government in accordance with its radical interpretation of *sharia* law. AMISOM has proven to be a formidable obstacle to al Shabaab's efforts, but al Shabaab has proven capable of hitting targets inside and outside of Somalia. Indeed, al Shabaab has been able to attract foreign fighters and is having success in attacking regional African targets.

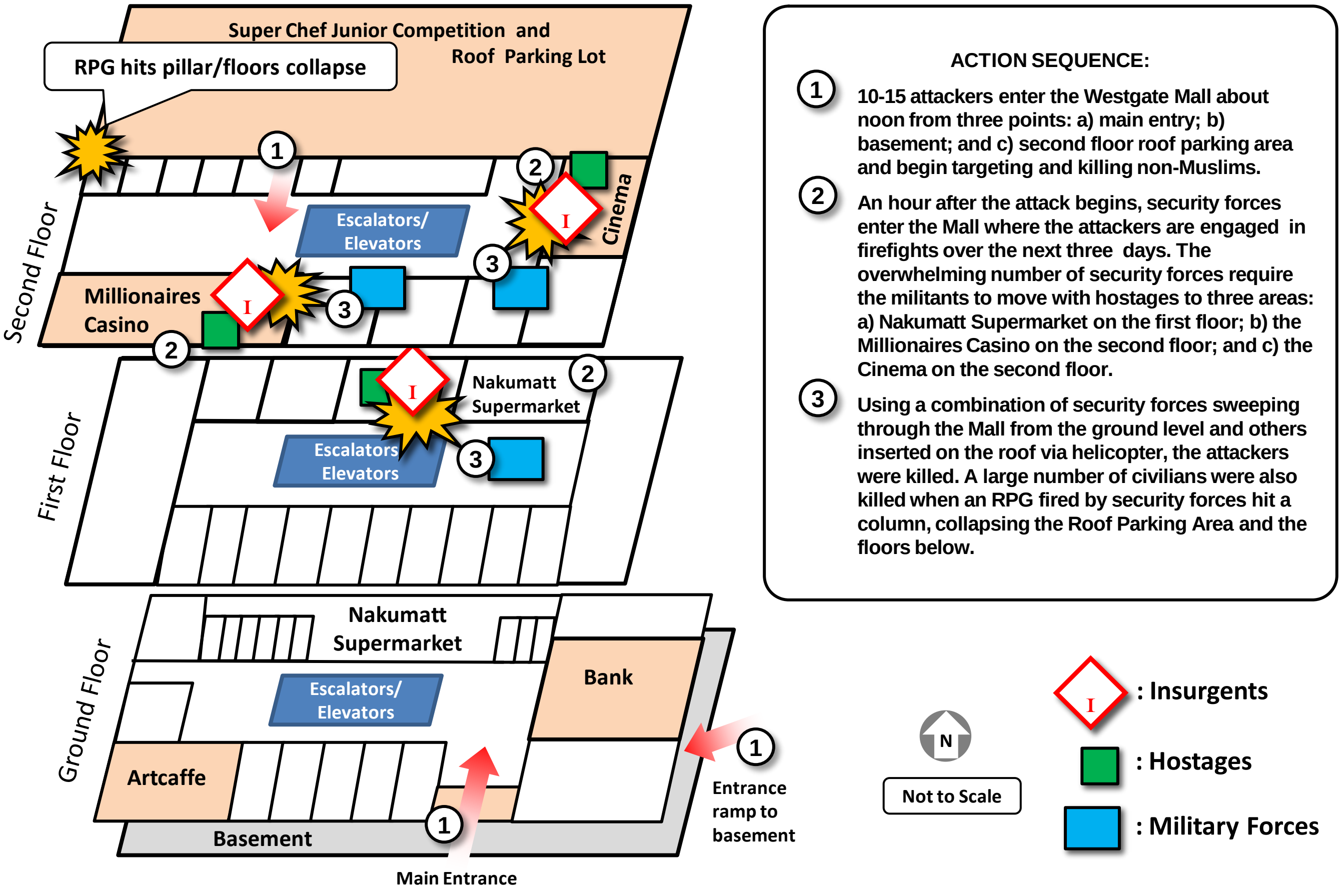
Kenya has been flooded with refugees fleeing decades of violence and insecurity in Somalia. Large numbers of refugees now residing in Kenya, many now Kenyan-born, have created safe havens for Somali terrorists and headaches for Kenyan security forces. One area of concern is the Eastleigh district in eastern Nairobi. Eastleigh is a thriving and economically productive neighborhood populated mostly by Somalis. The area allows Somali terrorists to easily hide, recruit, and lobby for funding. It has also been the site of terrorist attacks against targets that have included both Somalis and other Kenyans. A 19 November 2012 US State Department security message warned Americans to avoid Eastleigh due to unrest after an al Shabaab attack on a bus in Eastleigh. Follow-on clashes between Kenyans and Somalis and security forces have contributed to continued insecurity in Nairobi. Relations between security forces and the Somali community have been strained, as terrorist attacks increased with Kenya's involvement with AMISOM. Distrust and animosity continue to grow on both sides as Kenyan security forces use sweeps through Somali neighborhoods, detaining many Somalis, and Somali terrorists attack security forces from the midst of Somali neighborhoods.

Both the Kenyan government and al Shabaab attempted to use social media during the Westgate attack. Twitter has consistently shut down accounts thought to be created by al Shabaab shortly after they are created. In the nine months preceding the attack, at least twice, accounts believed to be al Shabaab's were shut down. Each time, however, accounts reappear under slightly different names. This makes it difficult to determine which are genuine and legitimately coming from al Shabaab. During the Westgate attack, an account believed to be linked to al Shabaab began putting out messages stating that the attack was in retaliation for Kenyan incursions into Somalia, and referred to bringing the fight to Kenyan infidels on their own ground. The account was shut down, but others using similar language appear regularly in a cycle.

The al Shabaab messages clearly responded to the international coverage of the attack. One area of note was the rumored existence of a female involved in the attack, referencing specifically the possibility of Samantha Lewthwaite's involvement. Lewthwaite is the British widow of one of the bombers that carried out the 7/7 attack in London in 2005. She is wanted in Kenya for possession of explosives and conspiracy to commit a felony, charges dating back to December 2011. Often referring to the "white widow" nickname the Western media has given Lewthwaite, al Shabaab sources denied the claim that any females were involved in the Westgate attack. Al Shabaab messages went so far as to claim there were sufficient young men willing to take part in these attacks and that they had no need to send their women into such military operations.

In the aftermath of the siege, al Shabaab sought to explain its defeat by accusing the Kenyan government of using chemical weapons. In a series of tweets believed to be linked to al Shabaab, the group states that being unable to defeat their mujahideen opponents inside the mall, the authorities used chemical gases. Al Shabaab further alleges that the Kenyan security forces used explosives to bury the bodies and evidence.

The clear advantage in communicating via social media goes to the government; however the Kenyan government was challenged by message inconsistencies. As an example, on the third day of the attack Kenyan Foreign Minister Amina Mohamed stated in a television interview that two to three Americans and one British woman were among the attackers. On the same evening, Mohamed's Cabinet Secretary Joseph Ole Lenku sent a tweet stating that all of the terrorists were male. The Monday following Saturday's attack, several accounts began suggesting the ordeal was coming to a close. Kenyan security forces retweeted congratulatory messages regarding the success of the operation. The reality was much different, causing the government's messages to lose credibility.



ACTION SEQUENCE:

1 10-15 attackers enter the Westgate Mall about noon from three points: a) main entry; b) basement; and c) second floor roof parking area and begin targeting and killing non-Muslims.

2 An hour after the attack begins, security forces enter the Mall where the attackers are engaged in firefights over the next three days. The overwhelming number of security forces require the militants to move with hostages to three areas: a) Nakumatt Supermarket on the first floor; b) the Millionaires Casino on the second floor; and c) the Cinema on the second floor.

3 Using a combination of security forces sweeping through the Mall from the ground level and others inserted on the roof via helicopter, the attackers were killed. A large number of civilians were also killed when an RPG fired by security forces hit a column, collapsing the Roof Parking Area and the floors below.

Figure 1. Insurgent entry points and final positions in Westgate Mall assault and hostage-taking

The attack lasted four days during which security forces attempted to secure the large, multi-level mall.

Saturday, 21 September 2013

About noon, the attackers entered the mall from three points: a) the front main entrance; b) a basement entrance; and c) a second floor parking area. It is likely those entering from the main entrance and those entering from the basement linked up on the ground level. Here the terrorists began shooting and throwing grenades, specifically targeting non-Muslims. Thousands of shoppers began fleeing and hiding. The al Shabaab militants strolled through stores and cafes quizzing potential victims on Muslim prayers and other Muslim-identifying questions in order to segregate Muslims from others. Reports indicated that some were tortured. Specifically targeted was the Israeli-owned Artcafe on the main floor.

The terrorists moving to the second floor via the roof parking area initially met 30 children and accompanying adults involved in a children's cooking contest. The terrorists threw a grenade and began shooting, killing an estimated 25 men, women, and children. Upon entering the second floor, they continued to target non-Muslims and began corralling hostages.

Thirty minutes into the attack, Kenyan security forces arrived and set up a perimeter around the mall. Thirty minutes after establishing a perimeter, the security forces entered the mall. Firefights between the attackers and security forces ensued during which the terrorists on the ground level consolidated in the Nakumatt Supermarket on the first floor.

Sunday, 22 September 2013

By Sunday, Kenyan officials believed there were approximately 10-15 attackers remaining. Gunfights continued throughout the day. At 1845 two helicopters landed on the roof as part of an operation to retake the mall. A large explosion was heard.

Monday, 23 September 2013

The remaining terrorists were holed up in three places with hostages. A group on the second floor held hostages in the Millionaires Casino and the Cinema. A second group was confined to the first floor Nakumatt Supermarket area. Four blasts were heard from outside the mall. At least one of these was caused by an rocket propelled grenade (RPG) fired by a member of the Kenyan security forces hitting a support column that collapsed a part of the roof car parking area and the levels below it.

Tuesday, 24 September 2013

In the early morning hours, gunfights ensued again, even though security forces were publically stating they had control of the mall. Security forces made sweeps through the mall where fires believed to be set by the al Shabaab militants filled parts of the building. By Tuesday evening, President Uhuru Kenyatta declared the building secured and the militants killed.

The Westgate Mall attack showed both patience and sophisticated planning, both evidence of an evolving and increasingly dangerous regional al Shabaab organization. Moving beyond attacks in Somalia with native Somalis, al Shabaab is now a regional threat with capabilities drawn from international fighters and resources. With a large population of Somalis and their growing resentment of Kenyan security forces, al Shabaab has found safe haven in Kenyan cities and among occupants of refugee camps. Sympathetic Somali businessmen are a ready resource of financial and other resources.

The Westgate attack took months of planning and positioning. It was a carefully chosen target for its immediate international impact. Either through bribery, lack of intelligence vigilance, or dumb luck, al Shabaab successfully operated a store out of the mall for months. This access to the mall allowed easy surveillance and the pre-positioning of weapons. Familiarity with the mall allowed some advantage, but only up to the point where the perpetrators had weapons superiority and a panicking mass of people. Once the Kenyan security forces appeared, the inevitable end should have been clear to the assailants. The intent, therefore, seems to have been to create as many non-Muslim and international casualties as possible. In this way al Shabaab weakened Kenya both economically and politically and punished it for its military operations in Somalia.

Al Shabaab has also made progress in using social media such as Twitter. During the siege, al Shabaab tweeted under a number of different names, most accounts being shut down soon after. The tweets, however, showed that al Shabaab was following and responding to international coverage of the attack. As a follow-up to the final defeat of the attackers, al Shabaab tweeted that the reason they were defeated was that the Kenyan government had used chemicals, and then demolished the roof parking area to cover up the deed. This is likely an attempt to tie the Kenyan government to international sensitivity to and concern over Syrian chemical weapons. At a minimum it was an incitement to other jihadis to join them in a fight against a Kenyan government that does not play fair.

The increasingly tense relations between ethnic Somalis (both those born in Kenya and immigrants), Kenyan security forces, and Kenyans generally, will continue to complicate the efforts to root out al Shabaab operatives from Kenya. The Westgate Mall attack will not make these relationships easier. Pressure from a citizenry demanding security and security officials, frustrated at not being able to provide that security, often cause overreach. The painstaking work of vetting intelligence data and responding proactively never keeps pace with demands made by a fearful public. The alternative to good intelligence work, however, will be to aid al Shabaab in its efforts to recruit those who feel persecuted and mistreated simply because they are Somali.

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
Terror
Hybrid
EXD
Irregular Opposing Forces
Decisive Action Training Environment
OE
TTP
DATE
Worldwide Equipment Guide
WEG
Red Diamond
Training
Enemy
OEA
Threat
TRISA
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

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

COMING in 2013:

TC 7-100.3
Irregular Opposing Forces

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

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

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

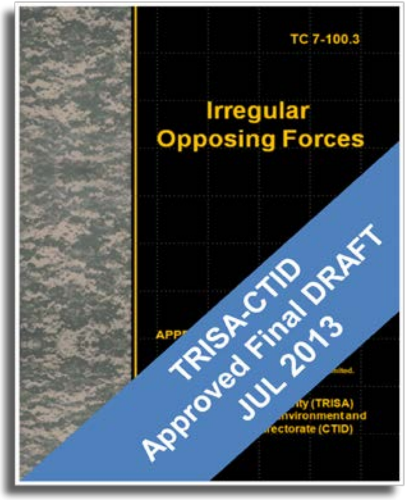
A: AKO access, see CTID Approved Final Draft TC 7-100.3
https://www.us.army.mil/suite/doc/40913959

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?

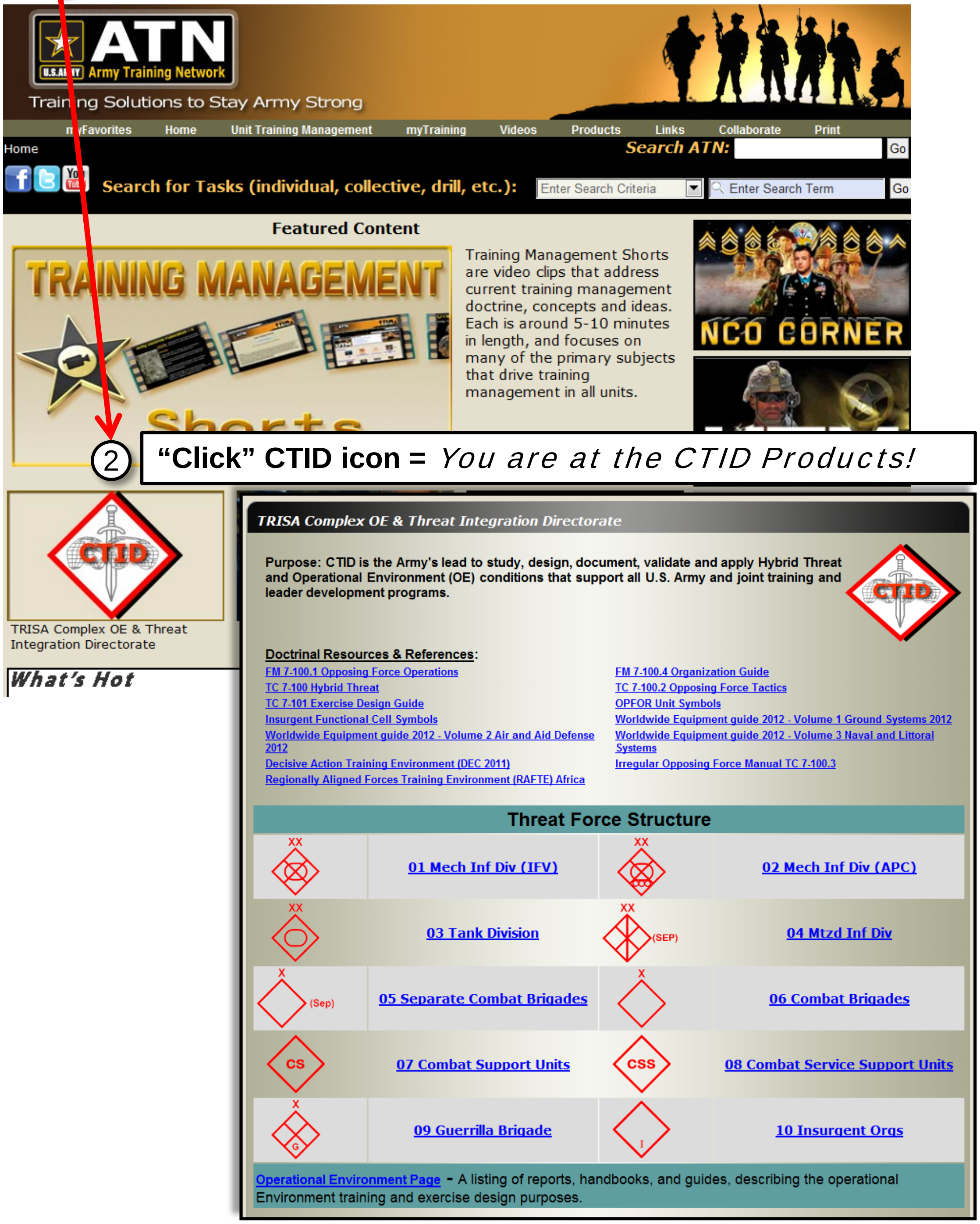
A: Send us a request for information (RFI).



“QUICK-EASY-EFFICIENT” = TWO “CLICKS” TO TRISA-CTID PRODUCTS

Go to Army Training Network

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



Training Management Shorts are video clips that address current training management doctrine, concepts and ideas. Each is around 5-10 minutes in length, and focuses on many of the primary subjects that drive training management in all units.

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

TRISA Complex OE & Threat Integration Directorate

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.

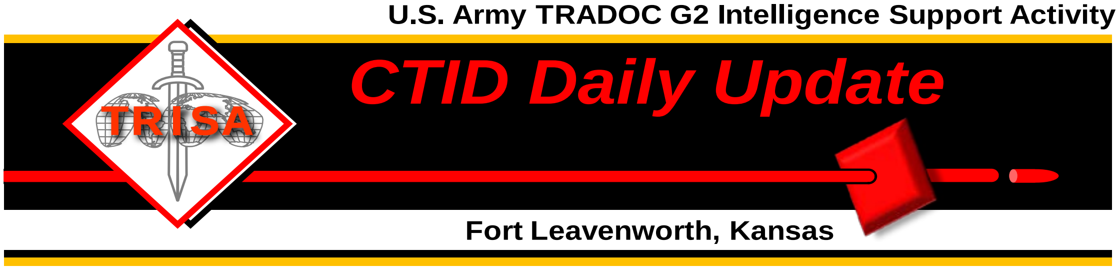
NEW! **For** *easy access to CTID Products on ATN—“click”*

https://atn.army.mil/dsp_template.aspx?dpID=379

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.



October 2013 List for Red Diamond:

2 October. Somalia: Al-Shabaab pledge terror campaign against Kenya

Russia: Four militants killed in special operation in Dagestan

4 October. Japan: US, Japan agree to expand security, defense cooperation

Libya: Russian Embassy in Libya attacked, one Libyan killed, four wounded

7 October. Al-Qaeda: US military captures Anas al-Liby in Tripoli

Afghanistan: Four US Soldiers killed by Afghanistan bomb

9 October. Al-Qaeda: Suez Canal targeted: Muslim Brotherhood fighters join forces with al-Qaeda insurgents

DPRK: North Korea restarts the Yongbyon plutonium reactor

11 October. Philippines: Villagers flee as MILF units clash in wake of deadly ambush in Maguindanao town

US: Canadian who spent seven years on the run pleads guilty to aiding arsons in US eco-terrorism case

16 October. Argentina: Two terrorist groups with ties to Hezbollah are operational in Latin America

Syria: 41 killed in Syria Kurd-Jihadist fighting

18 October. Al-Qaeda: AQAP video details suicide assaults against Yemeni bases in Shabwa

Cyber security: Indonesia passes China to become top source of cyber-attack traffic

U.S. ARMY
You are the first line of defense for
CYBERSECURITY.
STOP, THINK, CONNECT - ACT RESPONSIBLY
National Cybersecurity Awareness Month - October 2013
Army IA/Cybersecurity Awareness Week 14-18 October 2013

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