

# **Operational Environment Enterprise**

## **US TRADOC G2 Intelligence Support Activity**



# **Red Diamond**

**Complex Operational Environment  
and Threat Integration Directorate**

**Fort Leavenworth, KS**

**Volume 5, Issue 8**

**AUG 2014**

### **INSIDETHIS ISSUE**

UK Iron Resolve.....	4
Threat Recon .....	6
IED Bombing: Libya .	14
Antiterrorism-T3 .....	18
CTC Program .....	19
OE at JMRC.....	21
Terror in PRC .....	26
CTID POCs .....	30

**OEE Red Diamond  
published monthly  
by TRISA at CTID**

**Send suggestions to  
CTID**

**ATTN: Red Diamond  
Dr. Jon H. Moilanen  
CTID Operations  
BMA Contractor  
and  
Angela Wilkins  
Chief Editor  
BMA Contractor**



## **Antiterrorism Awareness and the Threat**

**August 2014-Army Antiterrorism Awareness Month**

by CTID Operations, Threats Terrorism Team (T3)

The Army used August 2014 to focus attention on *Army Antiterrorism Awareness*. One example of emphasis is to understand actions or suspicious activities that might indicate a pending swarm attack. The terrorist attack on Mumbai (2008) provides a model for Army learning. Consider the uncertain response and swarm tactics in your operational-institutional antiterrorism (AT) plans and exercises. Army leaders can shape awareness and understanding of threats, and integrate robust, realistic, and relevant threats into training and education venues. This suggests the value of AT training, professional education, and leader development to mitigate or prevent future incidents such as swarm attacks, home-grown violent extremism (HVE), and/or insider threat crimes and active shooter assaults.

Our Army must sustain a strong defensive posture to prevent violent acts and protect Army resources of people, infrastructure, and information. By leveraging lessons learned, case studies, doctrine, tactics, techniques, and antiterrorism assessments, the Army is better prepared and ready to combat terrorism.

### **Combating Terrorism (CbT)**

**The broader construct of CbT are actions, including antiterrorism (AT) and counterterrorism (CT), taken to oppose terrorism throughout the entire threat spectrum...CbT is both a battle of arms and ideas—a fight against the terrorists and the ideology which drives terrorism.**

**JP 3-07.2, Antiterrorism (2014)**

## RED DIAMOND TOPICS OF INTEREST

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

Following a cover article about *Army Antiterrorism Awareness*, this issue leads with an article on use of the *Decisive Action Training Environment* (DATE) and opposing force (OPFOR) in the United Kingdom's premier land training event for 2014, Exercise Iron Resolve (Ex IR). The UK Liaison Officer to TRISA discusses the 3<sup>rd</sup> UK Division training with operational environments (OEs) in [DATE 2.1](#).

Threat OPFOR tactics during reconnaissance are based on a composite of enemy and/or adversary actions experienced in recent and contemporary operations. "Threat Reconnaissance" reflects tactical functions as stated in US Army training circular [\(TC\) 7-100.2](#).

One article spotlights a "Targeted Assassination in Libya" technique to plant an improvised explosive device (IED) on the victim's vehicle. Another article details an incidence of terrorism with an IED event in

the Peoples Republic of China against citizens by a terrorist organization in a relevant population.

JMRC planners have adapted doctrine established in [Training Circular \(TC\) 7-101, Exercise Design](#), in order to synchronize the exercise scenario and promote shared understanding across JMRC's operations group. Every JMRC exercise includes a different set of training locations in Europe and different multinational participants on both BLUEFOR and OPFOR.

TRISA continues its regular situational awareness of terrorism and antiterrorism in our CTID training literature.

Email your topic recommendations to:

**Dr. Jon H. Moilanen, CTID Operations, BMA CTR**

**[jon.h.moilanen.ctr@mail.mil](mailto:jon.h.moilanen.ctr@mail.mil)**

and

**Angela M. Wilkins, Chief Editor, BMA CTR**

**[angela.m.wilkins7.ctr@mail.mil](mailto: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.



## Director's Corner: Thoughts for Training Readiness

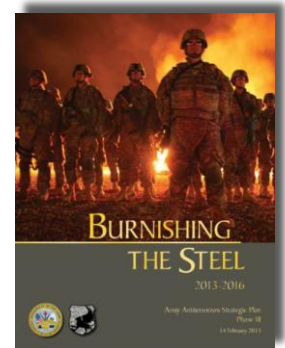


by [Jon Cleaves](#), Director, Complex Operational Environment and Threat Integration Directorate (TRISA-CTID)

August is US Army Antiterrorism (AT) Awareness Month. Terrorism is an enduring, persistent, worldwide threat to our Nation and Army forces. Knowing the threats and understanding enemies is fundamental to effective antiterrorism awareness. Understanding terrorism often centers on the emotional and psychological motivations that prompt such actions, as well as the physical impacts of terrorism. Terrorists use violence or the threat of violence.

Assessing and evaluating terrorism ranges a broad spectrum of threats including traditional state-sponsored terrorism, networks of non-state actors, insurgent organizations, guerrilla units, extremist groups, criminal organizations, and/or radicalized individuals acting alone. A clear understanding of adversaries and enemies remains key to ensuring the safety of US citizens at home and abroad from the threat of terrorism. As the defensive element of a global fight against terrorism, AT spans the full spectrum of Army operations that includes expeditionary, in-transit, garrison, standalone facilities, and individual protection.

The TRADOC G2 Intelligence Support Activity (TRISA) through its Complex Operational Environment and Threat Integration Directorate (CTID) teaches a “Threat Tactics” course at Fort Leavenworth that includes the threat of terrorism in current complex environments. Previous courseware is being revised with additional hybrid threat understanding for the next scheduled resident “Threat Tactics” five-day course in March 2015. Mobile training teams (MTT) are also available from CTID to conduct tailored threat tactics training at unit and activity locations.



The TRISA-CTID “Threat Tactics” course applies the *threat*—any combination of actors, entities, or forces that have the capability and intent to harm United States forces, United States national interests, or the homeland—as an *opposing force* (OPFOR). In accordance with AR 350-2, this OPFOR construct for Army training provides “a plausible, flexible military and/or paramilitary force representing a composite of varying capabilities of actual worldwide forces, used in lieu of a specific threat force for training and developing US forces.”

Terrorism and the tactics and techniques used by terrorists vary dependent on a number of circumstances and conditions to produce fear and/or anxiety in an intended audience. Actions can be small in scale and isolated, or combine as nearly simultaneous incidents. Other actions can be large scale and cause significant disruption or damage to social and economic systems such as tourism, financial networks, or agricultural production and delivery. Incidents over a period of time can be a factor used to erode the confidence of a relevant population, and challenge the legitimacy of a government or society terrorists target while promoting their own agenda for acceptance.

As CTID approaches its missions in fiscal year (FY) 2015, we will integrate the Army’s quarterly antiterrorism awareness themes into our doctrinal literature, education, and training venues, and support the *Army Antiterrorism Strategic Plan (ATSP) 2013-2016*. Quarterly themes for FY 2015 are:

- (1st Q) **Antiterrorism Criticality Assessments.**
- (2d Q) **Antiterrorism Operations in Field Units.**
- (3d Q) **Antiterrorism Area of Responsibility (AOR) Awareness.**
- (4<sup>th</sup> Q) **Antiterrorism Training.**

For more information, contact CTID: [penny.l.mellies.civ@mail.mil](mailto:penny.l.mellies.civ@mail.mil) or [jon.h.moilanen.ctr@mail.mil](mailto:jon.h.moilanen.ctr@mail.mil).

JON



# Decisive Action Training Environment



## 3 (UK) Division

## Capability Concept Demonstrator Exercise **IRON RESOLVE**

by [Matt Tucker](#), Warrant Officer, Class 2, UK LNO to TRADOC G2 Intelligence Support Activity (TRISA)

Over the last few years as the British Army has been rebalancing for post-Afghanistan conflicts, it has become increasingly interested in using the Decisive Action Training Environment (DATE) as an operational environment for training. During the last year, liaison and coordination has taken place with TRADOC, primarily conducted by the Land Scenario Centre (LSC) based in Warminster, England, and remarkable progress has been made. This October, the 3<sup>rd</sup> UK Division will partake in the UK's premier land training event for 2014 called Exercise Iron Resolve (Ex IR) and it will train on and against the TRISA-produced [DATE 2.1](#) and the [TC 7-100 Opposing Force Series](#).

### Who Are the 3<sup>rd</sup> UK Division?

The Iron Division traces its history back to 1809 when the Duke of Wellington first decided to adopt a permanent divisional structure in the British Army. The division's first General Officer Commanding (GOC) was Major General Picton, a Welshman, who molded the division in his own image: resolute, tough, slightly eccentric, and full of fighting spirit. Their battle honors include Waterloo and D-Day; they are based on Salisbury Plain and are the only UK division at continual operational readiness.

### Exercise Iron Resolve

Exercise IRON RESOLVE will test the 3<sup>rd</sup> Division in its preparedness for a major warfighting role whilst developing a people-centric approach. It will test Offensive Action, Enabling Action, and Defensive Action; Shaping and Influence Operations; and Divisional Deep Operations in a constructive environment. The scenario is bespoke for the exercise; it is based around an Arianian and Minarian coalition invasion of Atropia, with objectives to secure the Minchaevan Dam and capture oil fields in the Caspian Sea. The UK Division, as part of a Coalition Force, will deploy by sea to Baku and then plan and execute a number of operations culminating in the retaking of the hydro-electric dam. The scenario will be further developed for the division's subordinate brigades in 2015. (See Figure 1, next page.)

**TRADOC Support to Ex IR.** The exercise is deliberately being written, organized, and executed without US Army support to ensure that the DATE OE works for the British. However, there are a small number of observers from TRADOC G2 attending the exercise to provide mentorship. TRISA is supplying guidance on DATE methodology and providing training and assistance with the execution of the OPFOR. The Training Brain Operations Center (TBOC) will support the LSC by helping to deliver the complexity and depth of the operational environment through background message traffic and MSEL [master scenario events list] injects.



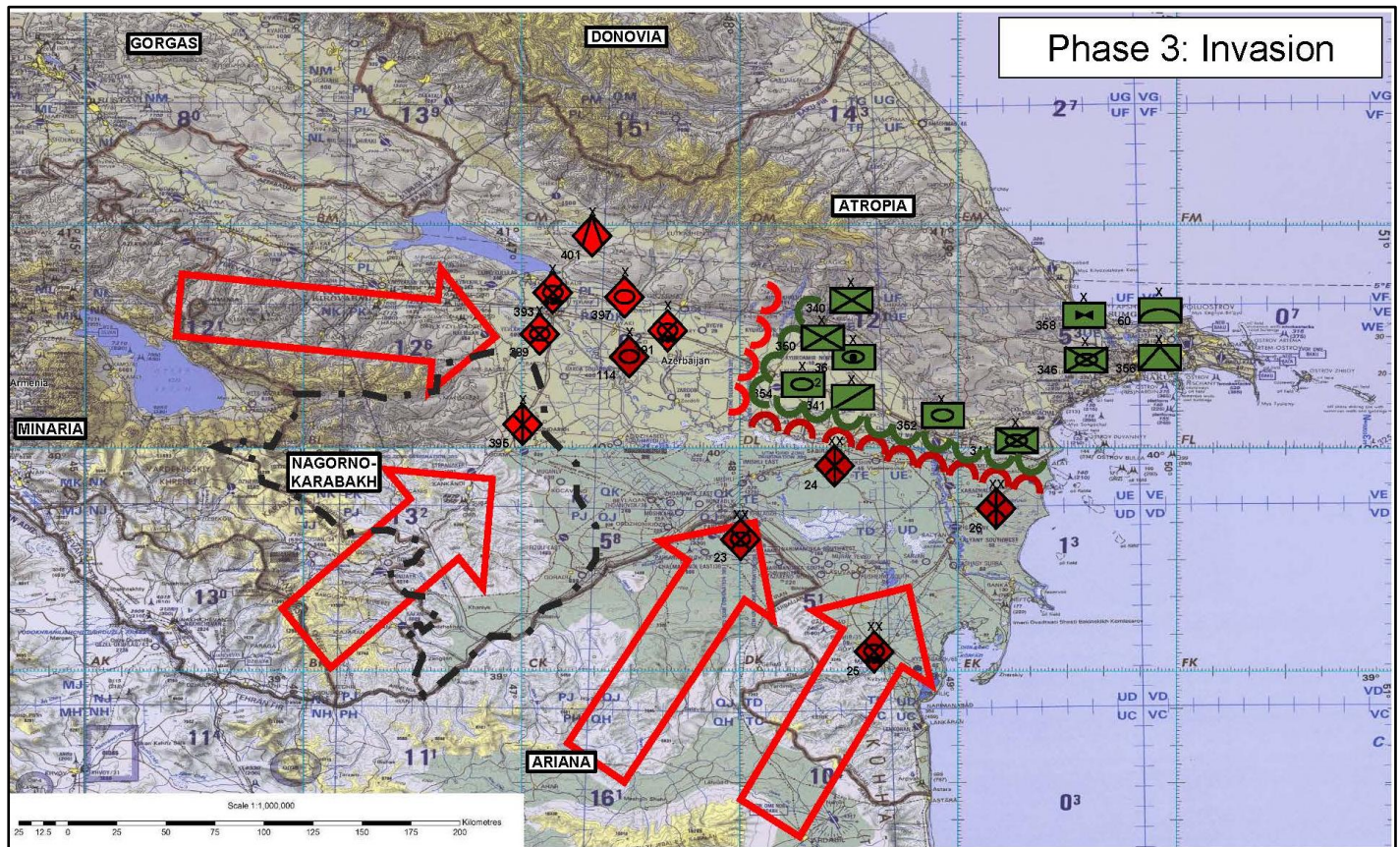


Figure 1. Exercise phase three concept (example)

**DATE in the British Army.** The British Army identified the need for an evidence-based composite operational environment and threat to frame its training a number of years ago, but the drive to test the DATE OE for suitability has been a recent initiative. Following Ex IR, the British Army Command Group will be delivered a briefing stating the suitability of DATE for British Army training and the associated resource bill. If approved, an implementation plan will be devised with the aspiration to use the DATE OE across Collective and Individual training at division level and below in the live, virtual, and constructive environments.

## DESCRIBING A THREAT AND A HYBRID THREAT—COMMON UNDERSTANDING

CTID Operations, Complex Operational Environment and Threat Integration Directorate (CTID)

### Threat

Any combination of actors, entities, or forces that have the capability and intent to harm United States forces, United States national interests, or the homeland.

### Hybrid Threat

The diverse and dynamic combination of regular forces, irregular forces, terrorist forces, and/or criminal elements unified to achieve mutually benefitting effects.

ADRP 3-0, *Unified Land Operations*





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

For threat forces, an essential component of military action is *reconnaissance*. Reconnaissance represents all measures associated with organizing, collecting, and studying information on an operational environment (OE) in areas of current and/or future operations. Aggressive and continuous reconnaissance supports timely accomplishment of combat missions with minimal losses.

The opposing force (OPFOR) in US Army training commits significant resources to any reconnaissance mission. Threat OPFOR tactics during reconnaissance are based on a composite of enemy and adversary actions experienced in recent or contemporary operations. Whether focused on reconnaissance or other tactical functions, the fundamental reference for threat tactics is US Army Training Circular [\(TC\) 7-100.2](#).

#### **Opposing Force (OPFOR)**

**An opposing force is a plausible, flexible military and/or paramilitary force representing a composite of varying capabilities of actual worldwide forces, used in lieu of a specific threat force for training and developing US forces.**

**Army Regulation 350-2, *Opposing Force (OPFOR) Program***

**The US Army TC 7-100 series describes the doctrine, organizations, and equipment of OPFOR and how to combine it with other operational variables of an operational environment to portray the qualities of a full range or tailored set of conditions appropriate to Army leader development, training, and education environments.**

Organizational structure of threat regular and irregular-paramilitary forces is presented with diagrams, weapons and systems listings, and narrative in field manual [\(FM\) 7-100.4](#) and its “[Threat Force Structure](#)” organization folders on the Army Training Network (ATN) website. This manual is transitioning to a US Army training circular 7-100.4 by 2015. Source data for irregular forces and elements such as guerrillas, insurgents, criminals, and active or passive supporters of such units, cells, and/or organizations is in [TC 7-100.3](#). This TC published in 2014 also addresses the specter of terrorism that can be employed by regular and irregular threats in complex OEs. Details on weapon system and equipment capabilities and limitations are located in volume 1 of the Army TRADOC G2 *Worldwide Equipment Guide* ([WEG](#)).

#### **Reconnaissance, Intelligence, Surveillance, and Target Acquisition (RISTA)**

Reconnaissance is part of the threat military function called *reconnaissance, intelligence, surveillance, and target acquisition* (RISTA). RISTA is the combination of capabilities, operations, and activities using all available means to obtain information concerning foreign nations; areas of actual or potential operations; and/or strength, capabilities, location, status, nature of operations, and intentions of hostile or potentially hostile forces or elements. Objectives include production of intelligence resulting from the collection, evaluation, analysis, and interpretation of such information. Detection, identification, and location of targets permit the effective decisions and employment of weapon systems.

## Reconnaissance Organizations

For the threat, the term *reconnaissance unit* refers to a unit composed of specialized reconnaissance teams and soldiers. In contrast, the threat term *reconnaissance element* refers to any unit or task organization given a specific reconnaissance mission regardless of the types of assets involved. A reconnaissance element is tailored to conduct designated functions. For example, signals reconnaissance assets include radio intercept and direction-finding (DF) and radar intercept and DF systems. These assets can also include specialized equipment designed to exploit signals from cellular, digital, satellite, fiber-optic, and computer network systems.

**Note.** In this threat reconnaissance context, the terms *unit* and *element* are not to be confused with the threat generic descriptions of *force* or *element*. These latter threat terms designate the generic size of a threat organization with a *force* being brigade-size or higher echelon. An *element* is battalion-size or lower echelon. (See chapter 2, TC 7-100.2 for additional information.)

### Reconnaissance Patrol

A *reconnaissance patrol* (RP) is generally a platoon-size tactical reconnaissance element with the mission of acquiring information about the enemy, terrain, and/or other OE conditions. While an RP is typically combined arms, it is organized based on the commander's requirements, available assets, and the particular OE.

The smallest element typically expected to conduct independent or semi-independent patrolling is a platoon-size, mounted and/or dismounted organization. A platoon is designed to—

- Serve as the base of forming a functional element or patrol.
- Conduct independent fire and maneuver when required.
- Fight as an integrated subordinate element of a company, battalion, or detachment.
- Execute a tactical task. A platoon is not typically tasked to perform two or more tactical tasks simultaneously. Platoons and squads can be task-organized for specified missions.



The threat distinguishes among various types of patrols under the descriptive term reconnaissance patrol. Although the various specific types of reconnaissance are beyond the scope of this article, units can be tailored as an independent reconnaissance patrol (IRP), officer reconnaissance patrol, engineer reconnaissance patrol (ENP), chemical, biological, radiological and nuclear (CBRN) reconnaissance patrol, or fighting patrol (FP).

Reconnaissance patrols may operate with *affiliated* and/or associated elements in an OE. In organizational charts, an affiliated status is reflected by a dashed line connecting the affiliated force to the unit with which it is affiliated. Command and control (C2) and/or coordination among threat elements in an affiliated relationship are based on mutual agreement of leaders and are temporary in nature. There is typically no formal indication of this affiliated relationship in threat plans and orders; however, the acronym AFL can be used next to unit title or symbol.

#### Affiliated Organization

**An organization operating in a unit's area of responsibility that the unit may be able to sufficiently influence to act in concert for mutual benefit and a limited time. No command and control relationship exists between an affiliated organization and the unit with which it operates. Affiliates are typically nonmilitary or paramilitary groups such as guerrilla units, insurgent cells, criminal organizations, or other actors in an operational environment.**

The example in Figure 1 displays a possible tailored configuration of a reconnaissance platoon in a mechanized infantry battalion in FM 7-100.4. In addition to the platoon's command reconnaissance squad, three reconnaissance squads, and high mobility reconnaissance squad, the platoon is task-organized with two main battle tanks, one self-propelled combination gun, and has an affiliated guerrilla squad.

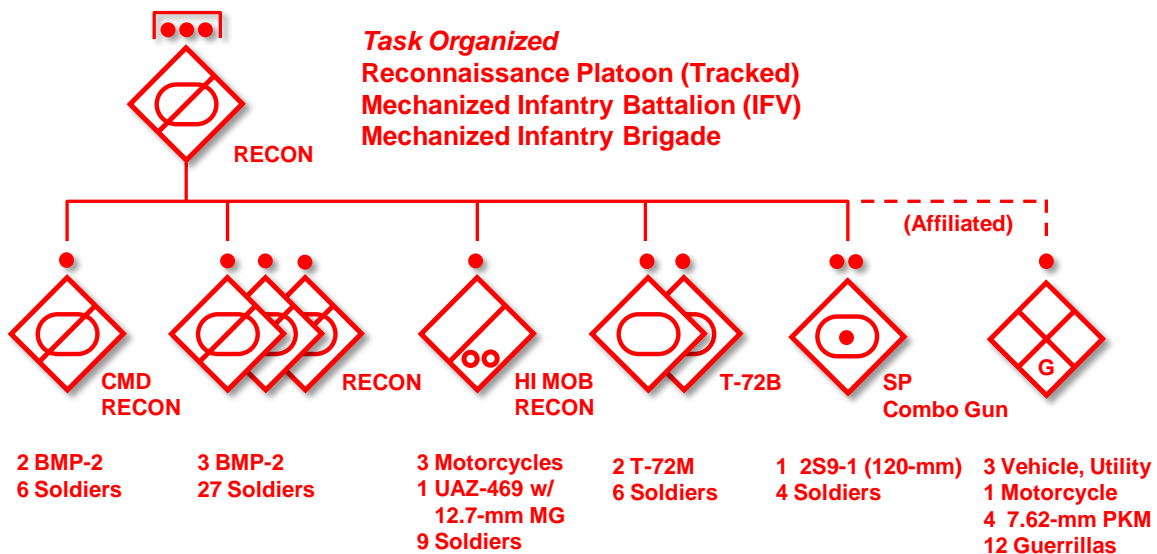


Figure 1. Platoon-size reconnaissance patrol (hybrid threat) (example)

The threat also uses the term reconnaissance patrol to describe a tactical reconnaissance element from a reconnaissance detachment. This type of RP is not independent because it is a subordinate of a larger reconnaissance unit.

#### Reconnaissance Detachment

The largest element the threat employs at the tactical level to supplement specialized reconnaissance units is the *reconnaissance detachment* (RD). This detachment is typically a task-organized combat arms company or battalion. This tailored organization often includes tanks, air defense, artillery, engineers, and/or CBRN capabilities. The RD normally employs platoon-size *reconnaissance patrols* (RPs) to reconnoiter specific objectives in an assigned zone of reconnaissance responsibility (ZORR).

#### Area of Responsibility (AOR)

The threat defines an *area of responsibility* (AOR) as the geographical area and associated airspace within which a commander has the authority to plan and conduct combat operations. An AOR is bounded by a *limit of responsibility* (LOR) beyond which the unit may not operate or fire without coordination through the next-higher headquarters.

An AOR typically consists of three basic zones: *battle zone*, *disruption zone*, and *support zone*.

#### Zone of Reconnaissance Responsibility (ZORR)

Each tactical-level unit down to battalion or detachment has one or more zone(s) of reconnaissance responsibility (ZORR). A ZORR is the combination of a unit's AOR and the area outside of the AOR that can be observed by the unit's technical sensors. As a ZORR extends into adjacent unit AORs, coordinated overlapping coverage prevents surprise and enemy exploitation of boundaries between AORs.

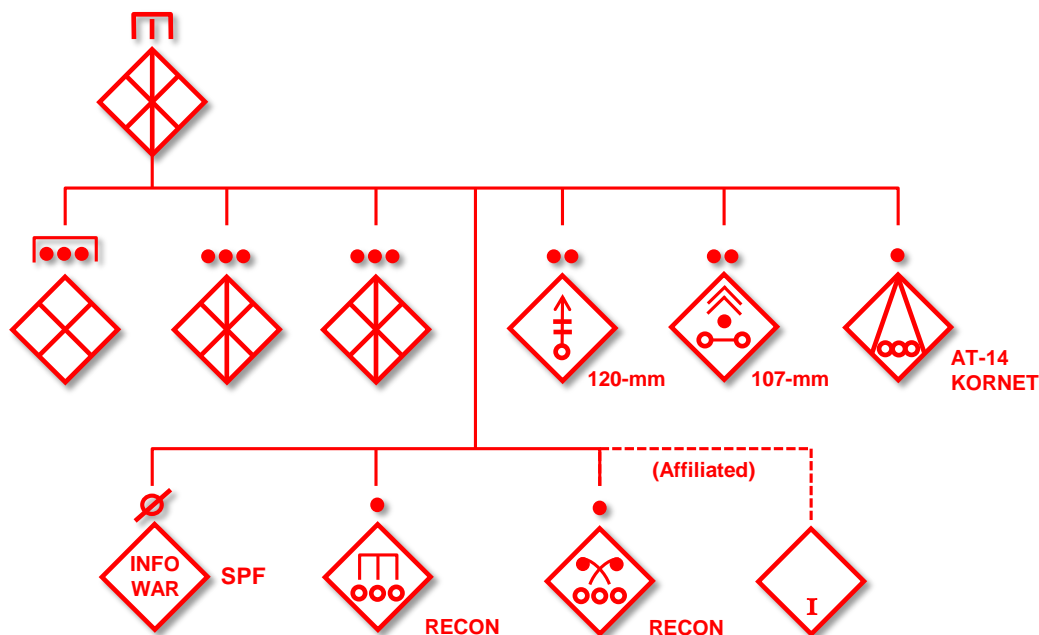
TC 7-100.2

Although an RD typically comprises significant combat weapon systems, the primary mission task of the detachment is reconnaissance. Figure 2 is a detachment example with significant capabilities based on assigned mission tasks. If encountering a weak enemy force, the RD commander might engage that force, take prisoners, and/or exploit other



tactical considerations. When the detachment encounters an enemy force that may compromise the reconnaissance mission, the RD commander typically will—

- Maintain observation contact with the enemy.
- Determine the composition and disposition of those forces.
- Report situational awareness to the higher headquarters.
- Continue its reconnaissance detachment mission.



**Figure 2. Company-size motorized rifle reconnaissance detachment (hybrid threat) (example)**

**Note.** An enemy of the threat may have difficulty in distinguishing the purpose of threat reconnaissance when making first contact and/or observing the actions of threat elements. Vehicle types and specialized equipment *can* be difficult to determine as either reconnaissance or main body elements.

Specialized reconnaissance assets are discussed in more detail in TC 7-100.2:

- Signals reconnaissance in chapter 7.
- Artillery target acquisition in chapter 9.
- Aerial reconnaissance in chapter 10.
- Air defense reconnaissance, early warning, and target acquisition in chapter 11.
- Engineer reconnaissance in chapter 12.
- CBRN reconnaissance in chapter 13.
- Special reconnaissance in chapter 15.

Examples that can be tailored into a reconnaissance detachment or act as an independent element include but are not limited to—

#### ***Mobility and Countermobility Reconnaissance***

Engineer units can also dispatch one or more engineer reconnaissance patrols. This type of patrol consists of a squad or a platoon of engineer specialists sent out to obtain engineer intelligence on the enemy and terrain of a designated OE. In enemy territory, it deploys as part of another ground reconnaissance element.

## Chemical Reconnaissance

Chemical defense units can establish CBRN observation posts (OPs) as well as CBRN reconnaissance patrols, or provide CBRN assets to an RP. Chemical defense units can also attach individual chemical and radiological specialists to reconnaissance, security, or reserve elements.

## Aerial Reconnaissance

Aerial reconnaissance includes visual observation, imagery, and signals reconnaissance from airborne platforms. These platforms may be either piloted fixed-wing or rotary-wing aircraft, or unmanned aerial vehicles (UAVs). Any aviation platform can be a collector. Information is transmitted or relayed in the most timely and practical manner.

When employing dedicated reconnaissance helicopters, equipment can include visual, thermal imaging, photographic, infrared, and signals reconnaissance. Helicopters and fixed-wing aircraft can perform reconnaissance tasks that complement insertion of threat elements to locations not practicable for ground maneuver reconnaissance vehicles.

The threat operates unmanned aerial vehicles (UAVs) at all echelon levels from the strategic through division, brigade, maneuver battalion, and some companies, as well as in specialized units such as special purpose forces (SPF) teams. There are two types of UAVs: the remotely piloted vehicle (RPV) and the drone. An RPV can be controlled by a remote ground station that transmits a flight path selected and/or adjusted by the controller. A drone can be programmed on a set course in its onboard flight control system prior to launch.



UAV

## Specialized Ground Reconnaissance

Tactical units may send out independent reconnaissance patrols (IRPs) to perform specialized ground reconnaissance. The size of such patrols can vary but is usually an augmented reconnaissance or combat arms platoon.

Examples of specialized assets that operate in conjunction with or separate from specialized ground reconnaissance are long-range reconnaissance (LRR) teams and/or special-purpose forces (SPF) teams. However, LRR teams typically operate deep in an area of responsibility (AOR) at distances up to 100 kilometers forward of the *battle line*. In another instance, a division tactical group (DTG) can receive an SPF unit or teams to support its integrated fires command (IFC) or to perform other special reconnaissance and direct action missions.



LRR

## Reconnaissance Task and Tactical Missions

The baseline task for threat conduct of tactical reconnaissance is listed in [TC 7-101, Exercise Design](#). Of the 24 threat tactical tasks, reconnaissance is an inherent aspect in all operations and missions.

Reconnaissance or surveillance is a typical precondition for offensive tasks such as—

- Assault.
- Ambush.
- Raid.
- Reconnaissance attack.

Reconnaissance techniques such as observing, listening, imaging, questioning, and/or interrogating relevant individuals in an OE may precede a tactical task that is deliberately planned for action, but occurs often as an emergent condition of any action. Similar reconnaissance tasks and techniques are appropriate for *planned* or *situational* defensive operations as discussed in TC 7-100.2.

Threat defensive actions are typically categorized in the threat context of *maneuver* or *area* defenses, or a combination of both types of defense. Tactical tasks in threat defense are typically related to—

- Simple battle positions (SBP).
- Complex battle positions (CBP).

The threat employs reconnaissance continuously in defensive operations with mission tasks related to the enemy, terrain, and other designated aspects of an OE. In the defense and in the absence of close contact with the enemy, a division, brigade, or tactical group may order reconnaissance patrols and/or detachments into a *disruption zone* to determine the enemy's composition, activities, and probable or possible avenues of attack.

The mission task is to establish and maintain contact with advancing enemy elements and forces, monitor and report enemy movement and maneuver, and provide current situational awareness and understanding to the threat commander. Once reconnaissance establishes and maintains contact with the enemy, attack timing is coordinated on the enemy's combat system by targeting and destroying subsystems that are critical to enemy combat power effectiveness. If successful, the disruption force can cause culmination of enemy offensive actions before the enemy enters the threat battle zone.

Skillful use of fires, maneuver, and or designated area defense in a disruption zone may disrupt and defeat enemy operations without significantly exposing threat force locations or intentions. RISTA assets typically include reconnaissance and counterreconnaissance elements in the disruption zone.

**Table 1. Threat Reconnaissance Task and Subtasks**

<b>Task 5.0 Reconnaissance</b>		<b>RE: TC 7-101 Exercise Design, Appendix B</b>
Task Description. <b>Reconnaissance</b> represents all measures associated with organizing, collecting, and studying information on the enemy, terrain, and weather in the area of upcoming battles.		
Subtasks for a reconnaissance are—		
5.1	<b>Fix Enemy Security Forces</b>	<ul style="list-style-type: none"> <li>Prevent the enemy from moving any part of his security force from a specific location for a specific period of time.</li> <li>The security element(s) making contact fix the enemy. (Security elements become fixing elements.)</li> <li>Security element(s) continue to provide early warning of approaching enemy forces and prevent them from gaining further information on the rest of the OPFOR force.</li> </ul>
5.2	<b>Find</b>	<ul style="list-style-type: none"> <li>Employ reconnaissance element(s) to locate selected reconnaissance targets.</li> </ul>
5.3	<b>Contact</b>	<ul style="list-style-type: none"> <li>Gain sensor contact between reconnaissance element(s) and their designated reconnaissance target(s).</li> </ul>
5.4	<b>Report</b>	<ul style="list-style-type: none"> <li>Provide accurate information on reconnaissance targets in a timely manner.</li> </ul>

In the event of unexpected contact with the enemy offensive or defensive actions, reconnaissance elements occupy a position from which to identify and report the strength, composition, and location of the enemy element or force. If a patrol or detachment acquires and observes enemy reconnaissance-security elements, its primary task is typically to avoid contact in order to continue to locate the main force as rapidly as possible. In the event of a surprise encounter with a small enemy element and when breaking contact is not an option, threat reconnaissance elements act decisively to destroy the enemy, capture prisoners if practical, and continue its mission.

#### **Reconnaissance Raid**

**The primary objective of a reconnaissance raid is to obtain information. Any damage or destruction of enemy installations is incidental. The raiding element is usually a reconnaissance or maneuver unit up to platoon size with specified augmentation to assist in exploiting the raid objective.**

**TC 7-100.2**



Threat reconnaissance is also employed continuously in the offense. A reconnaissance *raid* is one example of offensive action. Tasks may include fixing enemy security elements, or finding and reporting on enemy security actions without initiating direct contact. A task may include acquiring information on the terrain, the enemy's location, or gaps in enemy defenses. Tasks often require reconnoitering key objectives by physical observation and/or other collection capabilities, conducting terrain appreciation, and—when necessary—employing combat actions such as ambushes, assaults, or raids. Another offensive action is a reconnaissance *attack*.

#### **Reconnaissance Attack**

**A reconnaissance attack is a tactical offensive action that locates moving, dispersed, or concealed enemy elements to either fix or destroy the enemy elements. A reconnaissance attack may also be used by the commander to gain information on an enemy's location, dispositions, capabilities, and intentions. The reconnaissance attack is the most ambitious and least preferred method to obtain information. When other means of gaining information have failed, a detachment or unit of similar capabilities can undertake a reconnaissance attack.**

**TC 7-100.2**

#### **Training Implications**

Training of US Army units requires that Soldiers and leaders “know the threat—know the enemy.” This charter requires knowledge and situational understanding of how the threat or enemy acts and fights. Threat reconnaissance is continuous. When threat reconnaissance is destroyed or defeated, additional threat assets will be organized to sustain the threat RISTA mission and intent. Aspects of US Army training, educating, and developing Soldiers and leaders include being proficient in recognizing threat and enemy—

- Weapon systems and equipment.
- Tactics and techniques.
- Recent interactions with the local and regional relevant civilian populations.
- Recent affiliations or associations with regular and/or irregular forces in an OE.
- Recent and current use of military and paramilitary combat power.
- Conditional announcements or ultimatums on future actions or prohibitions.

The US Army Soldier and leader know and understand that an adversary in an OE may quickly become an enemy. Similarly, the relevant population in an OE will often include active and passive supporters to an adversary or enemy, but also hold the potential for effective US support to counter the objectives of an adversary or enemy.

#### **Adversary**

**A party acknowledged as potentially hostile to a friendly party and against which the use of force may be envisaged.**

**ADRP 1-02**

#### **Enemy**

**A party identified as hostile against which the use of force is authorized.**

**ADRP 1-02**

Readiness of US Army units will often be tested in the “first contact” with an adversary or enemy on the ground—between small tactical units—in complex and uncertain OEs. First contact will often be among varied reconnaissance elements with differing tasks and explicit or implicit rules of engagement (ROE). Separating aggressive yet legitimate reconnaissance of an adversary from combatant actions of an enemy can be a challenging determination in areas of persistent conflict with multiple actors.

Leaders in today's operational environments fully expect complex and uncertain conditions that will stress effective Army leader decisionmaking in mission accomplishment. As a fundamental training requirement, experiences must assure the opportunity to learn competence, proficiency, and expertise. US Army Soldiers and leaders must use mission command principles and disciplined self-initiative in home station training (HST), collective training, and other available forms of constructive-virtual-gaming simulations, live exercises, and education to apply professional knowledge, understanding, and skills to "know the threat—know the enemy."

**Note.** For easy access to threat training literature, use [Army Training Network](https://atn.army.mil). See below.

1. With common access card (CAC)--Enter <https://atn.army.mil>
2. Browse the **ATN front page** "hot buttons."
3. Search "**CTID Operational Environment Page**" for HQDA and TRADOC G2 threat training literature.
4. Search "**OPFOR & Hybrid Threat Doctrine**" for HQDA and TRADOC G2 threat training literature.

The screenshot shows the ATN homepage with the following elements:

- Header:** ATN logo, "U.S. ARMY Army Training Network", and the tagline "Training Solutions to Stay Army Strong". Navigation links include myFavorites, Home, Unit Training Management, myTraining, Videos, Products, Links, Collaborate, and Print.
- Search Bar:** "Search ATN:" with a "Go" button. Below it, "Search for Tasks (individual, collective, drill, etc.):" with "Enter Search Criteria" and "Enter Search Term" fields.
- Hot Buttons:**
  - Leader Development:** ATP 6-22.1 THE COUNSELING PROCESS, Army Leader Development Strategy 2013, Mission Training Complex-Joint Base Lewis-McChord Leadership Training and Development, FORSCOM Leader Development Toolbox, Army Accelerated Conversion.
  - Soldiers Skills:** SHARP Training, Warrior Tasks and Battle Drills, Mandatory Training (AR 350-1), Military Customs, Traditions & Courtesies, Army Suicide Prevention Program Manager (SPPM) Training, Posttraumatic Stress Disorder Self-Development and Unit Training.
  - Training for Operations:** Pre-Deployment Training, Traumatic Brain Injury (TBI) Training Support Package, CTID Operational Environment Page (highlighted with a red box), ITE and Blended Training Best Practices, Regionally Aligned Force United Nations Peacekeeping Training Program.
  - DA Training Environment:** Training Brain Repository Exercise Design Tool, Training for Decisive Action Stories of Mission Command, Common Framework of Scenarios Registry.
  - CoE & Proponent Training Pages:** TRADOC Centers of Excellence, Mission Command Training Resources, Fires Center of Excellence, Training Support Packages (TSP).
  - Echelons Above Brigade (EAB):** Regionally Aligned Forces (RAF) Pre-Deployment Training Message, ARFORGEN, Mandatory Training (AR 350-1), Center for Army Lessons Learned Handbooks.

Annotations on the right side of the screenshot:

- A red arrow points from the text "See <https://atn.army.mil/>" to the "CTID Operational Environment Page" link.
- A red arrow points from the text "Click and Browse" to the "OPFOR & Hybrid Threat Doctrine" link.



**Complex Operational Environment and Threat Integration Directorate (CTID)**

# Targeted Assassinations in Libya:

## Planting the Bomb

by [Laura Deatricks](#), Complex Operational Environment and Threat Integration Directorate (CGI Federal CTR)

When Muammar Qadhafi fell from power in the spring of 2011, jubilant citizens celebrated openly in the streets. They did so again at his death only a few months later. Many, however, discerned the difficult road ahead. Libya, a country that had been under strong dictatorial control for over 40 years, was now effectively led by no one. The National Transitional Council (NTC) was weak, and different cities and towns that had suffered during the fighting were already maneuvering for positions in the new government. The NTC had been unable to unite the different militias into a unified command before Qadhafi's death; they were no more successful afterward. Now, nearly three years after Qadhafi's death, various armed groups continue to battle for control in Libya, bringing continued instability to the country. These factions can be categorized into three broad types: adherents to the former regime, militant Islamists, and pro-Western groups. Ethnicity, tribalism, and region also play a significant role in these organizations, all of which are vying for both military and political power in post-Qadhafi Libya.

### Incidents

One technique that has recently been adopted in Libya is targeted assassination. Drive-by shootings are one common way to accomplish this goal. A second, increasingly frequent approach is to plant an improvised explosive device (IED) on the victim's vehicle, which then detonates at a later point in time. Attacks in which the latter technique was or may have been used include the following:



Figure 1. Map and location of Libya

- **2 September 2012:** An intelligence officer was killed and a second one wounded when a remote-controlled IED (RCIED) planted on their parked vehicle detonated after they got in; this attack occurred in a market district.<sup>1</sup>
- **4 November 2012:** An IED was planted in the undercarriage of a police car parked in front of a police station. It exploded before anyone entered the vehicle.<sup>2</sup>
- **16 January 2013:** Police officer Salah al-Wizry was killed when an IED planted in his vehicle exploded as he arrived home.<sup>3</sup>
- **11 June 2013:** An IED placed under an Italian Embassy staff car parked in a shopping area was discovered; it detonated shortly thereafter.<sup>4</sup>



- **26 June 2013:** Intelligence officer LTC Giuma Misrati was killed when an IED planted on his vehicle exploded as he was standing beside it.<sup>5</sup>
- **31 July 2013:** Former police sergeant Ahmed al-Barnawi and his young son were wounded when an IED placed under his vehicle exploded.<sup>6</sup>
- **2-3 August 2013:** Senior police Colonel Faouzi al-Oujli was wounded when an IED planted in his vehicle detonated while he was driving from Sabha to Benghazi.<sup>7</sup>
- **6 August 2013:** Civilian Hamed Ali al-Warfelli died when an IED under his vehicle detonated; security forces suspect a criminal motivation. Social media reports initially claimed it was an intelligence officer, causing at least one newspaper to suspect mistaken identity.<sup>8</sup>
- **29 August 2013:** Military prosecutor Colonel Yussef Ali al-Asseifar was killed when an IED planted on his vehicle exploded shortly after he attended noon prayers.<sup>9</sup>
- **17 September 2013:** Police Officer Mrajaa al-Aribi died when an IED placed on his vehicle detonated.<sup>10</sup>
- **29 September 2013:** Air Force LTC Ali alDaghani and police officer Nehib Bel Hacen al-Zwei both died near a marketplace, only yards from each other, when IEDs planted in both their vehicles detonated.<sup>11</sup>
- **13 October 2013:** Police Colonel Abdessalam al-Dursi was wounded when an IED planted in his vehicle detonated.<sup>12</sup>
- **14 October 2013:** Police officer Islam Faraj Assosa died when an IED under his vehicle detonated.<sup>13</sup>
- **26 October 2013:** Municipal elections official Idriss al-Ghadi's vehicle exploded in a parking lot; the official was not in the immediate area and no one was injured.<sup>14</sup>
- **3 November 2013:** Intelligence officer Suleiman al-Fissi and his toddler son were killed, and his wife and infant son wounded, when an IED under his vehicle detonated.<sup>15</sup>
- **6 November 2013:** Intelligence officer Abusif al-Mabruk died after an IED attached to his vehicle detonated.<sup>16</sup>
- **9 November 2013:** Prosecutor Mohamed al-Naass died when an IED planted on his car detonated.<sup>17</sup>
- **14 November 2013:** Air Force Chaplain Sheikh Muftah al-Fitouri was killed when an IED attached to his vehicle's undercarriage detonated.<sup>18</sup>
- **5 December 2013:** Intelligence officer Salah Hamouda was killed when an IED planted in the undercarriage of his car detonated while he was driving.<sup>19</sup>
- **8 December 2013:** Police Colonel Kamal Bezazah died after an IED under his vehicle detonated.<sup>20</sup>
- **8 December 2013:** An RCIED in a vehicle exploded after a police officer's funeral, killing one of the passengers.<sup>21</sup>
- **10 December 2013:** Navy Captain Khaled Bazama's vehicle exploded after he arrived downtown and parked it; no one was injured.<sup>22</sup>
- **19 December 2013:** Power plant manager Adam al-Mansouri was killed after leaving work when an IED under his vehicle detonated.<sup>23</sup>
- **21 January 2014:** Saiqa Special Forces member Muftah al-Shukri died when an IED planted in his vehicle's undercarriage detonated.<sup>24</sup>
- **10 February 2014:** An IED placed under former policeman Montasser Anwar Bennaser's vehicle exploded shortly after he dropped his son off at school.<sup>25</sup>
- **22 February 2014:** Commando Farag Abou Khosheim was killed when an IED planted in his vehicle detonated; his family was in the vehicle with him, but no information is available on their condition.<sup>26</sup>
- **9 April 2014:** Air Force officer Abdelhamid Tahar al-Imam died, and his wife and child were wounded, when an IED under his vehicle detonated.<sup>27</sup>
- **29 April 2014:** Security support officer Akram Emsallah was wounded when an IED planted on his vehicle detonated while he was driving.<sup>28</sup>
- **6 July 2014:** A commando died and his young son was wounded when an IED planted in his vehicle detonated while he was driving.<sup>29</sup>

## A Typical Example

On 29 August 2013, Colonel Yussef Ali al-Asseifar and his brother drove to a mosque in the al-Laythi neighborhood of Benghazi to attend noon prayers. A military prosecutor, Colonel al-Asseifar was involved in cases pertaining to targeted assassinations of politicians, military personnel, and journalists that had been perpetrated by the Qadhafi regime. While they were in the mosque, unknown assailants planted an IED on the colonel's white double-cab pickup truck. When prayers had concluded, the brothers came out of the mosque and re-entered the vehicle at around 1345 local time. They did not make it far; the IED detonated shortly thereafter at the intersection located directly in front of the mosque, killing both men.

The following diagram illustrates the tactics and techniques used in this attack. The detonation method for the IED is unknown; it may have been remote-controlled, timed, or victim-operated. The graphic shows the most likely techniques used for an RCIED.

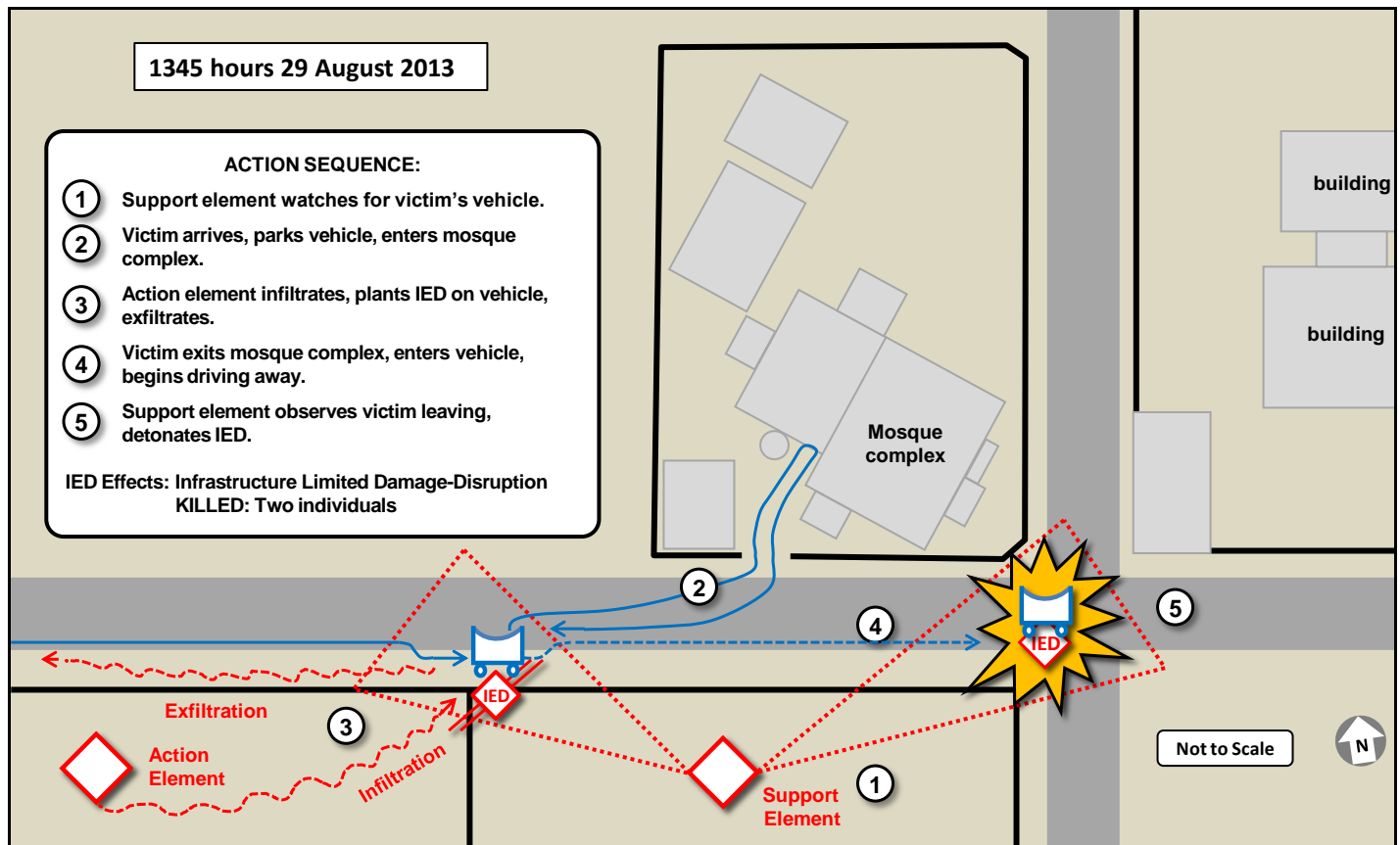


Figure 2. Details of 29 August 2013 attack

## Analysis

The victims of the aforementioned incidents were almost exclusively current or former members of the security forces, either police or military. Among the six exceptions, one was a foreign diplomat, three were involved with the government, one was attending a police officer's funeral, and one may have been a case of mistaken identity. Victims in five of the incidents were intelligence officers, lending support to the argument that the victims were specifically targeted. All but four of the attacks took place in Benghazi; of these, three targeted non-security personnel.

This technique requires preplanning and observation of the intended victim's daily routines to determine the time and location most likely to result in a successful attack. Of interest, some of the victims were driving the same type of vehicle: white four-door pickup trucks of similar size and appearance. It appears that certain security force officers receive an official vehicle of this type, which then doubles as a personal vehicle. If this is the case, spotting and tracking such personnel would be greatly simplified. It would also allow for targets of opportunity, in that a perpetrator could

choose a likely area and plant an IED on any official-looking vehicle found. The events of 29 September 2013, in which an air force officer and a police officer were killed within yards of each other, may have been such a case.

Three types of IEDs may have been used in these attacks: remote-controlled, victim-operated (VOIEDs), and timed devices. Of the incidents listed, two are known to have utilized RCIEDs. VOIEDs tied to a specific action, such as starting the vehicle or applying the brakes, are another possibility, as many of the victims were driving at the time of detonation. In at least five of the attacks – four of which were unsuccessful – no one was in the vehicle when the IED detonated, making a timed device more likely in these instances. Perpetrators most likely use a combination of the three, making their selection based on available materials and the intended victim's pattern of life.

While this technique was not unknown prior to July 2013, its use has grown considerably since then. Only seven instances were reported in the RAPID Weekly News Reports for the July 2011-June 2013 time period – four in Libya and three in Somalia. Since then, RAPID has reported at least 18 such instances in Libya, 13 in Somalia, and one in Tunisia. Due to the effectiveness of this technique, the trend is likely to continue, and may spread to other AFRICOM countries.

### Training Implications

Several aspects of this technique will make it of interest to trainers and scenario writers. First, it is an excellent scenario for intelligence and military police units. It would be easy to mimic in the home station training environment, and the small number of perpetrators allows for efficient use of role-players. Basic force protection tasks, such as checking an unsecured vehicle over before using it, could effectively counter such an attack. This technique would be consistent with typical methods used by insurgent and guerrilla forces that operate in the Decisive Action Training Environment (DATE) country of Atropia, such as SAPA and Sadvol.

### Notes

- <sup>1</sup> Omar al-Mosmari, "[Libyan intelligence officer killed in car bombing](#)," Ma'an News Agency, 4 September 2012; Hadeel al Shalchi, "[Explosion at Benghazi police station injures three](#)," Reuters, 4 November 2012.
- <sup>2</sup> Hadeel al Shalchi, "[Explosion at Benghazi police station injures three](#)," Reuters, 4 November 2012.
- <sup>3</sup> Reuters, "[Car bomb kills policeman in Benghazi as Libya violence escalates](#)," 16 January 2013.
- <sup>4</sup> BBC News, "[Bomb found under Italian embassy car in Libya](#)," 11 June 2013; Essam Mohamed, "[Tripoli car bomb targets Italian diplomats](#)," Magharebia, 12 June 2013.
- <sup>5</sup> PanArmenian, "[Bomb kills Libyan military intelligence officer](#)," 26 June 2013.
- <sup>6</sup> Agence France-Presse, "[Bomb wounds former policeman in Libya's Benghazi](#)," Daily Star (Lebanon), 31 July 2013.
- <sup>7</sup> Agence France-Presse, "[Senior Libyan policeman wounded by car bomb](#)," Fox News, 3 August 2013; Kristin Deasy, "[Car bomb in Libya's Benghazi kills 1](#)," Global Post, 6 August 2013.
- <sup>8</sup> Agence France-Presse, "[Man killed in car bomb in Libya's Benghazi](#)," Fox News, 6 August 2013; Kristin Deasy, "[Car bomb in Libya's Benghazi kills 1](#)," Global Post, 6 August 2013.
- <sup>9</sup> Agence France-Presse, "[Libyan prosecutor killed in car bomb](#)," Alakhbar, 29 August 2013; Ahmed Elumami, "[Military Prosecutor in Benghazi killed in car bomb attack](#)," Libya Herald, 30 August 2013; Indepth Africa, "[Libya: 'Bomb blast kills 2 in Benghazi'](#)," 30 August 2013; Jamahiriya News Agency, "[Military Prosecutor in Benghazi killed in car bomb attack](#)," 29 August 2013; Khalid Mahmoud, "[Libyan military prosecutor assassinated](#)," Asharq al-Awsat, 30 August 2013.
- <sup>10</sup> Agence France-Presse, "[Bomber kills police officer in Libya's Benghazi](#)," Now Media, 17 September 2013.
- <sup>11</sup> Agence France-Presse, "[Three army, police officers killed in Libya's Benghazi](#)," Modern Ghana, 29 September 2013; Associated Press, "[3 Libyan army officers assassinated in Benghazi](#)," New Zealand Herald, 30 September 2013.
- <sup>12</sup> Agence France-Presse, "[Gunmen kill Libya air force officer in Benghazi: Security](#)," Ahram Online (Egypt), 13 October 2013.
- <sup>13</sup> Maha Ellawati, "[More deaths in Benghazi](#)," Libya Herald, 14 October 2013.
- <sup>14</sup> Agence France-Presse, "[Car blast targets municipal election office in Libya](#)," Daily Star (Lebanon), 26 October 2013.
- <sup>15</sup> Agence France-Presse, "[Car bombing kills Libyan army officer](#)," Modern Ghana, 6 November 2013; Agence France-Presse, "[Libya army officer killed in Benghazi blast](#)," Modern Ghana, 3 November 2013; Al Bawaba, "[Libyan intelligence officer and his two-year old son killed in Benghazi car bomb attack](#)," 4 November 2013; Reuters, "[Car bomb kills intelligence officer in Libya's Benghazi](#)," Saudi Gazette, 5 November 2013.
- <sup>16</sup> Agence France-Presse, "[Car bombing kills Libyan army officer](#)," Modern Ghana, 6 November 2013.
- <sup>17</sup> Agence France-Presse, "[Attacks in eastern Libya kill six in under 24 hours](#)," Modern Ghana, 9 November 2013.
- <sup>18</sup> Now Media, "[Attacks in Libya's Benghazi kill two](#)," 14 November 2013.
- <sup>19</sup> Libya Herald, "[Intelligence officer murdered in Benghazi](#)," Shabab Libya, 5 December 2013.
- <sup>20</sup> Agence France-Presse, "[One killed in Libya cemetery blast](#)," Daily Star (Lebanon), 8 December 2013; Associated Press, "[Libya: Policeman dies of wounds from bombing](#)," New Zealand Herald, 9 December 2013.
- <sup>21</sup> Agence France-Presse, "[One killed in Libya cemetery blast](#)," Daily Star (Lebanon), 8 December 2013; Libya Herald, "[Navy captain survives car-bomb assassination attempt in Benghazi](#)," 10 December 2013; Noora Ibrahim, "[Bomb Kills Mourner at Military Intelligence Colonel's Funeral in Benghazi](#)," Jamahiriya News Agency, 5 November 2013.



- <sup>22</sup> Libya Herald, "[Navy captain survives car-bomb assassination attempt in Benghazi](#)," 10 December 2013.
- <sup>23</sup> Agence France-Presse, "[Libya bomb kills electricity plant manager](#)," NOW Media, 19 December 2013.
- <sup>24</sup> Libya Herald, "[Saiga Brigade member confirmed dead in Benghazi blast](#)," Shabab Libya, 21 January 2014.
- <sup>25</sup> Nadia Radhwan, "[Libya killing spree terrorises citizens](#)," Magharebia, 12 February 2014.
- <sup>26</sup> Vancouver Sun (Canada), "[Bomb Kills Libyan Commando In Car With Family](#)," 22 February 2014.
- <sup>27</sup> Agence France-Presse, "[Libya officer killed, family wounded when car explodes](#)," Modern Ghana, 9 April 2014.
- <sup>28</sup> Ayman Amzein, "[Benghazi Security Officer Injured In Second Attack](#)," Libya Herald, 29 April 2014.
- <sup>29</sup> Associated Press, "[Libya car bomb kills commando in the east](#)," New Zealand Herald, 6 July 2014.

## Additional Sources

- BBC News. "[Gaddafi's death prompts wild celebrations in Tripoli](#)." 20 October 2011.
- BBC News. "[Guide to key Libyan militias](#)." 20 May 2014.
- BBC News. "[Libya: The challenges ahead](#)." 21 October 2011.
- BBC News. "[Vying for a slice of power in the new Libya](#)." 5 October 2011.
- Chothia, Farouk. "[Why is Libya lawless?](#)" BBC News. 19 May 2014.
- CIA. "[World Factbook: Libya](#)." 30 July 2014.
- Cordesman, Anthony H. "[Next Steps in Libya \(Egypt, Tunisia, and Other States with New Regimes\)](#)." Center for Strategic & International Studies. 22 August 2011.
- Flanagan, Stephen. "[International Assistance to the New Libya](#)." Center for Strategic & International Studies. 1 November 2011.
- IHS Jane's. "[Libya: Executive Summary](#)." 28 May 2014.
- Joshi, Shashank. "[After Gaddafi: Libyan revolution 'still has far to go'](#)." BBC News. 21 October 2011.
- Rose, Zachary J. "[Libya: Still Waiting on a Viable State](#)." Geopolitical Monitor. 4 March 2013.
- Stratfor. "[Struggling Libyan Democracy](#)." 2 November 2012.

# Army Antiterrorism Awareness and TRADOC G2 OEE

**JUN**

**JUL**

**AUG**

## TRISA Threats Terrorism Team Advisory

### TRADOC G2 Operational Environment Enterprise (G2 OEE)

by [Kristin Lechowicz](#), Complex Operational Environment and Threat Integration Directorate (DAC)

Army Regulation 350-50

Training

**Combat  
Training  
Center  
Program**

Headquarters  
Department of the Army  
Washington, DC  
3 April 2013

**UNCLASSIFIED**

## Overview

# Combat Training Center Program Organization

**Legend:**

- COMMAND/SR LDR OVERSIGHT —
- SCHEDULING - - - - ->
- PROGRAM MGMT/COORDINATION - - - - -
- DIRECT SUPPORT AND COORDINATION - . . . -

**CTC Program Management**

**DA G-3/5/7\*** (Director of the CTC Program, Provide Training, Policy, Resources and Management)

- CG, TRADOC
  - CG, CAC
    - CAC-T
      - CTCD
      - MCTP
- CG, FORSCOM
  - NTC & Fort Irwin
  - JRTC & Fort Polk
- CG, USAREUR
  - JMTc
    - JMRC
    - ETC

**DA G-3 DOT\*\*** (Principal Advisor to the Director of the CTC Program)

- TGOSC
  - CoC / QR / Pgm Mgmt Review
- DCG, CA, TRADOC (CG, CAC) DA Responsible Official\*\*\*
  - CAC-T
    - CTCD
    - MCTP
- G-3, FORSCOM
- G-3, USAREUR

**Scheduling MCTP/ETC**

**Notes:**

- \* Reviews & Validates Policy, Concept of Ops, Status of Program
- \* Review & Recommend Priorities
- \* Recommends Actions to DA G-3/5/7
- \* Works Issues
- \* Recommends to TGOSC
- \*\*\* Designated to support the DA G-3/5/7 with the day-to-day Admin & Integration of the CTC Program

**Abbreviations:**

- TGOSC – Training General Officer Steering Committee
- MCTP – Mission Command Training Program
- ETC – Exportable Training Capability
- CoC – Council of Colonels
- QR – Quarterly Review

**Figure 1. Combat training center program organization and management**

AR 350-50 is a keystone document for members assigned to CTCs in a training or administrative capacity. This regulation puts forth the objectives, the hierarchy, responsibilities, and policy guidance for the CTC program. The document provides clear roles and responsibilities for command and control, management, and administration for the chain of command for the Army.

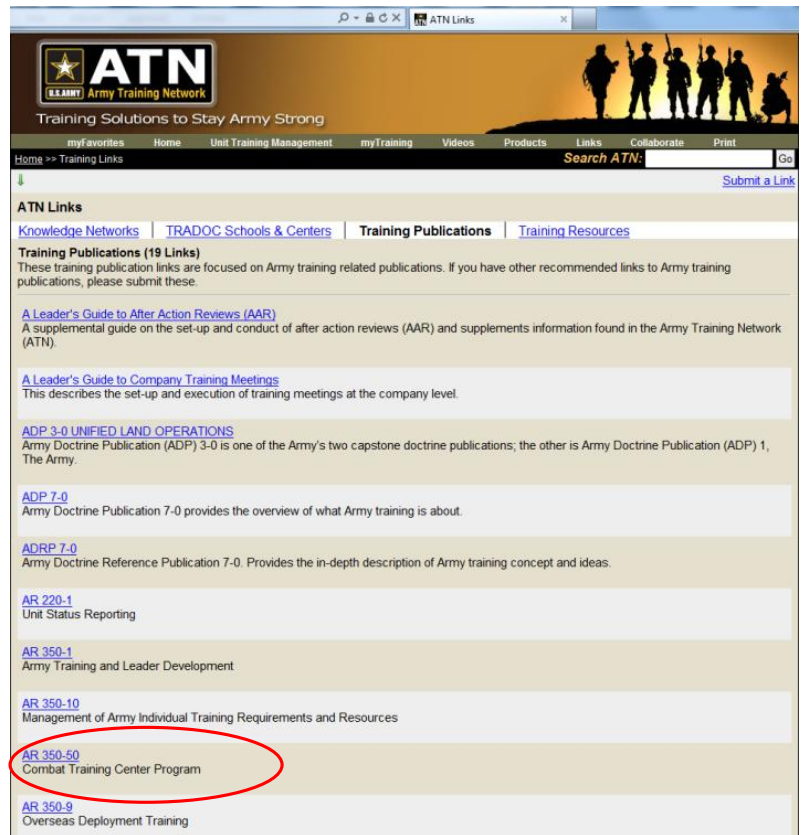
### Location

The most current copy of AR 350-50 (03April2013) can be found on the Army Training Network: See—

[https://atn.army.mil/dsp\\_Links.aspx](https://atn.army.mil/dsp_Links.aspx)

### Updates to AR 350-50:

- Adds Chief of Staff, Army vision and guidance
- Adds Joint context
- Updates CTC training focus
- Discusses role of mission rehearsal exercises and mission readiness exercises
- Adds Joint National Training Capability
- Adjusts the scope of CTCs
- Defines the scope and purpose of role players and civilians on the battlefield
- Adds a CTC Accreditation Program
- Adds provision for US Army Training and Doctrine Command operational environment assessment support to the Combat Training Centers on a semiannual basis.
- Changes Commanding General, US Army Forces Command “operational control” of Joint Readiness Training Center and National Training Center Operations Groups to “command”
- Assigns Commanding General, US Army Forces Command responsibility of providing doctrinally based, performance oriented after action reviews to the rotational training units
- Expands Army Special Operations Forces integration throughout the CTC Program
- Incorporates July 2004 Chief of Staff, Army guidance reference foreign nation integration into Combat Training Center training and the Deputy Chief of Staff, G-3/5/7 continental United States Combat Training Center approval Authority
- Aligns regulation with AR 350-1
- Changes Battle Command Training Program to Mission Command Training Program



**Figure 2. Army Training Network location**

The Army faces a multitude of adaptive threats worldwide. The training environment for the US Army requires the CTCs to mirror these global threats in a composite model, and AR 350-50 has been updated to meet these tasks. It provides a baseline document that allows the CTCs to set the conditions to match the threat. The updated document also allows for a shift (while not forgetting the lessons) from a counterinsurgency training focus to a decisive action and joint-based training environment at the CTCs. The multitude of changes within AR 350-50 set the baseline conditions for the US Army's CTC training environment that allows the Army to remain flexible, create adaptive leaders, and ensure a successful outcome on tomorrow's battlefield.





by CPT [Benjiman A. Smith](#), JMRC Intelligence and Operational Environment Planner

The Joint Multinational Readiness Center (JMRC) in Hohenfels, Germany, is characterized by a unique set of circumstances that forces planners to adjust elements of the operational environment (OE) for each rotational exercise. Every JMRC training exercise includes multinational partner nations portraying both rotational training unit (RTU) blue forces (BLUEFOR) and opposing forces (OPFOR), and incorporates multiple training centers in Europe. These exercises include a set of exercise objectives centered on multinational interoperability in a decisive action training environment (DATE). In addition, JMRC employs a variety of contracted and US Government (USG) organizations between the United States and Europe to contribute to the exercise design sequence.<sup>1</sup> Because of these factors, JMRC planners have adapted doctrine established in [Training Circular \(TC\) 7-101, Exercise Design](#), in order to synchronize the exercise scenario and promote shared understanding across JMRC's operations group. During the exercise design sequence for Exercise Combined Resolve II (which featured multinational battalions partnered with the European Rotational Force from 1<sup>st</sup> Cavalry Division), JMRC planners developed a systematic approach for adapting changes to the OE and constructed an OE design model to complement existing Army doctrine outlined in TC 7-101.<sup>2</sup>

**JMRC's UPDATED  
APPROACH**

**Table 2-1. Exercise design sequence**

Exercise Design Sequence	Phase 1 Initial Planning	Phase 2 Task and Countertask Development	Phase 3 PMESII-PT OE Development	Phase 4 Orders, Plans, and Instruction Development
<b>WHO:</b>	<ul style="list-style-type: none"> <li>Training Unit Commander</li> <li>Exercise Director</li> <li>Exercise Planner</li> <li>Senior Trainer</li> </ul>	<ul style="list-style-type: none"> <li>Exercise Planner</li> <li>OPFOR Commander</li> </ul>	<ul style="list-style-type: none"> <li>Exercise Planner</li> </ul>	<ul style="list-style-type: none"> <li>Exercise Planner</li> <li>Exercise Director</li> </ul>
<b>TOOLS:</b>	<ul style="list-style-type: none"> <li>Troop List</li> <li>Proposed Training Objectives</li> <li>AUTL/UJTL</li> <li>Requested Conditions</li> <li>Commander's Training Assessment</li> <li>Exercise Resources</li> <li>Exercise Director's Initial Guidance</li> </ul>	<ul style="list-style-type: none"> <li>Defined Exercise Parameters</li> <li>Prioritized Training Objectives (METL)</li> <li>TC 7-100 Series</li> <li>OPFOR Tactical Task List</li> <li>Worldwide Equipment Guide (WEG)*</li> </ul>	<ul style="list-style-type: none"> <li>OE Assessment (OEA)</li> <li>PMESII-PT Subvariables</li> <li>Prioritized Training Objectives (METL)</li> <li>OPFOR Countertasks</li> <li>OE/WFF Analysis Matrix</li> </ul>	<ul style="list-style-type: none"> <li>Defined OE</li> <li>TC 7-100 Series</li> <li>COA Sketch</li> <li>OPFOR OB</li> </ul>
<b>KEY DECISIONS:</b>	<ul style="list-style-type: none"> <li>Exercise Timeline</li> <li>Type of Exercise</li> <li>Operational Theme</li> <li>Existing OEA or Composite OE</li> </ul>	<ul style="list-style-type: none"> <li>Training Unit Tasks</li> <li>OPFOR Countertasks</li> <li>OPFOR OB*</li> <li>OPFOR Task Organization*</li> <li>OPFOR Tier Levels*</li> </ul>	<ul style="list-style-type: none"> <li>PMESII-PT Subvariable Selection</li> <li>Common Processes</li> <li>Key Events</li> </ul>	<ul style="list-style-type: none"> <li>Chronology of Key Events</li> <li>C-, M- and D-Day</li> <li>STARTEX</li> <li>Disposition of Forces</li> </ul>
<b>PRODUCTS:</b>	<ul style="list-style-type: none"> <li>Defined Exercise Parameters</li> <li>Prioritized Training Objectives (METL)</li> </ul>	<ul style="list-style-type: none"> <li>Developed Tasks and Countertasks</li> <li>OPFOR OB*</li> <li>OPFOR Task Organization*</li> <li>OPFOR Tier Levels*</li> </ul>	<ul style="list-style-type: none"> <li>OE/WFF Analysis</li> <li>Refined Training Objectives and Task Organization</li> <li>Developed OE</li> </ul>	<ul style="list-style-type: none"> <li>Higher Unit OPLANs and Orders</li> <li>OPFOR Orders</li> <li>ROE</li> <li>Role-Player Instructions</li> <li>Road to War</li> </ul>

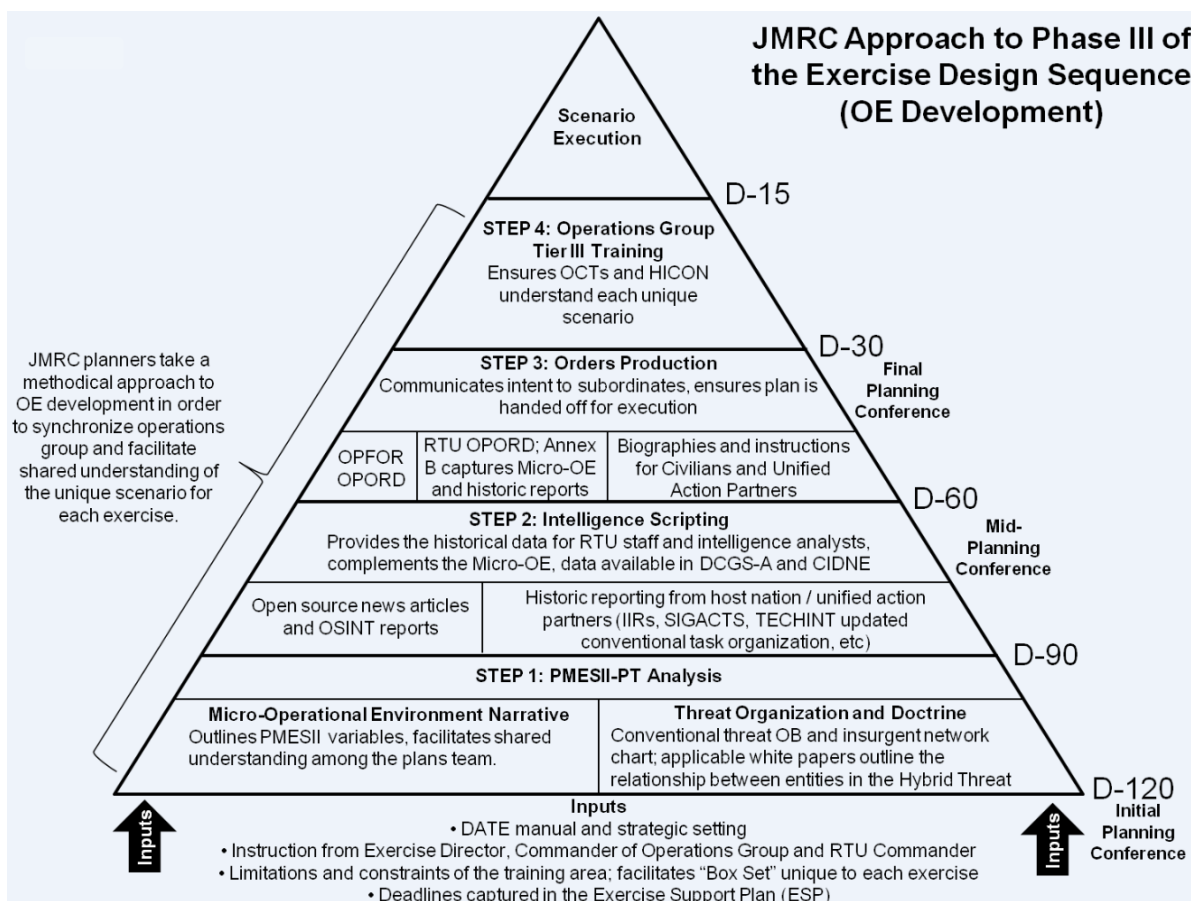
\* Phase 2 is the earliest point at which OPFOR OB and task organization, along with adjustment of OPFOR equipment tiers (using the WEG), could occur. However, this could also begin or be refined in phase 3 or phase 4.

Table 2-1 from TC 7-101 (Exercise Design) outlines the four phases of the exercise design sequence.

**Figure 1. Exercise design of operational environment for training**

TC 7-101, *Exercise Design*, outlines a methodology for designing and executing training exercises. This publication outlines four phases of the exercise design sequence: initial planning, task/counter-task development, OE development, and orders production (see figure 1, previous page).<sup>3</sup> JMRC planners use the framework established in this manual to outline the major conferences and events necessary to plan training exercises.

During the planning process for Combined Resolve II, JMRC planners developed a regimented approach to phase three of the exercise design sequence that outlines important steps in developing and implementing the OE for future training exercises (see figure 2). The goal of this process is to create an organized and complex scenario to challenge RTU intelligence and staff personnel. This process is specific to JMRC and accounts for how Department of the Army civilians and contractors augment the JMRC staff, but the model could be adapted to any organization looking to develop an OE for a training exercise. This process intends to supplement the exercise design sequence established in TC 7-101 and synchronizes the various USG organizations, contractors, and planners contributing to OE development. Phase three of the exercise design sequence (OE development) begins with inputs from phases one and two (initial planning and task/counter task development).



**Figure 2. An technique to exercise design for training**

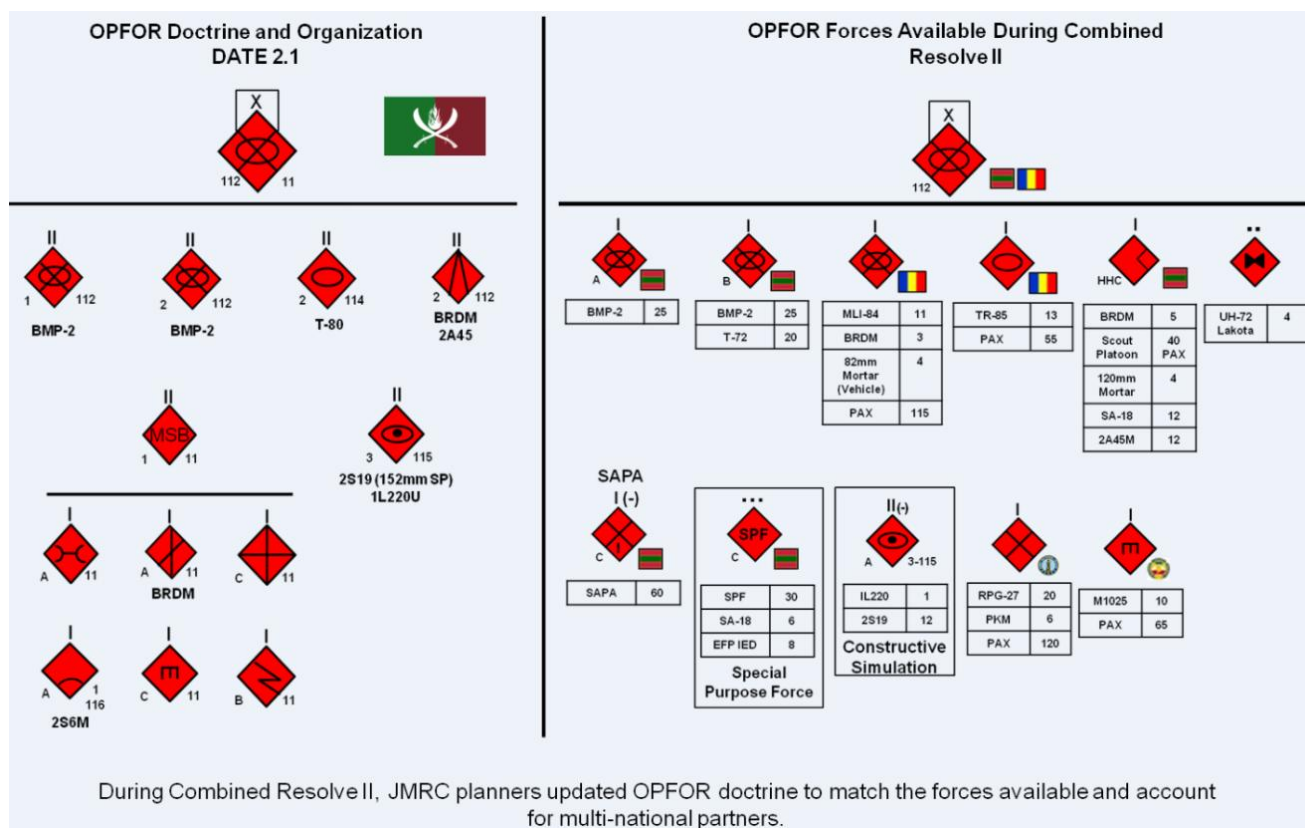
Inputs to phase three of the exercise design sequence are outlined in TC 7-101, table 2-1 and include establishing RTU training objectives/METL tasks, identifying participating US and multinational units, and outlining the physical and virtual boundaries of the training area. During phases one and two, JMRC planners receive guidance from the exercise director and the Commander of Operations Group in order to design the overall exercise scenario. JMRC also receives a list of training objectives from US and multinational units, usually focused on conducting Unified Land Operations (ULO). In addition, US and multinational units provide JMRC with a list of equipment, personnel, and mission command platforms intended for use during the exercise. Many of the inputs to phase three should be complete at the conclusion of the initial planning conference (about D-120). At the conclusion of the initial planning conference, JMRC planners use the OE development model outlined in figure 2 to supplement the exercise design sequence and synchronize OE planning. Step one of the OE development process began with PMESII-PT analysis.

## STEP 1: PMESII-PT Analysis

PMESII-PT analysis forms the base of the OE development pyramid and outlines the scenario used during the training exercise. Core documents developed in this step will synchronize the dispersed USG organizations and contracted agencies contributing to this process. The two basic documents created during this phase are the micro-operational environment narratives and the threat organization and doctrine.

Micro-operational environment narratives describe PMESII-PT variables for each specific town used during a training exercise. There are seven permanent towns in the Hohenfels training area, and each town is assigned a unique PMESII-PT assessment (usually not more than a paragraph for each variable) that describes the dynamics within the town and the interrelationships with other towns within the training area, and identifies critical civilians on the battlefield. This product also includes a listing of critical buildings that must be “in play” to complement the narrative. New micro-OE narratives are developed for each exercise to accommodate the different training areas used throughout Europe. The JMRC staff develops these micro-OEs in concert with the PMESII-PT variables outlined in DATE 2.1, but further refines the variables to make them specific to the JMRC training area. This narrative provides an organized and easy to read PMESII-PT assessment for operations group personnel. It also helps exercise planners understand the problem sets being presented to the RTU that could be further developed during the exercise.

JMRC derives threat organization and doctrine from TRISA publications like the Worldwide Equipment Guide ([WEG](#)) and [DATE 2.1](#), but JMRC planners must also account for the different weapons systems and vehicles for multinational units assigned to the OPFOR. In most exercises, JMRC planners task organize the OPFOR with multinational partner units and their organic equipment. As a consequence, JMRC planners change the OPFOR doctrine and organization, as established in DATE 2.1, to match the OPFOR forces available.



**Figure 3. Opposing force task organization for Combined Resolve II**

For Combined Resolve II, JMRC planners restructured the threat doctrinal template to include different weapons platforms not found in DATE 2.1, like the Romanian TR-85 Main Battle Tank and the MLI-84 Infantry Fighting Vehicle. In addition, JMRC planners created irregular forces' threat networks during PMESII-PT analysis and defined how those organizations interacted with the other PMESII-PT variables.



The documents developed in PMESII-PT analysis help operations group planners understand the basic problems being presented to the RTU and serve as a scenario answer key, but they present a limited set of challenges because the variables do not adequately reflect how the RTU typically receives information in a deployed setting. The intelligence warfighting function is doctrinally responsible for understanding the OE and helping commanders make decisions in complex environments. In light of this, JMRC planners provide the RTU a database of historic information that explains the OE variables and allows intelligence personnel to conduct all source analysis during the military decision-making process (MDMP). JMRC accomplishes this in step two of the OE development process by creating scripted intelligence reports and other historic data made available to the RTU during MDMP.

## **STEP 2: Intelligence Scripting**

Scripted intelligence reports in accessible databases form the backbone of historic material used by the RTU staff and intelligence personnel to conduct research in support of MDMP. After PMESII-PT development, JMRC issues instructions to a team of intelligence script writers who write unclassified historic initial impressions reports (IIRs), tactical reports (TACREPs), technical intelligence (TECHINT) reports, open-source intelligence (OSINT) reports, Department of State (DOS) cables, and other reports from unified action partners that give intelligence personnel and staff elements a pool of information to conduct research during mission analysis. The reports complement the micro-OE narratives and threat organization established in step one of the OE development process. For example, if the micro-OE identifies that a town mayor is hostile toward US forces, a news article or OSINT report housed in the historic database could further explain the mayor's grievance. Similarly, if the OPFOR task organization has changed to include multinational weapons systems not captured in DATE 2.1, a TECHINT report housed in the historic database could explain how the Arianian army purchased the platform and where it is located in the OPFOR order of battle. These reports prove vital to the OE design process because they distribute information critical to understanding the OE in the appropriate venue where BLUEFOR could expect to find the information if they were deployed. JMRC employs three different venues to appropriately present this information to the RTU.

JMRC displays historic reports to a US RTU through the Distributed Common Ground System – Army (DCGS-A) by establishing a database and using a search tool to find reports. For intelligence personnel in multinational partner nations, JMRC displays historic reports in the Combined Information Data Network Exchange (CIDNE). JMRC also recognizes that not every piece of relevant information will be available in an intelligence database (many reports from unified action partners are not) so additional reports are also housed in a JMRC Intellipedia site. Together, these databases enable JMRC to train critical staff functions at the battalion and brigade level with the tools available in a deployed environment. After populating the historic database with scripted intelligence products, JMRC planners move on to phase three of the OE development process: orders production.

## **STEP 3: Orders Production**

Step three of the OE development process includes the development of instructions to the exercise participants and ensures that the OE design will be executed effectively. The three major groups that require instructions are OPFOR, the RTU, and civilians on the battlefield. Instruction development includes writing an operations order (OPORD) for both OPFOR and the RTU's higher headquarters control (HICON) that references historic reporting from intelligence organizations and unified action partners. It is produced late in the OE design process to ensure that the order references critical historic reports that will help inform MDMP. Step three should occur between 30 and 60 days before an exercise begins, leaving enough time to use the HICON operations order during the leadership training program if desired.<sup>4</sup>

The HICON operations order is the most important OE design product that JMRC delivers to the training unit because it establishes the initial situation and orders the unit to conduct specific tasks nested with the OE. JMRC planners use the tasks identified in the HICON operations order to produce an OPFOR operations order with specific countertasks that complement RTU training objectives. For example, if the RTU is tasked to defend along a specific phase line in order to protect critical lines of communication, the OPFOR would be countertasked to seize the lines of communication. The OPORD serves as the culminating document that fuses all elements of the OE design process and delivers the overall OE scenario to the training unit in one condensed product. It is appropriate to highlight the importance of finalizing portions of the OE during the exercise design sequence, as changes to core documents can have dramatic impacts on products developed at later stages. A change that affects the "base" of the OE design pyramid requires JMRC to update



sometimes dozens of historic intelligence reports, and could easily desynchronize the OE design process. If changes to the core documents are necessary after the final planning conference, planners must be careful to update documents at every level of the OE design pyramid in order to maintain consistency within the scenario and avoid confusing the training unit.

In addition to these orders, JMRC also produces biographies and orders to civilians on the battlefield that instruct them on how to interact within the complex OE. The orders production step of the OE design process ensures that the detailed planning completed by the staff will be carried out effectively during the exercise. The final steps of the OE design process include rotation specific OE training for operations group and exercise execution.

#### **Steps 4 and 5: Operations Group Tier III Training and Exercise Execution<sup>5</sup>**

Once the JMRC plans staff completes orders production, it is important to train the remainder of Operations Group on the scenario before the exercise begins. Before each exercise, the JMRC plans staff conducts a series of briefings for each observer, coach, trainer (OCT) team to explain the scenario and promote shared understanding between the JMRC staff and the teams. This critical step facilitates after action reviews and empowers the OCT teams to better coach the RTU with respect to the OE. The relationship between irregular forces and conventional forces within the Combined Resolve II scenario provides an excellent example of the importance of preparatory training for operations group personnel before a rotational exercise. For Combined Resolve II, JMRC planners altered the scenario used in previous exercises by combining the efforts of the Arianian Special Purpose Forces with irregular forces early in the exercise to provide weapons and training. This change caused the irregular forces to be more hostile toward the RTU than they had in previous JMRC exercises. The RTU understood this relationship because they had access to the historic database of intelligence reports and the HICON OPORD addressed the dynamic between the special purpose forces and the irregular force. However, JMRC planners failed to adequately explain this important change to the OCTs before the exercise, which initially caused confusion among operations group when the irregular force began aggressively targeting the RTU. This confusion could have easily been avoided by providing operations group with a thorough scenario update prior to the start of the exercise. At the conclusion of Tier III training, operations group is prepared to begin the training exercise. JMRC training scenarios are synchronized and executed effectively by following the regimented OE development model designed by JMRC planners.

At JMRC, the OE is consistently analyzed and updated to support each training exercise. Every JMRC exercise includes a different set of training locations in Europe and different multinational participants on both BLUEFOR and OPFOR. These circumstances caused JMRC exercise planners to develop a methodical approach to designing and implementing the OE (captured in figure 2 the OE design pyramid) during exercise Combined Resolve II. This process complements the exercise design sequence outlined in TC 7-101 and guides planners at every level to coordinate the planning and execution of OE elements. This process could be adapted to assist planners for any exercise that requires a complex and dynamic OE to test the training audience.

#### **Notes**

<sup>1</sup> JMRC employs a variety of organizations to contribute to OE design including the TRADOC Intelligence Support Activity (TRISA), the Training Brain Operations Center (TBOC), the Joint IED Defeat Organization (JIEDDO), an operations order (OPORD) production team from Tapestry Solutions Inc., an in-house OE design team from Visual Awareness Technologies & Consulting Inc., and intelligence report writers from AT-Solutions Inc. This article does not address the specific roles and responsibilities of those organizations in the OE development process.

<sup>2</sup> The Combined Resolve II exercise included a unique set of multinational partner units and equipment, training tasks and physical/virtual locations. For Combined Resolve II, JMRC used the Ariana-Atropia border region as a strategic setting and used the macro-OE variables listed in DATE 2.1 as background information for the rotation. JMRC conducted the Combined Resolve II exercise in Hohenfels, Grafenwoehr, and Amberg training areas, which are distributed across southeastern Bavaria, Germany. Additionally, adjacent virtual units belonging to the US 70th Infantry Division were created in a simulated environment and located across southeastern Bavaria. JMRC also augmented the 1-4 Infantry Battalion (OPFOR) with multinational units, bringing unique equipment and capabilities to the scenario. Many of these limitations and constraints were identified during the initial planning conference, approximately 150 days before the start of the exercise. These limitations and constraints were critical inputs to the exercise design sequence established in TC 7-101.

<sup>3</sup> TC 7-101, *Exercise Design*, page 2-1. 26 November 2010.

<sup>4</sup> The leadership training program is a battalion and brigade staff training event that focuses on the military decision making process (MDMP) and is lead by JMRC observer, coach, trainer (OCT) teams.

<sup>5</sup> JMRC trains OCTs in three separate blocks of instruction, or tiers. Tiers I and II occur formally during JMRC in-processing; tier III is rotation specific and occurs before each rotation.



by [Steffany A. Trofino](#), Complex Operational Environment and Threat Integration Directorate (DAC)

Bordering eight Central Asian countries, the province of Xinjiang, China was once predominately populated by Turkic-speaking Muslims, known as ethnic Uighurs. In recent years, the region has become a focal point of growing and pervasive violence that manifests itself along ethnic fault lines. Tensions have substantially increased between minority Muslim Uighurs residing in the province and majority Buddhist Han who relocate to the province to capitalize on lucrative employment opportunities. Since April 2013, there have been a total of six terror attacks throughout China targeting police, government officials, and Han citizens, resulting in 109 victim fatalities. Previously, on average there were one to two violent incidents per year resulting in fewer casualties. The escalation of attacks within the past 18 months represents an increase in incidents that is three times the average annual rate.

Formerly known as East Turkistan, present-day Xinjiang province was subsumed into communist China in 1949. Indigenous Uighurs of the region traditionally identified with the Islamic culture of Central Asia, as opposed to the ethnic Han Buddhist culture of China, creating unrest between the two groups. As a result, Uighur society soon became the minority within the Chinese communist Han construct. As a minority, Uighurs were not afforded the same opportunities for education and employment as the majority Han society. During Xinjiang province's transition into communist China, the government initiated a brutal campaign of suppression against the minority Uighur society throughout the region. The xenophobic Chinese government made a concerted effort to buffer and isolate communist China from the traditional Islamic influence and culture Uighurs identified with.

After the collapse of the Soviet Union, several Islamic-based Central Asian states successfully gained independence from Russia. Seeking freedoms similar to those afforded Islamic neighboring states, influential Uighurs in Xinjiang unsuccessfully petitioned the Chinese government to have the territory reverted back to the historic name of East Turkistan and be granted full independence, instilling a sense of nationalism and recognition for minority Uighurs. In a continued effort to marginalize Uighur society and maintain control over the region, all requests for an independent East Turkistan state were denied by the Chinese government. With this action, China continued to synthetically suppress the collective identity of the former independent state of East Turkistan in an effort to limit Islamic influence within the country.

Today, ethnic tensions between Uighurs and Han are attributed to economic growth and development within the region. In the past decade, large deposits of minerals and natural resources have been discovered in the areas of Aksu and Karamay, spurring an oil and petrochemical boom. Economic growth has substantially increased throughout the province, as the oil and petrochemical industries account for 60% of its gross domestic product.<sup>1</sup> This wide-scale development has resulted in a new prosperity, creating higher-paying jobs that require skilled labor. With such advanced

development comes greater competition between minority, uneducated Uighurs and technologically-educated Han for advancements and economic opportunities.

Most development projects throughout Xinjiang are financed by wealthy Han businessmen from Beijing. Ethnic Uighurs feel that they are victims of discrimination, as the majority of high-paying jobs are provided to skilled Han Chinese with little regard given to Uighur men or women. Many Uighurs are left with low-paying manual labor jobs. This situation has been a primary source of contention over the years, which periodically takes the form of violent, anti-Han attacks perpetrated by radicalized Uighurs. The Urumqi market attack is the latest example, and remains the largest terrorism incident inside China to date.



Figure 1. Map of People's Republic of China

### The Attack

In the early morning hours of 22 May 2014, two SUVs broke through a fence in the Shayibake District of Urumqi, an area largely populated by the city's ethnic Han. As the SUVs sped down the open market, both vehicles struck and killed several elderly shoppers. Eyewitnesses indicated that neither vehicle had license plates, and occupants of both SUVs tossed paint can-type improvised explosive devices (IED) out of the vehicles' windows as they sped down the street, targeting large crowds of shoppers.<sup>2</sup> Several devices failed to detonate and were recovered later by police at the scene.<sup>3</sup>

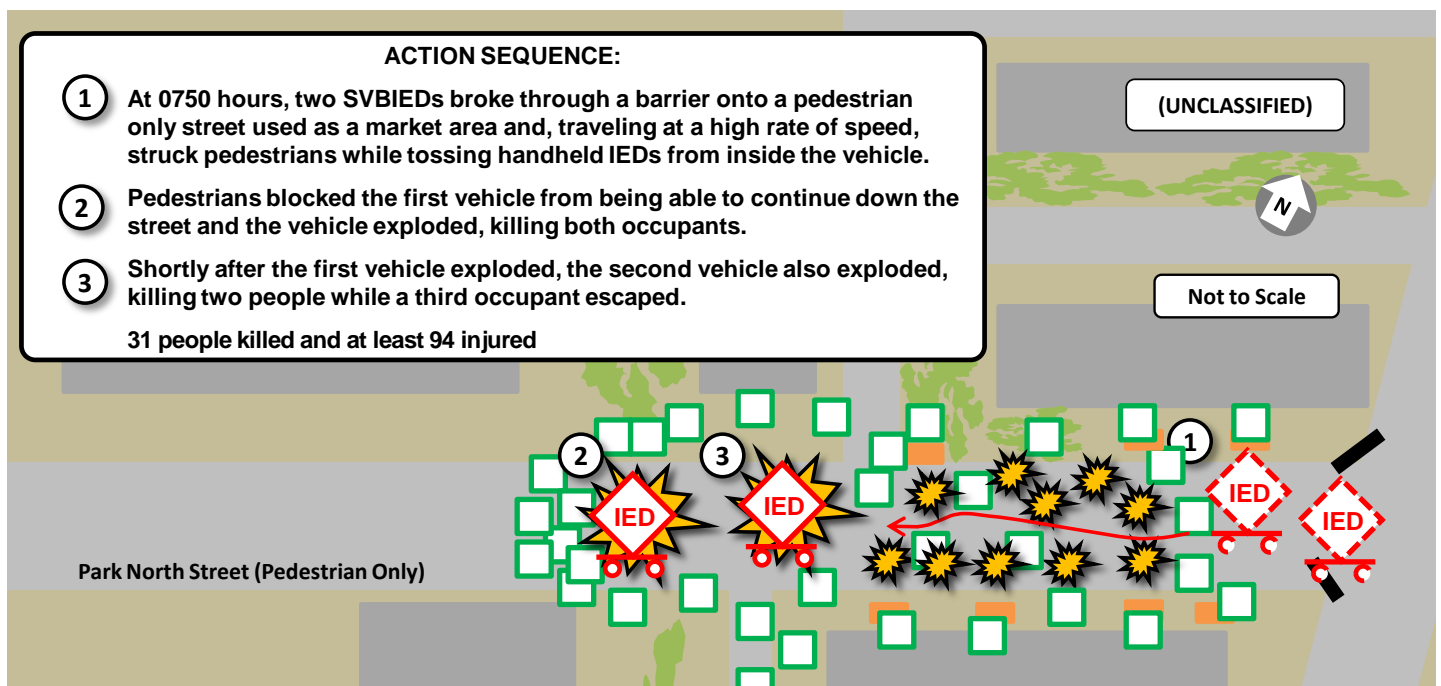


Figure 2. Attack diagram

The diagram below depicts the sequence of events that unfolded. Both vehicles traveled in a westerly direction and struck multiple elderly shoppers. As the SUVs continued down the market, passengers from both vehicles tossed IEDs out the windows into crowds of shoppers, resulting in additional victims. At the end of the street, one vehicle was blocked by a group of citizens using vendor carts, hampering it from moving farther.<sup>4</sup> After two minutes, that vehicle exploded, killing all occupants inside. The second vehicle came to a stop directly behind the first and also exploded, killing two of the three occupants. The third occupant escaped, but was later apprehended and held by Chinese police in

Bayingolin Prefecture, south Urumqi.<sup>5</sup> Responding quickly, police officials worked to seal off the crime scene from journalists and bystanders. Chinese officials indicated the attack was premeditated and the market specifically targeted due to large crowds of ethnic Han shoppers, who are known to gather in the early morning hours to shop for fresh fruit.

The use of vehicles as a weapon for terror is not a new tactic in China. A relatively recent incident occurred 4 August 2008, when two Uighur men stole a dump truck and purposely struck and killed 16 people. Another incident using a vehicle as a weapon of choice occurred five years later. On 28 October 2013 Usman Hasan, his wife Gulkiz Gini, and his mother Kuwanhan Reyim drove their SUV into a large crowd gathered at Tiananmen Square, a popular tourist site. After ramming security barricades and striking several tourists, the vehicle exploded, killing all three occupants and two tourists. Upon investigation, police found gas cans, knives, and steel rods inside the vehicle. Its license plate was traced to a Mr. Reyim, a Uighur resident of Xinjiang province, more than 1,300 miles from where the attack occurred in Beijing.<sup>6</sup>

Adapting their tactics, perpetrators of the Urumqi market attack removed license plates from both vehicles prior to the attack, thus precluding police officials from being able to trace either vehicle back to any specific person. By removing the license plates, the perpetrators learned from the Tiananmen Square error and made a conscious effort to avoid the previous mistake.

### **Regional Threat Actors**

The most well-known threat actor operating within and proliferating from Xinjiang province is East Turkestan Islamic Movement (ETIM), also referred to as Turkistan Islamic Party. Created in 1993 by two ethnic Uighurs, ETIM was established with a nationalistic ideological goal, identifying with the former Uighur independent state of East Turkistan in an effort to link the group with the struggles ethnic Uighurs have endured under harsh Chinese suppression. The primary goal of the organization was to establish a separate Islamic Uighur state, independent from Chinese Han influence and rule. When the movement failed to resonate with the local population, the original group disbanded in late 1993.

In February 1997, growing friction between ethnic Uighur and Han Chinese communities erupted in mass protests throughout Xinjiang province. Demonstrating against wage discrimination and low-paying manual labor jobs, hundreds of disgruntled Uighurs took to the streets, prompting a disproportionate, repressive police response. During this time, clashes between police forces and protesting Uighurs resulted in over 100 protester deaths.

In the context of this volatile social environment and with increased resolve to establish an independent Islamic State, Hasan Mahsum, an ethnic Uighur from Xinjiang's Kashgar region, reestablished ETIM in 1998 and quickly sought support from regional extremists in neighboring Afghanistan. Moving ETIM headquarters to Kabul, Mahsum became acquainted with al-Qaeda and Taliban leaders, who assisted ETIM with financial support and militant training.<sup>7</sup> Drawing from a base of despondent Uighurs from Xinjiang eager to support extremist causes, ETIM quickly recruited a small number of militants willing to travel to Afghanistan. From al-Qaeda and Taliban mentors in Afghanistan, new ETIM members gained valuable knowledge of militant tactics and explosives that were later used against coalition forces during Operation Enduring Freedom.<sup>8</sup>

Mahsum was killed in October 2003 by Pakistani officials in an al-Qaeda training camp in Kyber-Pakhtunkhwa, Pakistan. After Mahsum's death, splinter groups from ETIM began returning to Xinjiang province, bringing their knowledge and skill set of battlefield tactics with them. Since that time, members of ETIM have taken credit for several attacks inside China, including a series of bus bombings in the city of Kunming just prior to the Beijing Summer Olympics of 2008. Current estimates of ETIM strength levels vary widely. The United Nations indicates there are 200 active members with close associations to al-Qaeda.<sup>9</sup> While the group's members are known to operate regionally alongside al-Qaeda and Taliban militants in Afghanistan and Pakistan, recent reports also indicate that ETIM members have joined militant groups in Syria.<sup>10</sup> This would suggest the group has acquired the capacity to project forces well beyond its original base of operations inside Central Asia.

Common tactics of the organization include the use of explosives and small arms, and the use of vehicles as a weapon. Additionally, on 29 June 2012, members of the group attempted to hijack an aircraft in Urumqi but were unsuccessful.

The ETIM is the only terrorist organization operating within Xinjiang province known to have established links with al-Qaeda.<sup>11</sup> While ETIM has not claimed responsibility for the Urumqi market attack, the perpetrators are suspected of



being members of the group, as the tactics used in this attack closely resemble those associated with the organization. China continues to use the threat of terror in Xinjiang province as a pretext for further isolating and suppressing the minority Uighur population, which only increases the tension and discontent already prevalent throughout the province.<sup>12</sup> Intimidation tactics are often used throughout the region by public officials in an attempt to dissuade the populace from participating in acts of violence against the government. Public trials of individuals suspected of conducting acts of terror are common in the region.<sup>13</sup>

Continued efforts by the Chinese government to isolate and suppress the Uighur community will only result in greater tensions throughout the region. Additionally, this type of environment has the potential to be used to recruit impressionable Uighur youth into the terrorist organization. Increased economic growth and development will contribute to hotspots as competition for higher-paying wages will remain an issue. Understanding the historical context of ethnic disputes between the Uighur and Han cultures will be essential in establishing a viable and long-lasting political solution. Though desirable, this seems unlikely, as the Chinese government remains focused on preserving the cultural hegemony of Han society with little or no regard to other ethnic groups residing within its borders, especially groups who are heirs to an Islamic heritage.

Residing in close proximity to Pakistan and Afghanistan, ETIM members will continue to travel to neighboring states to acquire skill sets associated with terrorism. Once acquired, this knowledge can easily be transferred and tailored for use in China. This case study shows the need to monitor nationals who travel to foreign conflicts, gain training, and learn militant tactics. Such individuals then have the ability to return to their home country and apply this skill set at will.

### Training Implications

This attack provides several examples of tactics that can be used to support home station training. Most important are those actions directed against people gathered at markets, shopping centers, malls, and airports, all of which provide lucrative targets for acts of terror. Additionally, attacks can occur in combinations; a small hand-held IED may serve as a diversion or a prelude to a larger attack, including one that employs a suicide vehicle borne improvised explosive device.

### Notes

---

<sup>1</sup> ["Xinjiang profile,"](#) BBC News, 22 May 2014.

<sup>2</sup> ["Terrorist attack kills 31, injures 94 at Urumqi market,"](#) Xinhua, 23 May 2014.

<sup>3</sup> Andrew Jacobs, ["Suspects in China Market Attack Are Identified,"](#) The New York Times, 25 May 2014.

<sup>4</sup> ["Explosion in China's Xinjiang Region Kills 31,"](#) CCTV America, 22 May 2014.

<sup>5</sup> ["Urumqi attack: China arrests suspect in Xinjiang,"](#) BBC News, 24 May 2014.

<sup>6</sup> William Wan, ["Chinese police say Tiananmen Square crash was 'premeditated, violent, terrorist attack',"](#) The Washington Post, 30 October 2013.

<sup>7</sup> ["Chapter 8: Foreign Terrorist Organizations,"](#) US Department of State.

<sup>8</sup> Liu Zhun, ["Take fight to ETIM before threat grows,"](#) Global Times, 22 December 2013.

<sup>9</sup> United Nations, ["Security Council Committee pursuant to resolutions 1267 \(1999\) and 1989 \(2011\) concerning Al-Qaida and associated individuals and entities,"](#) 7 April 2011.

<sup>10</sup> Raffaello Pantucci, ["China Claims Uighur Militants Are Seeking a Syrian Battlefield,"](#) Terrorism Monitor Volume: 10 Issue: 22, Jamestown Foundation, 30 November 2012.

<sup>11</sup> Beina Xu, Holly Fletcher, and Jayshree Bajoria, ["The East Turkestan Islamic Movement \(ETIM\),"](#) Council on Foreign Relations, 1 April 2014.

<sup>12</sup> ["Country Reports: East Asia and Pacific Overview,"](#) Office of the Coordinator for Counterterrorism, US Department of State, 30 May 2013.

<sup>13</sup> JC Finley, ["China holds mass terror trial in sports stadium, sentencing 3 to death,"](#) United Press International, 29 May 2014.

## —What CTID Does for YOU—

## CTID Points of Contact

- ◆ Determine Operational Environment (OE) conditions for Army training, education, and leader development.
- ◆ Design, document, and integrate hybrid threat opposing forces (OPFOR) doctrine for near-term/midterm OEs.
- ◆ Develop and update threat methods, tactics, and techniques in HQDA Training Circular (TC) 7-100 series.
- ◆ Design and update Army exercise design methods in HQDA TC 7-101.
- ◆ Develop and update the US Army *Decisive Action Training Environment (DATE)*.
- ◆ Develop and update the US Army *Regionally Aligned Forces Training Environment (RAFTE)* products.
- ◆ Conduct Threat Tactics resident course at TRISA, Fort Leavenworth, KS.
- ◆ Conduct Threat Tactics mobile training team (MTT) at units and activities.
- ◆ Support terrorism-antiterrorism awareness in threat models and OEs.
- ◆ Research, author, and publish OE and threat related classified/unclassified documents for Army operational and institutional domains.
- ◆ Support Combat Training Centers (CTCs) and Home Station Training (HST) and OE Master Plan reviews and updates.
- ◆ Support TRADOC G-2 threat and OE accreditation program for Army Centers of Excellence (CoEs), schools, and collective training at sites for Army/USARR/ARNG.
- ◆ Respond to requests for information (RFIs) on threat and OE issues.

**Director, CTID** Jon Cleaves DSN: 552  
[jon.s.cleaves.civ@mail.mil](mailto:jon.s.cleaves.civ@mail.mil) 913.684.7975

**Deputy Director, CTID** Penny Mellies  
[penny.l.mellies.civ@mail.mil](mailto:penny.l.mellies.civ@mail.mil) 684.7920

**Operations–Analyst** Dr Jon Moilanen  
[jon.h.moilanen.ctr@mail.mil](mailto:jon.h.moilanen.ctr@mail.mil) BMA 684.7928

**Product Integration–Analyst** Angela Wilkins  
[angela.m.wilkins7.ctr@mail.mil](mailto:angela.m.wilkins7.ctr@mail.mil) BMA 684.7929

**Research & Analysis** DAC Jennifer Dunn  
[jennifer.v.dunn.civ@mail.mil](mailto:jennifer.v.dunn.civ@mail.mil) 684.7962

**Worldwide Equipment Guide** John Cantin  
[john.m.cantin.ctr@mail.mil](mailto:john.m.cantin.ctr@mail.mil) BMA 684.7952

**Military Analyst** H. David Pendleton  
[henry.d.pendleton.ctr@mail.mil](mailto:henry.d.pendleton.ctr@mail.mil) CGI 684.7946

**Military Analyst** Dr Jim Bird  
[james.r.bird.ctr@mail.mil](mailto:james.r.bird.ctr@mail.mil) Textron 684.7919

**Fusion** DAC Jerry England  
[jerry.j.england.civ@mail.mil](mailto:jerry.j.england.civ@mail.mil) 684.7934

**UK LNO** Warrant Officer Matt Tucker  
[matthew.j.tucker28.fm@mail.mil](mailto:matthew.j.tucker28.fm@mail.mil) 684-7994

**Military Analyst** Laura Deatrick  
[laura.m.deatrick.ctr@mail.mil](mailto:laura.m.deatrick.ctr@mail.mil) CGI 684.7925

**Military Analyst** Rick Burns  
[richard.b.burns4.ctr@mail.mil](mailto:richard.b.burns4.ctr@mail.mil) BMA 684.7897

**Exercise–Training Spt** DAC Walt Williams  
[walter.l.williams112.civ@mail.mil](mailto:walter.l.williams112.civ@mail.mil) 684.7923

**Military Analyst** DAC Steffany Trofino  
[steffany.a.trofino.civ@mail.mil](mailto:steffany.a.trofino.civ@mail.mil) 684.7960

**LNO to JMRC & JRTC** Mike Spight  
[michael.g.spight.ctr@mail.mil](mailto:michael.g.spight.ctr@mail.mil) CGI 684.7974

**LNO to MCTP** BMA Pat Madden  
[patrick.m.madden16.ctr@mail.mil](mailto:patrick.m.madden16.ctr@mail.mil) 684.7997

**Current Operations** LTC Shane Lee  
[shane.e.lee.mil@mail.mil](mailto:shane.e.lee.mil@mail.mil) 684.7907

**Current Operations** CPT Ari Fisher  
[ari.d.fisher.mil@mail.mil](mailto:ari.d.fisher.mil@mail.mil) 684.7939

**Military Analyst–NTC LNO** DAC Kris Lechowicz  
[kristin.d.lechowicz.civ@mail.mil](mailto:kristin.d.lechowicz.civ@mail.mil) 684.7922

**Military Analyst** (TBD)