Red Diamond
Threats Newsletter

TRADOC G-2 Operational Environment Enterprise
ACE Threats Integration

Fort Leavenworth, KS | Volume 7, Issue 01 | JAN 2016

INSIDE THIS ISSUE

OEE *Red Diamond* published by TRADOC G-2 OEE ACE Threats Integration

Send suggestions to:
ATTN: *Red Diamond*
Jon H. Moilanen (IDSI Ctr), G-2 ACE-TI Operations
and
Laura Deatrick (CGI Ctr), Editor

by TRADOC G-2 ACE Threats Integration, Operations

The TRADOC G-2 ACE Threats Integration Directorate (ACE-TI) will conduct the spring Threat Tactics Course (TTC) 7–11 March 2016 at Fort Leavenworth, KS. This course focuses on opposing force (OPFOR) tactics and techniques in training, professional education, and leader development venues based on the US Army Training Circular (TC) 7-100 series on opposing force threat doctrine. Instructors discuss concepts of threat tactics, actors, and operational environment conditions in small group seminar format. The course includes lecture, small group discussion vignettes, information warfare analysis, and in-class practical exercises. The *Decisive Action Training Environment* (DATE) is included in course materials.

The Threat Tactics Course represents 40 hours of instruction, Monday to Friday. The TTC is also available as a mobile training team (MTT) course that a requesting unit hosts for instructor cost of travel from Ft Leavenworth to the unit site. To inquire about available spaces in the March 2016 TTC, future TTC offerings, or to request an MTT, contact kristin.d.lechowicz.civ@mail.mil.

See **Threats Tactics Course** lessons on the Army Training Network (ATN) with CAC access: **https://atn.army.mil/dsp_template.aspx?dpID=447**

RED DIAMOND TOPICS OF INTEREST

by **Jon H. Moilanen**, TRADOC G-2 ACE Threats Integration, Operations, *Red Diamond* Newsletter (IDSI Ctr)

This issue of *Red Diamond* leads with an article on urban crime as an operational environment and is the first in a two-part article series that focuses primarily on environmental observations of crime, fear, and disorder. The second article will provide a more thorough analysis of how real-world threat actors conduct and leverage crime, fear, and disorder to their advantage and the impact they can have on US Army operations at the brigade combat team (BCT) level.

An article on complex battle position (CBP) as an opposing force (OPFOR) task presents an example when OPFOR defends key terrain. However, a CBP is typically a defensive location designed to avoid detection and employs a combination of complex terrain; camouflage, cover, concealment, and deception; and countermobility effort to protect OPFOR elements and/or other friendly elements-forces within the position from attack and deny seizure of the location by the enemy.

The US Army's iWATCH program is the highlight of an antiterrorism awareness article to encourage timely reporting of suspicious behavior to military or civilian law-enforcement agencies. The program focuses on protecting communities and activities from terrorist attack by being vigilant in awareness and immediately reporting unusual behavior in local communities.

The fall of Ramadi in May 2015 represented a significant success for ISIL. An update article previews information on a number of topics to the TRADOC G-2 *Threat Tactics Report: Islamic State of Iraq and the Levant*. The update describes how ISIL captured the city. The TTR update also includes a discussion of Sinjar tunnel networks as a means of protection against air strikes and for command and control, use of chemical weapons against Kurdish fighters, and details about ISIL financing operations.

The TRADOC G-2 ACE Threats Integration (ACE-TI) Directorate hosted a Working Group meeting on 8–11 December 2015 at Ft. Leavenworth, Kansas, for *Decisive Action Training Environment* (DATE 3.0). An article notes expanding use of DATE nationally and internationally, and describes ongoing coordination of current and future DATE concepts.

The Director's Corner accents an evolving concept of how the DATE may be adapted to regional environments and readiness conditions such as Europe, the Pacific region, Africa, and South America. The current DATE 2.2 (2015) remains focused in the Caucasus region but remains adaptable for training, professional education, and leader development venues.

The MTK-2 Meteorit article presents information from the current update to the TRADOC G-2 *Worldwide Equipment Guide* (WEG). As a Russian mine clearing system fielded in the early 1980s, the MTK-2 has two UR-77 rockets mounted on an adjustable turret. The main feature is the ability to deploy a large mineclearing line charge that is stored inside the vehicle for rapid breaching of obstacles in support of movement and maneuver of forces.

To be added to the *Red Diamond* e-distribution list, contact:

Dr. Jon H. Moilanen (IDSI Ctr)
G-2 ACE Threats Integration, Operations
jon.h.moilanen.ctr@mail.mil

Director's Corner
Thoughts for Training Readiness

by **Jon Cleaves**, Director, TRADOC G-2 ACE Threats Integration (DAC)

We held a DATE 3.0 Working Group meeting here at Ft Leavenworth 8-11 December 2015. Ninety-six persons from six countries attended at least part of the meeting. Representatives were present from the United States, Australia, Canada, the Netherlands, New Zealand, and the United Kingdom. The meeting consisted of a general session and Timeline Subgroup session on 8 Dec; Irregular Warfare and Maritime Subgroup sessions on 9 Dec; Order of Battle and Terrain Subgroup sessions on 10 Dec; and a final general session on 11 Dec.

Concurrent with that effort has been a hard look into how best to expand the reach of the DATE concept beyond the physical limitations of the South Caucasus region. I would assess as most likely that our leadership is going to greenlight a plan to build five separate DATEs—making use of the core information inherent in the current DATE, but providing one in each COCOM AOR: Europe, South Caucasus, Pacific, Africa, and South America. A proof of principle is being developed for a DATE Europe, with testing in a Warfighter exercise planned for early in the next FY. In this prototype, Donovia and Gorgas are translated onto European terrain and modified to suit European OE conditions. Keep on the lookout here in *Red Diamond* as we keep you apprised of developments in this area.

JON

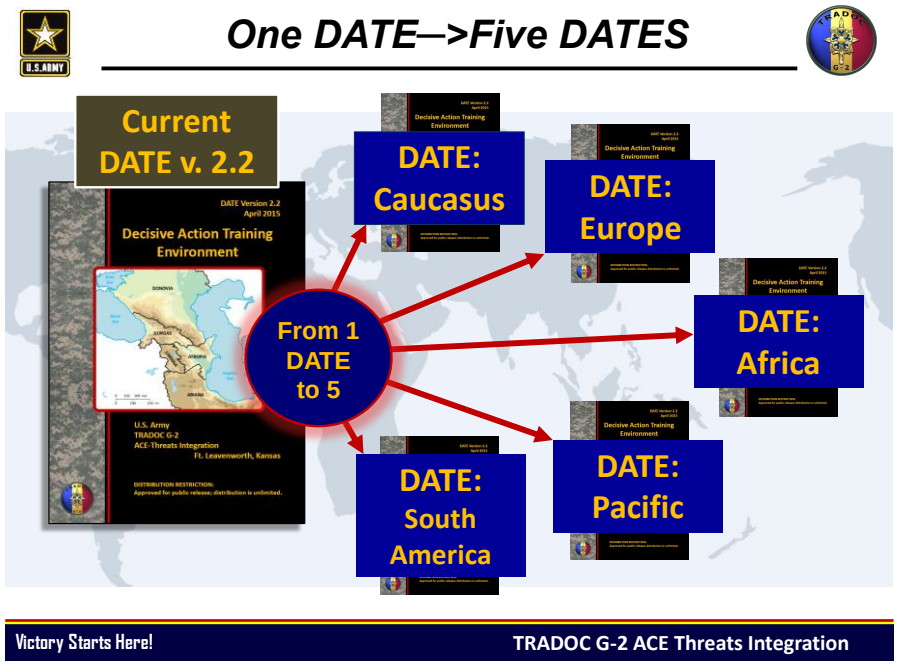


Figure 1. Concept for evolution of Decisive Action Training Environment

by CPT Nickolas Zappone, TRADOC G-2 ACE Threats Integration

For three weeks in December I was afforded the rare opportunity to embed with one of the Kansas City Police Department's (KCPD's) elite tactical units: the Street Crimes Unit (SCU) tactical squads (TAC). Comprised of highly-trained career police officers with experiences ranging from organized crime to gang enforcement to undercover narcotics, SCU TAC is essentially the enforcement apparatus for its parent organization. One echelon up, the SCU is a multifaceted organization subordinate to KCPD's Narcotics and Vice Division and comprised of a narcotics squad (undercover police officers); a gang enforcement squad; a vice squad (prostitution); an illegal firearms squad; and two seven-man tactical squads.

The purpose for this embed was to immerse myself in the contemporary urban crime environment in an effort to articulate crime as an opposing force (OPFOR) tactical task and to help accurately replicate the criminal signature on the battlefield, particularly with regard to street crime. This article will be the first in a two-part series and will focus primarily on environmental observations and manifestations of crime, fear, and disorder. The second article will provide a more thorough analysis of how real-world threat actors conduct and leverage crime, fear, and disorder to their advantage and the impact they have on Army operations, specifically at the brigade combat team (BCT) level. I encourage readers to compare and contrast my observations with personal experiences in urban environments overseas to help conceptualize the diverse manifestations of crime, fear, and disorder and the impacts they have on Army operations.

The Criminogenic Nature of the Inner City

Neighborhoods within Kansas City's inner city share many of the same salient characteristics as other large, domestic urban population centers. On prominent display were indicators of social and physical disorder such as extreme poverty; lack of economic opportunity and upward economic mobility; endemic abuse of narcotics; large numbers of single-parent families; low residential stability; physical decay; and high crime rates. These characteristics, which often personify high crime neighborhoods within the inner city, permeate nearly every aspect of day-to-day life for those living in marginalized communities and perpetuate a vicious cycle of illicit activity and dependence on the informal economy.

The aforementioned challenges have had a pernicious effect on the inhabitants of these neighborhoods, particularly young men. It is similar to experiences in Iraq and Afghanistan, where disaffected military-age males bolstered the ranks of insurgencies for some of the same timeless motivations young men in the inner city join street gangs and commit to lives of crime—power, profit, identity, score-settling, and a sense of brotherhood. In that vein, my anecdotal hypothesis is that gang culture in America's inner cities is so prevalent that these disaffected young men simply grow into it, invariably becoming products of its influence. In the inner city, one's proclivity to join a street gang, for example, is reinforced by social norms canonizing gang members and the gang life while vilifying government institutions and associated enforcement apparatuses.

Criminals from every level of the criminal stratum, ranging from unaffiliated street criminals to organized crime syndicates, will likely continue to leverage this dynamic to their advantage; however, street gangs are the principle benefactors. They isolate the neighborhoods on which they leach by infiltrating nearly every aspect of the social structure, giving them the ability to coerce, co-opt, and corrupt with ease. At times this relationship may be mutually beneficial, for they often

stabilize marginalized communities by acting as a shadow government. Examples abound, with the most prominent being: protection rackets designed to protect prostitutes from abusive customers; access to corrupt aldermen who can facilitate the continuation or restoration of essential services; job opportunities related to the illegal sale of narcotics; conflict and/or grievance resolution; and humanitarian assistance in the form of food and resource distribution. In a deployed environment, similar initiatives to create instability are counter to the Army's desired end state conditions.

Observations of Crime and Disorder

Crime and disorder have diverse manifestations across operational environments (OEs). What passes for crime and disorder in highly-integrated cities like Kansas City may not qualify in Rio de Janeiro or Lagos, which are moderately- and loosely-integrated cities, respectively. When analyzing crime and disorder it is important to remain cognizant of the notion that the rule of law and public order in an OE is relative to the culture (or cultures) within that OE. That having been said, listed below are my observations of how crime and disorder manifest themselves in Kansas City:

- Street crime is inherently amorphous. Affiliations and alliances are constantly shifting based on factors ranging from seemingly trivial slights to congenital hostility. Members constantly come and go for a variety of reasons, which further convolutes the criminal signature within the OE.
- The center of gravity for most street gangs in the Kansas City metropolitan area is the illegal sale of controlled substances, primarily crack cocaine, heroin, methamphetamine, and prescription drugs like oxycodone.
- Similar to major metropolitan areas like Los Angeles and Chicago, Kansas City street gangs identify with specific geographic areas (e.g. the 57th street gang). However, unlike Los Angeles and Chicago, Kansas City gangs do not go to great lengths to prevent/deter intrusions by rival gangs (e.g. murdering a rival gang member for being in the wrong neighborhood).
- To commit a targeted homicide, street gangs will employ deception by luring rival gang members to a location of their choosing through the use of a female accomplice. Typically, the female accomplice will solicit the target for a carnal encounter, and upon his arrival the target will be ambushed by multiple gang members equipped with small arms.
- The opportunistic nature of crime is very prevalent at the street-crime level. While some groups or individuals develop more sophisticated ways and acquire better means relative to those who are less criminally adept, the end goal is invariably quick and easy profit.
- There is evidence of hybrid gangs within the contemporary urban crime environment. Hybrid gangs can be characterized as those that are historically street gangs but have evolved and metastasized over time into something that looks more organized, hierarchical, and vertically integrated. Examples are MS-13 and the 18th Street Gang.
- Violence, particularly between street gangs, waxes and wanes due to economic issues like the maintenance of market share, access to suppliers, and control of geography (although not evidenced in Kansas City), but also because of acute and chronic grievances.
- Matriarchs, primarily mothers and grandmothers, are the principle facilitators of criminality because of their access to resources like shelter, transportation, subsistence, and money. An example of more active support would be receiving monthly payments for allowing drug dealers and/or street gangs to hide narcotics, money, and firearms in her residence. Yet another example of active support would be the straw purchase of firearms.
- Crime appears to manifest in pockets and potentially temporarily displaces or permanently relocates to areas where revenue generation is more lucrative and/or sustainment is more readily accessible.
- Street gangs, criminal cells, and individual criminals will use any means available to acquire the resources necessary to commit crime.
- More experienced career criminals employ countermeasures, conduct surveillance and counter-surveillance, conduct information warfare (INFOWAR), and protect assets. For example, one career criminal who was under indictment for being a member of a violent street gang implicated in homicides, narcotics sales, illegal firearms sales, and money laundering via a gangster rap label, employed a commercially-bought home surveillance system to serve as a sensor. The system was most likely linked to his mobile device, enabling him to observe the

delivery of his warrant in real-time while he hid at an alternate location. This level of sophistication was not observed for less-experienced criminal elements.

A key takeaway from this field study was that street crime and disorder are inextricably linked. Disorder may be further distilled to social disorder and physical disorder. Manifestations of these categories often violate statutes and ordinances, but tend to be innocuous relative to crimes against persons or property crime. Still, crime and disorder are most likely part of the same phenomenon, both stemming from structural characteristics specific to inner city neighborhoods with high concentrations of disadvantage.[1] Disorder may actually have more of an impact on people's perceived sense of security and stability, "because disorder can be observed, while crime, by contrast, is largely unobservable."[2]

Figure 1: Baltimore riots (video link)[3]

The recent riots in Ferguson, Missouri, and Baltimore, Maryland, are excellent examples of the impact disorder can have, not only on those communities directly affected by perceived injustices but also on society as a whole. The ubiquity of information—which is now easily accessible to the masses through the proliferation of information communications technologies—is clear, as event accounts spread like wildfire. Members of the citizenry are bombarded by information and misinformation alike: livestreaming, viral Facebook posts and Tweets, YouTube videos, and continuous—and potentially biased—media coverage all help form or solidify people's opinions. Additionally, these riots will likely have a cascading effect similar to those conditions created in Los Angeles, California, pursuant to the 1992 riots. In the decade afterward, the city of Los Angeles lost nearly $4 billion in taxable sales as businesses, investors, and residents were reluctant to stay.[4]

As probable conflict regions continue to modernize, it is plausible that similar events could unfold, potentially galvanizing support amongst the relevant population to mobilize against Army and/or host nation units. Threat actors may exploit disorder to their advantage, making use of episodic events like riots and looting to sensationalize grievances, thus contributing to the continuation of hostilities. The continuation of hostilities is of profound importance, particularly to the criminal element of the hybrid threat, because conflict provides opportunities to generate revenue and consolidate power.

The Erosion of Collective Efficacy

Collective efficacy can be defined as "cohesion among neighborhood residents combined with shared expectations for informal social control of public space."[5] Crime, fear, and disorder have a very deleterious effect on a neighborhood's perceived sense of stability and security. To combat these issues, a neighborhood must develop and sustain informal social control mechanisms to deter minor incivilities like public drunkenness, prostitution, and vandalism before they metastasize into more violent, predatory crimes like aggravated assault, armed robbery, and homicide.[6] The removal of street criminals is essential to creating a window of opportunity to cultivate collective efficacy within a neighborhood.

Unfortunately, my observations of high-crime neighborhoods within Kansas City's inner city leads me to believe that collective efficacy is low. Residents appear to accept disorder and crime as the status quo: intractable problems that have seemingly been present since time immemorial. High-speed car chases through residential streets; police officers delivering high-risk search warrants on known drug-stash houses; a crack-dealing ex-felon being apprehended in his front yard while his three small children watch after he sold to an undercover officer; and gang-related vigilante justice are simply commonplace. The level of apathy exhibited by many residents is disconcerting—to say the least—because "disorder triggers attributions and predications in the minds of insiders and outsiders alike, changing the calculus of prospective homebuyers, real estate agents, insurance agents, and investors. The extent of disorder reflects the extent of residents' effectiveness in improving their neighborhoods and may affect their willingness to sustain their activism."[7]

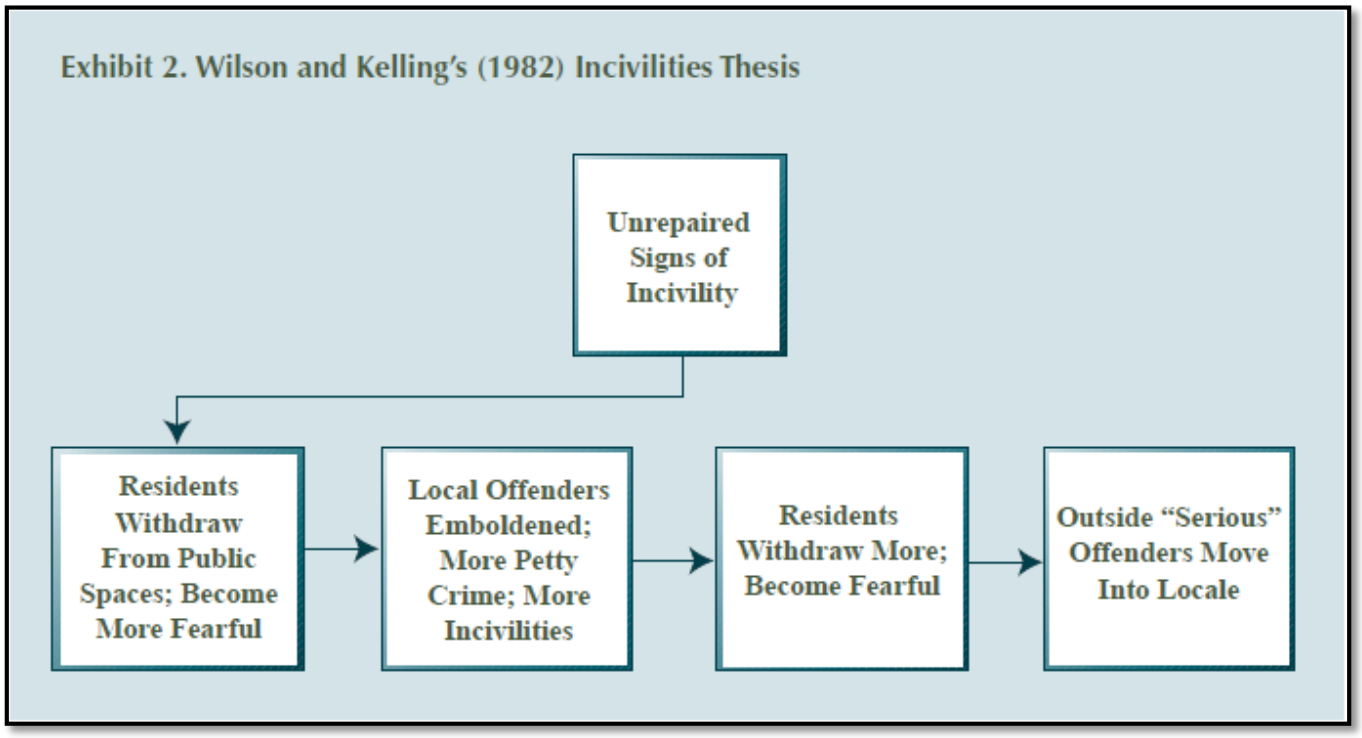


Figure 2: The Incivilities Thesis

Criminals will likely continue to use these poorly-governed spaces with weak collective efficacy as enclaves of impunity from which to operate. Attuned to the sentiment of the citizenry within these neighborhoods, criminals may seek to deepen the divide between residents and the local municipality in an effort to maintain or strengthen their hold on existing operational spaces. Furthermore, these poorly-governed spaces will serve as incubators of crime, fear, and disorder: virtual breeding grounds of criminality that, if uncontained, will spread to adjacent areas and may be targeted by malicious threat actors as recruitment zones.

Engendering Fear

Fear is a result of people's perceptions about crime and disorder. It can be conceptualized in four ways. "Three definitions are cognitive in nature, reflecting people's concern about crime, their assessments of personal risk of victimization, and the perceived threat of crime in their environment."[8] The final definition is behavioral and defines fear by the things people do in response to crime.[9] In a large, urban metropolitan area like Kansas City, gang-related violence can instill fear in those communities rife with street gangs, evoking behavioral responses. Parents may keep their children inside, resulting in taking time off from work or otherwise adjusting their schedules. Senior citizens may have to find an alternate way to get medical treatment. Local community-based organizations may have to be mobilized to deliver food to families too scared to walk to the store.[10]

It would be beneficial for Army units at the tactical level to be attuned to these emotive dimensions of fear because they may be indicative of larger problems. For example, a street gang may post a cautionary message on social media reminding community members of the penalty for cooperating with the police. Furthermore, fear influences people's perceived sense of security and stability within their neighborhood and influences decisionmaking.

After conducting a quick cost-benefit analysis, community members may be inclined to actively or passively support a threat actor because of the perceived weakness of the state. In Kansas City, for example, this inclination is reinforced by the widely-held belief that the Jackson County judicial system is very lenient, often imposing weak punishment on serious offenders who will inevitably be back on the street within 24 hours. Why implicate someone in a crime when you know that person will have the ability to seek retribution the next day?

Impact on Army Operations

The Army seemingly has a predilection for viewing the criminal element of the hybrid threat as mostly organized crime. Army doctrine and literature prefers to focus on combatting hierarchical, self-contained, vertically integrated, and, oftentimes, transnational groups, reminiscent of traditional organized crime families like the Italian-American mafia, Mexican drug trafficking organizations, or the Russian Organizatsiya. Our comfortability—and therefore tendency—with targeting these groups is logical: counterinsurgencies necessitate the employment of intelligence tools like the Distributed Common Ground System-Army (DCGS-A), Palantir, and i2 Analyst's Notebook to conduct social network analysis. However, the paucity of focus on what is widely considered to be street crime (e.g. aggravated assault, armed robbery, burglary, sexual assault) and disorder (e.g. substance abuse, homelessness, prostitution, vandalism) is concerning.

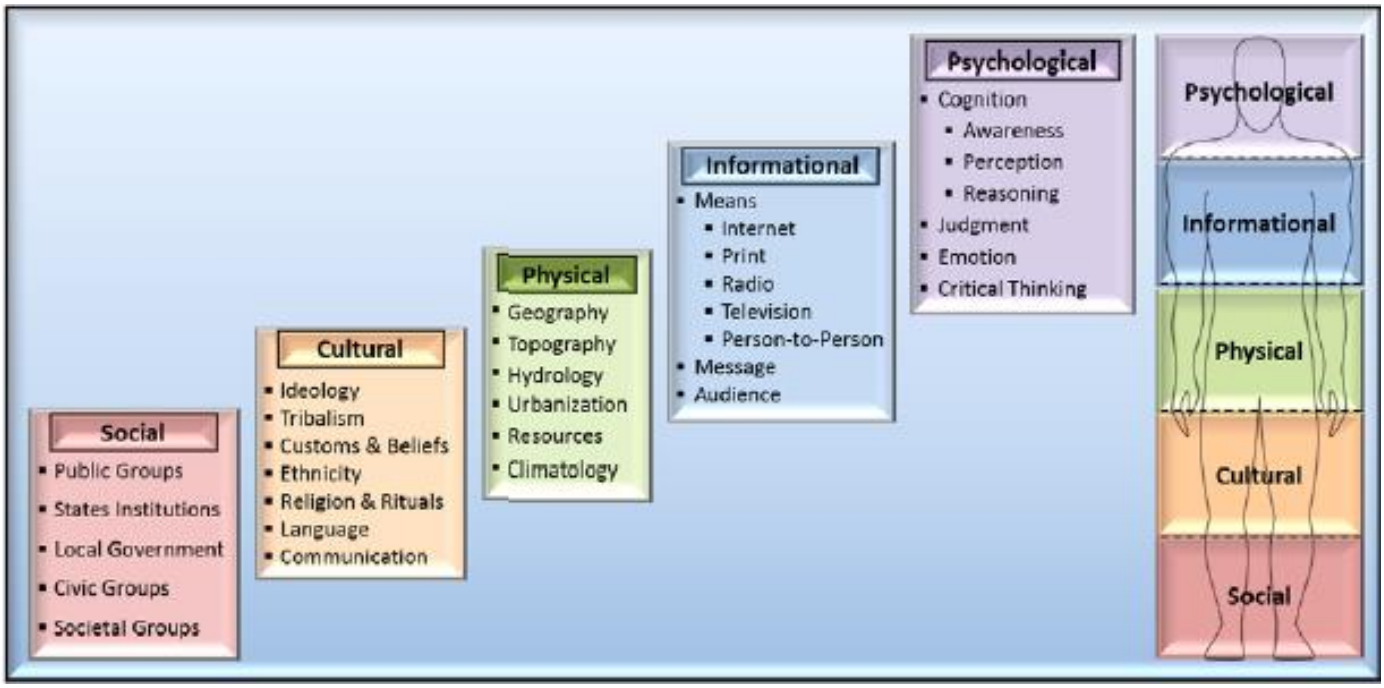


Figure 3: The elements shaping human decisionmaking and behavior

The Army relegates street crime at its own peril because a coherent, targeted response to street crime can disrupt threat actor operations in a meaningful way. By enabling host nation police forces to interdict criminal operations such as the production and sale of narcotics, prostitution, illegal gambling, counterfeiting, and cross-border smuggling, and human trafficking, Army units can reduce and/or disrupt the ways in which threat actors generate revenue, procure material, and maintain influence within an area of operations. Furthermore, a byproduct of successful interdiction is the legitimization of host nation police forces.

It would be beneficial for Army units to expend more intellectual capital on understanding the complex nature of street crime. The development and/or implementation of established or blended strategies to combat crime, fear, and disorder in order to consolidate gains should also be explored. By alchemizing counterinsurgency principles, policing strategies like community policing, "broken windows" and problem-oriented policing, and recent concepts concerning the human domain, BCTs may better "shape human decision-making and behavior to create desired effects."[11]

Author's note: My sincerest gratitude to the police officers of SCU TAC's 1910 and 1920 squads for making this field study possible, particularly Sergeant Scott Selock, P.O. Wes Lambright and P.O. John Pickens. Your unwavering professionalism, commitment to the preservation of constitutional liberties, and dedication to community is unparalleled. "To serve and protect."

Notes

[1] Robert Sampson and Stephen Raudenbush. "Disorder in Urban Neighborhoods—Does It Lead to Crime?" National Institute of Justice Research in Brief. February 2001.
[2] Robert Sampson and Stephen Raudenbush. "Disorder in Urban Neighborhoods—Does It Lead to Crime?" National Institute of Justice Research in Brief. February 2001.
[3] For another video of the Baltimore riots, see "Baltimore Protest Turns Violent" by Ford Fischer and Trey Yingst.
[4] Susie Poppick. "Can Ferguson Recover? The Lasting Economic Impact of Violent Unrest." Time Magazine. 25 November 2014.
[5] Robert Sampson and Stephen Raudenbush. "Disorder in Urban Neighborhoods—Does It Lead to Crime?" National Institute of Justice Research in Brief. February 2001.
[6] Robert Sampson and Stephen Raudenbush. "Disorder in Urban Neighborhoods—Does It Lead to Crime?" National Institute of Justice Research in Brief. February 2001.
[7] Robert Sampson and Stephen Raudenbush. "Disorder in Urban Neighborhoods—Does It Lead to Crime?" National Institute of Justice Research in Brief. February 2001.
[8] Wesley Skogan. "Measuring What Matters: Crime, Disorder, and Fear." National Institute of Justice and Officer of Community Oriented Policing Services. 1996.
[9] Wesley Skogan. "Measuring What Matters: Crime, Disorder, and Fear." National Institute of Justice and Officer of Community Oriented Policing Services. 1996.
[10] Sudhir Vankatesh. Gang Leader for a Day. Penguin Books. 2008; for a video on the effects of crime on a community, see "Living in Chicago's Gang Occupied Neighborhoods" by the Associated Press.
[11] US Special Operations Command. "Operating in the Human Domain, Version 1.0." 3 August 2015.

by Jon H. Moilanen, TRADOC G-2 ACE Threats Integration (IDSI Ctr)

When opposing forces (OPFOR) operate in rural or urban terrain, defenses can be constructed and fortified as complex battle positions and are comprised of multiple simple battle positions. A *complex battle position (CBP)* is typically a defensive location designed to employ a combination of complex terrain; camouflage, cover, concealment, and deception; and countermobility effort to protect the OPFOR elements and/or other friendly elements-forces within the position from detection and attack, as well as to deny seizure of the position by the enemy.[1]

Note. The OPFOR tasks, when approved by the TRADOC G-2 Threats Integration Directorate, are added to the G-27 resources of the TRADOC G-2 Virtual OPFOR Academy (VOA). With common access card (CAC) entry, you can visit the VOA resources to support training, professional education, and leader development at https://tbr.army.mil/voa/

Although a CBP is usually designed independently from other large OPFOR elements and/or friendly forces in an operational environment (OE), a CBP can be part of planned maneuver and/or area defensive measures. When a CBP protects elements and/or forces and provides sanctuary from which to launch local attacks, the location is typically not on or near an avenue of approach. However, when key terrain must be retained by an OPFOR, CBPs are designed to defend an area and prevent enemy forces from employing effective precision standoff attacks.[2] The two figures in this article illustrate this type of key terrain CBP defense.

The OPFOR may intend to continue a defense, conduct a delay, or—based on tactical conditions—successfully withdraw not in contact with an enemy until the OPFOR can resume offensive actions. A withdrawal can be conducted out of contact with an enemy or under pressure from an enemy. In both of these tactical situations, a CBP defense with multiple simple battle positions is altered only on the OPFOR commander-leader decision and subordinate OPFOR commander-leader understanding of the senior commander-leader's tactical intent. The tactical mission can require the OPFOR to accept decisive engagement in order to support a higher headquarters mission even if this action significantly degrades the combat power of OPFOR within and supporting the CBP.

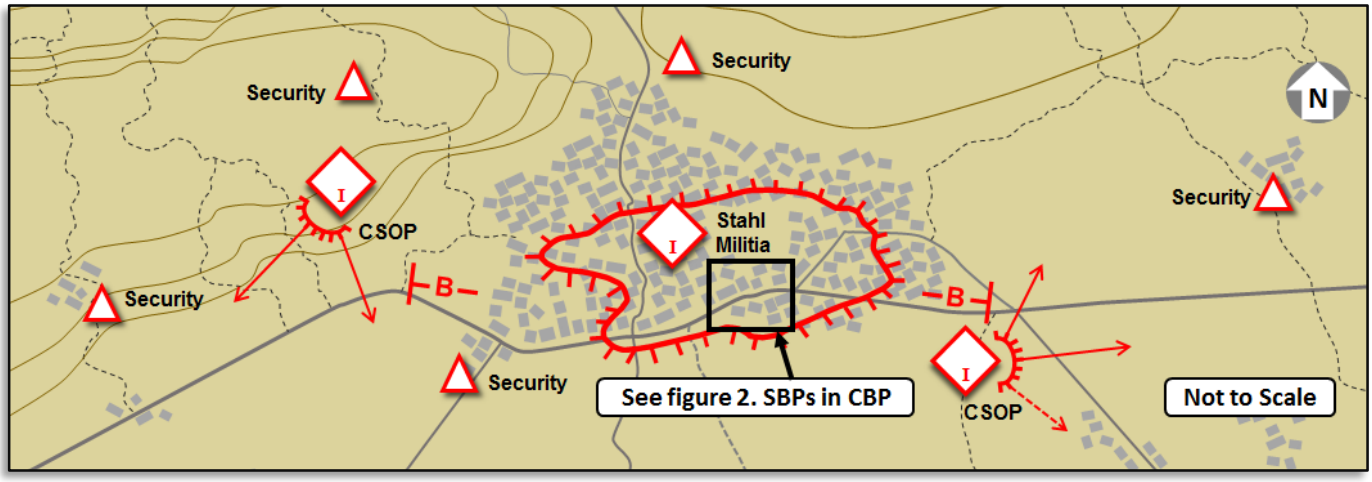


Figure 1. Complex battle position general sketch of key terrain defense (example)

A simple battle position (SBP) is a defensive location oriented on the most likely enemy avenues of approach.[3] CBPs typically have characteristics that distinguish them from SBPs to include:

- Limited avenues of approach toward the battle position,
- Avenues of approach that do exist are easily observable by the defending element and/or force,
- 360-degree defensive positioning and fires coverage,
- Engineer effort prioritized to camouflage, cover, concealment, and deception (C3D) complemented with countermobility actions focused to protect friendly forces while not revealing the CBP,
- Large combat service support (CSS) caches, and
- Sanctuary from which to launch local attacks when appropriate.

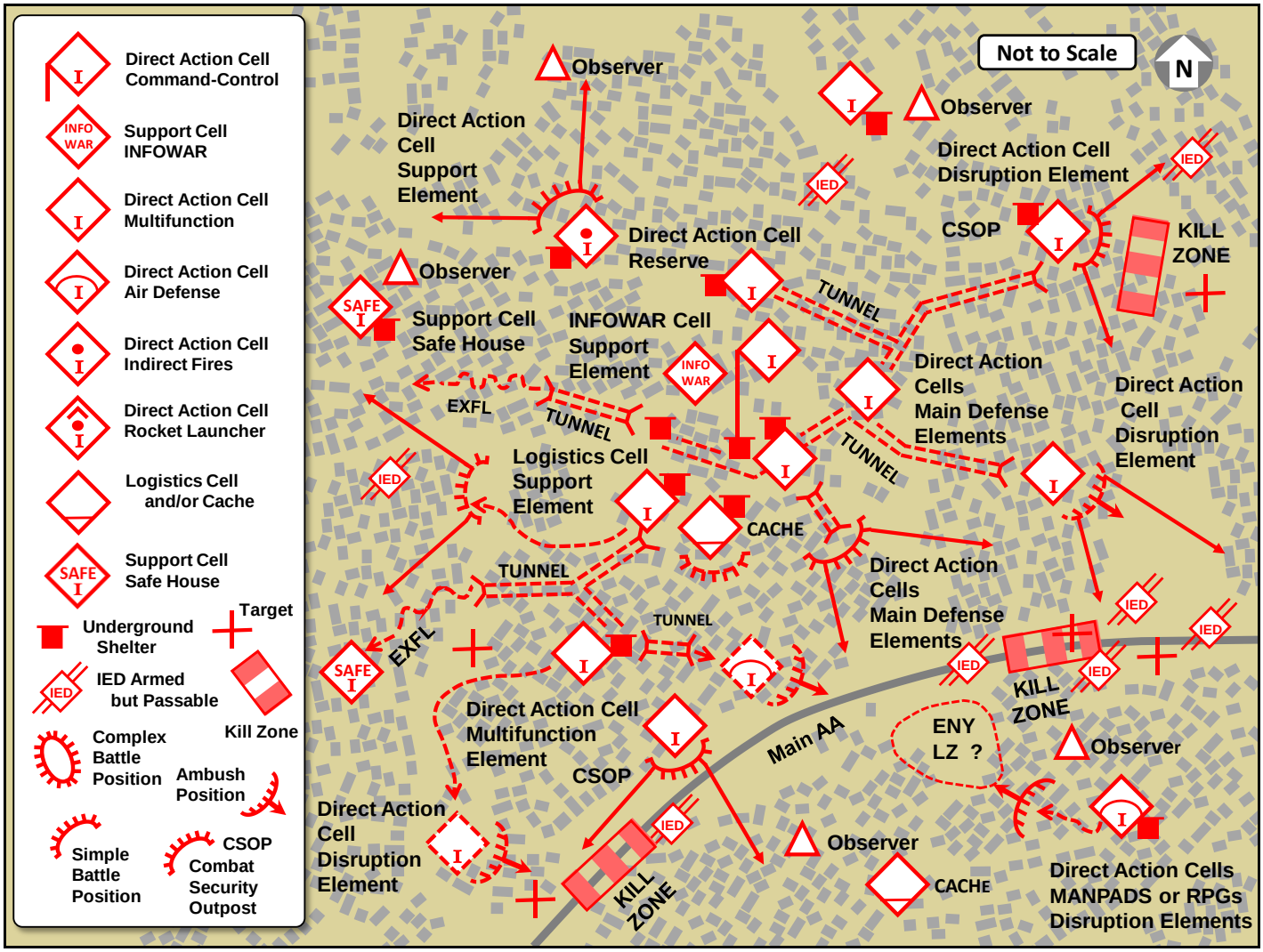


Figure 2. Simple battle positions integrated in a zone of a complex battle position (example)

The insurgent leader of a CBP organizes his subordinates as functional elements. Typical functional designations may include but do not necessarily require a—

- Disruption element,
- Main defense element,
- Reserve element,
- Support element, and
- Deception element.

Although these elements identify their tactical functions, defense of a CBP may require subtle differences or more than one of each type of element. The insurgent leader will determine whether or not to organize disruption elements in a disruption zone external to the CBP. He may determine that the manning and capabilities of his organization are more effectively used with security elements close to the defensive perimeter.

Whether near or distant from the CBP main defenses, security actions are disruption, active reconnaissance and surveillance, and counterreconnaissance. The main defense elements of a CBP are responsible for defeating an attacking force. These elements can be directed to delay an enemy while other cells or units withdraw from direct contact with the enemy or maneuver for a tactical advantage. CBPs are typically self-supporting in their defense. Fire support assets normally locate within the CBP but may also locate outside of the CBP perimeter to best employ specific fires. Elements from the CBP may attempt to integrate within local communities for the purpose of gathering information, collecting intelligence, and disseminating information warfare (INFOWAR) themes to gain the support of the local relevant population. Embedding with a local population can enhance as protection when this action restricts or precludes an enemy's ability to apply its full combat power.

OPFOR Tasks in US Army Training, Professional Education, and Leader Development

The TRADOC G-2 Analysis and Control Element (ACE) Threats Integration Directorate at Fort Leavenworth, Kansas, is refining the task, condition, and standard for an OPFOR complex battle position and its use in learning venues. Current operational considerations and emergent threats since the publication of OPFOR tasks in TC 7-101, *Exercise Design Guide* require this current evaluation and update of how to best portray threat and OPFOR tasks in learning conditions that span the live, virtual, constructive, and gaming (LVCG) environments of the US Army, allies, and partners. An OPFOR must be a realistic, robust, and relevant threat that challenges the capabilities and limitations of these forces in the execution of their military missions.

The TRADOC G-2 is the responsible official for the development, management, administration, integration, and approval functions of the OE and OPFOR Program across the US Army.[4] An OPFOR is a plausible, flexible, and free-thinking mixture of regular forces, irregular forces, and/or criminal elements representing a composite of varying capabilities of actual worldwide forces and capabilities (doctrine, tactics, organization, and equipment).

The OPFOR is used in lieu of a specific threat force for training and developing US forces, and can be configured to represent a hybrid threat.[5] The TRADOC G-2 Analysis and Control Element (ACE) Threats Integration Directorate serves as the US Army lead for the TRADOC G-2 to design, document, and integrate threat or OPFOR and OE conditions in support of all Army training, education, and leader development programs.[6]

Complex Battle Position Conditions

Tactical defensive actions normally represent all measures associated with organizing and implementing an undetected defensive posture within an assigned area of responsibility (AOR). When OPFOR capabilities are prioritized to a CBP, actions in systems warfare or other CBP support such as designated INFOWAR systems are integrated for immediate and progressive defensive improvements. A CBP at any OPFOR level of command and with any type elements and/or forces has the same basic subtasks.

For example, a tactical environment could present the following conditions as a mission task. The OPFOR is conducting operations independently or as part of a larger element or force and receives an operation order (OPORD) or fragmentary order (FRAGORD) to establish a CBP at a location and time specified. The order includes all applicable overlays and/or graphics. Task organization provides the combat power capabilities to accomplish the task. The OPFOR has communications with higher, adjacent, subordinate, and supporting elements. Friendly force and enemy coalition forces, noncombatants, government agencies, nongovernment organizations, and local and international media may be in the OE. The OPFOR is not constrained by standardized rules of engagement (ROE) and does not necessarily comply with international conventions or agreements on the conduct of warfare.

As an Army standard, the OPFOR conducts complex battle position (CBP) actions in accordance with tactics and techniques in TC 7-100.2 and/or TC 7-100.3, the order, and/or higher commander's guidance. The OPFOR commander or leader acknowledges the mission order, conducts reconnaissance and/or surveillance to accomplish security requirements, and

establishes the CBP. Stay-behind elements, on order, conduct follow-on tasks that can include but are not limited to reconnaissance and surveillance, and coordination to disrupt, delay, suppress, neutralize, defeat, and/or destroy designated enemy elements and/or capabilities. The OPFOR continues the mission.

The tasks and subtasks from initial plans to mission completion include five main tasks with several subtasks to each. A guide for selecting priorities of effort in training tasks to Army standard as an OPFOR is as follows:

PLAN

- Identify location that satisfies CBP purpose and supporting requirements.
- Identify reconnaissance and surveillance objectives for collection and analysis in support of AOR situational awareness and situational understanding requirements.
- Collect current information on enemy element-force capabilities and limitations and other operational environment information.
- Analyze *action* and *enabling* functions that must be performed to achieve mission success, such as tasks to deceive, defend, disrupt, suppress, fix, contain, neutralize, defeat, and/or destroy.
- Determine the functional tactics to be applied by *action, enabling,* and *support* elements.
- Identify task organization requirements for elements-forces by function in accordance with TC 7-100.2 and/or TC 7-100.3.
- Determine how and when functional elements act or enable security missions, defense, combat support, and combat service support of the CBP, and/or transition to other tasks-subtasks.

PREPARE

- Evaluate ongoing reconnaissance and surveillance to provide situational understanding of the enemy and the operational environment required for CBP success.
- Report regular, periodic, and/or unexpected information updates in a timely manner to satisfy the commander's critical information requirements and mission intent.
- Task organize elements-forces by function in accordance with TC 7-100.2/TC 7-100.3, which typically include disruption, main defense, reserve, and support.
- Coordinate the integration of available reconnaissance, intelligence, surveillance, and target acquisition (RISTA) assets for continuous and overlapping coverage of designated areas, zones, routes, and/or special objectives in the AOR, and zone of reconnaissance responsibility.
- Assess current counterreconnaissance actions to prevent the enemy from obtaining situational understanding of OPFOR intentions and/or CBP actions.
- Conduct mission and task rehearsals of *action* and *enabling* elements-forces.
- Confirm communications requirements and capabilities.
- Execute INFOWAR in support of the CBP.
- Conduct reconnaissance of withdrawal routes and/or exfiltration routes-lanes if a mission condition requires friendly elements-forces to vacate the CBP.

OCCUPY

- Establish a disruption zone with security elements-forces that provides 360-degree coverage.
- Move to designated positions and/or battle positions within the CBP that include disruption, main defense, reserve, support.

- Confirm coordination for battle handover between disruption elements-forces and main defense elements-forces and/or reserve.
- Integrate SBPs, fires plans, targets, and kill zones for defense.
- Emplace obstacles in defense of the CBP to reinforce terrain and canalize, disrupt, block, fix, or otherwise shape the AOR and probable/possible enemy actions.
- Position a reserve element-force for rapid movement-maneuver to support, on order, multiple CBP contingencies.
- Establish caches and sites in or near the CBP with redundant combat support (CS) and combat service support (CSS) capabilities.
- Protect CBP elements-forces with continual improvement of complex terrain, survivability measures, and C3D.
- Coordinate with friendly elements-forces not in the task organization and located outside of the main CBP perimeter that are capable of support assistance in contingencies.
- Confirm redundant command and control (C2) communications.
- Publish what conditions may require withdrawal of the CBP, and who [the commander] is authorized to direct any withdrawal from the CBP.
- Report completion of CBP defenses and support operations.
- Conduct systems warfare actions that focus on critical enemy subsystems.
- Execute INFOWAR in support of the defense.
- Improve CBP defenses with continuous review of C3D measures.

DEFEND

- Locate, track, and target enemy elements-forces approaching the CBP.
- Inform disruption elements-forces with current RISTA information to support CBP purpose.
- Execute INFOWAR technical and psychological capabilities to deceive, deter, and/or dissuade the enemy from entering the CBP area of operations.
- Report accurate tracking of enemy and friendly elements-forces counterreconnaissance success in CBP AOR.
- Arm or otherwise prepare readiness of explosives and other obstacles for execution.
- Conduct timely movement, maneuver, and/or positioning of friendly elements-forces to defend in the CBP battle zone.
- On order, engage designated enemy elements-forces with coordinated defenses to deceive, degrade, disrupt, defeat, and/or destroy the enemy.
- On order, direct the reserve to execute specified tasks in support of the CBP defense.
- Coordinate actions in the CBP support zone to sustain the defense.
- Maintain contact with the enemy by observation and/or technical sensor reconnaissance and surveillance means to sustain situational understanding and current information.
- Report regular, periodic, and/or unexpected information updates in a timely manner to satisfy the commander's critical information requirements and mission intent.
- Recommend if current tactical conditions require an adjustment to the CBP defense.

WITHDRAWAL

- If the OPFOR commander directs retention of the CBP, subordinate elements-forces continue the defense and reorganize combat power to accomplish assigned tasks.

- If the OPFOR commander determines that the CBP is decisively overmatched, the OPFOR commander can direct a withdrawal operation. Actions based on the tactical situation include but are not limited to:
  - Designate *disruption* zone and *main defense* direct and indirect fire elements-forces to remain in contact in order to delay the enemy elements-forces' attack into the CBP.
  - Conduct undetected and sequenced movement by designated CS and CSS elements-forces through withdrawal routes and/or exfiltration routes-lanes in order to disengage from enemy influence and occupy designated sites and/or sanctuary areas in the AOR.
  - Conduct withdrawal of designated *main defense* and *reserve* elements-forces through withdrawal routes and/or exfiltration routes-lanes in order to disengage from enemy influence and occupy designated sites and/or sanctuary areas in the AOR.
  - Update *disruption* elements-forces with current situational understanding to support destruction of enemy critical subsystems, logistics, and C2 in follow-on attack and/or support echelons.
  - On order, friendly elements-forces in contact with the enemy conduct a withdrawal under pressure, break contact, and occupy designated sites and/or sanctuary areas in the AOR.
- Report regular information updates of friendly elements-forces available for mission requirements.
- Execute tasks with stay-behind elements, when required, that can include but are not limited to surveillance, disrupt, defend, delay, suppress, neutralize, defeat, and/or destroy tasks.
- Employ continuous reconnaissance-surveillance at objective(s) to achieve situational understanding and provide early warning of enemy activities that can influence mission tasks. Continue the mission.

Performance Measures of Effectiveness

Assessing and/or evaluating successful conduct of a CBP uses the following performance measures. The measures identify critical OPFOR tactical actions during all phases of a CBP mission.

Table 1. Tactical task: Complex battle position

TACTICAL TASK : COMPLEX BATTLE POSITION		
No.	**Scale**	**Measure**
01	Yes/No	Reconnaissance tasks accomplished.
02	Yes/No	Key operational environment information obtained.
03	Yes/No	Report timely surveillance and intelligence.
04	Yes/No	Security operations provide 360-degree coverage.
05	Percent	Report CBP construction status to completion.
06	Percent	Camouflage, cover, concealment effective.
07	Yes/No	Deception actions effective.
08	Yes/No	Information warfare (INFOWAR) effective.
09	Yes/No	Report enemy incursions into disruption zone.
10	Yes/No	Counterreconnaissance actions effective.
11	Yes/No	CBP defense effective.
12	Yes/No	CBP defended for time specified by leader.
13	Percent	Friendly forces available to continue mission.
14	Percent	Specified systems warfare missions success.
15	Yes/No	Stay-behind elements achieve mission tasks.

Training Implications

A trainer, curriculum developer, and/or unit leader can use this OPFOR training literature on complex battle position to support OPFOR readiness. This baseline of tactical information and guidance can be adjusted to satisfy specific requirements in live training at combat training centers (CTCs); major exercises in constructive and virtual simulations; regional field training with allies and partners; and/or home station training (HST), Army professional education venues, and individual professional development.

Opposing Force

An OPFOR is a plausible, flexible, and free-thinking mixture of regular forces, irregular forces, and/or criminal elements representing a composite of varying capabilities of actual worldwide forces and capabilities (doctrine, tactics, organization, and equipment). The OPFOR is used in lieu of a specific threat force for training and developing US forces, and can be configured to represent a hybrid threat.

AR 350-2, *Operational Environment and Opposing Force Program* (2015)

Figure 3. Opposing force for training readiness

As the ACE Threats Integration directorate continues to refine and update the tasks, conditions, standard, and measures of performance for an OPFOR in US Army learning venues, the TRADOC G-2 is presenting easy on-line access to OPFOR readiness resources such as the TRADOC G-2 Virtual OPFOR Academy (VOA) with instructional vignettes and virtual simulations of OPFOR tactical actions. Other resources include updated OPFOR tasks, conditions, standards, and measures of performance posted to the Army's Combined Arms Strategies (CATS). Future articles in the TRADOC G-2 *Red Diamond* monthly newsletter will describe these and other aids in providing a realistic, robust, and relevant OPFOR to challenge specified and implied mission requirements for US Army readiness.

Notes

[1] Headquarters, Department of the Army. Training Circular 7-100.2, Opposing Force Tactics. TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. 9 December 2011. Para 4-108.

[2] Headquarters, Department of the Army. Training Circular 7-100.2, Opposing Force Tactics. TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. 9 December 2011. Para 4-102.

[3] Headquarters, Department of the Army. Training Circular 7-100.2, Opposing Force Tactics. TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. 9 December 2011. Para 4-107.

[4] Headquarters, Department of the Army. Army Regulation 350-2. Operational Environment and Opposing Force Program. 19 June 2015. Para 2-8a.

[5] Headquarters, Department of the Army. Army Regulation 350-2. Army Regulation 350-2. Operational Environment and Opposing Force Program. 19 June 2015. Para 1-5b.

[6] Headquarters, US Army Training and Doctrine Command. TRADOC Regulation 10-5-1, Organization and Functions. 20 July 2010. Para 8-18c(1)(a).

_____

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* (2012)

Look Back to Stay Ahead:
Tactics, Techniques, and Terrorism

by Jon H. Moilanen, TRADOC G-2 ACE Threats Integration, (IDSI Ctr)

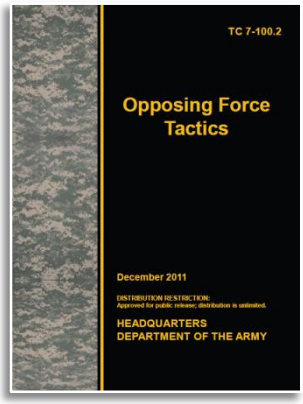
The array of extremist terrorist actors around the globe is broader, wider, and deeper than it has been at any time since 9/11, and the threat landscape is less predictable.[1]

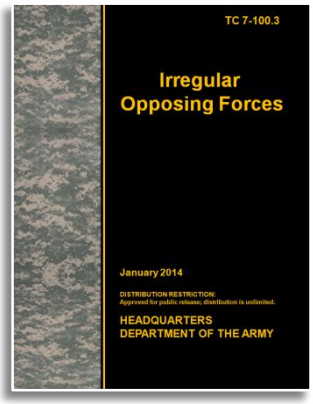
The Honorable Nicholas Rasmussen
Director, National Counterterrorism Center

Define the Problem: *Staying Ahead of the Terrorist Threat*

Two significant trends exist in the current complex threat environment. "First is the increasing ability of terrorist actors to communicate with each other outside our reach. The difficulty in collecting precise intelligence on terrorist intentions and the status of particular terrorist plots is increasing over time."[2] The second issue is "a proliferation of more rapidly evolving threat or plot vectors that emerge simply by an individual encouraged to take action, then quickly gathering the few resources needed and moving into an operational phase."[3] Given expanding US challenges to determine specific threat intentions early in their development through authorized surveillance and other collection means and increased incidents of terrorism by individuals or small groups as "homegrown" or extremist-inspired actors, each member of the Army Family has a direct role in the Army's antiterrorism program.

Terrorism is the "unlawful use of violence or threat of violence, often motivated by religious, political, or other ideological beliefs, to instill fear and coerce governments or societies in pursuit of goals that are usually political."[4] The psychological impact of potential violence can be as damaging as an actual act of violence. Whether terrorism is considered a strategy, operational concept, or tactic, each member of the Army Family has a responsibility to be an active agent in antiterrorism. A program of defensive measures can reduce vulnerability to terrorist acts and assist rapid containment of a terrorism threat by local military and/or civilian forces.[5] Success of this defense is a collective effort to improve detection, protection, and readiness.





Terrorism, as it affects an individual and his or her immediate surroundings, can be readily considered a threat tactic.[6] Having situational awareness and understanding of a threat is a first step in preparing for and acting to prevent an act of terrorism. The Training Circular (TC) 7-100 series for US Army training presents an unclassified overview of operational environment conditions and a composite of real-world threat capabilities and limitations for US Army training, professional education, and leader development. A recurring threat intention, which can include terrorism, is to cause significant psychological and/or physical effects on a relevant population—people—in order to enhance achieving a threat objective.

Know the Threats—Know the Enemy

Threats can be viewed as a spectrum with individuals being inspired through social media and perceived successes publicized in recurring news cycles, or individuals obtaining direct guidance and materiel assistance from irregular forces

and/or organizations such as the self-proclaimed Islamic State of Iraq and the Levant (ISIL).[7] Complex, large-scale plans and operations have decreased in recent years, as the threat adapts to a more distributed concept of operations in small-scale multiple vectors.[8] Attacks can be planned and executed within short time cycles by individuals with varied levels of training, weaponry, and expertise. Incidents of terrorism can range from the rogue action of a lone individual to the sanctioned or sponsored activities of large non-state organizations acting on behalf of or in conjunction with a state.[9]

Look back on acts of terrorism and learn from cogent observations and practical evidence. Identify the motivations that convinced or compelled an individual or group to act with terrorism. "The global jihadist movement continues to increasingly decentralize, both in terms of geography and command and control….This diffusion has led to an increase in threats by networks of like-minded violent extremists with allegiances to multiple groups. This evolution is the result of an adaptive enemy."[10] Whether acts of terrorism are deliberate, apparently random, and/or purposely haphazard, the physical, symbolic, and/or psychological effects can diminish the confidence of a relevant population in its key leaders and governing institutions.[11]

Look back on manifestations of terrorism on the United States homeland and the nation's presence among allies and partners throughout the world. Threat actions, honed from successes and failures of previous missions, are typically organized for violent application to a specific environment, target, and purpose. The threat "how-to" is a composite of refining tactics and techniques to action, compelled by motivations such as unresolved grievances, an extremist ideology or philosophy, or a disgruntled sense for revenge.

Look back on organizations such as al-Qaeda, its loose affiliates, and ISIL that garner sudden attention with sensational incidents on occasion and effective social media savvy. The Army Family member must also appreciate threats just as dangerous in a sole individual. Post-incident analyses of terrorism often demonstrate indicators or warnings that might have been identified and brought to the attention of organizational leaders, law enforcement officers, or other persons able to investigate concerns and preclude an act of terrorism. How do we as an Army Family stay ahead of the terrorist by using disciplined actions to prevent terrorism?

***Stay Ahead*—If You See Something, Say Something**

When you see something you know shouldn't be there, appears suspicious or out-of-place to normal activities, or someone's behavior seems abnormal and potentially hazardous—say something! You know what is normal in your everyday life and what just doesn't look right.

The US Department of Homeland Security (DHS) is committed to strengthening hometown security by creating partnerships with state, local, tribal, and territorial governments and the private sector, as well as with the communities they serve.[12] Informed and alert individuals in communities are the critical link in situational awareness of threats, timely reporting, and playing a responsible role in protecting our nation.

"If You See Something, Say Something™" is a US national campaign that raises public awareness of the indicators of terrorism and terrorism-related crime, as well as the importance of reporting suspicious activity to state and local law enforcement. This campaign engages every responsible citizen and member of the public in protecting themselves through situational awareness and, more importantly, a sense and commitment to report suspicious activity.

The Director of the National Counterterrorism Center notes that "in terms of propaganda and recruitment, they [ISIL] can generate further support for their movement, without carrying out catastrophic, mass-casualty attacks. And that's an innovation in the terrorist playbook that poses a great challenge."[13] Terrorist organizations understand that by motivating actors in their own locations to take action against Western countries and targets, these individuals or groups can be very effective. For example, "the Boston Marathon bombing underscores the threat from HVEs [homegrown violent extremists] who are motivated, often with little or no warning, to act violently by themselves or in small groups…These lone actors or insular groups who act autonomously are the most difficult to detect or disrupt."[14] Whether the ultimate aims of an irregular force are ideological, philosophical, and/or practical, terrorism will continue to be a vexing factor in future conflicts among and between state and non-state actors throughout the world.[15]

Are You Vigilant?—Do You iWATCH?

Due to the importance of identifying suspicious activity and the proper way to report it, the Department of the Army's Office of the Provost Marshal General developed and instituted an Army-wide antiterrorism awareness program called "iWATCH." Units, organizations, and activities promote the iWATCH program in the context of their localized and regional perspectives, and provide information and ideas to improve situational awareness of potential threats.[16]

An Army antiterrorism officer (ATO) notes a distinct role for everyone in the iWATCH program and that their active participation can prevent acts of terrorism activity and/or other criminal activity. "Everyone plays a key role in force protection...Even a minute detail being reported can stop an incident from happening."[17] The iWATCH program is a way to be more sensitive to indicators of possible terrorist activity and encourages timely reporting of suspicious behavior to military or civilian law-enforcement agencies. In addition, it creates a partnership between on-post and off-installation or activity organizations. Another ATO spotlights that "the program focuses on protecting our communities from terrorist attacks by spreading the word about being vigilant and responding immediately to any unusual behavior we witness in our local communities."[18]

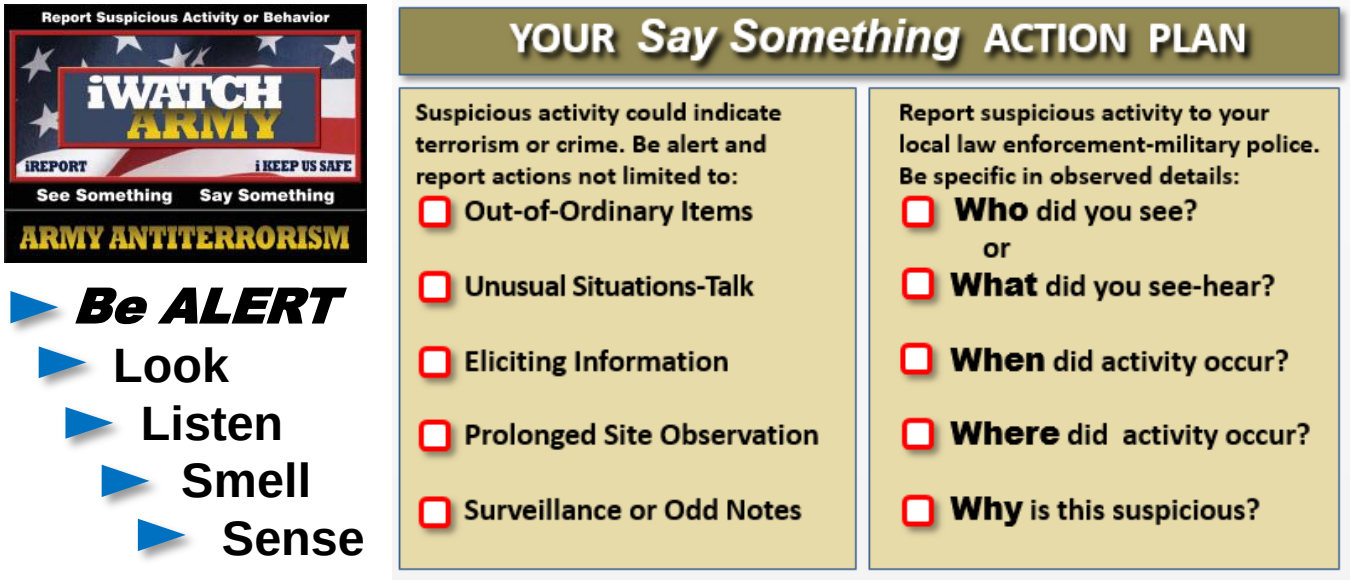


Figure 2. An action plan for protecting the Army Family

Your Personal Responsibility—*Be Ready*

iWATCH empowers the Army Family—soldiers, Army leaders, Department of the Army civilians, contractors, Army retirees, and family members—to be ***proactive*** in protecting where they live, work, and relax. Be vigilant. Be ready.

Find more AT resources on the Army Antiterrorism Enterprise Portal (ATEP) with common access card (CAC) entry.

Notes

[1] Rasmussen, Nicholas. "Hearing before the House Homeland Security Committee: Worldwide Threats and Homeland Security Challenges." US House of Representatives Homeland Security Committee. 21 October 2015.

[2] Rasmussen, Nicholas. "Hearing before the Senate Homeland Security and Governmental Affairs Committee: Threats to the Homeland." US Senate Homeland Security and Governmental Affairs Committee. 8 October 2015.

[3] Rasmussen, Nicholas. "Hearing before the Senate Homeland Security and Governmental Affairs Committee: Threats to the Homeland." US Senate Homeland Security and Governmental Affairs Committee. 8 October 2015.

[4] US Department of Defense. Joint Publication 1-02, DOD Dictionary of Military and Associated Terms: Terrorism. 8 November 2010, as amended through 15 October 2015.

[5] US Department of Defense. Joint Publication 1-02, DOD Dictionary of Military and Associated Terms: Antiterrorism. 8 November 2010, as amended through 15 October 2015; A complement of antiterrorism is counterterrorism, which the Department of Defense defines as "activities and

operations taken to neutralize terrorists and their organizations and networks in order to render them incapable of using violence to instill fear and coerce governments or societies to achieve their goals."

[6] Headquarters, Department of the Army. Training Circular 7-100.3, Irregular Opposing Forces. TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. 17 January 2014. Chapter 6, para. 1.

[7] Rasmussen, Nicholas. "Hearing before the House Homeland Security Committee: Worldwide Threats and Homeland Security Challenges." US House of Representatives Homeland Security Committee. 21 October 2015.

[8] Rasmussen, Nicholas. "Hearing before the House Homeland Security Committee: Worldwide Threats and Homeland Security Challenges." US House of Representatives Homeland Security Committee. 21 October 2015.

[9] Headquarters, Department of the Army. Training Circular 7-100.3, Irregular Opposing Forces. TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. 17 January 2014. Chapter 6.

[10] Rasmussen, Nicholas. "Hearing before the Senate Committee on Homeland Security and Governmental Affairs: Cyber Security, Terrorism, and Beyond: Addressing Evolving Threats to the Homeland." US Senate Homeland Security and Governmental Affairs Committee. 10 September 2014.

[11] Headquarters, Department of the Army. Training Circular 7-100.3, Irregular Opposing Forces. TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. 17 January 2014. Chapter 6, para. 1.

[12] US Department of Homeland Security. "If You See Something, Say Something: It Takes a Community to Protect a Community." Retrieved 1 December 2015.

[13] Rasmussen, Nicholas. "Hearing before the Senate Homeland Security and Governmental Affairs Committee: Threats to the Homeland." US Senate Homeland Security and Governmental Affairs Committee. 8 October 2015.

[14] Rasmussen, Nicholas. "Hearing before the Senate Committee on Homeland Security and Governmental Affairs: Cyber Security, Terrorism, and Beyond: Addressing Evolving Threats to the Homeland." US Senate Homeland Security and Governmental Affairs Committee. 10 September 2014.

[15] Headquarters, Department of the Army. Training Circular 7-100.3, Irregular Opposing Forces. TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. 17 January 2014. Chapter 6, para. 146.

[16] US Army Military District of Washington. "iWATCH." Retrieved 29 November 2015.

[17] US Army Installation Management Command Public Affairs. "iWatch promotes community awareness." Army.Mil. 20 July 2010.

[18] Talley, Aaron. "Army antiterrorism program asks all to iWATCH." Army.Mil. 20 February 2015.

by Rick Burns, TRADOC G-2 ACE Threats Integration (BMA CTR)

The forthcoming update to the Threat Tactics Report: Islamic State of Iraq and the Levant (TTR: ISIL) contains updated information on a number of developing areas. The fall of Ramadi in May 2015 represented a significant victory for ISIL. Utilizing offensive tactics consistent with hybrid threat integrated attack doctrine outlined in TC 7-100.2, Opposing Force Tactics, ISIL was able to occupy the strategic city of Ramadi.[1] The update contains a case study describing how ISIL captured the city. The TTR update also includes a discussion of Sinjar tunnel networks as a means of protection against air strikes and for command and control; use of chemical weapons against Kurdish fighters; and details about ISIL financing.

An area of particular interest to readers is ISIL's international expansion. While ISIL's momentum in Iraq and Syria has been stalled, its direct and indirect influence internationally has contributed to its ongoing narrative of a worldwide caliphate. ISIL has benefited significantly from early successes in Iraq and Syria. These successes have inspired a variety of international relationships ranging from tacit acceptance to active pledges of allegiance and active recruitment of international fighters. All of these relationships, projected along a continuum of support, add to the narrative that ISIL is successfully creating a worldwide caliphate. Leaders in countries where these organizations exist must now consider two additional contributors to their internal instability: first, increased violence and disruption from traditional terrorist organizations inspired by ISIL's success and, second, seasoned fighters returning from Iraq and Syria with new-found skills. The update provides a sampling of how ISIL is affecting countries outside its base operations in Iraq and Syria.[2]

Figure 1. ISIL fighter

Below are examples of some of the countries discussed in the update.

Philippines

In August 2014, two hardline Filipino Muslim groups, Bangsamoro Islamic Freedom Fighters (BIFF) and Abu Sayaf rebels, allied themselves with ISIL. BIFF spokesman Abu Misry Mama verified to an Agence France-Presse reporter that BIFF has an alliance with ISIL. The BIFF spokesman stated that the group had no plans to impose ISIL's radical form of Islam, referring to ISIL's beheadings, mass executions, taking child brides, etc. Mama also stated BIFF had not sent any fighters to support ISIL's operations in Iraq and Syria and the organization was not recruiting for ISIL. Another video, alleging support for ISIL by Abu Sayaf senior leader Isnilo Hapilon, has also been posted. Philippine military spokesman LTC Ramon Zagala stated the videos were only propaganda.[3] Armed Forces of the Philippines chief of staff GEN Gregorio Pio Catapang Jr. maintained earlier this year that there is no intelligence that indicates an ISIL presence in the Philippines and that BIFF, Abu Sayaf, and privately armed groups are not supported by ISIL.[4]

France

Following an al Qaeda-inspired attack on the satirical magazine Charlie Hebdo in January 2015, eight ISIL-affiliated terrorists conducted coordinated attacks on civilians at outdoor restaurants, a concert hall, and a soccer stadium on Friday, 13 November 2015, with evidence that other targets had been planned. The attackers killed 132 people and injured hundreds more using rifles and bombs. At least nine participants died from suicide-bomb detonations or direct contact with French security forces and two are still believed at large. The attackers included Belgian, French, and Syrian citizens, suggesting home-grown radicalization and cross-border travel for trainers and planners.[5]

Nigeria

In March 2015, Boko Haram's leader Abubakar Shekau posted an audio message to the group's Twitter account pledging allegiance to ISIL.[6] ISIL spokesman Abu Mohammad al Adnani validated the acceptance of the pledge and described it as an expansion of the caliphate to West Africa.[7] Influence from ISIL can be seen in an improved and increasing Boko Haram social media presence. The newly-formed relationship with ISIL will open up new opportunities for acquisition of and training on new weapon systems and improved tactics in response to an intensified Nigerian military counterinsurgency. Improvement in the use of air defense weapons will be particularly challenging for the Nigerian air force's current air superiority. For a more detailed treatment of ISIL's relationship with and operations in Nigeria, see Threat Tactics Report: Boko Haram.

Figure 2: ISIL militants

Saudi Arabia

Due to Saudi Arabia's geographic possession of Islam's holiest sites, ISIL sees it as a significant target. According to the Soufan Group, the second-largest number of foreign fighters and the most suicide bombers within the ISIL organization come from Saudi Arabia.[8] It is likely that ISIL has placed sleeper cells within the country, waiting for opportunities to attack even as the group is continually frustrated by the Saudi government's conscious and effective crackdown on insurgent activities.[9]

In November 2014, ISIL declared wilayats [provinces] in Saudi Arabia and began conducting attacks. ISIL attacks included an unsuccessful plot to bomb the American embassy in Riyadh, drive-by shootings at police and security personnel, attacks on Shia mosques, and suicide bombings.[10] Wilayat Najd claimed responsibility for an attack on 22 May 2015 that killed 21 Shia Muslim worshippers and wounded 80 other worshippers inside a mosque in al Qadeeh village. A month later, Wilayat Najd followed up this assault with a suicide attack against the Kuwaiti Shia Muslim mosque of Imam Sadiq. The attack killed 27 people and wounded 227 more.[11]

Implications for Training

Training should focus on tactics outlined in the hybrid threat doctrine described in the TC 7-100 series. These publications describe hybrid threats and summarize the manner in which such threats may operationally organize to fight US forces.

They also explain the strategy, operations, tactics, and organization of the hybrid threat that represents a composite of actual threat forces as an opposing force (OPFOR) for training exercises.

Notes

[1] Headquarters, Department of the Army. Training Circular 7-100.2, Opposing Force Tactics. TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. 9 December 2011.

[2] See Thomas Lynch's "The Islamic State as Icarus: A Critical Assessment of an Untenable Threat," published by the Wilson Center in 2015, for a chart detailing ISIL-affiliated organizations by region and level of support.

[3] Agence France-Presse. "Philippine Militants Pledge Allegiance to ISIS Jihadists." Rappler. 15 August 2014.

[4] GMA News Online. "AFP: No ISIS Militants in the Philippines." 27 April 2015.

[5] Thomas Sanderson. "The Paris Attacks." Center for Strategic and International Studies. 16 November 2015; BBC News. "Paris Attacks: Who Were the Attackers?" 24 November 2015.

[6] BBC News. "Nigeria's Boko Haram Pledges Allegiance to Islamic State." 7 March 2015; Adam Chandler. "The Islamic State of Boko Haram?" The Atlantic. 9 March 2015.

[7] Agence France-Presse. "IS Welcomes Boko Haram Allegiance: Tape." Yahoo! News. 12 March 2015.

[8] The Soufan Group. "The Islamic State's Looming Fight with Saudi Arabia." 6 January 2015.

[9] Harleen Gambhir. "The ISIS Regional Strategy for Yemen and Saudi Arabia." The Institute for the Study of War. 22 March 2015.

[10] Harleen Gambhir. "The ISIS Regional Strategy for Yemen and Saudi Arabia." The Institute for the Study of War. 22 March 2015; Nolwenn Bourillon-Bervas. "OSINT Summary: Islamic State Suicide Attack Kills at Least 15 People in Saudi Arabia's Asir." IHS Jane's 360. 6 August 2015.

[11] Karen Yourish, Derek Watkins, and Tom Giratikanon. "Recent Attacks Demonstrate Islamic State's Ability to Both Inspire and Coordinate Terror." The New York Times. 7 December 2015.

by Laura Deatrick, TRADOC G-2 ACE Threats Integration (CGI Ctr)

The ACE Threats Integration (ACE-TI) Directorate of TRADOC G-2 recently hosted a *Decisive Action Training Environment* (DATE 3.0) Working Group meeting on 8–11 December 2015 at Ft. Leavenworth, KS. Due to DATE's widespread and increasing use both nationally and internationally, ACE-TI has been coordinating the active involvement of current and future DATE users in this update process. Ninety-six persons from six countries attended at least part of the meeting, including representatives from the United States, Australia, Canada, the Netherlands, New Zealand, and the United Kingdom. The meeting consisted of two general sessions and separate gatherings for each of the subgroups, namely Timeline, Irregular Warfare, Maritime, Order of Battle, and Terrain. A considerable amount of work was accomplished and will be used to modify DATE regardless of what form it takes in the near future.

General Sessions

Jon Cleaves, ACE-TI Director, spoke on the history of DATE and the vision for version 3.0 at that time. He reviewed the reasons for the creation of DATE and the benefits of a common operational environment for training, the role of ACE-TI in the development of DATE-based scenarios, and the use of Regionally-Aligned Force Training Environments (RAFTEs). Mr. Cleaves then discussed the issue of maritime access to the DATE region and the need for a DATE-based exercise database. He also announced the planned reversion of DATE country borders in version 3.0 to the international borders found in version 2.1.

Figure 1. *Decisive Action Training Environment* general session December 2015

Laura Deatrick reviewed the overall mission of each subgroup and led a discussion on which combatant commands (COCOMs) should have DATE countries in their area of responsibility (AOR). The general consensus of the working group was to not specify a COCOM in DATE; rather, the exercise designer would designate COCOMs and their respective AORs to meet training needs. Mrs. Deatrick also announced that Angela McClain-Wilkins would be taking over her duties as primary lead on DATE.

Timeline Subgroup

The Timeline Subgroup completed 14 tasks and determined a way ahead for the one remaining. The dates of several key events were determined, such as the founding and election cycle of each country and the timing of certain regional armed conflicts. Several inconsistencies involving dates and related events were also resolved. The subgroup recommended that references to real names of regional countries outside the five DATE operational environments, such as Iraq, be removed.

It was determined that ACE-TI would review the DATE timeline and bring any additional concerns to the attention of the subgroup, write guidance on use of sliding dates, and investigate adding a timeline graphic to DATE.

Irregular Warfare Subgroup

The Irregular Warfare Subgroup spent the majority of its time in filling out a large matrix containing 30 irregular threat groups with 14 required data fields each, such as size and ideology. Information was completed for all actors except for three Gorgas insurgent groups that were not being used by the majority of participants. Two insurgent groups were deleted, as they contained "real world" Kurdish and Baluchi insurgent organizations and there were already several other fictional insurgency groups that could cover the areas affected.

Additional threat actors discussed or added to this matrix were the South Atropia True Believers, mercenaries, tribes and militias, and the Atropia State of Islam, the last being created during the working group. Input was provided for the Atropia State of Islam by two combat training centers (CTCs), and creation of the South Atropia True Believers is pending input from a third CTC. The subgroup discussed the presence of tribes and militias for special operations forces training and determined that the militia brigades in the current force structure could be easily adapted as required. The potential need for different categories of mercenaries and methods of creating them were also discussed. Human trafficking was eliminated from the list of threat group activities due to US federal laws dealing with this issue. Each threat group's area of operation was plotted on a digital map and subsequently saved to MS PowerPoint files for easy reference. After completing the matrix it was then handed over to the Order of Battle Subgroup as an aid for determining Irregular Forces' orders of battle.

Order of Battle (OB) Subgroup

The subgroup identified many new military structures for recommended inclusion in DATE 3.0. ACE-TI proposed creating more modular units to mix and match on an as-needed basis, which would have the added benefit of simplifying the creation of new structures. Among the new suggested structures were irregular forces, many of which were sufficiently covered by ACE-TI's modular unit proposal. One irregular organization—the newly-created Atropia State of Islam—will be built from scratch by ACE-TI and the Mission Command Training Program's (MCTP's) Operations Group X-Ray. The Intelligence Center of Excellence provided structures for criminal organizations that, once approved by ACE-TI, will be put into the DATE OB and formatted for the Army Training Network.

MCTP advocated the need for customized support in certain areas, such as transportation units and engineer assets. These structures will eventually add more realism to the threat force structure and will provide a place marker for necessary capabilities to enable support to specialized units throughout DATE.

The naval structure was determined to be sufficient for current DATE usage. It is expected that new interests will be generated in the naval OB if changes are made to the environment. MCTP exercise 16-4 will have joint participation and it is expected that this will also provide feedback and possible development for the naval OB.

Maritime Subgroup

The aim of the Maritime working group was to establish if there was a requirement to adjust the DATE environment to better facilitate joint training, specifically the employment of maritime assets. The group was also to establish a course of action (COA) to meet any requirements and to subsequently propose it to the Chain of Command.

The group collected and analyzed joint requirements from across the US training continuum and Coalition partners. It was agreed that DATE does not need to facilitate naval blue-water training, but should develop the littoral environment to create realistic conditions to train aspects of joint operations such as joint forced entry, joint targeting, amphibious operations, and logistics. To develop the littoral it was agreed to propose that the Caspian Sea be fictionally enlarged two- to three-fold, but access to blue water be limited by a channel and a concern over piracy. In addition, the group proposed that the real-world Montreux Convention that limits access through the Dardanelles and the Bosporus to the Black Sea be removed by DATE to create better access to the Black Sea, thus enabling the same aspects of joint operations to be trained on DATE's western coast.

It was proposed that a chain of three islands be created in the newly-enlarged Caspian Sea on which and from which operations can be conducted and mounted. The three islands would be modelled on the Hawaiian Islands and be placed approximately 100 miles from the coast.

The task of creating the fictional terrain necessary to exercise the improved littoral environment was discussed by the Terrain Subgroup and forms part of a larger terrain-based action item (see below).

Terrain Subgroup

The Terrain Subgroup decided that international and provincial borders would mirror those of the real world as much as possible. Exceptions include Atropian borders, which would mirror those used by the live-training CTCs, as applicable, with MCTP assisting ACE-TI in determining the remaining borders. Donovian provinces would remain unchanged and would be mapped as closely as possible to those shown in DATE 2.2. The subgroup determined that terrain and infrastructure for the Hachzi Peninsula and the Caspian Sea "bump-out" should mirror that of the southwest United States (bordering the National Training Center—NTC) with appropriate elevation adjustments.

The subgroup discussed the Maritime Subgroup's proposal regarding the Caspian Sea, which was met with general approval. It also concluded that non-DATE countries in the region should go unnamed. The subgroup recommended that terrain and infrastructure data be developed at the UNCLASSIFIED, Unlimited Distribution level, and that it be developed for all five DATE countries in their entirety.

Of note, the National Simulation Center (NSC) has tasked SE Core with creating constructive terrain for DATE for distribution across the DATE user group. Both NSC and SE Core representatives attended the subgroup meeting. SE Core observed that, if so tasked by NSC, it could incorporate many of these decisions into its current work with minimal impact.

Summary

Each subgroup addressed tasks that had been distributed to members beforehand, which were either completed or had a way-ahead determined. Significant actions included the refinement of current irregular threat actors and the creation of two new groups by the Irregular Warfare Subgroup; agreement on DATE threat force group OBs or a path of action for their creation by the Order of Battle Subgroup; the determination of several key events by the Timeline Subgroup; consensus on a proposal regarding naval access to the Caspian and Black Seas by the Maritime Subgroup; and agreement on a method of defining borders and creating fictitious terrain for DATE countries by the Terrain Subgroup.

Figure 2. Subgroup breakout sessions

Several proposals were made by the subgroups. The Order of Battle Subgroup proposed that more modular OB structures be created to allow more flexibility and ease in creating OBs for new entities. The Maritime Subgroup proposed that the Caspian Sea be increased two- to three-fold; that three islands be added to it; that a channel allowing naval access to it be created; that piracy be added to limit freedom of movement; and that unfettered access to the Black Sea be created through the lifting of the Montreux Convention in the DATE world. The Terrain Subgroup strongly encouraged terrain and infrastructure data to be developed at the UNCLASSIFIED, Unlimited Distribution level, for ease of sharing with allies.

The following major action items were determined: the finalization of new threat groups and their orders of battle; the definition of relevant international and provincial borders of the DATE countries by ACE-TI and the CTCs; and adoption of the Maritime Subgroup's proposal regarding access to the Caspian and Black Seas.

For questions or to submit comments or suggestions for improvements to DATE, please contact Angela McClain-Wilkins at 913-684-7929 or angela.m.mcclain-wilkins.civ@mail.mil.

Use US Army TC 7-100 Series for Threats and OPFOR: Training for Readiness

TRADOC G-2 *Worldwide Equipment Guide*: MTK-2 Mineclearing System Meteorit

Figure 1. MTK-2

by Jerry England, TRADOC G-2 ACE Threats Integration (DAC)

The MTK-2 Meteorit is a Russian mineclearing system that entered service in the early 1980s and was used in operations in Syria. The MTK-2 has two UR-77 rockets mounted on an adjustable turret. The main feature of the UR-77 is its ability to deploy a large mineclearing line charge that is stored inside the vehicle. Such a capability can greatly support a maneuver force's ability to breach a particular area of the battlefield by explosively breaching obstacles and enabling freedom of movement to follow-on forces.

Based on recent online videos, as well as historical reporting from the Russo-Chechnyan war, the Meteorit can also clear mobility corridors in urban area, as was the case in the Damascus suburb of Jobar in 2014.[1] The Meteorit appears to have been designed as a brigade-level asset and was considered an important weapon during the battle for Komsomolskoye in Chechnya in 2000.[2] In that battle, mass use of the MTK-2 assisted the Russian maneuver brigade in seizing the town by launching the one-ton line charges into fortified enemy fighting positions. The explosion and subsequent blast wave destroyed not only personnel and weapons, but also booby traps used by defending forces.

System Capabilities and Characteristics

The MTK-2 is operated by a two-man crew and can be maneuvered into position just beyond the serviceable target. The Meteorit has an erectable superstructure that houses the two UR-77 rockets. Each rocket can range up to 500 meters and can pull a one-ton, 93 meter-long mine clearance line charge. Each line charge contains approximately eight kilograms of plastic explosives per meter and will produces a 100 meter by 7 meter blast radius. Once in position, the time to deployment averages four minutes.[3] The MTK-2 clears lanes in minefields by using rocket-propelled charges. The charges are launched onto the minefield and then detonated using an electronic initiation device by the vehicle commander-operator from within the vehicle. The charge can be fired on land or in the water. The MTK-2 can operate in chemical, biological, radiological, and nuclear environments. The Meteorit is approximately 8.43 meters long, 3.1 meters high, and 2.8 meters wide. It is mounted on a standard 2S1 Gvozdika 122-mm stable gun chassis. The Meteorit has a maximum road speed of 60 kilometers per hour, a cruising range of 500 kilometers, and it can move in up to 4.5 meters of water.[4]

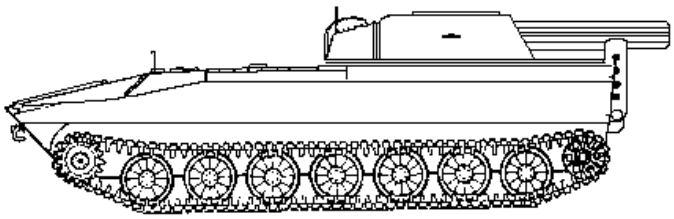
Employment

The MTK-2 was first reported in Syria via social media.[5] The MTK-2 is effective as a breaching system against minefields and other obstacles. Since the war in Chechnya, the MTK-2 has also been used in a direct-fire mode as Russian soldiers employed it against fortified fighting positions suspected of being mined with improvised explosive devices. The use of a system with such a wide explosive radius is intended to provide freedom of maneuver for troops and other assault weapons such as tanks. The UR-77 line charges are said to be able to destroy streets and surrounding structures. This ability to clear obstacles using the UR-77 line charges saves time on an assault and provides relief to sapper squads that are the lead or primary assault elements on fixed enemy positions.[6]

System Proliferation

The Meteorit was a standard engineer platform for Russia forces and former Commonwealth of Independent States (CIS) countries. The recent shipment of this platform to Syria indicates the reliance on Russian technology by the Assad regime for a range of combat systems. An older version based on the BTR-50 chassis was developed with a similar mission set; these systems were reportedly used in conflicts in Africa and the Middle East.

RUSSIAN TRACKED MINECLEARING VEHICLE MTK-2



SYSTEM	SPECIFICATIONS	FEATURES (CONT.)	SPECIFICATIONS
System		Max Swim:	INA
Alternative Designations:	UR-77 mineclearing vehicle, M1979	Fording Depths (m):	4.5
Date Of Introduction:	1981	Radios, Frequency, and Range:	INA
Proliferation:	Former Soviet Union and former Warsaw Pact armies	Vertical Step (m):	INA
Description:		**Mineclearing Equipment**	
Crew:	2	Type:	Explosive line
Troop Capacity:	Information not available (INA)	Charges Used:	UZP-77, UZ-67
Chassis:	Based on the 2S1	Length of Charge (m):	93
Combat Weight (Mt):	15.5	Length of Charge Feed (m):	See Notes
Length Overall (m):	8.4	Size of Lane in AT Minefield (m):	See Notes
Height Overall (m):	3.1	Breaching Time (min):	3 to 5
Width Overall (m)	2.8	Variants	INA
Ground Pressure (kg/cm2):	INA	**Notes**	The MTK-2 clears lanes in minefields by using rocket-propelled charges. The charges are launched onto the minefield and then detonated by the vehicle commander-operator from within the vehicle. The charge can be fired on land or in the water.
Automotive Performance			
Engine Type:	INA		
HP:	INA		
Cruising Range (km):	500		
Speed (km/h):			
Max Road:	60		
Max Off-Road:	30		

Training Implications

The MTK-2 and similar systems have the ability to neutralize enemy obstacles and can be used as direct-fire weapons against fortified fighting positions. The large explosive charge in these systems means that many traditional defenses can be defeated as long as the MTK gets within range to deploy its payload. When used as an enabling element for an offensive operation, the hybrid threat can employ the MTK-2 to assist an assault force in breaching enemy defenses rapidly. Countermeasures may include extending the depth of obstacle belts so as to prevent the MTK from penetrating all the way into the enemy's position. Early warning and incept of an MTK-2 before it is able to release its payload is a preferred method for neutralizing the capability of this platform.

Threat Doctrine Manifestations

Engineers are an element of the hybrid threat's engineering activities. Per Training Circular (TC) 7-100.2, *Opposing Force Tactics*, "The primary engineer missions performed in combat are reconnaissance, mobility, countermobility, and survivability."[7] This capability is available in the engineer battalion of the Hybrid Threat Force Structure on the Army Training Network.

Notes

[1] Aks alser. "Assad Army uses Russian U-77 to bomb Damascus—Jobar." YouTube. 10 October 2014.

[2] Ian Roberts. "Misc Drawings/FD Scale Vehicles/Land Vehicles—Real-life/Organizational Charts/Russia—Engineer Battalion of the Mechanized Infantry Brigade 2008." 2008; Alexander Pashin. "Armed Conflicts: Russian Army Operations and Weaponry During Second Military Campaign in Chechnya." Moscow Defense Brief. June 2015.

[3] IHS Jane's. "Jane's Mines And Mine Clearance 1997-98, Mineclearing Equipment, Russian Federation And Associated States (CIS)." 1997.

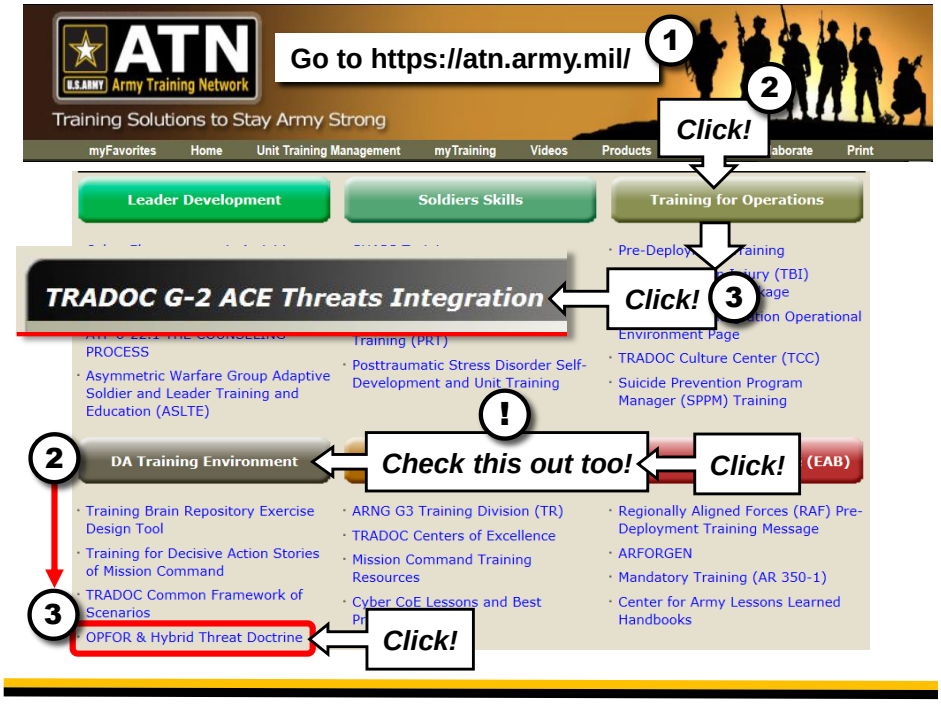
[4] US Army, TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. Worldwide Equipment Guide – Volume 1: Ground Systems. August 2014. Pg 8-38.

[5] Majd Arar. "The Russian mine-clearing UR-77 on #Damascus southern highway leaving Mazeh Mil. Airport & heading to Jobar." Twitter. 10 October 2014.

[6] Headquarters, Department of the Army. Training Circular 7-100.2, Opposing Force Tactics. TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. 9 December 2011. Pg 15-9.

[7] Headquarters, Department of the Army. Training Circular 7-100.2, Opposing Force Tactics. TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. 9 December 2011. Pg 12-1.

Find the Threats and Opposing Force Products on ATN



What ACE Threats Integration Supports for YOUR Readiness

- 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-learning model in TC 7-101/7-102.
- 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 Course resident at 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/USAR/ARNG.
- Respond to requests for information (RFIs) on threat and OE issues.

ACE Threats Integration POCs

DIR, ACE Threats Integration	jon.s.cleaves.civ@mail.mil	Jon Cleaves 913.684.7975
Dep Director DSN:552	jennifer.v.dunn.civ@mail.mil	DAC Jennifer Dunn 684.7962
Military Analyst/Operations	jon.h.moilanen.ctr@mail.mil	Dr. Jon Moilanen IDSI 684.7928
Intelligence Specialist	jerry.j.england.civ@mail.mil	DAC Jerry England 684.7934
Senior Threats Officer	james.d.hunt50.mil@mail.mil	MAJ Jay Hunt 684.7960
Intel Specialist-NTC LNO	kristin.d.lechowicz.civ@mail.mil	DAC Kris Lechowicz 684.7922
(UK) LNO	matthew.j.tucker28.fm@mail.mil	Warrant Officer Matt Tucker 684-7994
Intelligence Specialist-DATE	angela.m.mcclain-wilkins.civ@mail.mil	DAC Angela Wilkins 684.7929
Intelligence Specialist	walter.l.williams112.civ@mail.mil	DAC Walt Williams 684.7923
Threat Tactics	nickolas.m.zappone.mil@mail.mil	CPT Nikolas Zappone 684.7939
Military Analyst	james.r.bird.ctr@mail.mil	Dr. Jim Bird IDSI 684.5963
Military Analyst	richard.b.burns4.ctr@mail.mil	Rick Burns BMA 684.7897
Military Analyst & WEG	john.m.cantin.ctr@mail.mil	John Cantin BMA 684.7952
Military Analyst-Editing	laura.m.deatrick.ctr@mail.mil	Laura Deatrick CGI 684.7925
Mil Analyst-MCTP LNO	patrick.m.madden16.ctr@mail.mil	BMA Pat Madden 684.7997
Military Analyst	henry.d.pendleton.ctr@mail.mil	H. David Pendleton CGI 684.7946
Mil Analyst-JMRC LNO	michael.g.spight.ctr@mail.mil	Mike Spight CGI 684.7974
Mil Analyst-JRTC LNO Threat Tec	james.m.williams257.ctr@mail.mil	Marc Williams 684-7943
Military Analyst (Vacant)		CTR (TBD)
Intel Specialist-Analyst (Vacant)		DAC (TBD)