Operational Environment Enterprise
US TRADOC G2 Intelligence Support Activity

Red Diamond

Complex Operational Environment
and Threat Integration Directorate

Fort Leavenworth, KS | Volume 5, Issue 11 | NOV 2014

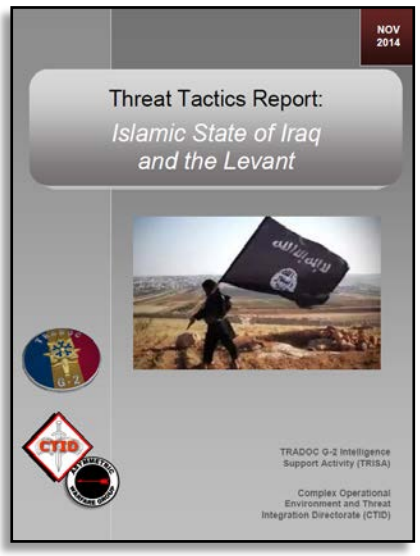
INSIDE THIS ISSUE

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 and
Product Integration
BMA Contractor

TTR: ISLAMIC STATE OF IRAQ AND THE LEVANT

by Complex Operational Environment and Threat Integration Directorate (TRISA-CTID)



The Islamic State of Iraq and the Levant (ISIL) in Syria and northern Iraq and its successes to date are due largely to effective recruitment, intra-insurgent conflict, large cash reserves, and ineffective opponents. This TRISA-CTID *Threat Tactics Report* (TTR) identifies key aspects of tactics and techniques used by ISIL in the region, and unlike its predecessors and competitors, is a paramilitary insurgency. While baseline techniques used by ISIL do not differ significantly from those employed since its early days as an al-Qaeda affiliate in Iraq, its capabilities have increased in scope and complexity. The ready availability of recruits and foreigners attracted to ISIL successes, use of information warfare (INFOWAR), a campaign of terrorism, and large amounts of money for payroll and purchasing war materiel are critical considerations to how ISIL is fighting in land operations. ISIL has demonstrated the ability to execute military tactics that require a level of competence and control uncommon in recent experience.

ISIL is an evolution of an insurgent group that has changed its name to reflect an extremist ideology and expanded geographic vision for power and influence. ISIL executes military tactics to the best of its capability and although ISIL demonstrates a capability greater than that shown by previous insurgencies in the region, ISIL is still not a best practice in a number of warfighting functions and key tactical tasks.

See Army Training Network (ATN) and the "Training for Operations" button. Go to "CTID Operational Environment Page" and find "Threat Tactics Reports."

RED DIAMOND TOPICS OF INTEREST

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

This month's cover page spotlights a new product out of TRISA-CTID, a *Threat Tactics Report (TTR)*. The first TTR covers ISIL and represents a collaborative effort with the Asymmetric Warfare Group (AWG). TRISA CTID will develop future TTRs to be published on the Army Training Network (ATN) throughout 2015.

Several articles in this issue describe different types of threat actor capabilities and tactics to be represented in US Army training: threat commando brigade, threat information warfare (INFOWAR) with analysis of a rogue state actor, and actions of non-state actors in complex operational environments such as HAMAS.

CTID observations from a recent Warfighter Exercise (14-5B) provide insights on how the OPFOR created a challenging and uncompromising enemy in defensive and offensive actions.

Threat models for use in Army training, professional education, and leader learning are in development at CTID and in conjunction with the Military Intelligence School. Assault is one of many threat tasks being refined for instruction and practical exercise in resident and mobile training team (MTT) training courses.

Email your topic recommendations to:

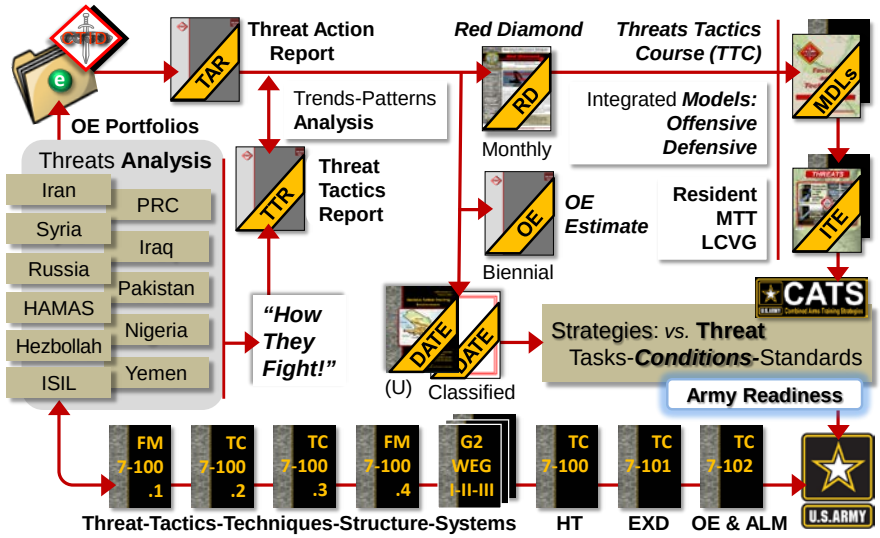
Dr. Jon H. Moilanen, CTID Operations, BMA CTR
jon.h.moilanen.ctr@mail.mil
and
Angela M. Wilkins, Chief Editor and Product Integration, BMA CTR
angela.m.wilkins7.ctr@mail.mil

Director's Corner:
Thoughts for Training Readiness

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

Situational awareness and understanding of the threat, as an opposing force (OPFOR), is essential to training tasks to US Army standards. Leaders prioritize tasks in training from a unit mission essential task list (METL) or designated mission tasks from a higher headquarters, and aim to achieve standards as published by the Army. ***Conditions*** are a statement of the learning environment in which tasks are experienced within a training framework of task/action-condition-standard (AR 350-1). Threats integration is critical to the Army's training, professional education, and leader development learning environments. An opposing force (OPFOR) is a plausible, flexible military and/or paramilitary force representing a composite of varying capabilities of actual worldwide forces (doctrine, tactics, organization, and equipment) used in lieu of a specific threat force for training and developing US forces (AR 350-2). As part of any live, constructive, and virtual simulation and gaming, training event, training development, and/or other developmental functions, the OPFOR must be realistic, robust, and relevant to the task being trained. (See figure below.)

CTID Threats Integration



CTID serves as the Army lead, within the TRADOC G2 Operational Environment Enterprise (G2 OEE), for designing, documenting, and integrating threat or OPFOR and operational environment (OE) conditions in support of all Army training, education, and leader development programs (TRADOC Reg 10-5-1). CTID produces and updates the HQDA Training Circular 7-100 series on regular and irregular forces, hybrid threats, exercise design, OE use in the Army Learning Model (ALM), and related OPFOR products. CTID threats integration embeds analysis of threats in regional and global hotspots with trends and patterns to future impacts in a challenging OE and OPFOR. Specific analysis in a *Threat Action Report, Threat Tactics Report,* and other documents embed observations into the *Decisive Action Training Environment* (DATE), threat models being integrated into curriculum at the Military Intelligence School/Center of Excellence (CoE), and CTID resident training or mobile training teams (MTTs) on threats and an OPFOR. As task-based, event-driven guidance for achieving and sustaining Army readiness, the Army's Combined Arms Training Strategies (CATS) must present an OPFOR with the rigor of an uncompromising adversary or enemy—for effective Army learning.

JON

Boko Haram and Shifting Techniques: *Towns under Fire*

by Laura Deatrick, CTID (CGI Ctr)

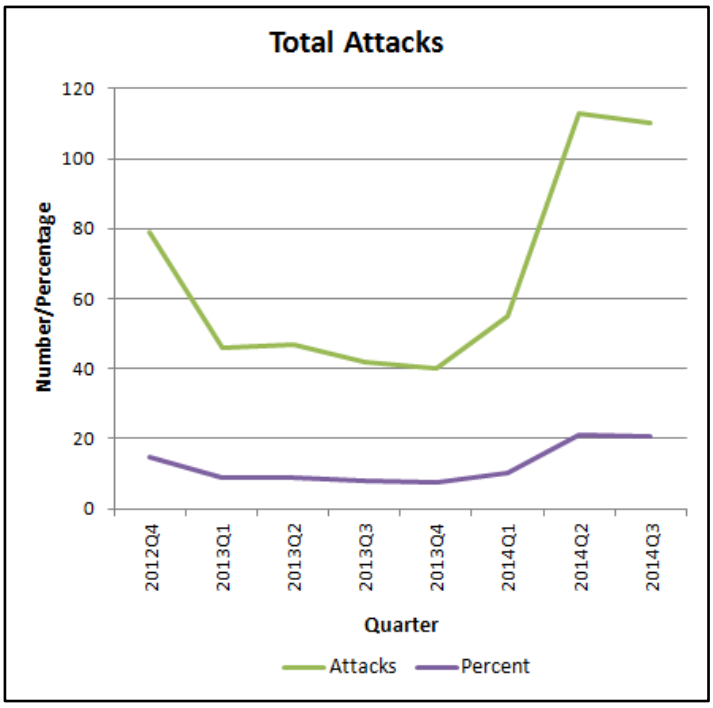
Boko Haram is an Islamist insurgent group operating in Nigeria that has been militarily active since late 2003. Operating primarily in the northern half of the country, its main objective is to establish an Islamic state in Nigeria and institute sharia law throughout the entire country. During this time, the group's techniques have shifted from small simple raids using crude weapons—including clubs and machetes—to simultaneous complex attacks utilizing small arms fire, rocket-propelled grenades, and improvised explosive devices (IEDs) against multiple targets. This article will discuss a particular trend—that of targeting entire towns—and review one such attack in depth.

Shifting Techniques*

From October 2012–September 2014, Boko Haram is known or suspected to have conducted 532 separate attacks, with a mean average of 67 and a median average of 51 per quarter.

***Attack information was obtained from the Armed Conflict Location & Event Data Project. For more information, see the "Methodology and Data Sources" section at the end of this article.**

One disturbing trend that developed during this time has been that of attacking entire villages. At the beginning of the study period, it was not uncommon for Boko Haram to enter a town and destroy multiple specific buildings, primarily those related to the government, education, or religion. Civilian homes and shops, however, were usually left undisturbed. For example, on 12 December 2012, Boko Haram attacked Nassaraw in Kano State, Nigeria. Targeted locations included a police station and three churches, all of which were burned down.



During the same quarter the group would also enter a village and either randomly or systemically attempt to kill the residents, but civilian homes would be left standing. Only one event in the first quarter of the study period (2012Q4) involved the possible attempted destruction of an entire town: an attack on Damboa in Borno State, Nigeria, in which Boko Haram torched both homes and government buildings.

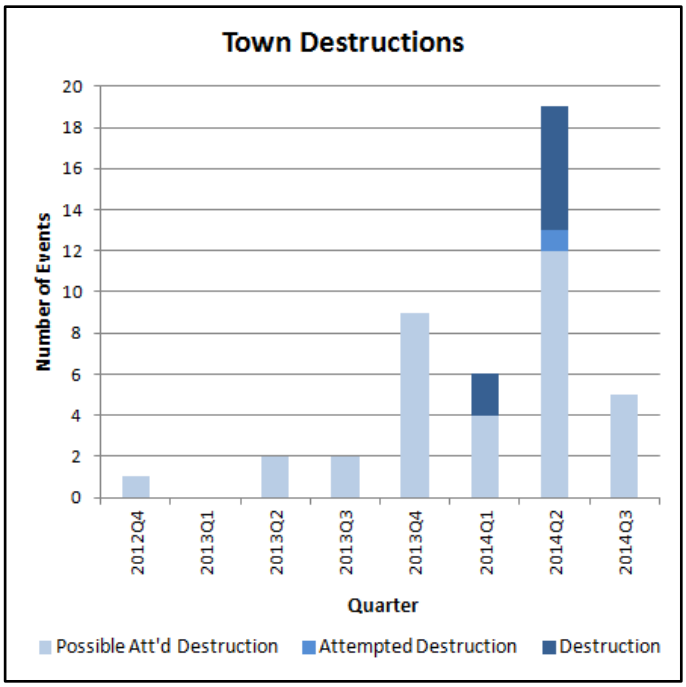
The second quarter (2013Q1) was equally quiet in this regard—there were no recorded events in which the group may have attempted to physically destroy an entire village.

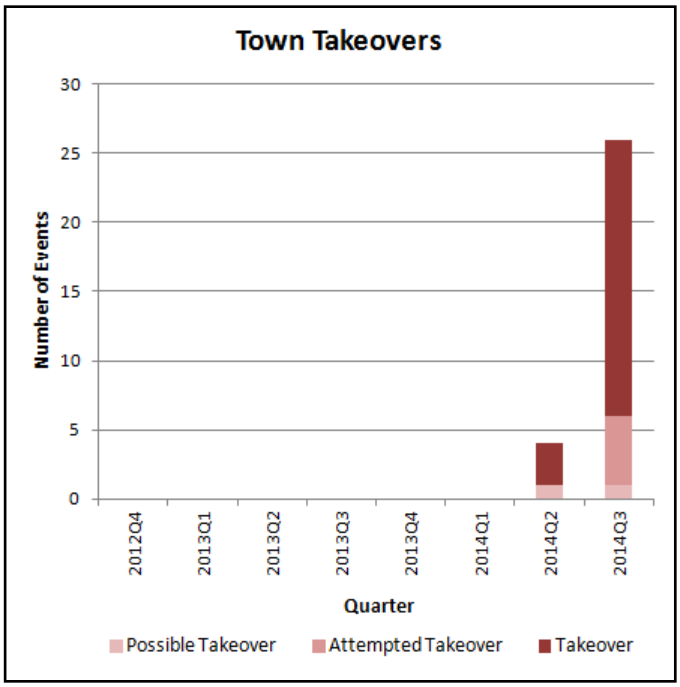
This began to change in the third quarter of the study period (2013Q2). Two attacks that may have been attempts to destroy entire towns occurred that quarter: one in April and the other in June.

One attack began as an ambush on a security vehicle and escalated in violence, resulting in around 200 civilian buildings—both shops and homes—being burned down.

The second was an attack on a village in which Boko Haram purposefully burned unspecified buildings. Two more attacks occurred in 2013Q3, both involved mass casualties (100+ each) and the destruction of houses and businesses.

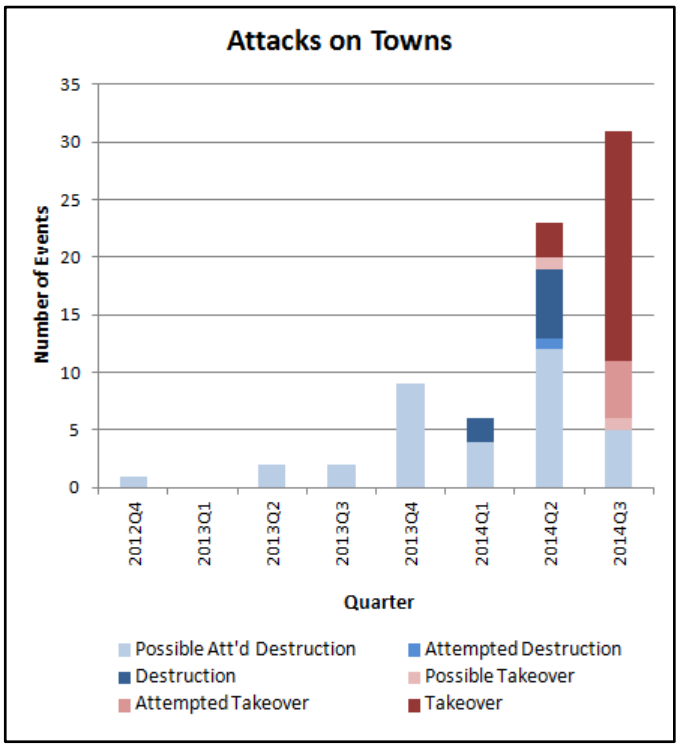
The upward trend continued in 2013Q4 with the possible attempted destruction of nine different villages in Nigeria, all involving casualties and the destruction—usually by fire—of anywhere from 10 to over 300 buildings per town. The





number of attacks dropped to six in 2014Q1, but included the first two cases where towns were reported as being destroyed outright (defined as destruction of more than 70% of a town's buildings). 2014Q2 was the worst in the study period: Boko Haram may have attempted to destroy 12 villages, clearly attempted to do so for one, and successfully destroyed an additional six towns.

The number of attacks in which Boko Haram may have attempted to demolish entire towns dropped significantly in 2014Q3 to five, but not because the group eased up on its activity. Instead, this reduction signaled yet another shift: from destroying villages to taking control of the town. This change had begun in the previous quarter (2014Q2), when Boko Haram had taken over three different towns—denoted by the group raising its flag above the towns after attacking them—and possibly taking over a fourth. The following quarter saw a rapid expansion of this technique: in 2014Q3 the group succeeded in taking over 20 villages, may have done so in one more, and attempted to take over an additional five.



Attack on Gamboru, Borno State, Nigeria

The town of Gamboru, Nigeria, lies on the country's far northeastern border with Cameroon, only a few kilometers south of Lake Chad. As of early May 2014, Gamboru boasted a large international market—approximately six acres in size—where traders from Nigeria, Cameroon, and nearby Chad would come to

trade their wares. Mondays were a traditional market day, and 5 May was no exception. Activity in the town was likely normal but tense. Gamboru's young men had formed a local defense force to augment security forces in protecting the town against potential attacks by Boko Haram. The latter had kidnapped around 200 schoolgirls from the town of Chibok, around 250 km southwest of Gamboru, during the previous month. Reports had been circulating that the kidnapped girls and their captors had been spotted on the road to Lake Chad, and the military forces normally stationed at the town had been redeployed just hours before to search for the girls.

Suddenly, up to 400 gunmen wearing military fatigues and armed with AK-47s, rocket-propelled grenades (RPGs), petrol bombs, and other IEDs drove into town in pickup trucks, motorcycles, and armored personnel carriers (APCs) stolen from the Nigerian military. Shouting "Allahu Akbar [God is Great]," the militants drove to the marketplace, where they shot people on sight, burned down stores, and set fire to vehicles. Several people locked themselves into shops to protect themselves, but to no avail. The attackers threw petrol bombs and other IEDs at these buildings and shot RPGs at them, setting the structures on fire and killing those inside. (See figure 1.)

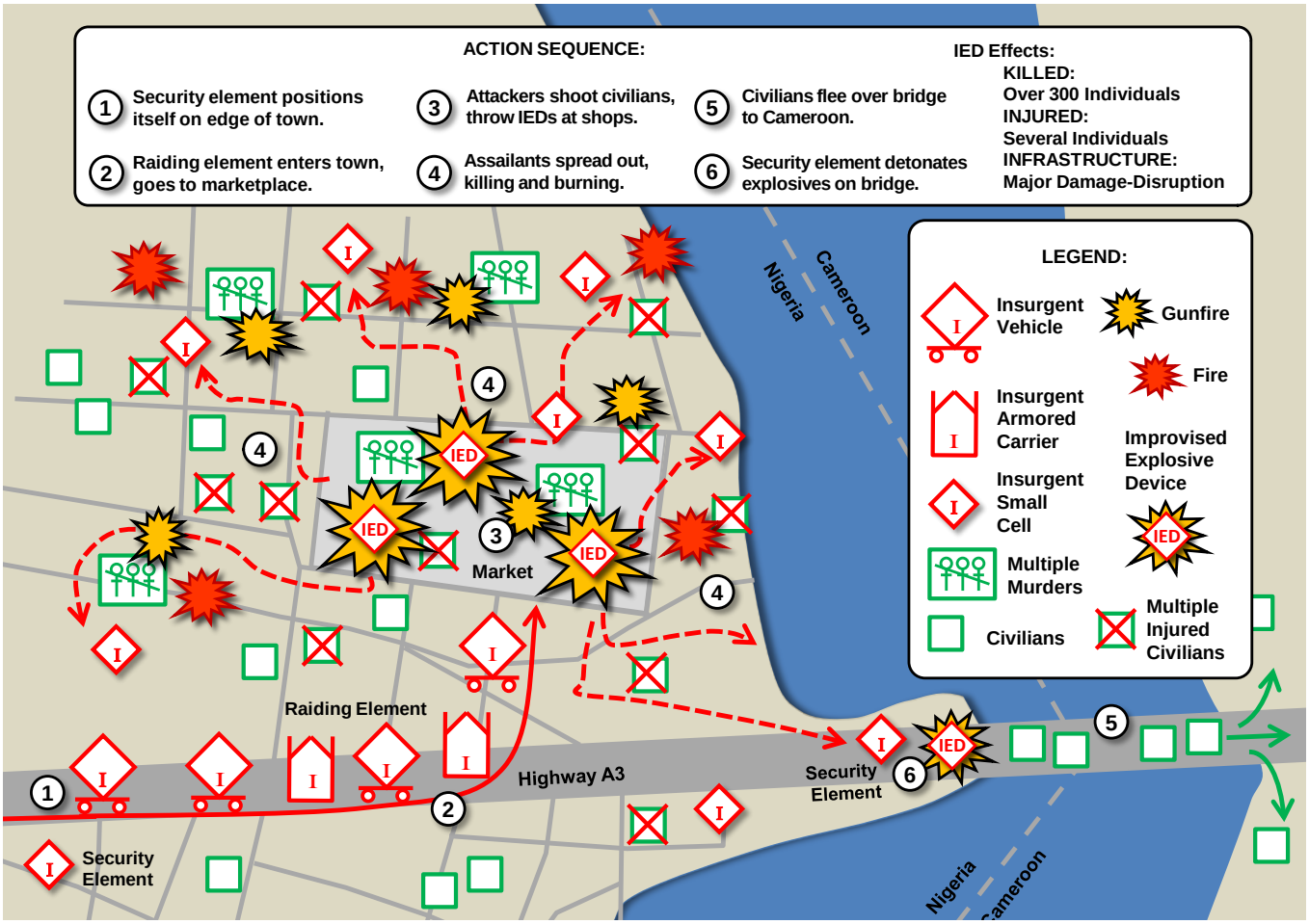


Figure 1. Attack on Gamboru

After devastating the marketplace, the assailants then proceeded throughout the town, shooting people on sight and burning down homes, shops, vehicles, and government buildings. Many civilians fled over the bridge to nearby Cameroon for safety, but this escape route was later cut when the militants used explosives in an attempt to destroy the bridge. The police, border guards, and local defense force fought the militants, but were too few in number and inadequately armed to repel the attack.

Over 300 people—primarily civilians—died in the attack and an unknown number suffered injuries. Hundreds of buildings and vehicles were burned. The international market, hospital, police station, and the local customs office were all destroyed. Different reports described the town as "destroyed," "razed," and "burned to ashes." The bridge between Nigeria and Cameroon was seriously damaged, limiting traffic between the two countries.

Analysis

The attack on Gamboru in northeast Nigeria was likely retaliatory in nature. The townspeople had established a local defense force and were allied with Nigerian security forces, thus placing the town on the side of the government. Other towns had been attacked by Boko Haram for the same reason during the study period, both before and after this event.

During the past two years, Boko Haram has undergone a rapid evolution in techniques: from destroying specific targeted buildings, to devastating entire villages, to taking control of towns. Three things stand out about this development, first of which is the change in targets. In the beginning of the study period, Boko Haram focused on specific types of stationary targets for physical destruction, primarily those relating to the government (local headquarters), security (police stations/military bases), education (schools), and/or religion (churches). While the group continued to perform such attacks throughout the study period, it also broadened its target set to include civilian targets (homes and businesses), and then expanded/generalized to entire towns. In doing so, the group effectively expanded its definition of the enemy from those belonging to or associated with certain institutions, e.g. education, to the general populace.

The second aspect of this development that stands out is the shift in underlying tactics. At the beginning of the study period, Boko Haram was engaging in raids: it would destroy a stationary target and then withdraw to safe territory. By the end of the period the group was performing assaults, where it would attack and then physically occupy an enemy-held position. The focus changed from attacking the enemy within his territory to seizing terrain and holding it. For more information on how threat forces perform assaults and raids, see TC 7-100.2, Opposing Force Tactics pages 3-20–3-26 and 3-36–3-40, respectively.

Figure 2. Location of Gamboru in Nigeria

The final item that stands out is the speed with which the techniques evolved. Only 18 months passed from when Boko Haram began to focus on destroying towns to when it discarded that method in favor of holding them instead. The speed and intensity with which the group adopted the latter was even faster: from four incidents in one quarter to 26 events in the next.

This shift in both tactics and techniques is consistent with one of Boko Haram's stated goals: that of establishing an Islamic state. Nigerian security forces have been fighting Boko Haram for control of the northern part of the country for several years, but with minimal success. The insurgent group likely believes that the balance of power has tilted enough in its favor to take and hold territory without fear. Boko Haram also apparently feels that it has progressed far enough to have met the goal of establishing an Islamic state: on 24 August 2014, the group released a video declaring that its most recently conquered town was now part of an Islamic Caliphate.

Training Implications

While a specific threat force may typically follow a certain tactic or utilize a given set of techniques, the continued use of said tactic or techniques is never certain. Threat actors such as Boko Haram are not tied to institutional thinking, and are both agile and quick to adapt their methods as needed in order to further their goals.

Two groups contained in the Decisive Action Training Environment (DATE 2.1) that would use the techniques discussed in this article are the Multiple Minarian Factions (MMF) and the Free Artzak Movement (FAM). These two organizations are on opposite sides of Atropia's conflict with Minaria over the Artzak region: FAM wishes to see Artzak return to Atropian control, while MMF is fighting to ensure Minaria's continued supremacy over the territory.

Methodology and Data Sources

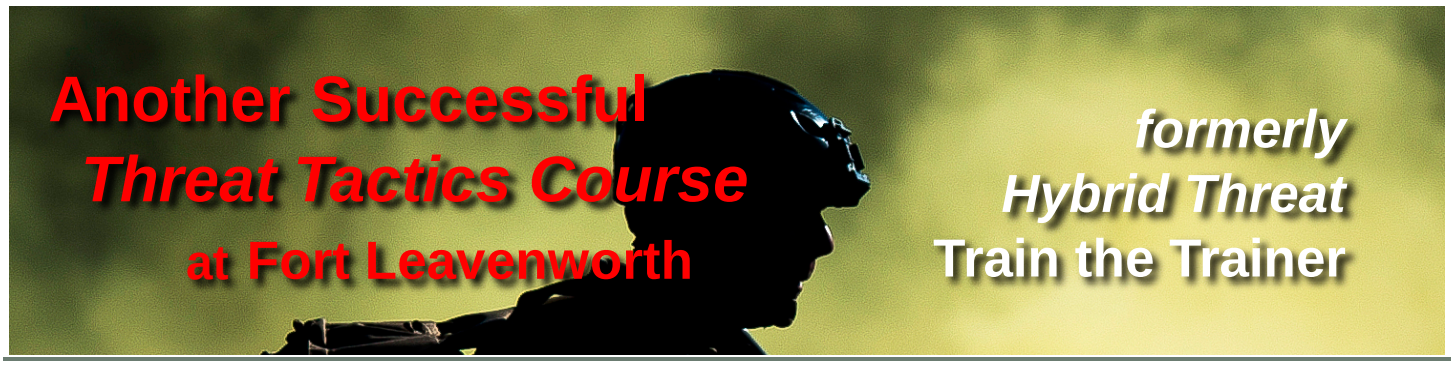
To examine techniques used by Boko Haram during the past two years, the author used data contained in the Armed Conflict Location & Event Data Project (ACLED), operated by the University of Sussex. This database contains information on violent events of a political/governance nature that occur in dozens of countries, including Nigeria. Incidents occurring from 1 October 2012 through 30 September 2014 were considered. The author analyzed events that were known or suspected to be initiated by Boko Haram. For example, an attack on a police station by Boko Haram gunmen would be included, but a raid by Nigerian security forces on a suspected Boko Haram hideout would not. Events for 2012 and 2013 came from the ACLED Version 4 (1997-2013) All Africa Dataset, while 2014 events were from the ACLED Realtime Data 20140101-20141004.

Occasionally an attack on multiple villages would only be recorded as one event in the ACLED database. In such cases, the author recorded multiple separate attacks; one for each village. Attacks on multiple targets within the same city/town/village on the same day were recorded as one attack. Multi-day attacks against one village were also recorded as one event.

References

ABC News (Australia). "Boko Haram attack in Nigerian town kills hundreds, witnesses say." 8 May 2014.
Agence France-Presse. "Boko Haram kills scores, burns market, customs office, police station, shops in fresh attack." African Spotlight. 5 May 2014.
Ajakaye, Rafiu. "Nigeria finds 50 charred bodies after Boko Haram attack." Anadolu Agency (Turkey). 8 May 2014.
American Interest. "Terrorist Attack Leaves Over 300 Dead in Nigeria." 7 May 2014.
Armed Conflict Location & Event Data Project (ACLED). "ACLED Realtime Data 20140101-20141004." 4 October 2014.
Armed Conflict Location & Event Data Project (ACLED). "ACLED Version 4 (1997-2013) All Africa Dataset." 31 December 2014.
Associated Press. "Hundreds killed by Islamic extremists, Nigerian official says." The Star. 7 May 2014.
Associated Press. "Nigeria residents in Gamboru village attacked by Boko Haram say they'll flee country." CBS News. 12 May 2014.
BBC News. "Nigeria confirms market massacre blamed on Boko Haram." 8 May 2014.
Deutsche Welle. "Boko Haram declares caliphate in Nigerian town under rebel control." 24 August 2014.
DPA. "Report: More than 200 killed in northern Nigeria Boko Haram attack." Haaretz. 7 May 2014.
Grossman, Laura. "Boko Haram's new caliphate." 25 August 2014.
Nossiter, Adam. "Islamist Militants Kill Hundreds of Civilians in Northeastern Nigeria." New York Times. 7 May 2014.
Ola, Lanre. "Islamist attack kills 125 in northeast Nigeria." Reuters. 7 May 2014.
Olugbode, Michael. "Nigeria: Another 300 Killed in Attack On Border Town With Cameroun." AllAfrica. 7 May 2014.
Raleigh, Clionadh, Andrew Linke, Håvard Hegre and Joakim Karlsen. "Introducing ACLED-Armed Conflict Location and Event Data." *Journal of Peace Research* 47(5) 1-10. 2010.
Simpson, John. "Gamburo: The town Boko Haram destroyed." BBC News. 13 May 2014.
Soley-Cerro and CNN Wire. "Amid Calls for Action, Boko Haram Strikes Again, Attacks Nigerian Village." KTLA. 7 May 2014.
Talk of Naija. "Gamboru Residents To Relocate Over Boko Haram Massacre." 12 May 2014.
TRADOC G-2 Intelligence Support Activity - CTID. Threat Report: Boko Haram. 15 March 2012.
Vinograd, Cassandra. "Suspected Boko Haram Militants Kill Hundreds in Nigeria Town." NBC News. 7 May 2014.
Windrem, Robert. "While World Watches ISIS, Boko Haram Declares Its Own Caliphate in Nigeria." NBC News. 15 September 2014.
Williams, Itohowo (poster). "Boko Haram: Nigeria has failed us; we'll relocate to Cameroon – Mourning Gamboru residents." Blog4All News. 12 May 2014.

———————



by Jennifer Dunn, CTID (DAC) and CPT Ari Fisher, CTID

This past August, CTID hosted a Hybrid Threat Train the Trainer (HTT3) class here at Fort Leavenworth. The class was a resounding success with over 60 students traveling from installations and units both within the CONUS and OCONUS. Our student roster was, again, extremely diverse. We had students from across the Army along with a small contingent of students from an Air Force Intelligence Squadron.

The most recent class disposition was unique in that we were fortunate enough to welcome some additional students from organizations that are not regular participants in the course. These new students were instructors from the US Army Command and General Staff College, international officers representing four different countries (United Kingdom, Spain, Denmark, and Italy), and representation from the National Ground Intelligence Center (NGIC).

This highlights the diversity of our student attendees, not only in terms of what service, country, or organization from which they come, but also what types of duty positions they fill and their familiarity (or lack thereof) with the hybrid threat and threat tactics. Some students are observer controller/trainers (OC/Ts) from training centers, while other students are serving in a designated OPFOR role-player slot. Some students are responsible for training Soldiers in a classroom environment on topics related to threat tactics, while other students are battalion intelligence officers, operations officers, or intelligence analysts responsible for understanding threat tactics and concepts.

This breakdown of class participants helps illustrate the main reasons students typically take our class. The first reason, which mostly applies to students involved in training, is to gain an understanding of threat tactics in order to be able to replicate those tactics in a training, education, or leader development environment. This enables OPFOR role players, scenario developers, and others involved in the learning process to ensure that rotational training units (RTUs) are training against a challenging, realistic threat actor employing threat tactics being used by threat actors from around the world. Additionally, these students help ensure that RTUs are exposed to operational environment (OE) conditions that are present in OEs from regions around the world, further enriching the training experience.

The second reason some students take our class, which applies to students with an intelligence or analytical background, is to gain an understanding on general principles of threat tactics so that they can take this information and use it to inform intelligence analysis. Approaching our threat tactics lessons from this perspective is a relatively new paradigm and has resulted in a close partnership between CTID and the Intelligence Center of Excellence (ICoE).

Fundamental to this approach is the further distilled articulation of functional tactics, as defined in TC 7-100 and further articulated in TC 7-100.2, into Threat Models that were piloted in September's HTT3 and refined for March's Threat Tactics Course. Eventually, there will be a library of threat models from which to draw upon depicting threat actions in various conditions, however the models will depict the six primary threat tactical actions.

Currently, we have four approved Threat Models—Assault, Ambush, Raid, and Reconnaissance Attack—as our first tools in this new kit bag designed to assist intelligence analysts in both learning and predicting threat actions. Threat Models are also in development for defensive actions and operations, and use threat concpets such as simple battle positions (SBP) and complex battle positions (CBP) in dynamic and uncertain operational environments.

Figure 1. A sampling of threats training in recent resident courses at TRISA-CTID

Threat Tactics Course (TTC)

Since the needs of our audience have become so clearly defined by the attendees of our threat tactics training, CTID has implemented some significant changes in the curriculum of the course to better serve these two primary reasons students attend our course. This effort is being tackled by a team of CTID analysts: LTC Shane Lee, CPT Ari Fisher, and Mr. Kris Lechowicz. They are supported administratively by Ms. Steffany Trofino. Together, this team created a new curriculum for our threat tactics training which will be debuted at our next training event scheduled for 9-13 March 2015. This revamped threat tactics course is known as the Threat Tactics Course (TTC). You may have already received your invitation or noticed an announcement for the event on the Army Training Network's homepage.

Threat Models will be used by the ICoE in teaching new Army intelligence analysts how to analyze the threat. These models will be used to inform the development of "threat/adversary templates" in the Intelligence Preparation of the Battlefield process. ("Threat/adversary templates" have replaced what was once referred to as "doctrinal templates").

This course is similar to the Hybrid Threat Train the Trainer in that it provides a foundation for understanding the basics of threat tactics, but this is where the similarities end. The schedule has been completely revamped and new courses of instruction are currently under development. The biggest changes to the courses of instruction include a reduction in the amount of time spent discussing the various actors and an increase in the amount of dedicated to specific tactical actions. Additionally, analysts are in the midst of developing entirely *new* courses on warfighter function topics such as information warfare (INFOWAR), reconnaissance, air defense, and fires. These courses are designed to provide additional insight into how threat tactics incorporate these functions and are based on material already present in the TC 7-100 series and the Worldwide Equipment Guide.

If you have any questions on the changes to the curriculum of the course, please get in touch with LTC Lee. If you would like to register for a course, please contact Ms. Steffany Trofino.

Threat Force Structure: Commando Brigade

by Jerry England, CTID (DAC)

At the request of exercise designers, a revision of the Hybrid Threat Commando Brigade for future exercises has been initiated to reflect a lethal rapid reaction attack capability. The new brigade is designed with capabilities observed in conflict zones throughout the complex operational environment. Threat elements in the current Ukrainian crisis have used light armored vehicles to rapidly capture key components of the Ukrainian defense complex in a series of tactical skirmishes resulting in an operationally successful integrated attack.

Recent success of commando style operations in the Ukraine has renewed interest in this type of threat capability among exercise designers. Examples include commando unit's isolation of Ukrainian Naval facilities in Crimea through physical destruction of communications lines and other forms of infrastructure.[1] The rapid attack tactics employed by these units ensured that key facilities were seized with a minimum amount of Soldiers needed to complete the mission. Studies conducted by the Foreign Military Studies Office suggest that Russian GRU Spetsnaz, Airborne, and Naval Infantry units will be modernized to enable smaller formations to move rapidly and control territory during "politically sensitive" operations.

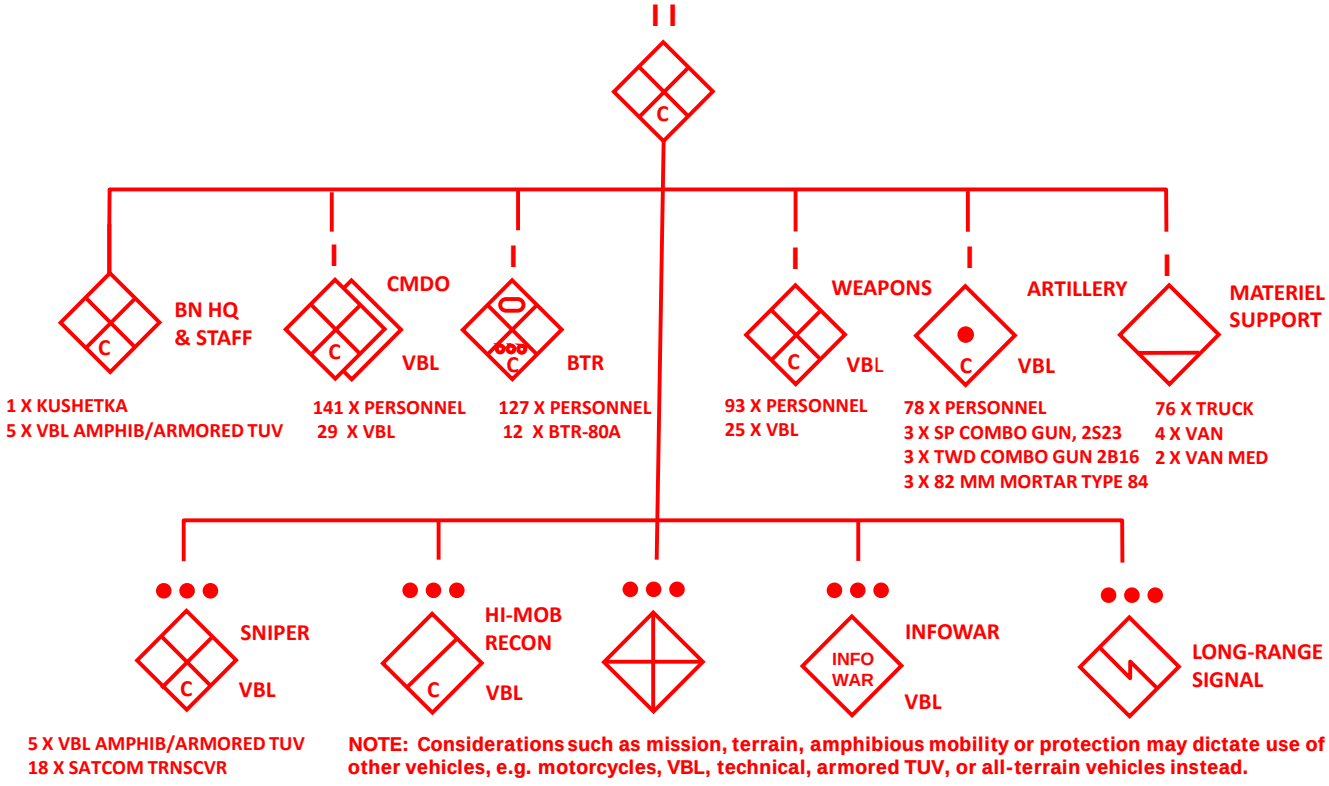


Figure 1. Commando Battalion, TRISA-CTID, 2014

The key enablers for this type of restructuring include designing units based on a new tactical utility vehicle similar to the TIGER GAZ 2330 and expanded command and control capability at the tactical level.[2] The designation of these units by Russian officials as "peacekeepers" implies that operations by these units would be limited to missions such as peace enforcement.[3] However, an assessment of activities in the Ukrainian conflict illustrates the intent of these peacekeepers to maintain the role of traditional Spetsnaz units. Only the best units are designated peacekeepers, and they all receive the best weapons.

The Hybrid Threat Commando Brigade will be used for a range of missions, including—

- Collecting information on deployment of enemy forces and reserve unit movement.
- Collecting information on logistics facilities and seaports.
- Collecting information on enemy aircraft operating from forward airfields.
- Conducting reconnaissance of terrain and enemy forces, in support of the offense.
- Locating and destroying enemy WMD.
- Conducting platoon-size or smaller raids and ambushes and destroying critical military or civilian targets in enemy territory.
- Conducing larger-scale (company- or battalion-size) raids and ambushes in the disruption zone or in enemy territory.
- Clearing LOCs for use by supported units during the offense or defense.
- Clearing or emplacing obstacles.
- Acting as an anti-landing reserve.
- Conducting surprise attacks on enemy forces.
- Creating disturbances after infiltrating into enemy territory.
- Acting as a functional force or element—or part of one—in a combined arms tactical action.

The inclusion of a rapid reaction attack capability in the Threat Force Structure addresses tactics observed in Ukraine that have evolved during conflicts in Chechnya and, to some extent, Georgia.[4] The typical Commando Battalion in the Hybrid Threat Force Structure will include a maneuver force based on the VBL light tactical utility vehicle, an APC Company of BTR-80s, a long range Signal Platoon, as well as an Artillery Battery.

Tactics observed in the Middle East by Commando Forces such as Hezbollah or Iraqi Special Forces could also be represented by the commando Hybrid Threat Force Structure by simply changing the primary mover from a VBL to a tactical utility vehicle with a civilian-based platform known as a technical.

Figure 2. Russian Tiger vehicle leads armored carriers

Notes

[1] Shane Harris, Hack Attack Russia's first targets in Ukraine: its cell phones and Internet lines, Foreign Policy, 3 March 2014.
[2] Ivan Petrov and Ivan Stolnikov,"Among the Military in Crimea They Managed to See a Chechen Battalion and Airborne Troops from Ulyanovsk," Moscow RBK Daily Online, 6 March 2014, (Translated by Foreign Military Studies Office 17 March 2014).
[3] DOD, JP3-07, PEACE OPERATIONS, 1 August 2012.
[4] Lester W. Grau, Changing Russian Urban Tactics: The Aftermath of the Battle for Grozny, Foreign Military Studies Office, 8 July 1995.

MISSION COMMAND TRAINING PROGRAM (MCTP) WARFIGHTER EXERCISE (WFX) 14-5B

by Patrick Madden, CTID (BMA Ctr)

MCTP WFX 14-5B was a distributed, simulation supported, division level, tactical command post exercise. This exercise was held at the Mission Training Complex, Leavenworth, Kansas from 17-26 June 2014. 14-5B was one of four division-level exercises conducted by MCTP, Operations Group X-Ray during fiscal year 2014. The majority of WFXs are based on the Decisive Action Training Environment (DATE) and the Army Training Circular 7-100 series of publications. The discussion that follows describes the unique features of WFX 14-5B as well as the exercise design conditions and execution of this DATE-based exercise. (See figure 1.)

Unique to WFX 14-5B and the previous WFX (14-4A) was the successful effort by MCTP to increase efficiencies in planning efforts since both WFXs involved light infantry divisions from the Army National Guard. As a result, both the 42nd and the 34th divisions attended the same conferences and used the same basic scenario and exercise timeline even though each division trained one month apart.

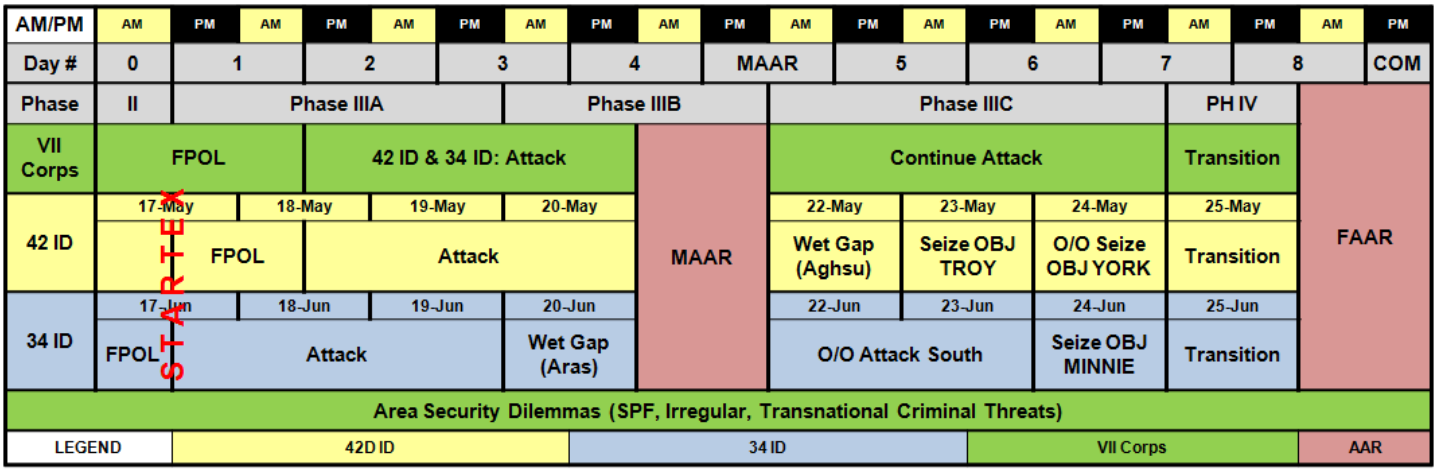


Figure 1. WFX 14-5B exercise timeline

Also distinctive was a planned effort by MCTP to use both WFXs to separately evaluate automation systems that could potentially provide their World Class Opposing Force (WCOPFOR) with timely intelligence collection and a common operational picture (COP) of the battlefield. Since 2011, when the WCOPFOR lost its ability to continue using the All Source Analysis System (ASAS), they have relied on the use of a manual interface to screen and sort thousands of electronic intelligence reports from the WARSIM Intelligence Model (WIM) to determine the enemy situation. Unlike the WCOPFOR, training divisions have relatively large intelligence staffs and the automated Distributed Common Ground System-Army (DCGS-A) which enables them to process and analyze WIM data, as well as provide input for the COP. As noted by previous TRADOC G2 assistance visits to the WCOPFOR, this shortfall has created an unequal simulated playing field.

In response to this critical, automated deficiency, MCTP used WFX 14-4A to evaluate a proprietary system called Red Intelligence Driver (RID). This was followed by WFX 14-5B which was used to evaluate the Distributed Common Ground System-Army (DCGS-A). Both of these automated systems were used by the WCOPFOR during these exercises and received input from WIM. Results of the evaluations were consolidated and submitted to MCTP by the WCOPFOR.

Accreditation

During WFX 14-5B there was also an Operational Environment/Opposing Forces (OE/OPFOR) Accreditation Visit. The team was comprised of personnel from TRADOC G2 as well as the Combined Arms Center's Combat Training Center Directorate. This combined team used the TRADOC G2 Accreditation Standards Guide as the basis for the accreditation. The accreditation visit focused on specific areas such as: equipping and manning of the OPFOR, replication of the OE,

how well the DATE scenario and hybrid threat (HT) are replicated, and how OPFOR tactics are planned and executed. Once completed, a formal out-brief of the results, as well as a written report, were provided to MCTP. Of note was that this was MCTP's first DATE-based accreditation visit.

Training Units

The training division for this exercise was the 34th Infantry Division from the Army National Guard. Supporting the 34th were seven brigades consisting of three brigade combat teams (BCTs) as well as artillery, aviation, maneuver enhancement, and engineer brigades. Three additional training units, one artillery and two sustainment brigades, also supported but were not part of the 34th. It is important to point out that most of these units had never trained together. The 34th and supporting units were part of a larger simulated, notional force consisting of the 42nd and 82nd divisions under the control of VII Corps which served as the high command (HICOM). VII Corps was staffed by the 38th ID and also served as the Army component of a notional Combined Joint Task Force (CJTF) 12. See Figure 2 which highlights the training units in blue. All other units listed in other colors were either simulated by MCTP, small response cells, and HICOM or not exercised but part of the overall exercise design.

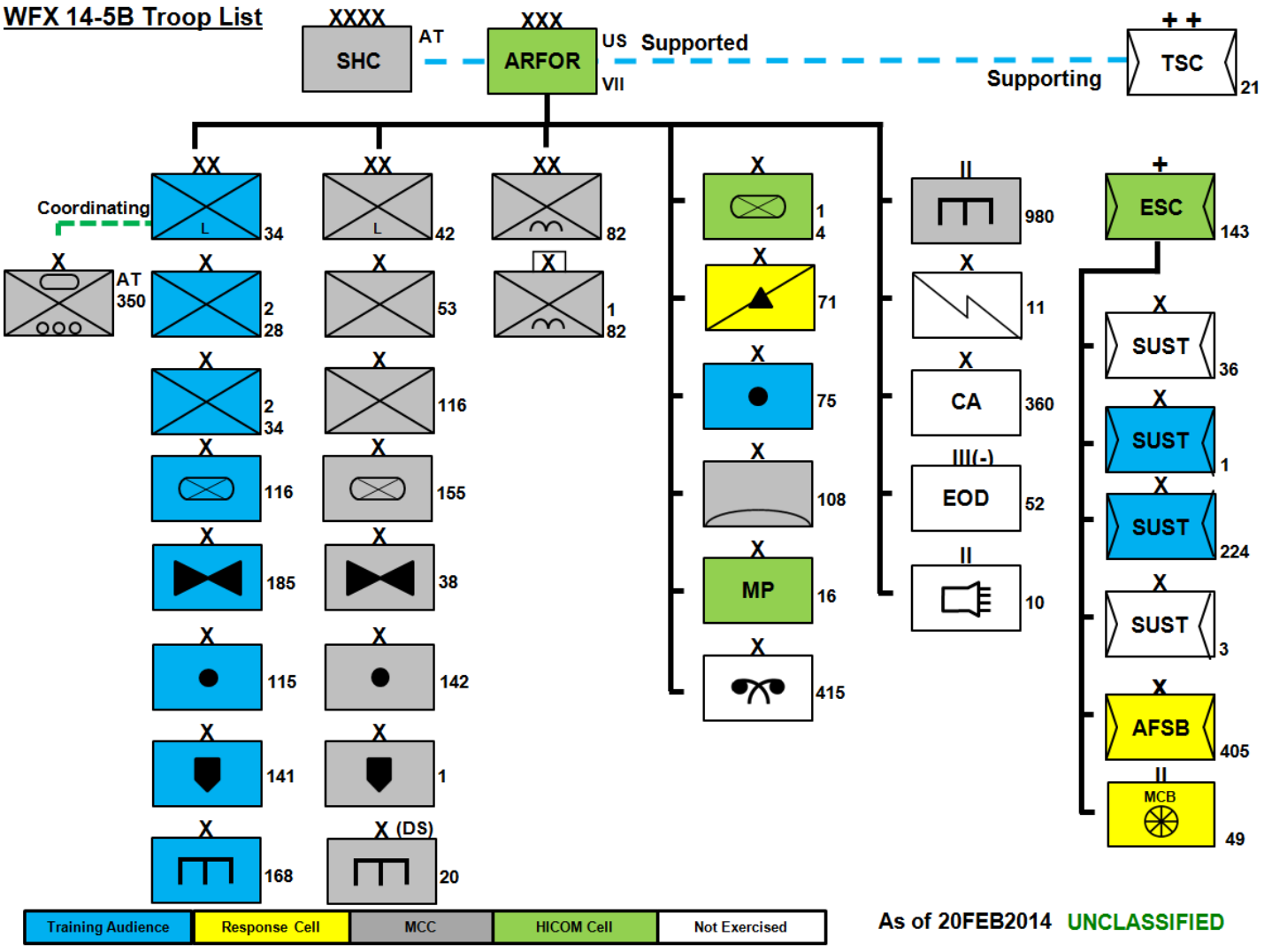


Figure 2. WFX 14-5B troop list

Exercise Scenario

The scenario leading up to the beginning of the exercise involved a successful invasion of Atropia by Ariana. Operational strategic-command (OSC) 2 from Ariana invaded with three division tactical groups (DTGs). OSC 2 controlled most of central and eastern Atropia with the exception of the city of Baku, which was defended by two Atropian brigades. In

response to this invasion, CJTF 12 deployed their forces from the Black Sea Port of Poti, Gorgas into western Atropia in order to attack, defeat, and force the withdrawal of OSC 2 to Ariana. As part of this offensive operation, the 82nd Airborne Division(-) successfully completed a non-combatant evacuation operation (NEO), and secured the US embassy and key infrastructure in Baku.

The 42nd and the 34th conducted a forward passage of lines (FPOL) with remnants of Atropian brigades in order to attack in zone against the 18th and 20th DTGs respectively. When the exercise started, the 34th was already in their battle positions. See Figure 3 below for a focused illustration of the displacement of forces which include the 34th in an attack position and the 82nd(-) having completed the NEO prior to the start of the exercise.

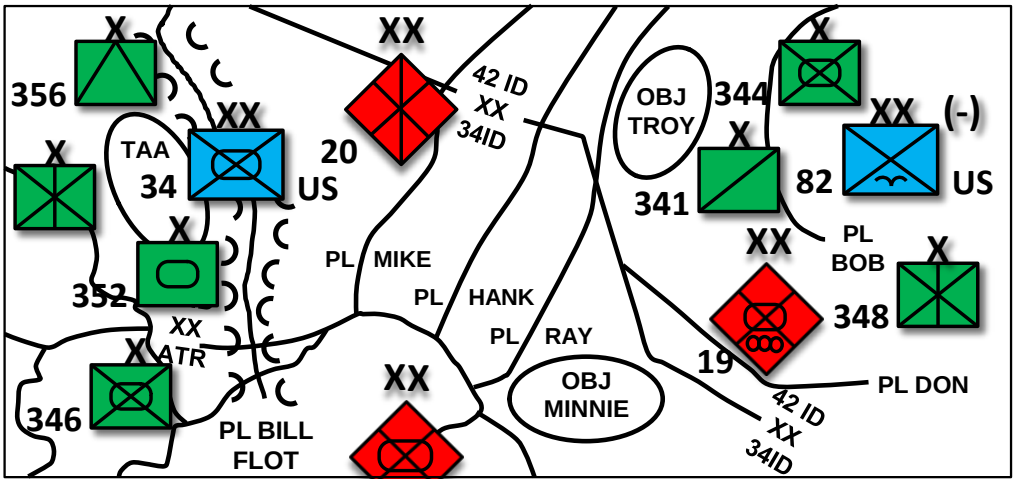


Figure 3. WFX 14-B STARTEX conditions

The exercise for the 34th was organized into Phases II-IV. Phase II was the FPOL, Phase IIIA was the attack, Phase IIIB was the Wet Gap crossing of the Aras River, Phase IIIC was, on order, to attack south to seize Objective Minnie (see Figure 3), and Phase IV was transition to stability operations. There was no specified phase to plan or conduct a deliberate defense during this exercise. Training objectives for the 34th were the following:

- Exercise mission command using the operations process to employ forces in Unified Land Operations (ULO) through decisive action (combination of offense, defense & stability tasks) by means of combined arms maneuver.
- Execute the operations process through mission command training, the warfighter exercise and effective integration of offensive, defensive and stability tasks.
- Refine division tactical battle rhythm for ULO.
- Refine the commander's visualization board.
- Develop and maintain ULO COP processes.
- Prioritize and synchronize the employment of joint fires and effects using the division targeting process.
- Establish a tactical information network and system.
- Provide intelligence analysis to support the division targeting process.
- Refine the division sustainment processes.
- Refine the division information and knowledge management architecture, systems and processes.

Opposing Force (OPFOR)

Opposing the 34th from OSC 2 was the 20th DTG. The 20th DTG's mission was to conduct an area defense west of the Aras River to prevent enemy elements from crossing, in order to allow OSC 2 to retain critical infrastructure sites. The planned end-state was that enemy forces were destroyed, with no offensive ability to cross the Aras River, allowing the 20th DTG to retain defensive positions along the river. For details on the composition of the 20th DTG units, see Figure 4.

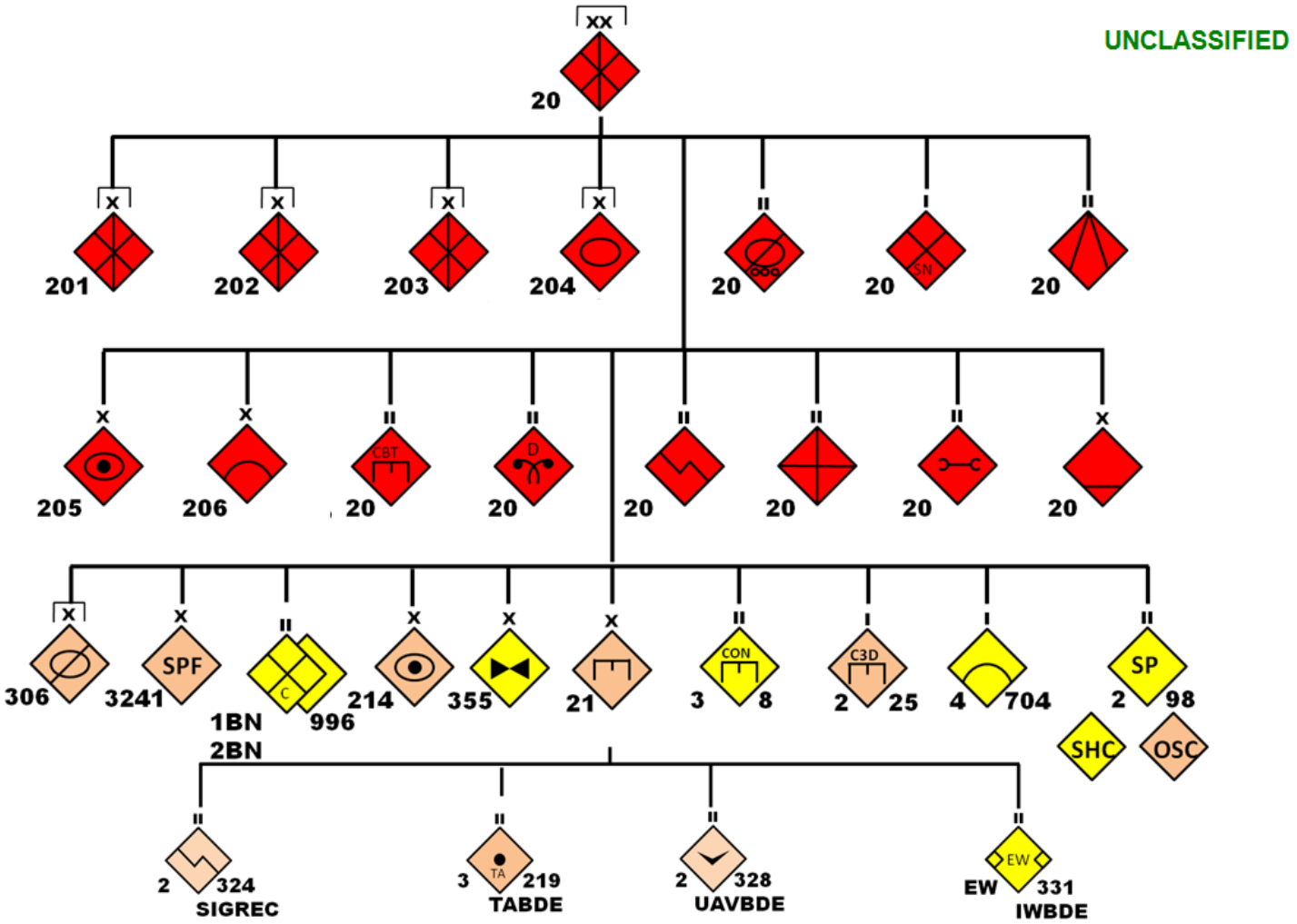


Figure 4. WFX 14-B composition of 20th DTG units

The overall strength of the 20th DTG at the beginning of the exercise was approximately 60 percent as a result of previous attrition during the invasion of Atropia. Therefore, the WCOPFOR chose the area defense tactic since it is specifically used "in situations where the OPFOR must deny key areas (or access to them) or where it is overmatched."[1] The other reasons area defense was selected was the availability of complex terrain and ability to conduct counterattacks, which was a key task assigned to the 20th.

As with most of the OPFOR defensive and offensive tactics, the area defense includes disruption, battle, and support zones. The key task for the 20th DTG Reconnaissance Brigade in the disruption zone was to disrupt and delay enemy forces for 36 hours. This enabled the 203rd, 202nd, and 201st brigade tactical groups (BTGs) in the battle zone to build extensive obstacles, complex battle positions, and kill zones in order to block enemy forces from crossing the Aras River. These efforts were also designed in order to enable the 304th brigade tactical group (BTG) from OSC 2, located on the boundary between the 18th and 20th DTGs, to counterattack into the northern flank of the 34th to force their attack to culminate. The support zone included logistics, long range fires, and the 204th BTG(-) which was the 20th DTG reserve to be committed to reinforce the defensive effort if required. Throughout the disruption and battle zones, artillery units had preplanned targets plotted in kill zones, obstacles, major avenues of approach, and likely river crossing sites. There were also successful efforts to use deception units in the battle zone to divert shaping fires from the 34th and VII Corps.

In addition to the WCOPFOR regular forces described in the previous paragraphs, there was an extensive effort to use special-purpose forces (SPF) and irregular forces throughout the 34th and VII Corps area of operations. The purpose was to challenge the training unit's ability to execute wide area security (WAS). Soft targets such as airfields, major supply

routes, and logistical support areas were attacked throughout the exercise. Both SPF and insurgent groups were also very effective in conducting reconnaissance, calling for indirect fires, and executing ambushes. These attacks were planned and executed simultaneously throughout Gorgas and Atropia.

As the attack progressed significant attrition occurred with the 34th and the 20th DTG. The reasons behind this attrition are not unique to this exercise nor the units involved. The 34th, like many training units, struggled with the initial use of its artillery. Problems with artillery such as: synchronizing fires with its maneuver forces, clearing airspace, counterbattery, and the lack of cohesive preparatory fires with VII Corps contributed to failure in neutralizing the 20th DTG's fire support systems. Associated with this problem were sporadic outages of critical automation systems such as DCGS-A which can provide input to targeting systems. These and other factors allowed the 20th to disrupt the 34th's operations tempo with direct and indirect fires. This in turn contributed to delays on their wet gap crossing of the Kuras River, overwhelmed the casualty evacuation system, and exacerbated the effects of critical supplies that were being routinely attacked by SPF and irregular forces.

As the 34th improved the use of their artillery, the 20th DTG experienced more losses. However, the most significant 20th DTG attrition throughout this exercise was from rotary and fixed wing aircraft due to exercise restrictions. Unlike the 34th, the 20th was not allowed to reconstitute its artillery, air defense artillery, or fixed wing aircraft. The 20th was restricted in the use of its long and medium range air defense systems which made it vulnerable to air attacks. An example of losses due to restrictions on key weapon systems was the approved 304th BTG(-) counterattack. Restrictions prevented them from using their constituent air defense battalion. This enabled the 34th to destroy the counterattack force with their attack helicopters, without committing significant maneuver forces or suppression of enemy air defense planning.

Toward the end of the exercise, the 20th continued to hold most of their defensive positions on the eastern side of the Aras River in order to facilitate the withdrawal of OSC 2 units to Ariana. However, both the 20th and OSC 2 reserve BTGs were destroyed by fixed wing aircraft and unable to reinforce the area defense. Most of the units from the 20th were approximately 20-30 percent strength could not have defended much longer.

Despite heavy losses on both sides, the WCOPFOR significantly challenged the 34th Infantry Division and its supporting units. Most, if not all, of the training unit objectives were accomplished during the exercise. As the 34th conducted combined arms maneuver and wide area security they learned from their mistakes and continued to improve. MCTP and their senior mentors did an impressive job in training, advising, and coaching all training units through this exercise. MCTP is to be commended for efficient planning and completing a very complex exercise with active, guard, and reserve units, to include a robust scenario based on the Decisive Action Training Environment.

Notes

[1] US Department of the Army, Training Circular 7-100.2, *Opposing Force Tactics*, August 2011, p. 4-14.

by Steffany A. Trofino, CTID (DAC)

HAMAS is based on the premise of liberating Palestinians from regional Israeli dominance. It is important to understand that HAMAS is not a formally-recognized political party by the United Nations (UN) and is structured more as a de facto organization that militarily seized control over Gaza in 2007, two years after Israel relinquished occupation of the territory. HAMAS is designated a terrorist organization by several countries including the US, United Kingdom, Israel, Australia, Egypt, Japan, Canada, and New Zealand. Further, as of 1999 HAMAS has been banned in Jordan and more recently, Egypt. In order to function effectively and validate its legitimacy among Palestinians who elected the organization to preside over Gaza in 2006, HAMAS maintains three primary roles which garner support and trust from the local population: welfare services, military activities (security), and political activities which it uses to gain financial support.

Social Welfare Structure

HAMAS manages a broad spectrum of social welfare programs and activities throughout Gaza, known locally as Dawa. Schools, medical facilities, youth camps, charities, and fundraising activities are but a few of the services performed by HAMAS and provided to Gaza residents.[1] This continued commitment to social welfare programs was an integral factor in the organization being elected to power by Palestinians during the 2006 Palestinian election.

Through its social welfare activities HAMAS controls hospitals, schools, charities, and more. Once controlled, HAMAS then has the ability to use these facilities as meeting places, weapon storage facilities, or a means to launder money through local charity committees.[2]

Demographically, Gaza is twice the size of Washington DC, with a total land area of 360 square km. Sharing a 13 km border with Egypt and a 59 km border with Israel, the total population within the territory is estimated to be slightly over 1.8 million residents.[3] Having such a large population condensed into a relatively small geographic region, coupled with a land, air, and sea blockade imposed against Gaza by Israel due to HAMAS' attacks against Israel, unemployment rates have steadily risen over the years.

As the enclave is largely surrounded by Israeli territory, Israel maintains it is necessary to heavily monitor goods, supplies, services and persons entering or leaving Gaza in an effort to diminish HAMAS' ability to manufacture weapons which later could be used against Israel. With a continued stagnation of movement against persons who seek employment outside of the enclave, opportunities to gain meaningful employment are limited. Additionally, most goods and services entering Gaza are based largely on humanitarian needs and include medical supplies and services as well as products that support agriculture development.

Currently, the 2014 unemployment rate for men is reported to be 36.9% and for women it is listed at 64.7%.[4] This has a second order effect of increasing the welfare needs of the region that HAMAS must ultimately support in order to maintain its legitimacy with the population.

Military Wing

HAMAS' military wing is known as Izz al-Din al-Qassam Brigades (al-Qassam Brigades). Established in 1992, it is estimated to have 13,000 well-trained, well-equipped personnel.[5] Israeli Defense Force (IDF) officials state several hundred members were trained in Syria prior to the Syrian civil war by both Syrian and Iranian military personnel. Unique to more advanced military structures, the al-Qassam Brigades is independent from the leadership structure of HAMAS and does not rely on HAMAS for decision-making processes. It serves more as a complementary structure, working in collaboration with HAMAS while retaining full leadership and decision-making control over all its operations. It is a symbiotic relationship as, without HAMAS, al-Qassam Brigades would not have military capabilities such as multiple rocket launchers and anti-tank weapons, nor would HAMAS have a security apparatus to conduct military strikes against Israel.

The current leader of al-Qassam Brigades is Palestinian-born Mohammed Deif. Deif secured his leadership position in July 2002 after Israeli Forces conducted an airstrike killing then al-Qassam Brigades leader Salah Shehade. Little is known of Deif other than he is reported to be in his 50s and is believed to have been mentored by Yehya Ayyash, the renowned HAMAS bombmaker known as the Engineer and who founded al-Qassam Brigades.[6] Deif has survived multiple Israeli assignation attempts, with the most recent occurring 20 August 2014 when Israeli forces launched an airstrike targeting his home. While Deif is reported to have escaped, his wife and seven-month-old son were killed in the airstrike.[7]

Political Structure

HAMAS's de facto leadership structure is widely disbursed. Prior to the Syrian civil war, HAMAS leadership operated mostly from Damascus. After the onset of the civil war and HAMAS's subsequent support of the Free Syrian Army, its headquarters was relocated to Doha, Qatar.

The highest decision-making body overseeing HAMAS operations is referred to as the Political Bureau, and includes 15 elected members operating in exile throughout the Middle East and Sudan. The current chairman of the Political Bureau is Khaled Mashal, who remains in exile in Qatar. The bureau's members are elected by local representatives of specific Gaza or West Bank communities. These local representatives are referred to as General Consultative Council members and are subordinate to the Political Bureau.

The Shura council is directly subordinate to the General Consultative Council and, as such, it is the most tangible conduit of HAMAS, directly servicing the needs of Palestinians and implementing policy in specific geographic locations. Whether it is a city, town, or village, Shura council members implement orders as directed by General Consultative Council members, who in turn received their orders from the Political Bureau. This construct is fundamentally grass roots in nature, but effective.

HAMAS's strategic objectives are broad and include overseeing the return of all Palestinian lands to its people, the rite of passage throughout Palestinian territory, the release of Israeli-held Palestinian prisoners, and an end to the economic blockade currently surrounding the enclave. Presently, the most significant is the latter, as crippling sanctions over the years have significantly impacted the organization's ability to operate effectively. As a result, HAMAS is reliant on outside entities for assistance and support; most notably from Iran and Qatar.

Taking lessons learned from its military engagements with Israel and adapting tactics to overcome challenges may achieve limited success for the organization, but not lasting or sustaining political objectives. HAMAS's leadership recognizes its limitations, both regionally and politically. In an effort to achieve enduring political success, in April 2014 HAMAS sought partnership with the Palestinian Authority and the Fatah party who preside over the West Bank. Under a unity agreement signed by both Fatah and HAMAS, the two sides were to form an interim government by mid-May 2014 and hold parliamentary elections in November 2014. However, due to the ongoing conflict between HAMAS and Israel and the subsequent military engagement of Operation Protective Edge, this did not occur.[8] Without regional partnership, financial and political stability will begin to erode over a period of time.

External Support to HAMAS

Financially, HAMAS is in need of substantial support, as multiple economic variables are beginning to strain the organization's operations. Political shifts throughout the Middle East, a heightened need to replenish rapidly-depleting

weapon stocks, and growing unemployment throughout Gaza with the second order effects of raising the needs of welfare services throughout the region all have compounding negative effects on the organization's financial position and strain HAMAS' functional capabilities.

After HAMAS militarily seized control over Gaza in 2007, Israel initiated an economic blockade isolating the enclave from needed goods and services. Through brokered negotiations, some humanitarian goods and services were permitted into the region, controlled through Israeli checkpoints. In the aftermath of the Arab Spring, governments that HAMAS relied on for financial support and assistance in the provision of supplies no longer retained power or influence within the region. The previous ruling power of Egypt, the Muslim Brotherhood, once a primary financial supporter of HAMAS, has been replaced by a pro-Western government that has turned against the organization.

With the new Egyptian leadership in place, the once relied upon vital link between HAMAS and the outside marketplace is slowly being shut down. In the fall of 2013, the Egyptian government began to close various tunnels within Egyptian territory which were used by HAMAS to smuggle goods and services into the enclave.

With transport routes dwindling, HAMAS will find it increasingly more difficult to replenish needed supplies in the region. Such supplies include ammunition, fuel, repair parts and equipment necessary to rearm, refuel, and repair or refurbish battle damaged weapons and equipment. For example, during the summer of 2014 and its military engagement with Israel, HAMAS launched a total of 4,591 rockets into Israeli territory.[9] The steady depletion of ammunition during a protracted military engagement where needed transport routes were being shut off from the outside possibly resulted in a cascading negative effect on HAMAS's military capabilities. Also, lacking the ability to replenish military supplies may ultimately be the reason HAMAS sought political partnership with the Palestinian Authority during the spring of 2014.

The need to seek an outside link via regional partnership, with an opportunity to secure materials and services has become increasingly more apparent for HAMAS. Furthermore, Syria who was once a primary conduit of financial support to HAMAS by way of funneling money to the organization from Iran, has withdrawn all of its assistance as a result of HAMAS' link to Syria's opposition, the Free Syrian Army.[10]

With limited economic, political, and material support remaining in the region, HAMAS is now in a state of transition. Combined with a need to repair or replace battle damaged equipment and little options left for resupply of critical items such as fuel, ammunition, and various repair parts, the significance of dual-use material and technology may rise for HAMAS in the near term. The ability to adapt to challenges in a resource constrained environment will be a pivotal factor in HAMAS's stability over the next several months.

Training Implications

- If legitimacy is maintained with the population the organization serves, political organizations do not need international recognition to be effective.
- Continuing to militarily engage opposing forces whose supply links have been cut off will cause a force to adapt to lack of resources and revert to dual-use material or technology in times of need.
- A paramilitary wing of an organization does not need to be under the direct control of a political organization to be effective.

Notes

[1] "Country Reports on Terrorism 2013," US Department of State, April 2014.
[2] Matthew Levitt, "Blood Money," *The Wall Street Journal*, 4 June 2003.
[3] "Gaza Strip," CIA World Factbook, 22 June 2014.
[4] "United Nations Seminar on Assistance to the Palestinian People," United Nations General Assembly, 1 July 2014.

by LTC Shane E. Lee, CTID

Regular Force (Threat Model Design): Assault

The purpose of a Threat Model is to aid in assessing and evaluating the threat, and understanding how a threat can affect friendly operations. Threat actors will have obvious, as well as subtle, differences in how they approach situations and problem solving. Understanding these differences is essential in understanding how a threat force will react in a given situation. The intelligence staff conducts threat evaluation and develops threat models as part of the general intelligence knowledge task of support to force generation. Using this information, the intelligence staff refines threat models, as necessary, to support intelligence preparation of the battlefield (IPB).

When analyzing a well-known threat, the intelligence staff may be able to rely on previously developed threat models. When analyzing a new or unfamiliar threat, the intelligence staff may need to evaluate the threat and develop models. (For information related to IPB, see ATP 2-01.3 *Intelligence Preparation of the Battlefield/Battlespace*, Chapter 5.)

Threat Model design requires the following steps:

1. Identify mission
2. Identify functions and elements to accomplish mission
3. Provide task and purpose to elements
4. Identify available resources
5. Develop concept of operations (CONOP)
6. Conduct functional analysis for desired mission accomplishment

This article will discuss Threat Model design steps 1-4 by demonstrating a regular force prosecuting an *assault* with the mission to seize critical infrastructure. Follow-up articles will discuss the CONOP and functional analysis used in executing the actions and tactics of a regular force conducting an assault against a US area defense.

An *assault* is an attack that destroys an enemy force through firepower and the physical occupation of and/or destruction of its position. An assault is the basic form of opposing force (OPFOR) tactical action. Therefore, other types of offensive action may include an element that conducts an assault to complete the mission. (For information related to assault options, see TC 7-100.2, Opposing Force Tactics, Chapter 3.)

OPFOR commanders of detachments, battalions, and below select the tactical action best suited to accomplish their mission. Units at this level are typically called upon to execute one combat mission at a time.

> **Note.** Any battalion or company receiving additional assets from a higher command becomes a task-organized battalion-size detachment (BDET) or company-size detachment (CDET).

Assault

An assault is an attack that destroys an enemy force through firepower and the physical occupation and/or destruction of his position.

TC 7-100.2, *Opposing Force Tactics*

Assaults are characterized by these qualities:

- **Isolation** of the objective through security
- **Suppression** of the enemy force
- **Assault** is violent fire and maneuver against the enemy

In order to isolate the objective the commander will maneuver and employ enabling functions (reconnaissance elements, security elements, fires elements, and fixing elements) to ensure additional enemy forces do not join the battle unexpectedly, continue to provide early warning, prevent the enemy from gaining further information, and prevent enemy maneuver. *(Note.* Security elements may become fixing elements.)

Suppression of the enemy force is provided through lethal and nonlethal means in order to permit the assault element to move against the enemy position without receiving destructive fire. The commander will employ the action function through violent fire and maneuver against the enemy which is accomplished through the assault element, from the direction where least return fire is possible.

The assault element employs surprise, limited visibility, complex terrain, and camouflage, concealment, cover, and deception (C3D) to attain the enemy position while remaining combat effective. The assault element will maneuver to seize the enemy position, destroying any forces there. During the conduct of an assault, the commander or leader in charge of an element may have to make use of whatever units can take advantage of a window of opportunity. The tactical vignette in this article incorporates mission tasks of isolate, suppress, and assault as an *action* element or *enabling* element that support an assault. (Figure 1 is a task-organized company detachment.)

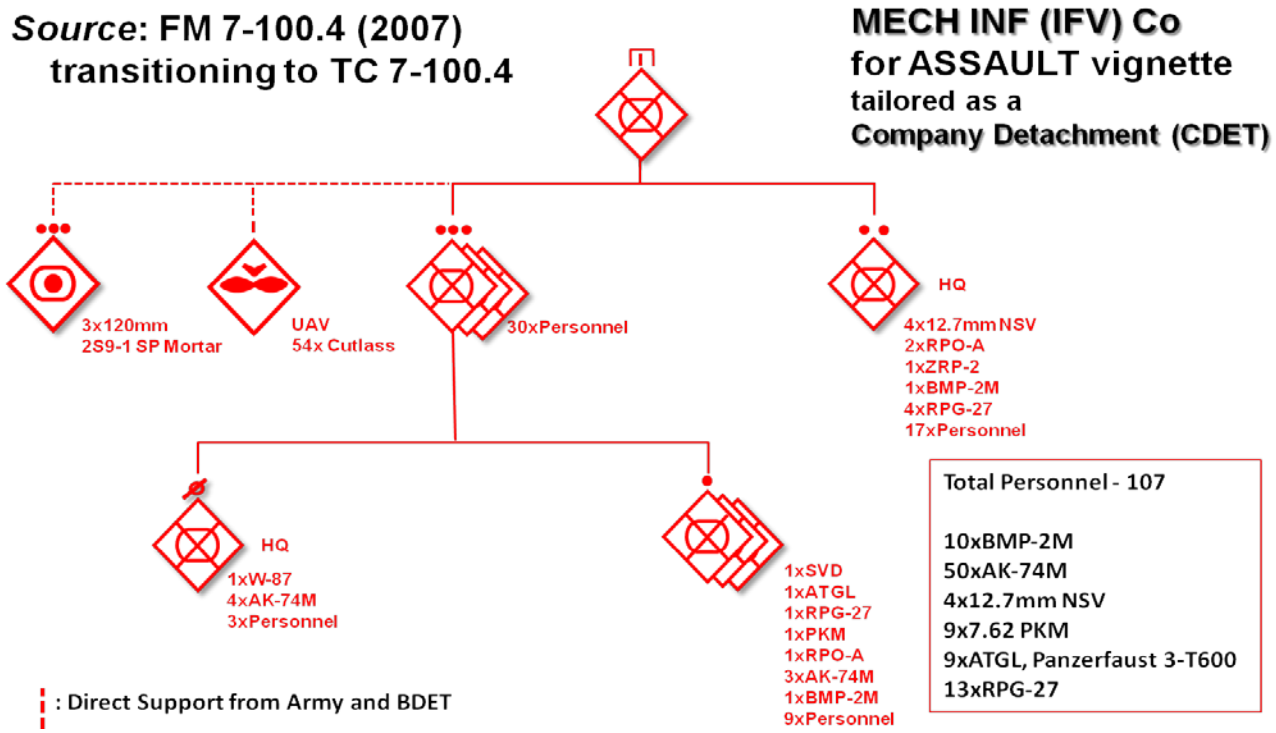


Figure 1. Task organized mechanized infantry company (IFV) detachment (CDET)

Action and Enabling Functions

At threat battalion and below echelon, one part of the unit conducting a particular action is normally responsible for performing the action function or task that accomplishes the overall mission objective of that action. At battalion and below echelon that part can be called the *action* element.

In relation to the action function or force, all other parts of the organization conducting an action provide enabling functions of various kinds. These parts can be called an enabling element.

TC 7-100.2, *Opposing Force Tactics*

Functional Organization for an Assault

Depending on the tactical situation, a commander organizing an assault may designate various mission elements. There may be more than one of each type element. For example, the CDET commander will use a term such as *fires, fixing, reconnaissance, security,* or *assault* element to best describe an element's function. (See Figure 2.)

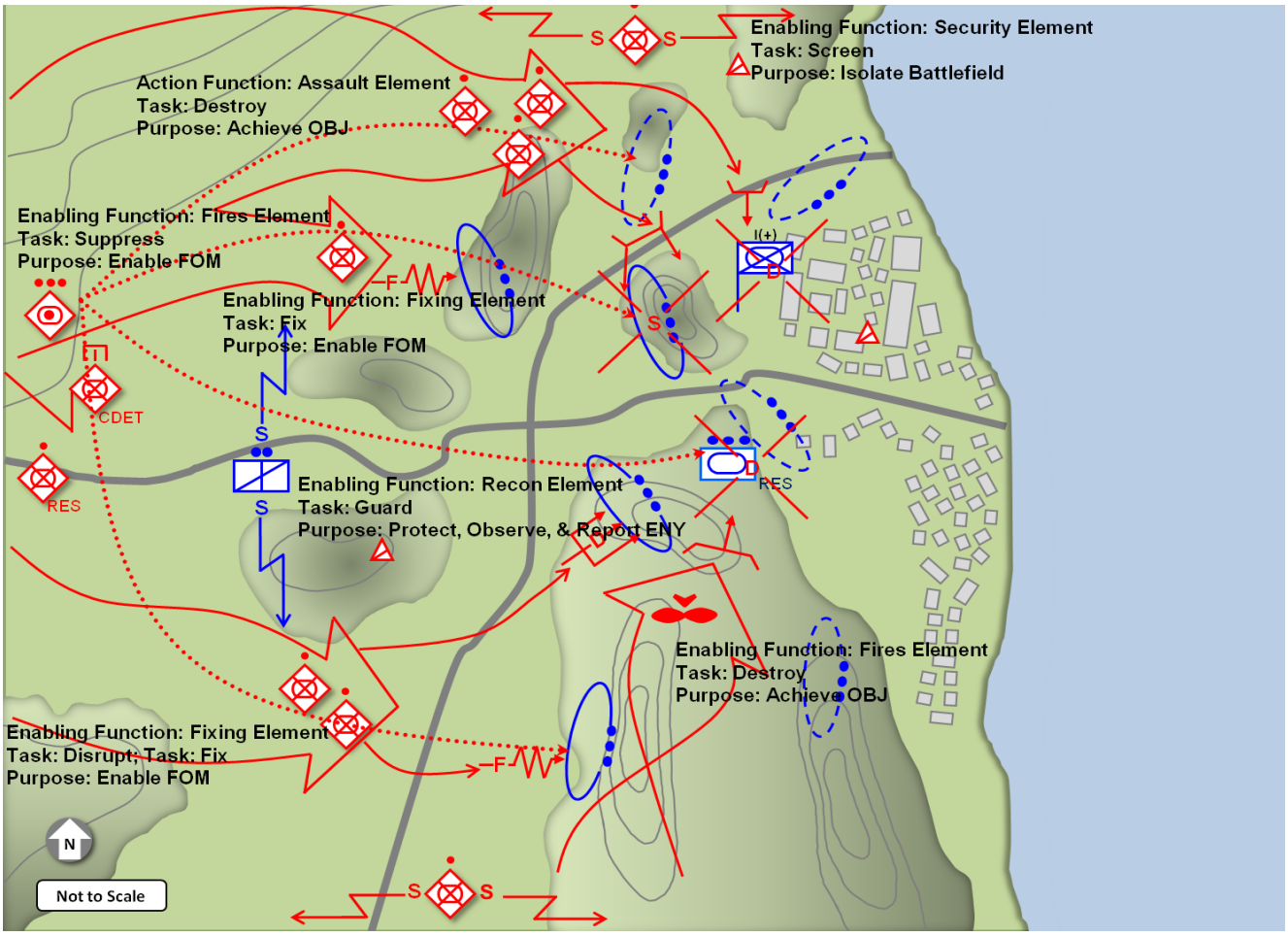


Figure 2. Assault functions of a task-organized company detachment (CDET) (example)

Enabling Functions

Reconnaissance Element(s)

In this vignette, reconnaissance elements receive indications that enemy elements are within the CDET's area of responsibility (AOR). The CDET commander requires identification and reporting on the location of enemy reconnaissance patrols, security observation posts (OPs), and battle positions (BPs). The reconnaissance elements are to

monitor the movements of enemy roving patrols, OPs, and/or BPs but not initiate contact with the enemy. Therefore, the reconnaissance task is to guard.

Reconnaissance elements that precede other elements of the assault section–size elements from the Mechanized Infantry CDET are self-contained for combat service support (CSS). These elements conduct tactical movement with preplanned indirect fire support. Once they have conducted reconnaissance throughout their zone and report from the vicinity of their objective, they may be directed to become security elements with specified tasks.

Security Element(s)

The CDET commander orders first platoon commander to configure the unit to accomplish designated tasks providing two security elements, one north and one south of the main supply route, and provide three teams as the reconnaissance element. These security elements are *screening* and can work in conjunction with reconnaissance elements. The security elements ensure additional enemy forces do not prevent the action element from accomplishing the mission by maintaining a tactical advantage.

Fires Element(s)

Due to prior battalion combat losses in indirect fires capability, the battalion commander provides the CDET commander with a platoon of three 120-mm 2S9-1 self-propelled mortars and one company of 54x Cutlass armed unmanned aerial vehicles (UAV). Fire support in an assault focuses on—

- Fires in support of reconnaissance, security, and/or action elements in contact with enemy
- Support movement of reconnaissance, security, and/or action elements
- Suppression and/or destruction of a fixed enemy
- Destroy enemy reserve and C2

The CDET commander has the 120-mm mortar platoon and UAV company maneuver to firing positions near the central corridor avenue of approach.

Fixing Element(s)

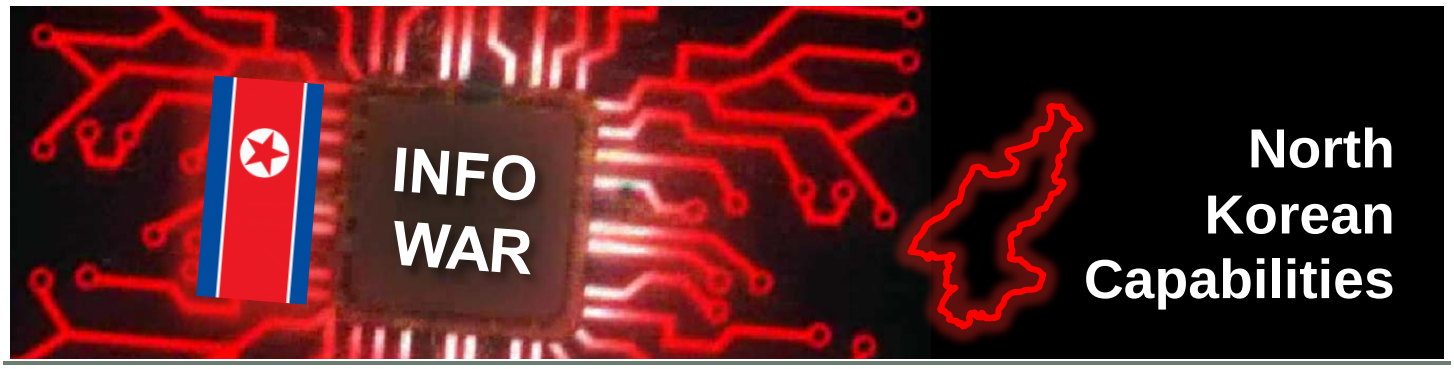
The CDET commander orders his second platoon commander to configure the unit to accomplish designated tasks. Second platoon is the CDET's primary *fixing* element against what is suspected to be the enemy area defense BPs that are protecting critical infrastructure. *Fixing* elements ensure that the enemy forces in the main BPs are fixed and disrupted to enable freedom of movement for the action elements to accomplish the mission of destroying enemy C2.

Action Function

Assault Element(s)

The CDET commander orders his third platoon commander to configure the unit to accomplish designated tasks. Third platoon is the CDET's assault element against the suspected enemy C2. Assault elements will conduct a tactical movement and establish support by fire and attack by fire positions against the enemy C2. The assault elements are enabled through the successful reconnaissance and security elements that isolate the battlefield, supported by fires and fixing elements which prevent enemy forces from massing fires and maneuvering to protect critical infrastructure. (For more information on CDET organization and operations, see TC 7-100.2, Chapter 2 and 3.)

Note. The Complex Operational Environment and Threat Integration Directorate (CTID) is the Army lead, within the TRADOC G2 Operational Environment Enterprise (G2 OEE), for designing, documenting, and integrating threat or OPFOR and operational environment (OE) conditions in support of all Army training, education, and leader development programs (TRADOC Reg 10-5-1). Threat models of tactics and techniques are being integrated into the TRISA-CTID Threat Tactics Course (TTC) resident at Fort Leavenworth and mobile training team (MTT) instructional packages.



by H. David Pendleton, CTID (CGI Ctr)

Introduction

Even though a young Kim Jung-un took control of the Democratic People's Republic of Korea (DPRK) or North Korea, as it is more commonly known, on 17 December 2011, information in the DPRK is just as tightly controlled now as it was in the previous regimes of Kim's father and grandfather. Most common DPRK citizens are deprived of truthful domestic and foreign information and only receive information that the regime wants their people to receive. While the DPRK elites know slightly more about the outside world than the common North Korean citizen, the information is still often filtered by the government.

North Korea has excelled at four of the seven information warfare (INFOWAR) capabilities for over a decade. TC 7-100.2, *Opposing Force Tactics* defines INFOWAR as "specifically planned and integrated actions taken to achieve an information advantage at critical points and times. The primary goals of INFOWAR are to "Influence an enemy's decisionmaking through his collected and available information, information systems, and information-based processes" and to "Retain the ability to employ friendly information and information-based processes and systems."[1]

The DPRK government continues to hone its Physical Destruction, and Protection and Security Measures, and Perception Management skills within the information environment while it attempts to improve its Deception skills. Since 2008 when TRISA published the Information Environment Assessment (IEA) that included a section on North Korea, the DPRK has improved its performance in the other three INFOWAR capabilities—Electronic Warfare, Information Attack, and Computer Warfare capabilities.[2] While North Korea's conventional military equipment continues to become more obsolete due to the aging of equipment, the DPRK has continued to improve its asymmetric warfare capabilities. This is especially true for North Korea's INFOWAR activities.[3]

The North Korean people rely almost exclusively on the state-run media for its information. DPRK residents caught with illegal media of any type are often sent to labor camps unless the violator is able to bribe the arresting official. Only 80,000 North Koreans can access the Internet and most of those are affiliated with the government. While less than 5% of the population can access a landline telephone, the number of North Koreans with cell phones continues to rise. The latest numbers place the number of DPRK citizens with cell phones in a range from 1.5 to 2 million users.

Most North Koreans can only access radios locked to monitor only pre-approved official government stations such as the Korean Central Broadcasting Station. Some courageous North Koreans have modified their radios to obtain the non-approved stations, but at great risk for themselves and their families. For those North Koreans with access to televisions, they must watch the Korean Central Television Station, a Korean Workers' party outlet; the Korea TV Broadcasting Station for Education and Culture, previously Kaesong TV; or Mansudae Television for cultural events. There are a few radio stations in South Korea that can be heard across the mutual border between the two Koreas, if the DPRK citizen wishes to take the risk to listen to the broadcasts. DPRK citizens can also obtain information through government controlled newspapers that include the Rodong Sinmun, a Korean Workers' Party daily; the Joson Immigun, a Korean People's Army daily; the Minju Choseon, a government published paper; or the Rodongja Sinmum, a trade union publication.[4]

This article is the first in a two-part series that will examine the current status of the seven INFOWAR capabilities in North Korea: Electronic Warfare, Computer Warfare, Information Attack, Deception, Physical Destruction, Protection and Security Measures, and Perception Management. The first article will provide a timeline of various North Korean INFOWAR events and the first three capabilities. The second article will cover the final four capabilities, an analytical review of the capabilities, and training implications for units.

North Korean INFOWAR Activity, 2004-2014:

This is a timeline of significant North Korean INFOWAR activities since 2004, but the list is not all-inclusive.[5]

- 2004: North Korea gains access to 33 South Korean military communication networks during a joint US-South Korean military exercise.
- June 2006: The US Department of State computer network receives an attack from the East Asia-Pacific region at the same time the US was engaged with North Korea on nuclear missile testing.
- July 2006: The North Korean Unit 121 breaches South Korean and US military networks in South Korea.
- October 2007: North Korea tests a logic bomb.
- June 2009: North Korea publically states that it is fully ready for any form of high-tech war.
- July 2009: Around the American Independence Day, a DarkSeoul distributed denial of service (DDoS) and disk-wiping malware targets US government, South Korean government, media, and financial websites.
- 2009: North Korea likely plants "Operation Troy" malware.
- June 2010: Symantec detects DarkSeoul BackdoorPrioxer.
- October 2010: The Korean Central News Agency website becomes the first known North Korean connection to the Internet.
- March 2011: The "10 Days of Rain" attack by the DarkSeoul DDoS and disk-wiping malware against South Korean media, financial, and critical infrastructure targets occurs. Attacks against South Korean and American military systems also occur.
- March 2011: North Korea jams South Korean GPS.
- 2011: Reports indicate that North Korea attempted to conduct a DDoS attack again the Incheon Airport.
- April 2011: The South Korean Nonghyup Bank receives a DDoS attack.
- June 2012: The South Korean newspaper, JoongAng Ilbo, receives a computer network attack.
- September 2012: North Korea and Iran announce an agreement to combat their common enemies in cyberspace.
- October 2012: South Korean detects the DarkSeoul Downloader.Castov.
- 20 March 2013: Disk-wiping attacks occur against South Korean financial institutions and media organizations not soon after South Korean–American joint military training exercise began on 11 March 2013. The Whois Team later claims responsibility for the attacks.
- March 2013: The New Romantic Cyber Army Team later claims responsibility for the 20 March 2013 attacks.
- 14 March 2013: North Korea experiences a 36-hour Internet outage. The DPRK blames hackers for the attack.
- March 2013: North Korean websites receive a series of attacks from "Anonymous" calling it "#OpNorthKorea."
- April 2013: "Anonymous" allegedly hacks Uriminzokkiri, a North Korean run website, and takes over its Twitter and Flickr pages.
- May 2013: DarkSeoul conducts attacks on South Korean financial institutions.
- June 2013: DarkSeoul conducts DDoS attacks against a South Korean government server.
- September 2013: Information is released on the Kimsuky malware that targeted South Korean think tanks.
- March and April 2014: North Korean drones are found along the North and South Korean border on the southern side. Besides reconnaissance purposes, the drones could also be used to drop propaganda leaflets.

Electronic Warfare (EW)

Electronic Warfare consists of measures conducted to control or deny a military's use of the electromagnetic spectrum. EW capabilities allow an actor to exploit, deceive, degrade, or disrupt, damage, or destroy sensors, processors, and command and control (C2) nodes. As a minimum, EW's goal is to control the use of the electromagnetic spectrum at critical locations and times in the operational environment (OE) to attack a specific system. There are three types of EW: Electronic Attack (EA), Electronic Protection (EP), and Electronic Warfare Support (ES). EA is an offensive attack with the most common method known as jamming. EP is a defensive tactic used to stop EA. ES is used to search for, intercept, identify, and/or locate electromagnetic energy devices.

The North Korean military operates approximately 50 Ground Control Intercept (GCI) and EW bases throughout the country. Each GCI station provides overlapping coverage of the entire country, particularly around the demilitarized

zone (DMZ). Due to their unique relationship, the coverage along the DPRK border with the People's Republic of China (PRC) is significantly lighter than the coverage along the DMZ. The terrain masking caused by the mountainous terrain in North Korean causes gaps in low-altitude coverage of both GCI and EW systems in various parts of the country.

The following chart highlights the North Korean EW systems. Each system is capable of performing EW missions or attacking UAV C2 systems and/or ISR [intelligence, surveillance, and reconnaissance] platforms in support of the North Korean government or military.

DPRK EW Systems	Fixed Wing Aircraft	Rotary Wing Aircraft	Mobile Ground-Based (Various)	Fixed Sites Local/Global (30+/-)	Satellite (0)	Submarine
Communications Intelligence (COMINT)	X	X	X	X		X
Electronics Intelligence (ELINT)	X	X	X	X		
Measurement & Signature Intelligence (MASINT)			X			
Image Intelligence (IMINT)	X	X		X		X
Jamming		X	X			
Electronic Countermeasures (ECM)	X	X				

Jamming

The DPRK government often jams undesirable radio and television broadcasts within North Korea as a means to restrict the flow of information to and from its citizens. The jamming of foreign short-wave radio stations is done with white noise or beeping. The DPRK government knows it cannot jam all the frequencies all the time, so it offers pre-tuned, short-wave radios to its citizens. While black market radios that can receive the normal radio frequencies are available on the gray market, any North Korean found with one faces the possibility of a long sentence in one of the country's many labor camps.

North Korea does not jam any of South Korea's commercial television and radio stations, but does jam any of the stations owned by the South Korean government. Due to recurrent electrical shortages throughout North Korea, there is actually less jamming in the current time period than in the 1970s.

North Korea has the ability to jam signals used by other militaries, often with Russian-designed equipment. Targets include satellites that operate GPS where some reports state a device mounted on vehicles could jam any GPS signal up to 100 km away based upon the equipment's power.[6] North Korea jammed South Korea's GPS signals during a joint US-South Korean military exercise. In April and May 2013, North Korea jammed GPS signals in South Korea for almost two weeks playing havoc with air traffic control and maritime transit. This extensive period of jamming affected 618 Korean passenger planes, 17 American civilian airplanes, 31 other foreign airlines' planes, and one US military aircraft. Additionally, 122 ships reported GPS malfunctions including eight South Korean coast guard patrol boats. The DPRK government in Pyongyang vehemently denied any part in the jamming that took place over the two-week period. North Korea can also jam their enemy's communications, radar, or other equipment through the use of high-power

microwaves. See the Threat Report, "NK GPS Jamming Jun 2012," for detailed information on one of these series of jamming attacks by North Korea on South Korea.[7]

Signals Intelligence (SIGINT)

North Korea uses a variety of Electronic Intelligence Warfare (EIW) units to gather signals intelligence (SIGINT) at all levels. At the national level, these units include the Electronic Warfare Bureau (EWB), the 121st Surveillance Battalion, and the 204th Enemy Attack Bureau. There are also additional EIW units in the North Korean naval and air force units. The Korean People's Army (KPA) EWB administers of all SIGINT, EW, and EIW assets in the military. The EWB coordinates with the Communications Bureau and Reconnaissance Bureau's Technical/ Radio Department to oversee both offensive and defensive EW and EIW operations.

Figure 1. Spoon Rest D radar

At the KPA corps level, the EW/SIGINT Battalion and the Communications Regiment are responsible for EW and SIGINT. At the division level, the EW/SIGINT battalion or company and a communications battalion share responsibility for SIGINT and EW. While it is believed that almost all divisions deployed along the DMZ field an EW/SIGINT company, some rear area divisions may not contain such a unit. No matter what type of division, SIGINT, EW, and EIW trained officers will serve as staff officers. Unique to the forward deployed divisions along the DMZ is a police battalion that commands eight to twelve companies that operates a wide range of ground surveillance equipment, including radar, infrared, and thermal imaging devices, seismic sensors, and acoustic devices.

The DPRK uses the following radar systems for ES. See the Worldwide Equipment Guide (WEG) for more detailed information on selected radar systems' capabilities.[8] Most of these radars are used more often for locating targets rather than jamming signals.

DPRK Radar	Long Range (km)	Medium Range (km)	Short Range (km)	Target Acquisition	Direction Finding	Height Finding	Early Warning	Transportation
5N87 Back Net	300-390	NA	250	Yes	No	No	Yes	Vehicle Mobile
Back Trap	410+	NA	NA	No	No	No	Yes	Vehicle Mobile
Big Back	600+	NA	NA	No	No	No	Yes	Vehicle Mobile
Dog Ear	500	80	25-500	Yes	Yes	No	No	Vehicle Mobile
Fansong* A/B/C/E/F	145 (C, E)	120 (A, B)	40-70 (A-E)	No	No	No	No	Vehicle Mobile
HQ-2 Gin Sling*	95+	NA	NA	Yes	Yes	No	Yes	Vehicle Mobile
Low Blow*	110	NA	80	Yes	No	No	No	Vehicle Mobile

DPRK Radar	Long Range (km)	Medium Range (km)	Short Range (km)	Target Acquisition	Direction Finding	Height Finding	Early Warning	Transportation
Odd Pair	385	NA	250	Yes	No	Yes	No	Vehicle Mobile
P-8 Knife Rest A	370	NA	NA	No	No	No	Yes	Vehicle Mobile
P-10 Knife Rest B/C	185-280	NA	70	No	No	No	Yes	Vehicle Mobile
P-14 Tall King	610+	595	500	No	No	No	Yes	Vehicle Mobile
P-12 Spoon Rest A/C/D	275	NA	NA	Yes	No	No	No	Vehicle Mobile
P-15 Flat Face	250	NA	NA	Yes	No	No	No	Vehicle Mobile
P-15M Squat Eye	200	NA	NA	Yes	No	No	No	Vehicle Mobile
36D6 Tin Shield	360	NA	NA	Yes	No	No	Yes	Vehicle Mobile
SJ-202	UNK	NA	NA	Yes	No	No	No	Vehicle Mobile
Square Pair#	160	NA	NA	Yes	No	No	No	Vehicle Mobile
*Capable of performing fire control functions; # Target acquisition and fire control are a dual use mode								

Signals Reconnaissance

North Korea operates both satellites and unmanned aerial vehicles (UAV) even though the initial satellite launch claimed by the DPRK government in 1998 may have been a hoax. If nothing else is true regarding the DPRK space program, North Korea probably leases satellite service from Russia, China, or Pakistan for military and government use. North Korea has purchased several UAVs from Russia and China for operations along and inside the South Korean border. These UAVs include the PRC D-5, the Pchela-1T, and the DR-3 Reys. See the WEG and the 2008 EIA for additional information on these UAVs' capabilities. Several North Korean UAVs have crashed in South Korea including one in early 2014. The UAVs appeared to be Chinese made, but the company in China denied any involvement in the violation of South Korean airspace.[9]

The DPRK has purchased a number of EW/SIGINT-equipped systems from China, Russia, Iraq, Iran, and Pakistan over the last several decades. While some of the equipment may be obsolete, the equipment is still functional. The Chinese made Hongqi-2 (HQ-2), based on the Russian S-75 (NATO designation: SA-2 Guideline) is a surface-to-air missile system, but it also operates a passive radar designed to identify, acquire, and track strategic bombers, reconnaissance aircraft, air-to-ground missiles, and ballistic missiles. The HQ-2 is also equipped with an anti-jamming device. North Korea also purchased the Kolchuga passive radar system from Ukraine. The Kolchuga operates three detection and tracking stations and is outfitted with a C2 node capable of analysis. All aircraft ELINT/MASINT emissions (autonomous navigation aids, radar altimeters, Doppler radars, fire-control radars, and IFF signals) can be intercepted and analyzed at a 90% probability of target identification and recognition. The DPRK also purchased the "Tamara," another passive radar system from the Czechs. This fully-mobile system can record and analyze all aircraft emissions such as attack and navigation radars, communication radios, terrain-following radars, etc. The Tamara has a range of only 19 km, and requires the placement of systems to continue to track the aircraft.

Computer Warfare (CW)

Computer Warfare consists of attacks that concentrate specifically on the computer systems, networks, and/or nodes. North Korea focuses their CW techniques on South Korean and American systems, especially those used by the military forces stationed on the peninsula. CW activities range from hacking and denial of service to the insertion of malicious software (viruses, worms, logic bombs, or Trojan horses).[10] DPRK CW concentrates on computer systems, networks, and/or C2 nodes. North Korean CW will disrupt military operations, communications, and Internet intelligence collection efforts.

Hacking

In 1998, the DPRK created Unit 121, a military unit dedicated to INFOWAR. In 2008, the estimate of personnel in this INFOWAR unit ranged from approximately 500 to 1,700 individuals. The latest figures from South Korean sources now brings the number to over 5,900 hackers throughout North Korea making the DPRK the third largest cyber unit in the world after the United States and Russia. The organization and relationship between these various INFOWAR units is both convoluted and difficult to determine. In 2007, about 1% of the North Korean military budget was dedicated to INFOWAR. Four other offices or units involved in computer hacking are Office 91 that operates out of the Mangkyungdae district in Pyongyang and is headed by a WPA colonel with a staff of 80 personnel; Lab 110 (or Unit 110) that is purported to contain a technical reconnaissance team responsible for computer network infiltration; the Central party Investigative Group Unit 35 (or Office 35); and Bureau 225 that operates under the control of the Workers' Party of Korea (WPK). Lab 110 possibly uses the name "DarkSeoul" when conducting their attacks against South Korean computer networks. Unit 121 probably trains its personnel at Mirim College, a five-year university that is sometimes referred to as the Automated Warfare Institute (AWI) or the University of the Gifted. Approximately 100 soldiers graduate annually with the skills to hack foreign computer networks.[11]

Denial of Service

The DPRK possesses the ability to conduct advanced DDoS activities with viruses and malicious code. There have been instances in the past where North Korean viruses have brought the South Korean Internet service to a near standstill. In 2013, South Korea blamed North Korea for DDoS against some of their government agencies and media websites. During the previous year, South Korea arrested five individuals affiliated with North Korean hackers who used video games as a medium to launch cyber attacks and infect computers as a DDoS. The DPRK may have also attempted to conduct DDoS against Japanese computer systems and South Korean financial institutes.[12]

Malicious Software

Since at least 2007 when the DPRK reportedly tested its first logic bomb, North Korea has demonstrated the ability to insert malicious software onto targets via the Worldwide Web. In response, the UN Security Council agreed to ban sales of mainframe computers and laptop personal computers to DPRK, but this will not stop North Korea from pursuing its INFOWAR development program. Unit 121 continues to maintain its current skills while improving with new technology purchased from China and Russia.

Information Attack (IA)

Information Attack, also sometimes called Cyber Attack, focuses on the intentional disruption or distortion of information in a manner that supports a comprehensive INFOWAR campaign. Unlike CW attacks that target the information systems, an IA targets the information on the network or computer itself. Attacks to the commercial Internet by civilian hackers have demonstrated the vulnerability of information systems to innovative and flexible penetration, disruption, or distortion techniques. IAs continuously expand upon these methods. North Korea has demonstrated the ability to access websites and change the information on the website. Sometimes, the DPRK has taken responsibility for the attacks in messages left on various webpages.

Note. This article is to be continued in a Part 2 with planned *Red Diamond* publication in early 2015.

Notes

[1] United States Army, Training Circular (TC) 7-100.2, "Opposing Force Tactics," December 2011, p 7-1.
[2] United States Army, "Information Environment Assessment (IEA)," Training and Doctrine Command (TRADOC) G2 Intelligence Support Activity (TRISA) Threats, June 2008.
[3] Hewlett-Packard Development Company, "Profiling an enigma: The mystery of North Korea's cyber threat landscape," HP Security Briefing, Episode 16, August 2014, p 1.
[4] BBC, "North Korea issues mobile phone etiquette guidelines," 29 September 2014; CIA World Factbook, "North Korea," 20 June 2014.
[5] Tim Junio, "More Shots Fired on the Cyber Front: Key Takeaways from Operation Troy," Huffington Post, 11 July 2013; Symantec, "Four Years of DarkSeoul Cyber attacks Against South Korea Continue on Anniversary of Korean War," 26 June 2013; The Jerusalem Post, "Iran, North Korea unite against 'common enemies'," 1 September 2012; Martyn Williams, "North Korea's Internet returns after 36-hour outage," IDG News Service Via Computer World, 15 March 2013; Walter Hickey, "Cyber War: North Korea is Getting Dangerously Good At Knocking Out Networks," Business Insider, 8 June 2012; Sean Gallagher, "North Korea pumps up the GPS jamming in week-long attack," ARS Technical, 9 May 2012; Hewlett-Packard Development Company, "Profiling an enigma: The mystery of North Korea's cyber threat landscape," HP Security Briefing, Episode 16, August 2014, pp 43-44.
[6] Phys Org, "North Korea upgrades jamming devices: report," 6 September 2011.
[7] United States Army, Training and Doctrine Command (TRADOC), Intelligence Support Activity (TRISA), "North Korean Jamming of GPS Systems," June 2012; Walter Hickey, "Cyber War: North Korea is Getting Dangerously Good At Knocking Out Networks," Business Insider, 8 June 2012; Sean Gallagher, "North Korea pumps up the GPS jamming in week-long attack," ARS Technica, 9 May 2012; Voice of America, "North Korea Appears Capable of Jamming GPS Receivers," 6 October 2010; Phys Org, "North Korea upgrades jamming devices: report," 6 September 2011; Bob Brewin, "North Korean GPS Jamming Update," Next Government, 10 May 2012; North Korea Tech, "Pyongyang denies GPS jamming," 19 May 2012; Hewlett-Packard Development Company, "Profiling an enigma: The mystery of North Korea's cyber threat landscape," HP Security Briefing, Episode 16, August 2014, p 36.
[8] Military Periscope, "Weapons/Systems/Platforms: Sensors/Electronics—Ground Radars," Undated; Global Security, "TN87/Back net," Undated; Global Security, "Fan Song," Undated; Global Security, "Gin Sling," Undated; Global Security, "Low Blow," Undated; Global Security, "Knife Rest," Undated; Global Security, "P-14/5N84A/Tall King," Undated; Global Security, "Spoon Rest," Undated; Global Security, "Flat Face," Undated; Global Security, "Tin Shield," Undated.
[9] South China Morning Post, "North Korean Drones Not Theirs Says Chinese Retailer," 6 April 2014; Hewlett-Packard Development Company, "Profiling an enigma: The mystery of North Korea's cyber threat landscape," HP Security Briefing, Episode 16, August 2014, p 36.
[10] A virus is a program or piece of code that is loaded onto a computer without the user's knowledge and runs against their wishes. Viruses can replicate themselves and are manmade. A simple virus is relatively easy to produce. A worm is a program or algorithm that replicates itself over a computer network and usually performs malicious actions, such as using up a computer's resources and possibly shutting the entire computer system down. Logic bombs, also called slag code, is a programming code that is added to an application's software or operating system that lies dormant until a predetermined period of time or event occurs that triggers the code into action. Logic bombs are typically malicious in intent and usually perform in the same manner as a virus or Trojan horse once it is activated. A Trojan horse is a destructive program that masquerades as a benign application. Unlike viruses, Trojan horses do not replicate themselves, but they can be just as destructive. Some Trojan horse programs claim to rid a computer of viruses, but instead actually introduce viruses into the computer or computer system.
[11] Darren Pauli, "NORKS hacker corps reaches 5,900 sworn cyber soldiers – report," The Register, 7 July 2014; Hewlett-Packard Development Company, "Profiling an enigma: The mystery of North Korea's cyber threat landscape," HP Security Briefing, Episode 16, August 2014, pp 2, 20-22, 48-50; Jane's Sentinel Security Assessment, "Strategic Weapons Systems," North Korea, 23 July 2014.
[12] Darren Pauli, "NORKS hacker corps reaches 5,900 sworn cyber soldiers – report," The Register, 7 July 2014; Dancho Danchev, "North Korea ships malware-infected games to South Korean users, uses them to launch DDoS attacks," ZD Net, 7 June 2012; Hewlett-Packard Development Company, "Profiling an enigma: The mystery of North Korea's cyber threat landscape," HP Security Briefing, Episode 16, August 2014, p 26-27.

———————

—What CTID Does for YOU—

- 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.

CTID Points of Contact

Director, CTID	Jon Cleaves	DSN: 552
jon.s.cleaves.civ@mail.mil		913.684.7975
Deputy Director, CTID	Penny Mellies	
penny.l.mellies.civ@mail.mil		684.7920
Operations-Analyst	Dr Jon Moilanen	
jon.h.moilanen.ctr@mail.mil	BMA	684.7928
Product Integration-Analyst	Angela Wilkins	
angela.m.wilkins7.ctr@mail.mil	BMA	684.7929
Research & Analysis	DAC Jennifer Dunn	
jennifer.v.dunn.civ@mail.mil		684.7962
Worldwide Equipment Guide	John Cantin	
john.m.cantin.ctr@mail.mil	BMA	684.7952
Military Analyst	H. David Pendleton	
henry.d.pendleton.ctr@mail.mil	CGI	684.7946
Fusion	DAC Jerry England	
jerry.j.england.civ@mail.mil		684.7934
UK LNO	Warrant Officer Matt Tucker	
matthew.j.tucker28.fm@mail.mil		684-7994
Military Analyst	Laura Deatrick	
laura.m.deatrick.ctr@mail.mil	CGI	684.7925
Military Analyst	Rick Burns	
richard.b.burns4.ctr@mail.mil	BMA	684.7897
Exercise-Training Spt	DAC Walt Williams	
walter.l.williams112.civ@mail.mil		684.7923
Military Analyst	DAC Steffany Trofino	
steffany.a.trofino.civ@mail.mil		684.7943
LNO to JMRC & JRTC	Mike Spight	
michael.g.spight.ctr@mail.mil	CGI	684.7974
LNO to MCTP	BMA Pat Madden	
patrick.m.madden16.ctr@mail.mil		684.7997
Current Operations	LTC Shane Lee	
shane.e.lee.mil@mail.mil		684.7907
Threat Tactics & CoEs LNO	CPT Ari Fisher	
ari.d.fisher.mil@mail.mil		684.7939
Intel Specialist-NTC LNO	DAC Kris Lechowicz	
kristin.d.lechowicz.civ@mail.mil		684.7922
Intel Specialist-Analyst		(TBD)