Operational Environment Enterprise
US TRADOC G2 Intelligence Support Activity

# Red Diamond

Complex Operational Environment
and Threat Integration Directorate

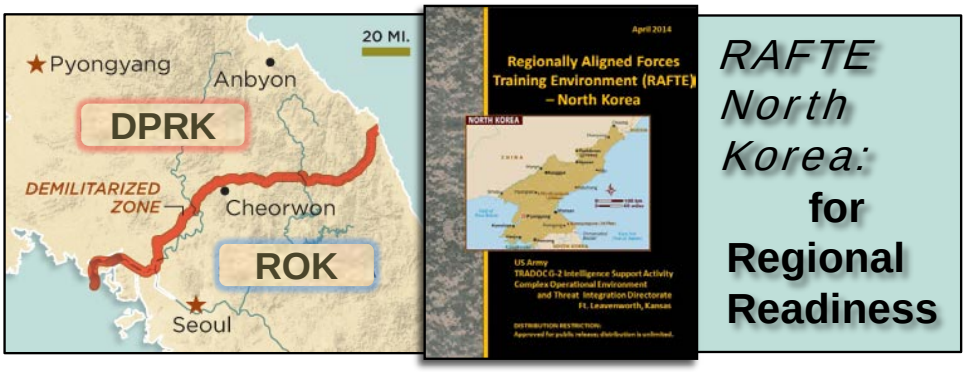
Fort Leavenworth, KS | Volume 5, Issue 5 | MAY 2014

INSIDETHIS 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
BMA Contractor




## RAFTE North Korea: for Regional Readiness

by Angela Wilkins, Operational Environment Assessment Team (BMA Ctr)

TRISA CTID released a second **R**egionally **A**ligned **F**orces **T**raining **E**nvironment (RAFTE) product this month. RAFTEs are supplements to the Army's key source for training, the Decisive Action Training Environment (DATE) version 2.1, which provides operational environment (OE) conditions and opposing force (OPFOR) structure for development of a hybrid threat that will challenge US forces. The DATE document allows for a great deal of flexibility in scenario development, but is not a scenario itself. Despite the breadth of OE conditions and built in flexibility found in DATE, if a unit needs to train for a known part of the world, a RATFE can provide even more streamlined information to trainers to use for a decisive action exercise.

The RAFTE-North Korea identifies the conditions unique to the North Korean OE–meaning they are not captured as part of the baseline conditions in DATE–and describes how to achieve those OE-specific conditions in training by modifying existing DATE conditions. By using a RAFTE, resources and time can be programmed and used more effectively in support of training exercise objectives across all venues.

All RAFTEs are formatted in the same way for ease of application of the information to a DATE-based exercise. The conditions in RAFTEs are identified through the PMESII-PT variable construct. [The acronym PMESII-PT = political, military, economic, social, information, infrastructure, physical environment, and time.]

# *RED DIAMOND* TOPICS OF INTEREST

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

This issue of the *Red Diamond* newsletter spotlights the Regionally Aligned Force Training Environment-North Korea (RAFTE-North Korea). The DATE remains the basis for operational environment (OE) conditions in training.

The Foreign Military Studies Office (FMSO) provides insight on Russian Rapid Reaction Forces (RRF). The Russian Armed Forces are currently experimenting with the establishment of an RRF Command.

The March 2014 terrorist attack at the Serena Hotel in Kabul shook the confidence of Afghans and foreigners within its protective perimeter. The failure in enclave protection was due to lax security.

The BRDM article describes the vehicle's proliferation and variants, specifications, capabilities, and inherent vulnerabilities. The hybrid threat uses the BRDM as readily available and relatively inexpensive.

The cyber lifecycle article focuses on attack and assess phases. The threat uses information warfare (INFOWAR) among its cyber electromagnetic activities.

Rotation 14-04 at the National Training center (NTC) was the fifth DATE rotation that challenged units in complex operational environments and hybrid threat.

Reconnaissance attack is one of several threat offensive actions. This vignette portrays a guerrilla-based hybrid threat tactic against a repressive regional authority.

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, 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)

The TRADOC G2 Operational Environment Enterprise (G2 OEE) is developing a series of integrated training products that provide the Army Soldier, leader, and Army civilian with a "G2 Starter Kit" on threat opposing force (OPFOR) tactics and techniques for improved Army readiness in training, professional education, and leader development. The TRISA Complex Operational Environment and Threat Integration Directorate (CTID) is the lead proponent for coordinating this TRADOC G2 multimedia suite of tactical actions and enabling functions, modeling analysis, combat camera-like episodes from collective training events, and ability to complement the family of live, constructive, virtual, and gaming simulations. Other principle G2 partners in this initiative are the TRISA Operational Environment Laboratory; TRISA Wargaming, Experimentation, Test and Evaluation Directorate (WETED); and the Training Brain Operations Center (TBOC).

A prototype of the integrated training product "G2 Starter Kit" is a PDF document with instructional presentations on a threat *raid* tactic and training publications, One Semi-Automated Forces (OneSAF) models and simulations analysis, embedded TBOC simulations, and other G2 OEE resources. A link will be available soon on Army Training Network (ATN).

An epub designed for mobile devices is another prototype initiative. When this epub is formally released in the near future, you will download the program file to your common access card (CAC)-enabled machine. Moving the file via CD-ROM to a location that allows you to move the file to your mobile device, you can view on iOS devices in iBooks and on android devices if you use Gitden Reader (a free epub reader) and view this epub version 3 ebook. There are other free epub readers for android, but if they don't support epub version 3 you will not be able to view the videos in this epub.


**Figure 1. Cover snapshot of integrated training products G2 starter kit for raid tactic (prototype)**

TRISA-CTID will provide an update on the PDF package and epub in the *Red Diamond* when this Army learning initiative is fully operational. These capabilities will enhance home station training, collective training, and self development.

***JON***

 *(Continued from p.1)*

For each unique condition, a definition is provided for understanding, then the manifestation of that condition in the North Korean OE is clearly explained. Finally, trainers are provided with a *possible* way to modify conditions in DATE to make them match the specific OE conditions needed for training exercises (application of condition to DATE). Below is an example from *RAFTE-North Korea* of a North Korean Military condition:

**Unique North Korean Condition: *Government Embraces the Concept of a Preemptive Attack***

**Definition of Condition:** A country publically declares that it possesses the right to preemptively strike against any country deemed to be an enemy.

**North Korean Manifestation of Condition:** The North Korean government has publically announced that it will attack first any perceived enemy if it feels the country is threatened. In the past, North Korea sank the South Korean ship, the Cheonan, with no warning. North Korea has also moved artillery and missiles to its border with South Korea, and also to the eastern coast of the Korean peninsula, within shelling range of Japanese Islands.

**Application of Condition to DATE: *Make one of the DATE countries announce a preemptive strike policy:***

***Ariana.*** Fearing isolation from the West, Ariana announces that it will conduct preemptive strikes against Israel, the United States, Western Europe, or any other country that it feels is a threat to the continuation of the current Arianian regime. **The Arianian military initiates actions prerequisite for launching a preemptive strike.**

Note that the "Application of Condition to DATE" section is, as stated above, only a possible way to make the necessary modification to DATE to achieve the unique North Korean condition. Trainers and scenario writers can make other DATE-compliant modifications as necessary to achieve required training tasks.

The second section of each RAFTE tells trainers if there are baseline conditions in DATE that are NOT present in the RAFTE's OE. For instance, in DATE, there are theocracies, but not in North Korea. So, in the Political section of the RAFTE-North Korea, theocracy is identified as a condition in DATE, but not in North Korea, as North Korea is controlled by a secular, communist government that is led, essentially, by one man. Therefore, while using DATE to train for North Korea, it should be noted that a country with a theocratic government would not apply for scenario development.

**RAFTE**

**A RAFTE (pronounced "raft," not "rafty") is a *supplement* to DATE that can be used when training must occur for operations in a known part of the world. A RAFTE identifies the conditions of a selected operational environment (OE) that are unique from what is already in the DATE. It will enable training based on current conditions specific to an OE, in this case North Korea. RAFTEs are different but not separate from the DATE.**

Questions or comments about RAFTE-North Korea, DATE, RAFTE-Africa, or the upcoming RAFTE-Pacific should be addressed to the OEA Team at TRISA-CTID. Contact information is included on the last page of each *Red Diamond* newsletter.


by Charles Bartles, TRISA Foreign Military Studies Office (FMSO)

Since the collapse of the Soviet Union, the Russian military has struggled to match its forces against likely threats. It has been slow in transitioning from a large conscript army focused on large-scale, high intensity warfare with NATO to one focused more on immediate threats, namely small-scale regional conflicts, terrorism, proliferation, and insurgency. These types of threats are often handled by units called rapid reaction forces (RRF), such as the usual first responders – i.e., the Russian Airborne forces (VDV) – but the term has been used in an ad-hoc manner. In order to combat these challenges and perform peacekeeping duties, the Russian Armed Forces are currently experimenting with the establishment of an RRF Command. This is not a new concept in the Russian Armed Forces; the idea has been discussed several times since the collapse of the Soviet Union.[1] In the last year the issue has again gained momentum, culminating in a November 2013 announcement that the RRF Command would be activated in 2014. Although the details are still being worked out, the Russian RRF will be approximately 70,000-80,000 members strong, primarily built around the VDV. These forces are apparently intended to have an air-land-sea capability, and would be well suited to handle current threats, as well as to perform peacekeeping duties.[2]

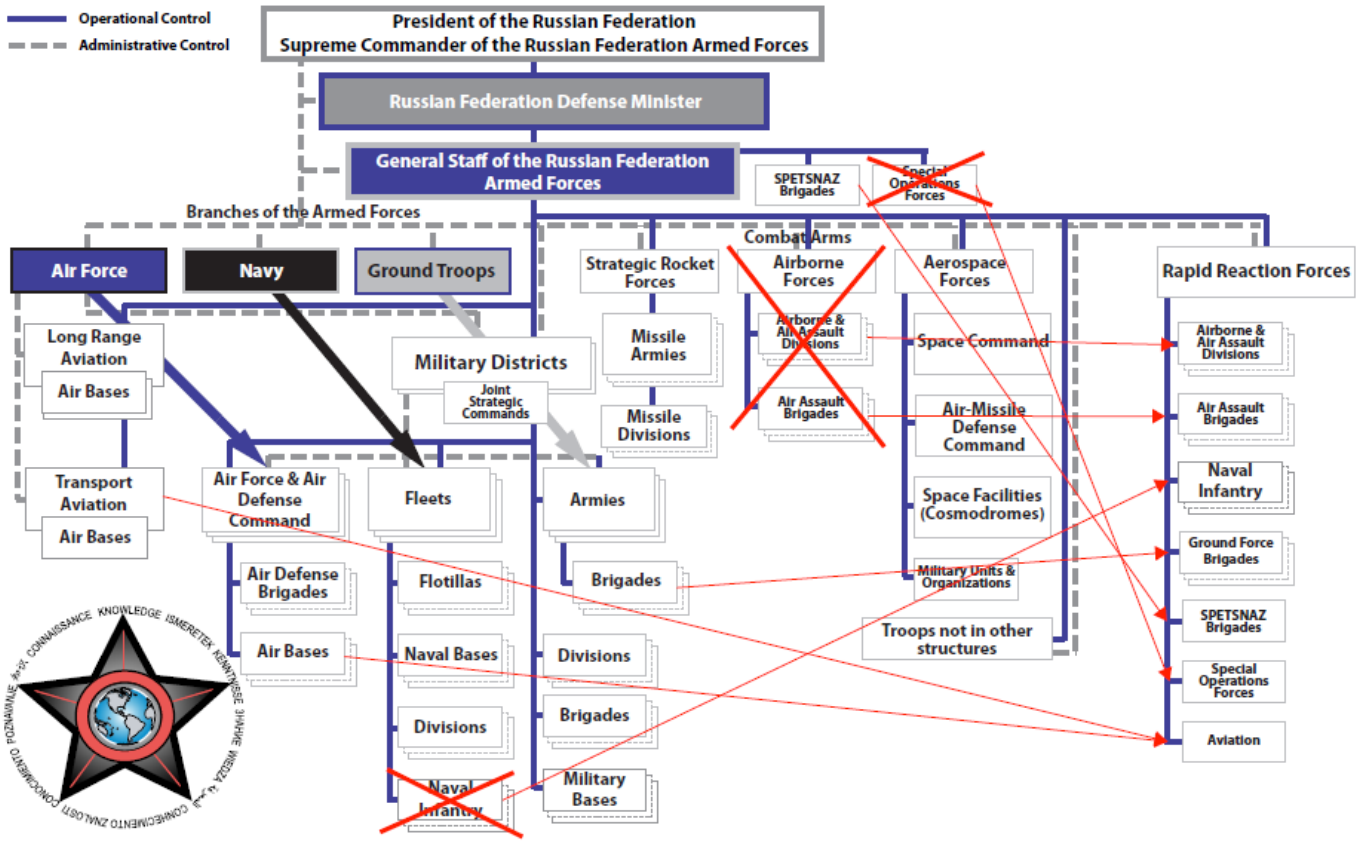



**Figure 1. Proposed Russian rapid reaction force (example) *Source:* FMSO**

**Air**

In order to quickly deploy forces, proponents of the Russian RRF suggest that an organic lift capability is required for the organization. In the current scheme of organization the VDV are required to request aircraft for long-distance transport and jump operations through the Transport Aviation Command (VTA), which is part of the Russian Air Force. By the same token, VDV and Ground Force commanders must request Army aviation (helicopter, light reconnaissance, and tactical strike) support through the Air Force.[3] In the new scheme, select elements of Army aviation and VTA that are in support of the RRF would be placed under operational control of the RRF commander.[4] Even under the most optimistic proposals of RRF proponents, it is almost a certainty that any major movement (air, land, or sea) would require some level of support from the Russian Transportation Directorate (VOCO), which is very roughly the US TRANSCOM equivalent.[5]

**Land**

The land component of the RRF is based upon three motorized rifle brigades (MRB) and select SPETSNAZ units. Relative to their strategic purpose, these units are located in or near internal hot spots, such as the volatile North Caucuses region, and external hotspots, such as Georgia and Armenia, where direct action or peacekeeping assets could be required on short order. The 34th MRB (Mountain) in Zelenchukskaya, Karachay-Cherkessia, and the 33rd Reconnaissance Brigade (Mountain) in the city of Botlikh in the Republic of Dagestan are the primary force projection components of the proposed RRF land assets.[6] (The 33rd Reconnaissance Brigade would probably be better termed as a reduced strength MRB.)[7]

Traditionally in the Soviet/Russian model of armed forces, peacekeeping activities have typically been delegated to select VDV units. The VDV still have the majority of peacekeeping assets in the Russian Armed Forces, with one brigade (31st Air Assault Brigade, Ulyanovsk) dedicated to general peacekeeping and several other battalions trained for operations in a United Nations "blue helmet" capacity.[8] The Russian Ground Forces' 15th Separate MRB (Peacekeeping) in Samara is Russia's first attempt to design a unit from the "ground up" as a peacekeeping unit, instead of simply designating existing units with the task.[9]


**Figure 2. Russian airborne division in rapid reaction force model (example) *Source:* FMSO**

There has been reporting that select SPETSNAZ brigades would be included in the RRF. It is unlikely that all SPETSNAZ brigades will be placed in the RRF, as the former are the "eyes and ears" of the Intelligence Directorate of the General Staff and are also used for direct action in the enemy rear to support conventional Ground Forces movement. SPETSNAZ brigades usually consist of three detachments (*otriads*), which are roughly battalion-sized elements commanded by a colonel. These brigades are deemed "elite," but they are often manned with conscripts, as opposed to contract soldiers

(*kontraktniki*). As a whole, SPETSNAZ brigades have a higher percentage of *kontraktniki* than the average Ground Forces unit, but a lower percentage of *kontraktniki* than the average VDV unit.

**Sea**

The RRF will include all Naval Infantry assets. The Naval Infantry is currently part of the Coastal Defense Troops, along with the Coastal Defense Artillery. Naval Infantry units are co-located with each of the four fleets and one flotilla, totaling approximately 9,000 troops. It is already in the process of a major overhaul to improve equipment and training, and has recently announced plans to expand by turning the 3rd Naval Infantry Regiment of the Pacific Fleet and the 61st Naval Infantry Regiment of the Northern Fleet into full fledged brigades.[10] The Naval Infantry enjoys close ties with the VDV, dating at least back to the Great Patriotic War, when certain Naval Infantry units were commanded by VDV officers.[11] The close ties have continued to today, as Naval Infantry units have select units on jump status, and naval infantrymen routinely train at the VDV training center in Ryazan. The current commander of the Coastal Defense Troops is a career VDV officer.[12] As for other naval assets, there has been some mention of including large amphibious landing craft in the RRF. Although not specifically mentioned, several companies of Naval SPETSNAZ could also be included.

**Special Operations Forces**

As with the SPETSNAZ brigades, Russian special operations forces are currently under direct control of the Intelligence Directorate of the General Staff. There has been little reporting on the size or units in these forces, but in the Russian system all special operations forces are SPETSNAZ units, but not all SPETSNAZ units are special operations forces, so it is likely that the latter are collocated with SPETSNAZ brigades.[13] Presumably, Russian special operations forces conduct similar activities as their US counterparts, but, in contrast to US special operations forces, the premier Russian special operations forces are under the jurisdiction of the Russian Federal Security Service. Although current plans call for the inclusion of special operations forces in the RRF, it seems difficult to believe the Intelligence Directorate of the General Staff would surrender such an asset.

**Airborne (VDV)**

The core of the Russian RRF is built around the VDV, with approximately 35,000 paratroopers. The Russian VDV is significantly different than its Western counterparts: structurally the VDV is a mechanized force and is divided between parachute and air assault units. In terms of function, the Russian VDV fulfills many of the same roles as those in the West, but also fills another niche not filled by Western airborne forces, that of a reliable enforcer for politically sensitive operations. This role began in Soviet times, with the Soviet invasion of Hungary in 1956 to quell the Hungarian uprising. VDV units began quietly occupying Hungary weeks before overt Soviet action began, and after the commencement of hostilities they gained a reputation for quickly and efficiently seizing objectives in an urban battle space to which conventional Soviet commanders were not accustomed. In all, 1,710 paratroopers were decorated in the Hungarian campaign, including four recipients of the Soviet Union's highest award, the Hero of the Soviet Union. In total, the VDV garnered 18% of the total medals awarded for the campaign, despite only having 6% of the troops. The VDV's actions in Hungary set a precedent in the Soviet Armed Forces of using the VDV as special operation forces are used in the West, namely to enter an area of operations discretely and then begin conducting operations. This pattern played out again in the 1968 Czech uprising, when the VDV flew into the Prague Airport in commercial aircraft and then began fanning out through the city with commandeered vehicles in order to quickly secure Czech command and control and communications infrastructure. This role of the VDV in Soviet times has undoubtedly been inherited by today's Russian VDV.[14] Although exact details have yet to emerge, there has been reporting that VDV units are involved in current operations in Crimea, and if previous behaviors are indicators of current activities, it will likely be discovered that the VDV elements began arriving there well before masked gunmen started showing up on the streets of Crimea.[15]

**Command and Control**

The VDV headquarters will be expanded to provide command and control of the RRF, and there has been reporting that the 38th Signal Regiment at Medvesh Ozera will be elevated to a command and control brigade.[16] What is less certain is where the RRF will fall as an organization in the Ministry of Defense hierarchy. There has been command initiative given to placing them at the four-star level, putting the organization on par with the four operational strategic commands, among which the country is divided.[17] Another possibility is that a newly formed RRF would simply attain the same

position in the Russian Ministry of Defense hierarchy that the VDV currently occupies, that of an independent branch of the Armed Forces, commanded by a three-star level officer.

**Strategic Land Power**

From a Russian perspective, if the RRF is put at the same level as the four regional operational strategic commands, by definition they will be considered as a functional strategic asset. Even if the RRF are placed in some other command, however, these forces will likely still be regarded as a strategic asset by Russia, because the Russians view the tactical, operational, and strategic levels of warfare differently than the West. In the West these levels are typically defined by echelon size (battalion, corps, army, front, theater, task force, etc.), but in the Russian system these levels are more nuanced. The Russian system defines them not by the echelon of the unit, but rather by the unit's scope of mission. For instance, a corps operating under an army group would be considered to be acting at a tactical level, but if the same corps were detached and began operating under a front-level command, it would be considered to be acting at the operational level. By the same token, a brigade is usually considered to act at the tactical level, but in a conflict with a much smaller opponent like in the Russo-Georgian War, a brigade could be a "war winner," and therefore be a strategic asset.[18] Given that at least some components of the RRF will probably engage in most, if not all high profile missions, they will most likely be considered a strategic asset, and a true strategic land power.

**CSTO Obligations**

In Russia's capacity as the unofficial leader of the Collective Security Treaty Organization (CSTO), the Russian Federation established a Collective Rapid Reaction Force (CRRF) of CSTO member states, with a focus on Central Asia. "The agreement on the CRRF was signed on June 14, 2009 which aimed at repelling aggression, carrying out special operation[s] and fighting terrorism. The CRRF is also responsible for responding to emergency situations and providing emergency humanitarian assistance, reinforcing armed forces covering national borders and guarding member-states' public and military facilities, and resolving challenges identified by the CSTO's Collective Security Council."[19] The Russian Federation satisfies its CSTO obligations with two VDV units (98th Airborne Division and the 31st Air Assault Brigade) that are dual-hatted as being both in the Russian and CSTO RRF.

The 2010 riots in Osh, Kyrgyzstan, caused something of a crisis when the Kyrgyz President requested CSTO assistance to quell the violence. The request was officially denied because it was solely an "internal matter," but there was later some back pedaling that the situation could have been handled differently.[20] The lesson for Russia in this instance may well have been that although multilateral security organizations appeal to a sense of international cooperation, they are often not expedient, and consensus does not always reach the right (Russian-desired) outcome. In short, multilateral cooperation is good, but not always reliable, requiring the Russian Federation to keep its own assets to handle such situations, if required.

**Outlook**

Despite a November announcement that the RRF would be operational this year, there has been no reporting as of yet on the establishment of the RRF.[21] The official rollout of the RRF may have been put on hold due to the crisis in Ukraine or other unrelated matters. As some reporting explains, the core components of the proposed RRF (VDV, Naval Infantry, SPETSNAZ) are already operating in Crimea, raising the possibility that the RRF have already been activated and Crimea may be their first campaign.[22]

**Notes**

[1] Roger N. McDermott, Jamestown Foundation, *Moscow Plans Rapid Reaction Forces and Professional Soldiers Again*, 12 March 2013, Eurasia Daily Monitor Volume: 10 Issue: 46, available at: http://www.refworld.org/docid/51407c6c2.html, accessed 16 March 2014.

[2] Vladimir Mukhin, "Vladimir Shamanov is Ready for Rapid Reactions: Yet Another Combat Arm will Become an Effective Reserve of the Supreme Commander in Chief." *Nezavisimaya Gazeta* Online 19-23 April 2013,< http://www.ng.ru/>, accessed 16 March 2014.

[3] Col. (ret.) Nikolai Malyshev, Lt. Col. Ivan Korolyov, Lt. Col. Vyacheslav Silyuntsev, "Army Aviation Today," *Military Thought*, Volume 4, 2013.

[4] Vladimir Mukhin, "Vladimir Shamanov's Rapid Reaction: An Edict on the Formation of a New Type of Troops Could Be Signed by the End of the Year," *Nezavisimaya Gazeta* Online, 18 November 2013, < http://www.ng.ru/>, accessed 17 March 2013.

[5] Roger N. McDermott, "Russia's Strategic Mobility: Supporting 'Hard Power' to 2020?", *Swedish Defence Research Agency*, April 2013,< http://www.foi.se/ReportFiles/foir_3587.pdf>.

[6] Vladimir Mukhin, "Vladimir Shamanov's Rapid Reaction: An Edict on the Formation of a New Type of Troops Could Be Signed by the End of the Year," *Nezavisimaya Gazeta* Online, 18 November 2013, <http://www.ng.ru/>, accessed 17 March 2013.

[7] Georgian military affairs website:http://www.geo-army.ge/index.php?option=com_content&view=article&id=221&Itemid=120&lang=en,accessed 17 March 2014.
[8] Andrey Bondarenko, "Peacekeepers in Blue Berets," *Red Star*, 18 June 2013, <http://www.redstar.ru>, accessed 16 March 2014.
[9] Vladimir Mukhin, "Special Forces Have Taken Aim at Sochi. Armed Conflicts on Russia's Borders Are Possible This Fall," *Nezavisimaya Gazeta* Online, 14 May 2013, <http://www.ng.ru/>, accessed 17 March 2014.
[10] Naval Infantry Brigades to be Reestablished in Pacific, Northern Fleets" *RIA Novosti* Online, 27 November 2013, < http://rian.ru/ >, accessed 17 March 201; Russian Federation Ministry of Defense Website, "Navy Coastal Defense Troops Chief Major-General Aleksandr Kolpachenko Tells of the Development of the Coastal Defense Troops and Naval Infantry," 1 January 2014, <http://www.mil.ru>, accessed 17 March 2014.
[11] Steve Zaloga, *Inside the Blue Berets: A Combat History of Soviet and Russian Airborne Forces, 1930-1995*. Novato, CA: Presidio, 1995.
[12] Russian Wikipedia website: <ru.wikipedia.org/wiki/Колпаченко,_Александр_Николаевич>, accessed 17 March 2014.
[13] Yuriy Gavrilov, "The General Staff Has Been Authorized To Report: Russia Is Creating Special Operations Forces," *Rossiyskaya Gazeta*, 7 March 2013, <http://rg.ru/> , accessed 17 March 2014; William H. Burgess, *Inside Spetsnaz : Soviet Special Operations : A Critical Analysis*, Novato, CA: Presidio, 1990.
[14] Steve Zaloga, *Inside the Blue Berets: A Combat History of Soviet and Russian Airborne Forces, 1930-1995*. Novato, CA: Presidio, 1995.
[15] 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, <http://top.rbc.ru/politics/06/03/2014/909718.shtml>, accessed 17 March 2014.
[16] Vladimir Mukhin, "Vladimir Shamanov's Rapid Reaction: An Edict on the Formation of a New Type of Troops Could Be Signed by the End of the Year," *Nezavisimaya Gazeta* Online, 18 November 2013, <http://www.ng.ru/>, accessed 17 March 2013.
[17] Igor Andreyev, "Shamanov: Russia Needs a Fifth Military District, Mobile and Peacekeeping," *RIA Novosti* Online, 24 April 2013, < http://rian.ru/ >, accessed 17 March 2014.
[18] David M. Glantz, *Soviet Military Operational Art: In Pursuit of Deep Battle*, London, England: F. Cass, 1991; Author's conversation with COL (ret.) David M. Glantz on 19 December 2013.
[19] Dadan Upadhyay, "NATO versus CSTO: The Clash between Competing Military Alliances," *Global Research* website 11 January 2012, <http://www.globalresearch.ca/nato-versus-csto-the-clash-between-competing-military-alliances/28612 >, accessed 17 March 2014.
[20] "CSTO Made no Blunders In Kyrgyzstan Violence" *RIA Novosti* Online, 10 December 2010,<http://en.ria.ru/exsoviet/20101210/161720235.html>, accessed 17 March 2014.
[21] Vladimir Mukhin, "Vladimir Shamanov's Rapid Reaction: An Edict on the Formation of a New Type of Troops Could Be Signed by the End of the Year," *Nezavisimaya Gazeta* Online, 18 November 2013, <http://www.ng.ru/>, accessed 17 March 2013.
[22] 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, <http://top.rbc.ru/politics/06/03/2014/909718.shtml>, accessed 17 March 2014.

---

# THE BRDM: THE MULTI-PURPOSE RECONNAISSANCE VEHICLE

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

In 1957, when the *Bronirovannaya Razvedyvatelnaya Dozornaya Mashina* (BRDM) scout car made its debut in the Soviet Union, few could have predicted that over the next 50 years this vehicle would become one of the primary reconnaissance vehicles in the military of over 80 countries, serve as the chassis for a number of anti-tank weapons, and eventually come to be used as a platform for an anti-aircraft weapons system.

Wherever American soldiers may deploy in the world today, it is very likely that they will encounter some type of BRDM variant—used either by a hybrid threat or friendly coalition forces. Knowing the capabilities as well as the vulnerabilities of the BRDM family of vehicles will enable American forces to either defeat the hybrid threat or serve our allies in the most advantageous manner possible. The Threat Report, *The BRDM Scout Car,* released by CTID in May 2014, highlights the vehicle's proliferation; describes the BRDM's specifications, capabilities, and variants; explains the vehicle's inherent weaknesses that can be exploited by adversaries; and depicts ways in which the hybrid threat may deploy the BRDM.

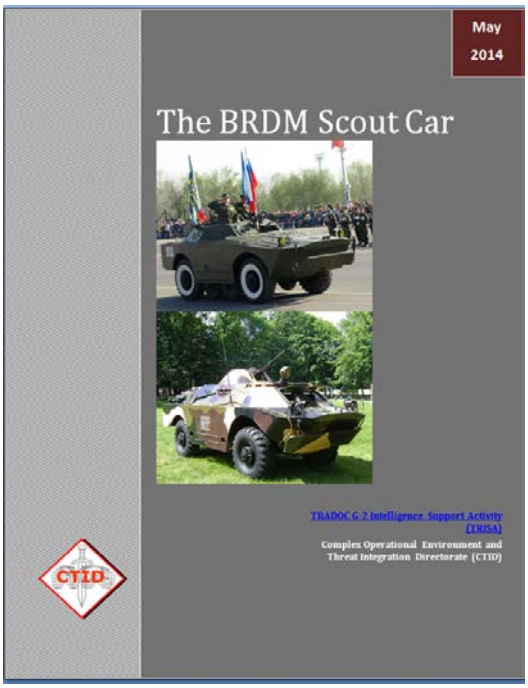
The world's militaries or police forces in over 80 countries use some form of BRDM variant. Somewhere between 6,800 and over 10,000 of the vehicles remain in active service or in a reserve status. Ten countries still operate the very outdated BRDM-1s, 41 countries use only BRDM-2 or its more modern variants, the remaining countries use combined fleets of BRDM-1s and BRDM-2s.

While initially fielded as a reconnaissance vehicle, many variants exist, including some that feature anti-tank guided missile (ATGM) systems such as the AT-3 Sagger, the AT-4 Spigot, or the AT-5 Spandrel. Other BRDM variations include

those tailored for nuclear, biological, and chemical (NBC) detection; command and control purposes; or in the case of the SA-9 Gaskin surface-to-air missile, air defense artillery.

**BRDM History**

The BRDM, now called the BRDM-1, first appeared in 1957 as a scout car with 4 X 4 off-road capabilities, and was designed to keep pace with the Soviet PT-76 light tank on reconnaissance missions. The literal translation of the Russian Разведывательная Дозорная Машина (Soviet nomenclature for the BRDM) is "armored reconnaissance/patrol vehicle." Over several decades, the Soviet Union produced more than 10,000 BRDMs, including its several variant models. The vehicle could lower four belly wheels housed in its interior to improve traction and to cross small ditches. It could also cross water obstacles by means of a rear-mounted water jet.




Despite the improved capabilities of BRDMs over World War II era scout vehicles, they contained several flaws. In 1963, the Soviet Union introduced the BRDM-2 to correct the following perceived vehicle deficiencies: the gunner needed to expose himself to enemy fire in order to use the vehicle's weapons systems, a lack of NBC protection, and no night-driving capability. The BRDM-2 eliminated most of these problems by moving the engine to the vehicle's rear; improving road, off-road, and amphibious capabilities; introducing an NBC overpressure system designed to protect the crew when the hatches were all closed; and furnishing both the driver and commander with night vision equipment. By the time the BRDM-2 assembly line shut down in 1989, the Soviet Union had produced over 7,200 vehicles and exported them to approximately 40 countries.

**BRDM-1**

The original BRDM along with its variants all possessed essentially the same characteristics. The vehicle could travel 90 km/h on the road and 9 km/h on the water, and had a standard cruising range of 750 km. A typical crew consisted of four men, including a driver, co-driver, commander, and gunner. Armor thickness varied, but was 10 mm deep at the vehicle's front end, where the greatest enemy threat was expected. The basic version of the BRDM came equipped with primary armament consisting of either the 12.7-mm DShK (*Degtyaryova-Shpagina Krupnokaliberny)* 1938/46 heavy machine gun or a 14.5-mm KPV (*Krupnokaliberniy Pulemyot Vladimirova)* heavy machine gun. Secondary weapons on many versions included two 7.62-mm SGMB medium machine guns on side pintle mounts, based on a variant of the SG-43 Goryunov machine gun. Major variants of the BRDM-1 were the BRDM-Rkh radiological-chemical reconnaissance vehicle; the BRDM-U command vehicle; and anti-tank platforms that featured the AT-1 Snapper, AT-2 Swatter, or AT-3 Sagger anti-tank missile systems.

**BRDM-2**

The BRDM-2 corrected several drawbacks associated with its predecessor. Besides those improvements already mentioned, the newer BRDM model protected the gunner with a turret, featured a centralized tire pressure regulation system, and added an infrared searchlight. Retaining a crew of four, other improvements included a road speed that increased to 95 km/h and a swifter water speed of 10 km/h, thicker armor all around with a maximum of 14 mm in the hull nose plate, the placement of an internal winch mounted in the front of the hull (for self-recovery purposes), and individual firing ports on both sides of the hull. The primary turret-mounted weapon was typically the 14.5-mm KPVT (*Krupnokaliberniy Pulemyot Vladimirova)* heavy machine gun, augmented by a single 7.62-mm *Pulemyot Kalashnikova* (PKT) coaxial mounted machine gun. Variants of the newer model included the BRDM-2Rkh radiological-chemical reconnaissance vehicle; the BRDM-2U, BRDM-2K, or R-1A/R-5 command vehicles; the 9P122 with AT-3 Sagger; the

9P124 with AT-2 Swatter; the 9P133 with AT-3C Sagger; the 9P137 with AT-5 Spandrel; the 9P148 with either the AT-4 Spigot or AT-5; and the SA-9 Gaskin anti-aircraft missile system.

**Proliferation**

Although the Soviet Union initially manufactured the BRDM, other former Soviet bloc countries still produce variants of the vehicle or continue to upgrade their existing stocks. These variants include the BRDM-B (BRDM-2s overhauled by the Czech Republic); the BRDM-2 Model 96i; the BRDM-2-M97 (Zbik-B or BRDM-2B); and the BRDM-2-M98 (Zbik-A/BRDM-2A), manufactured in Poland. Russia continues to upgrade BRDMs produced by the Soviet Union at the Arzamas Machinery Plant, formally designating them as BRDM-2As. These models have an increased on-the-road operating speed of 110 km/h. Russia has also installed the HOT-3 Anti-Tank Missile system, produced by a European consortium led by France and Germany, on some of its BRDMs.

BRDMs are also available for purchase through civilian channels. Advertisements on the Internet can be easily found enjoining the public to buy BRDMs at a starting price of only $6,680. Prices vary depending on the individual vehicle's age, condition, and number of miles driven. These prices range from $22,999 for a 1983 BRDM-2 in good condition with 248 miles on its odometer, to $25,500 for a 1990 BRDM-2 with 620 odometer miles, in ideal condition. While these vehicles are advertized as no longer capable of meeting combat readiness standards, for a reasonable price they probably can be retrofitted with armaments and other equipment tailored to meet the needs of prospective purchasers.

**BRDM Weaknesses and Hybrid Threat Adaptations**

Both the BRDM-1 and BRDM-2 share similar weaknesses. The parts of the vehicles most vulnerable for attack include the side panels above the four main wheels, the driver's compartment, the area between the wheel wells, the top and bottom where the hull armor is thinnest, the tires, the rear fuel tanks on the BRDM-2, and the back of the BRDM-2's turret.

The hybrid threat could employ the BRDM in a number of ways: as a scout vehicle for use by conventional or non-conventional forces; as a personnel carrier with additional troops riding on the vehicle's exterior; as an anti-tank missile platform; as an anti-aircraft system; or as a command vehicle, communications vehicle, convoy security vehicle, forward observation vehicle, or even as a forward support supply vehicle. The BRDM's ability to traverse difficult terrain while protecting its occupants against small arms fire renders the vehicle suitable for a broad spectrum of purposes.

The hybrid threat may use the BRDM for a number of reasons. First, BRDMs are readily available, as there are approximately 80 countries that still use one or more of its variants. Second, the BRDM is relatively inexpensive compared with other military vehicles, especially armor. While the purchase price of a modern main battle tank is at least $4 million, BRDMs equipped with older model anti-tank missile systems can be acquired for less than three percent of that amount. Finally, wheeled military vehicles are cheaper to operate and require less maintenance than tracked vehicles.

Wherever the American military deploys in the world, it is likely to find a BRDM on the battlefield. Sun Tzu wrote in *The Art of War*, "If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle."[1] Knowing the capabilities and limitations of the hybrid threats' weapons systems is the first step for soldiers to be successful on the battlefield. For more details, see the BRDM Threat Report on Army Training Network (ATN).

**Notes**

[1] Military Quotes, "Sun Tzu Quotes, The Art of War Quotes, Sun Tzu Quotations.


by Jerry England, Threat Assessment Team (DAC)

Military operations rely on Information and Communications Technology (ICT) more now than ever before. The exposure of military systems and information resources to cyber attack is a reality as more warfighting functions become integrated with software and computer applications. As the threat continues to develop offensive cyber operations, the risk of computer warfare and information attack against friendly capabilities increases. For this reason, understanding the tactics and techniques of cyber attacks is a useful approach to addressing this emerging element of the hybrid threat. Devising a model for threat cyber operations based on current tactics and terminology will assist exercise designers to include threat cyber operations and meet future training objectives. The discussion below illustrates a model for describing the threat cyber attack lifecycle that focuses on exploiting the target for threat offensive cyber operations.

**Cyber Attack Lifecycle (Recap)**

The threat conducts cyber attacks through a six-step process designated the Cyber Attack Lifecycle. The six steps may or may not occur sequentially and the threat can skip or repeat steps as it is appropriate. The steps in the Cyber Attack Lifecycle are —

- Reconnaissance.
- Infiltration.
- Establish Command and Control (C2) (formerly Establish Lodgment).
- Exploit Target.
- Deliver Attack.
- Assess and Exploit Effects.

**DELIVER ATTACK**

Threat attack techniques vary based on tactical tasks, objective, and the desired end state. Attacks can compromise future access to a target system. For this reason, the threat will evaluate the value of the target system and the intelligence it provides before deciding whether to deny, degrade, or destroy the target. Even for data harvesting operations, such as persistent threats, the downloading of large volumes of data could trigger alarms in the enemy's cyber defense system and may cause the enemy to patch the previously undiscovered vulnerability and thus render the system unavailable for future exploitation. When the decision to launch the attack is made, the threat must consider the second and third order effects of the attack. If the threat requires uninterrupted access to the target for future operations, the threat must weigh the risk of discovery now against the need for future access before choosing that course of action. The risk associated with the attack can be characterized by the chance of compromise that might stop future exploitation and the relative payoff for the immediate attack. The operational requirements to consider are —

- Protection and security.
- Precision.
- Sustained effects.

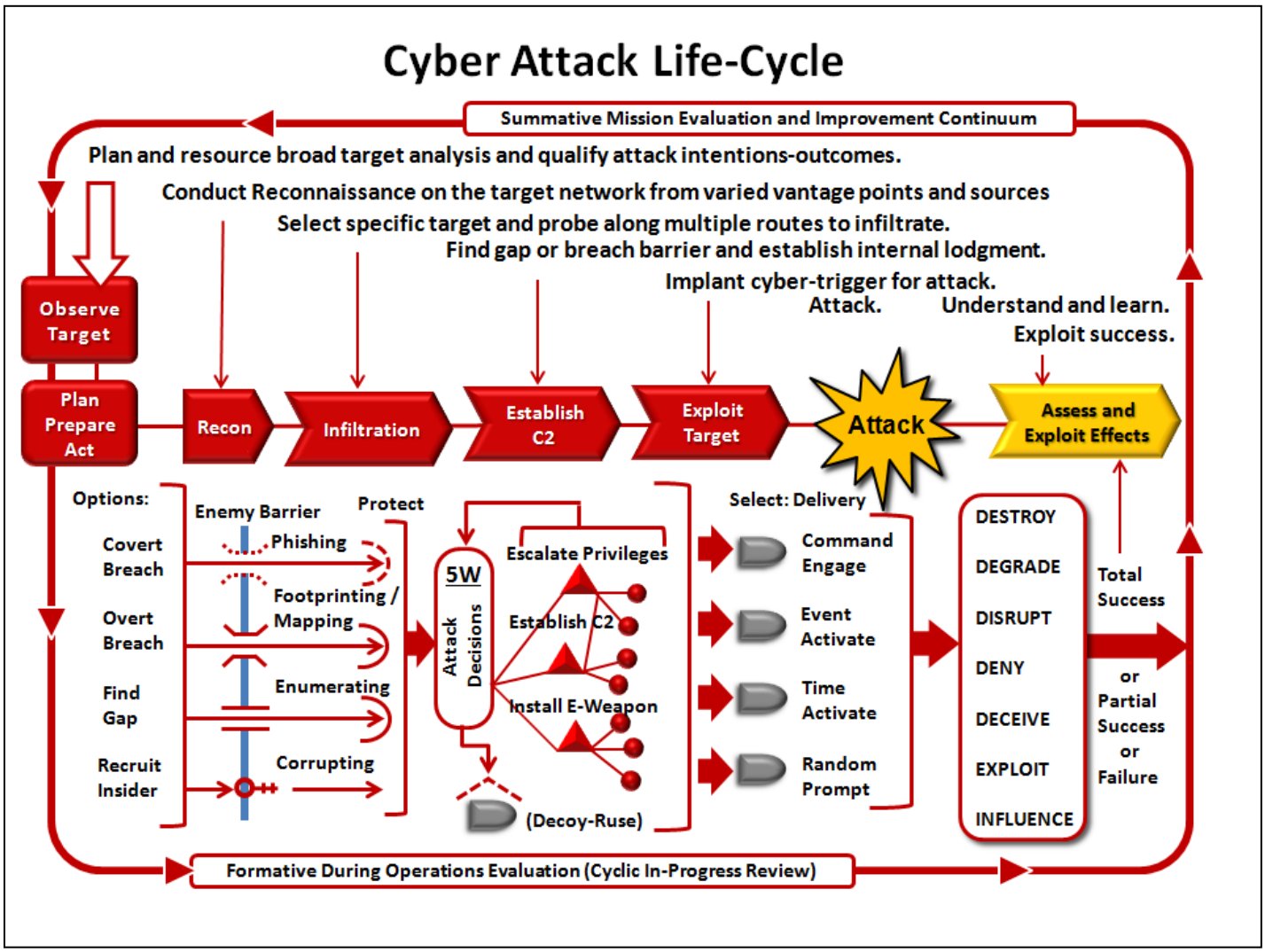



**Figure 1. Cyber attack lifecycle *Source:* TRISA-CTID (2013)**

**Protection and Security Measures**

Protection and security measures encompass a wide range of activities, incorporating the elements of deception and information assurance. Successfully conducted protection and security measures significantly enhance the replication of a successful attack and can stall or prevent the enemy from attributing the attack to the responsible threat actor. A disadvantage may be derived from the logistics or coordination involved in implementing protection and security measures, especially during time sensitive operations. When successfully used, protection and security measures are force multipliers that allow the threat to produce cyber effects without fear of discovery by enemy forces. The use of a third country's infrastructure, including trunk lines and ISPs, as well as other masking techniques, such as spoofing and web server mirroring, along with diligent application of operations security measures, can assist in obtaining the requisite access for a precision attack or ensure that the effects of the attack can be sustained as long as needed. The threat will develop malicious executables that are multifunctional and able to evade virus protection measures in order to steal information, spy on the enemy, and control target systems covertly.[1]

**Precision**

A precision attack requires in-depth knowledge of the target and, in particular, the cyber system's security vulnerabilities. Research conducted across multiple functional domains allows the threat to attack complex systems. Usually the specific parameters are programmed into the executable code of the cyber weapon; some precision attacks may require an actual user interface in order to guide the weapon to the intended target or to ensure that the payload is deployed at the most optimal time. In most cases, the electronic weapon's code specifies the conditions in which the

payload will deploy. The threat can write into cyber weapon the characteristics of the target system, such as software configurations, vulnerable applications, and specific users, and load the data into the weapon's electronic guidance system.

**Sustained Effects**

Malware that the threat designs to remain on a targeted cyber system can be programmed to continuously produce its effects for an extended period of time. Command and control is mainly for monitoring purposes and does not usually involve direct user interface as long as the electronic weapon achieves its intended results. Programs designed to harvest information, compress it, and send it to threat intelligence activities can run automatically with little or no user interaction. If a large amount of data is sent out of the targeted system, the activity may alert monitoring devices. In these situations, the threat may operate a user interface to break up the harvested data into small chunks to avoid detection. Computer worms designed to infiltrate targeted cyber systems can operate autonomously before releasing its payload while continuously regenerating and spreading throughout the system.

**Attack Timing and Principles of Operations**

The timing of cyber attacks to coincide with specific operational maneuvers on the physical battlefield supports threat operations. Coordination between the ground forces and the information warfare (INFOWAR) activity will ensure that the attack takes place at the proper time. Cyber and electronic activities can influence operations and can initiate offensive operations for ground forces. For example, if data is gained about important supplies that are en route to enemy troops, this information could influence the threat to begin an attack early in order to control tempo and attempt to conclude regional operations before the extra-regional force arrives. Cyber attacks that are initiated early in the conflict are not only designed to set the tempo of the conflict, but also to control the informational environment. The first phases of the Cyber Attack Lifecycle, when executed properly, will enable the threat to perform cyber attacks that achieve operational gains through perception management, denial, or limited access to networks and networked resources.

The threat will mount both local attacks using insiders and remote attacks through a variety of network-based means. Additionally, threat actors will conduct either structured or unstructured attacks based on the technical expertise of the attacker. The level at which a threat can attack from a remote location and achieve the objective expands the enemy's area of concern and requires more resources than originally anticipated to deal with the threat.[2] This is also an indicator of the threat's sophistication in cyber operations. (For a discussion of threat tier levels, see *Red Diamond*, Volume 4, Issue 10 OCT 2013 p 27, "Infiltration and the Cyber Attack Lifecycle").

| | Internal | External |
|---|---|---|
| **Unstructured** | **Ex. insider threat (possibly accidental); least sophisticated** | **Ex. global hacktivism; variable sophistication** |
| **Structured** | **Ex. intentional insider threat; medium sophistication** | **Ex. state sponsored; potentially most sophisticated** |

**Figure 2. General cyber attack methods *Source:* TRISA-CTID (2014)**

**Tactical Tasks[3]**

TC 7-100.2 *Opposing Force Tactics* describes INFOWAR tactical tasks that are designed to leverage the seven elements of INFOWAR in conjunction with other OPFOR capabilities. Computer Warfare and Information Attack are the elements of INFOWAR involved in Cyber Electromagnetic activities. Because of the ubiquitous nature of computers and networked resources, the INFOWAR tactical tasks can easily be applied to cyber activities. Particular activities such as influence and deception operations; degradation of internet, financial, and government services; as well as physical destruction of trunk lines connecting the targets to the rest of the world are all examples of threat capabilities that are common to the hybrid threat.[4]

Another classification that is useful when planning operations is to divide the tactical tasks as primarily protective or offensive. The table below is designed to give examples of expected primary cyber tasks during all phases of threat

operations. While all tactical tasks are performed at all levels of strategic operations, the list below is intended to show a progression to active cyber operations as well as differentiate between structured and unstructured approaches. Remote attacks that affect all sectors of a country's economy and infrastructure are legitimate targets for the threat.

| Tactical Task | Local Operations Examples | Remote Operations Examples |
|---|---|---|
| Influence (offensive)- Influence beliefs, motive, etc. to support OPFOR objectives. | Locally influenced online propaganda (unstructured) | Global Hacktivism, Defacement (unstructured/ structured) |
| Deceive (protective)-Mislead and disorient enemy decisionmakers. | False messaging with embedded malware, trolling social media (structured) | Phishing, Spoofing / False Flag Internet presence (unstructured/structured) |
| Deny (protective)-Limit the enemy's ability to collect or disseminate information on the OPFOR. | code words, jargon, non-attributable computing devices, (unstructured/structured) | Encryption, Obfuscation, Stenography, DNS reflected flood (structured) |
| Degrade (offensive)-Reduce the effectiveness of the enemy's information infrastructure. | Non compliance with protection and security countermeasures (unstructured/structured) | Attack critical infrastructure, Denial of service attack, data breaches (structured) |
| Disrupt (protective)-Target enemy observation and sensors impede information dominance. | AD / A2 operations (structured) | Telecom transport attack (structured) |
| Exploit (offensive)- Use the enemy's C2 or RISTA capabilities to the advantage of the OPFOR. | Intentional OPSEC violations, release of classified information, penetration of enemy C2 systems (structured) | Advanced persistent threat (structured) |
| Destroy (offensive)- Physically render ineffective. | Lethal force, sabotage (unstructured/structured) | Precision network attack (structured) |

**Figure 3. Cyber tactical tasks (structured and unstructured) *Source:* TRISA-CTID (2014)**

**ASSESS AND EXPLOIT EFFECTS**

The result of a cyber attack has intelligence value whether the electronic attack succeeds or fails. Pinpointing the exact reason why an attack fails gives the threat valuable information about the protections of the targeted system and the effectiveness of the method used. Verifying the success of an attack means revisiting the entire attack lifecycle to see if the method can be reused or replicated. Additionally, observable changes in the enemy's operations can be directly related to a cyber attack. Broad policy changes that lengthen or complicate the decision-making process will be viewed as a success if they are caused by a cyber attack.

Once the decision to attack is made, the threat will continue to exploit the system as long as possible, including mounting multiple attacks over time to ensure the desired results. Electronic mission success happens by first assessing

the success of the initial action and deciding how to proceed. Options can be built into the plan that address the duration of the attack and possible follow-on activities. The threat will also record any lessons learned and use that information for future cyber warfare operations.

**Notes**

[1]Channel 4 News. Russian cyber attacks on Ukraine: The Georgia template. May 2014.
[2] Tech-Faq. Understanding Network Attacks. October 2012.
[3] TRISA. TC 7-100.2, Opposing Force Tactics. Chapter 7 Information Warfare. Pp 7-15. 2011.
[4] John Bumgartner. A Cyber History Of The Ukraine Conflict. Dark Reading. March 2014.
[5] Radware. Threat Alert - Ukraine-Russia Global Conflict. May 2014.


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

On 20 March 2014, ahead of Afghanistan's national elections, four youth killed nine people inside the Serena Hotel-Kabul, long believed to be a fortress against the violence happening around it. Leading up to the April national election, this attack shook the confidence of both the Afghans and foreigners who believed themselves safe within its protective perimeter. The Taliban took credit for the attack in which the four gunmen were also killed. Hiding small pistols in their socks, the four youth were able to pass through a number of security stations, hide for three hours, and then emerge in the dining area where they began shooting people, seemingly at random.

The 5 April 2014 Afghanistan national election has meaning for a number of reasons. First, and foremost, it was the first democratic hand-over of national power ever to occur inside the country. President Hamid Karzai is constitutionally blocked from seeking a third term as president. Karzai has also refused to sign a status of forces agreement, leaving final decisions as to the number and configuration of NATO forces left in Afghanistan after 2014 to his successor. Pre-election Taliban violence tested the resolve and capabilities of Afghan security forces ahead of the election. Whether or not Afghan voters are able to feel relatively safe voting at the polls is a critical test for Afghan security forces.

An email sent to media outlets in March 2014 by Spokesman Zabihullah Mujahid stated that the Taliban would target anyone involved in the elections, and warned the government against using public buildings such as mosques and schools for polling purposes. The message called upon fighters for the cause to use all available force to disrupt the elections. Implied in the warning was that individual Afghans should stay home under threat of attacks targeting them. The Taliban warning came with credibility won through years of successful attacks across Afghanistan. The Free and Fair Election Forum of Afghanistan (FEFA) reported uneasiness among campaign workers, inspired by Taliban warnings of violence. Beginning with the launch of political campaigns in February 2014, FEFA documented specific assassinations and attacks on campaign workers.

The Aga Khan Development Network (AKDN) renovated the old Kabul Hotel, which previously had been devastated by decades of conflict. In 2002, the government of Afghanistan asked the AKDN to renovate the old hotel as a safe haven for visitors, especially foreigners. The AKDN completed renovation and opened the historic 1945 hotel in November 2005. In January 2008, four Taliban militants equipped with suicide vests, grenades, and small arms attacked the 177-room hotel, killing six foreigners.

From the outset, the Serena Hotel was designed with both security and maintenance of the historic Kabul Hotel structure in mind. The hotel, which would primarily serve foreign visitors supporting the democratic aspirations of Afghanistan, would inevitably become a desired target for the Taliban. The $25 million hotel was constructed of reinforced concrete, both for reasons of security and to protect against summer heat and winter cold. The building, sitting in the heart of the city and surrounded on three sides by roads, posed significant security concerns.

The design of the hotel attempted to keep the rooms as far from the roads as possible. Interior buildings were built some distance away from the three roads that framed the hotel complex. The fourth side of the complex was an abandoned building, but none of the guest rooms opened onto that side. The courtyard surrounding the hotel, complete with a large open area in the front and small linear space along the sides, provided distancing to guests, sheltering them somewhat from the danger of attacks from outside the compound. The Montreal-based architect of the Serena Hotel-Kabul, Romesh Khosal, stated that the design afforded as much protection as possible from an external attack, while maintaining the historical façade of the old Kabul Hotel. Security procedures require that all guests be subjected to several layers of security checks before being allowed to enter the hotel.

Surveillance video captured the four attackers passing through hotel security. (To watch the surveillance video, click on the screen capture below.) All four gunmen were consistently described as youth under the age of 18. The video shows the gunmen, first going through at least two pat-downs and a metal detector, then emerging inside the hotel with guns smuggled in their socks. They were captured on video inside the hotel at 18:59 hours. At approximately 2100 hours, the gunmen entered one of the hotel restaurants and began firing, seemingly at random. Before dying themselves, the attackers managed to kill popular Afghan journalist Sardar Ahmad of *Agence France-Presse*, along with his wife and two daughters and five other foreigners. Hotel staff ushered some guests into the safety of the basement safe room.


**Figure 1. Surveillance video of terrorists entering Serena hotel**

Afghan National Security Forces arrived within half an hour, surrounding the hotel. The Afghan quick reaction force, which may have included as many as thirty US Soldiers, began clearing the hotel in search of the gunmen. The last two surviving attackers made their final stand from a bathroom. By midnight, all four gunmen had been killed, and the hotel was secured.

The Serena Hotel-Kabul attack on 20 March 2014 underscores the vulnerability of any place viewed as a target by an enemy. The hotel was designed to be a secure island in the midst of an insecure and unstable city, catering to the

security needs of foreign and Afghan leaders. The facility was specifically designed to protect guests inside the hotel from an external attack. Security measures were developed to protect the hotel from being penetrated. In the end, lax implementation of those security measures allowed a blatant penetration of the hotel's security perimeter. Perhaps the age of the attackers was a factor, or their dress and deportment failed to arouse suspicion. Lack of vigilance, however, allowed penetration of the security perimeter.

The impact of the Serena Hotel-Kabul attack was immediate and significant. Two international election monitoring groups, the National Democratic Institute and the Organisation for Security and Co-operation in Europe, removed their personnel from Afghanistan in the aftermath of the attack. Although the Taliban immediately claimed responsibility, President Karzai raised the specter of Pakistan's Inter-Services Intelligence (ISI) directorate involvement, further increasing pre-election tensions. Security failures do not happen in a vacuum, but have a rippling and cumulative effect.

The professional performance of the Afghan security forces (ASF) may be lost amidst the tragedy and dashed hopes of creating a truly safe haven in a place like present-day Afghanistan. Initial indications are that security forces arrived quickly, cordoned off the area, then found and killed the gunmen. It can be imagined that there could have been more casualties without the interdiction of the ASF. While a significant security failure, the Serena Hotel-Kabul attack may be seen as a glimmer of hope for the increasing capability of the Afghan security forces.


**Figure 2. Pistols and identification papers used by terrorists in the Serena hotel attack**

A number of lessons can be learned from the Serena Hotel-Kabul attack. Security policies and procedures mean nothing if not effectively and vigilantly implemented. The failure of the Serena Hotel was not in the procedures, but in the vigilance of those charged with security. The enemy will always attempt to exploit weakness. There were likely other attempts to penetrate the security perimeter of the hotel. It only takes one dropping of the guard to succeed. Security failures have rippling and cumulative effects beyond any discrete event. The successful attack on the Serena Hotel-Kabul, viewed as a fortress, and the timing ahead of the national elections, affected both Afghan citizens and foreigners tasked with election monitoring and other support for the Afghan government.

_____


**Opposing Force (OPFOR) Insights: DATE Rotation 14-04 at the National Training Center**

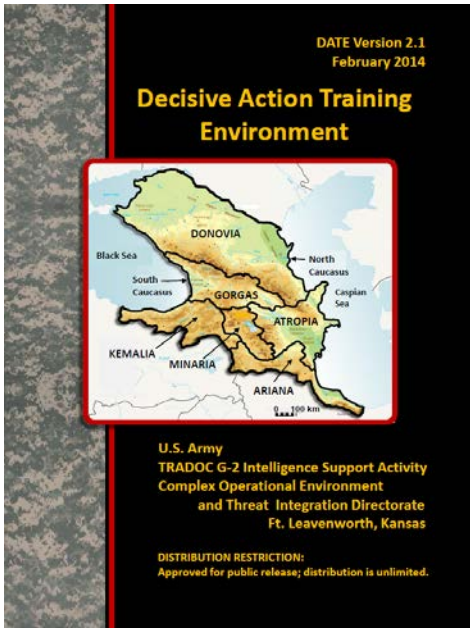
by LTC Shane Lee, Training, Education, & Leader Development Team, NTC Liaison

The National Training Center (NTC), Fort Irwin, CA, executed its fifth Decisive Action Training Environment (DATE) Rotation against an Armored Brigade Combat Team (ABCT) over 15-28 February 2014. Identified as Rotation 14-04, the Rotational Training Unit (RTU) was the 1st ABCT/1st Cavalry Division, which is stationed in FT Hood, TX.

This was the fifth DATE rotation planned, coordinated, and executed by the NTC Operations Group (Ops Grp); its Opposing Force (OPFOR), consisting of 11th Armored Cavalry Regiment (ACR); and its Observer/Controller (OC) Teams. This effort by the NTC proves that RTUs and our OPFOR executing DATE Rotations will be challenged by the complex operational environment and the hybrid threat which we will face in future conflicts. While there are certainly areas for improvement within the OPFOR, they are greatly exceeded in number by areas that should be sustained as NTC begins the planning sequence for DATE rotations for FY14, FY15, and beyond. This success is entirely attributable to the aggressive and positive attitude displayed by NTC personnel in learning and mastering the principles behind the hybrid threat (HT), OPFOR tactics, techniques, and procedures (TTP), the DATE, and an exercise design process developed specifically for HT-based DATE rotations.

**Setting the Stage**

NTC personnel began to prepare for this exercise in August 2013. Over the next six months, TRISA and NTC maintained contact and TRISA responded to requests for final or draft documents such as the update on DATE or TC 7-102, *Operational Environment and Army Learning*. Although the DATE was going through updates and improvements all during the planning sequence, NTC Ops GRP used the current DATE in developing the training environment they wanted in order to build an exercise that would provide a rigorous challenge for the 1/1 ABCT. In addition to providing reach-back support, TRISA also deployed personnel to the 14-04 Initial Planning Conference in August 2013. TRISA also presented one Mobile Training Team "HT Train the Trainer" session for 1/1 ABCT in October 2013.




The 1/1 ABCT Commander's training objectives were established and provided early on and enabled the OPFOR and Ops Grp personnel to develop a plan using countertask analysis to determine what tactics and TTP would best challenge the RTU's training objectives. The RTU's training objectives were Conduct Mission Command, Conduct Offensive Operations, Conduct Defensive Operations, Provide Fire Support, Conduct Stability Operations, Conduct Security Operations. NTC Ops GRP built a scenario based on the OE from the DATE: a mission to support the government of Atropia against the threat posed by Donovian and Atropian guerrillas and criminal groups present on their soil, with the RTU responding to the Atropian government's request for assistance, and the issuance of a CJTF OPORD.

Of course, part of the OE conditions set by the Ops Grp was the design of an OPFOR that would challenge the RTU's training objectives. NTC 11th ACR task organized to form the 11th Division Tactical Group (DTG) which consisted of the 111th, 112th, and 113th Brigade Tactical Groups (BTG). The overall structure of the DTG was consistent with DATE; however, replication of threat systems (Tier 1-4) was not always possible. Limitations were identified in the lack of personnel to operate equipment, proper visual modification of equipment, and inconsistencies between NTC personnel on threat systems available and proper resourcing or task organizing within a hybrid threat scenario. 11th ACR (OPFOR), was challenged even further in portraying all of the capabilities of a guerrilla and criminal force (insurgent and terrorist forces were not portrayed) that would test the RTU's security operations.

**Execution**

**BP1: Training Days (TD) 7-9*, TD9 1/1 ABCT transitions to Defense and Wide Area Security.**

**MISSION:** 11th DTG attacks to defeat 344th ATR MECH BDE and 1/1 CD NLT 220600FEB13, and seizes Gardakert in order to allow the 81st DTG (OSC-S Exploitation force) to seize OBJ FOX (Kvarill, Swabrot, and the Nastasi Army Depot in Chelisi) and create conditions to return Erdabil province to Donovian control.

**Commander's Intent:** The purpose of our operation is to prevent US and Atropian forces from maneuvering against the OCS-S's exploitation force.

**Key Tasks**

- Seize Gardakert
- Seize Key Terrain IVO Red Pass & East Gate
- Destroy enemy fire support assets
- Destroy enemy information collection abilities
- Disrupt enemy C2 IOT separate tactical units from higher command
- Limit enemy freedom of movement and maneuver through conventional and unconventional means
- Disrupt enemy's sustainment operations in depth

**Endstate:** All CJTF forces in Erdabil Provinces are destroyed, defeated, or expelled. Donovian government appointed leaders are established in positions in Erdabil government. Erdabil Province is secured and all Atropian sympathizers identified and removed. 11th DTG forces consolidate gains in Erdabil Province.

**BP2: Training Days (TD) 9*-11, TD9 1/1 ABCT transitions to Defense and Wide Area Security.**

**MISSION:** O/O the 11th DTG attacks to defeat Atropian and US defenses and seizes key terrain IOT enable the 81st DTG (OSC-S Exploitation force) to seize OBJ FOX and the create conditions to return Erdabil Province to Donovian control.

**Commander's Intent:** The purpose of our operation is to prevent US and Atropian forces from maneuvering against the OCS-S's exploitation force.

**Key Tasks:**

- Defeat 1/1 CD
- Seize Gardakert
- Seize Key Terrain IVO Red Pass & East Gate
- Destroy enemy fire support assets
- Destroy enemy information collection abilities
- Disrupt enemy C2 IOT separate tactical units from higher command

**Endstate:** All CJTF forces in Erdabil Provinces are destroyed, defeated, or expelled. Donovian government appointed leaders are established in positions in Erdabil government. Erdabil Province is secured and all Atropian sympathizers identified and removed. 11th DTG forces consolidate gains in Erdabil Province.

**BP3: Training Days (TD) 12-14, 1/1 ABCT transitions to Reconnaissance and Attack.**

**MISSION:** NLT 270600FEB14 11th DTG defends key terrain in Northern Erdabil province, defeats 52ID and Atropian attacks to enable the OSC-S Main Effort to establish their defense.

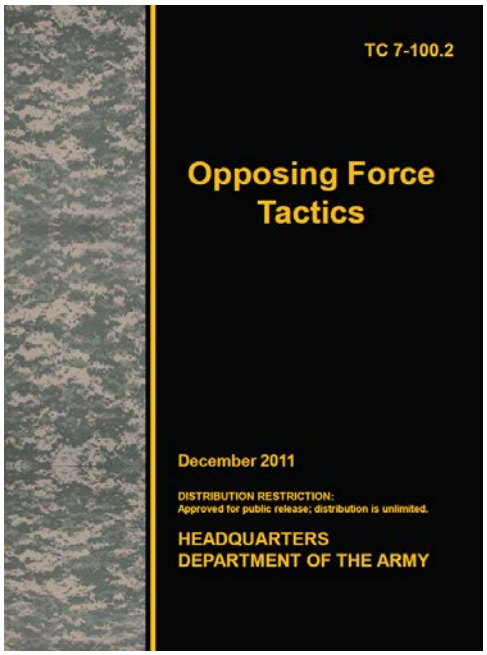
**Commander's Intent:** The purpose of our operation is to prevent US and Atropian forces from seizing key military and urban areas IVO the IB.

**Key Tasks:**

- Retain gains of key terrain in Erdabil Province
- Resume offensive operations as soon as possible.
- Regenerate combat capability in key units
- Defeat/neutralize enemy information collection abilities
- Disrupt enemy C2 IOT separate tactical units from higher command and reduce the effectiveness of their communications
- Maintain LOCs with forward units to enable a rapid resumption of the offensive

**Endstate:** Key and complex terrain retained in Erdabil. CF CATKs are defeated. Sufficient combat power regenerated to resume offensive operations by 11th DTG forces.

During the OPFOR planning and execution it is clear that US doctrine is deeply instilled in our fighting force. The lessons learned from years of experience are hard to overcome when portraying the hybrid threat. Opposing force tactics (i.e. hybrid threat) utilize different techniques, procedures, and terms to achieve the same endstate as US tactics. To be the most efficient fighting force in the world, you must have the best opposing force training centers in the world. This is a very minor point as the OPFOR (11 ACR) continues to integrate the principles of TC 7-101, TC 7-100, and TC 7-100.2 into its SOPs and corporate memory.




The 111th BTG's execution of the "Attack" (US doctrinal term) was a great example of an "Integrated Attack" (OPFOR tactics), starting with a Line of Departure (LOD) at 1800hrs with elements of the 11th DTG and 111th BTG Reconnaissance. Assignment of C2 measures supported the operation, but identification of only two types of command posts (CP) could prove to be a limiting factor for future rotations. 111th BTG conducted all operations from either a Main CP or a Forward (Mobile) CP, which limits C2 for indirect fires, sustainment, alternate, auxiliary, and deception. During the integrated attack, 111th BTG forces were arrayed as DTG Recon, BDETs, fires, logistics, information warfare, and integrated guerrilla elements of the Bilasuvar Freedom Brigade (BFB). The BFB's key tasks: Disrupt support and logistical operations in order to facilitate a separation of the Erdabil Province from Atropia and Observe and Collect on Atropian and US forces in Erdabil Province in order to identify units and equipment types/TTP and intentions.

Putting the differences of terms aside, the 111th BTG's planned offense was to gain control of key terrain. The 111th BTG combined arms rehearsal (CAR) made it clear that the mission was to seize the objective and not defeat or destroy the enemy. One of the courses of action chosen to accomplish this mission was through a rough alliance with the BFB. The

111th BTG and BFB were able to share information, which was conducted primarily through the DTG/BTG Recon. Of note: OPFOR could include COAs with SPF or CDETs tasked to train and fight with the BFB – this was not the case during DATE Rotation 14-04. The reconnaissance operated within a three-day period, with the DTG/BTG and BFB collecting and harassing 1/1 ABCT as soon as they established a tactical assembly area (TAA). Little to no security in the 1/1 ABCT TAA allowed the BFB to integrate into the internally displaced persons (IDP) and refugee flow caused by Donovian offensive operations into Atropia. The BFB were extremely successful in testing the wide area security (WAS) of the RTU, leading to the theft of vehicles, destruction of communications sites, capturing US Soldiers, and smuggling items. Criminals within the area carried details on smuggling routes for munitions/weapons and plan to remove chemicals from the area for transfer to the BFB.

Integrated with the reconnaissance actions in Atropia, the 111th BTG provided fire support. In addition, the BTG Recon teams conducted call for fire against the RTU C2, logistics nodes, and populace using both high explosives and non-persistent chemical strikes. BFB were also successful in destroying 1/1 ABCTs MLRS and one RETRANS site prior to the LD of 1/1 ABCT main body, limiting communications and long range artillery strikes against Donovian C2, artillery, and logistics hubs.

111th BTG movement techniques are still a work in progress and are being addressed by the OPFOR CDR. The 111th BTG units were referenced as MIBN (mechanized infantry battalions), which is not in accordance with current OPFOR Tactics terminology from TC 100.2, which identifies the task organized force below the brigades as a battalion detachment (BDET). “A detachment is a battalion or company designated to perform a specific mission and allocated the forces necessary to do so” (smallest combined arms formation). (TC 7-100.2, p 2-8)

Once the lead BDETs reached the city they began to maneuver in preparation for an integrated attack and push through 1/1 ABCT forces to secure OBJs to the east. Lead elements established contact with 1/1 ABCT Recon and lead squadrons, reacting to direct fires, indirect fires, and air attack. 111th BTG successfully conducted fires and maneuver and dominated the tempo of combat. ADA systems successfully shot down AH64s, Shadow, and Gray Eagle to limit US Forces from fully establishing Air Superiority during the initial phase of battle. 111th BTG COA sketch depicted the employment of action and enabling forces; however, during the execution, commanders on the ground quickly adjusted plans and action force was not maintained. Near the end of the BP 1, 111th BTG forces were 1x BDET+ capable of maneuvering east to their objective, with most of 1/1 ABCT squadrons below 50% strength and reporting that they were no longer mission capable. Simulation of US Air Force assets destroyed nearly a full BDET, effectively closing out BP1.

During BP2, the 111th BTG would “Attack” to defeat US forces and seize key objectives for follow-on forces. BFB continue to disrupt the RTU during the defensive preparation. However, the RTU training value is diminished by ignoring wide area security and leaving most population centers unsecured; a similar trend was seen with the security of IDPs and refugees. 11th DTG “Attacks” to seize key terrain (OBJ McCoy, OBJ Kirk, and OBJ Spock). The 111th BTG attacked west to east through a mountain pass. Movement techniques and procedures are being addressed and corrected to avoid column formations across unrestricted terrain. If the RTU were to maintain air superiority, a vast majority of the 111th BTG would have been destroyed prior to reaching the first objective. However, the RTU lost multiple F-15s, AH-64s, and Gray Eagles from 11th DTG Air Defense systems.

Once the main force moved through the mountain pass, forces maneuvered into attack positions. One of 111th BTG enablers (information warfare) was key combat multiplier for the attack. Effective coordination within the staff provided a near seamless integrated attack using IW, Fires, Aviation, Maneuver, etc. 111th BTG and the BFB provided little consideration to population centers in the amount of civilian casualties. This is a positive point that is exploited through OPFOR tactics vs. US tactics.

The BFB remained in population centers conducting IED and IDF, mostly on Atropian civilians and RTU targets of opportunity. Depending on the RTU, they may focus more efforts on WAS. 1/1 ABCT’s lack of WAS resulted in chemical munitions dispersed throughout cities, executed political figures, and the police killed or fleeing.

**Figure 1. Tactical operations at the National Training Center**

During BP3, the 11th DTG reconsolidated just east of the Donovian Border and is establishing defensive positions. During the deep fight, an AH-64 was shot down near the city of Razish. The pilot was captured and later found dead in a cave. 1/1 ABCT moved into the city, to exploit the cell responsible for the PR event; resulting in one civilian KIA and one detained with no site exploitation. The rest of the city was not secured and the chemical weapons sites were not searched.

The establishment of a defensive position by either a DTG or BTG requires an in-depth assessment of battle damage to the overall force. Equipment ratios in the defense were set low, reflecting an element that is conducting an offensive operation with a deep line of communication for logistics support. The 11th DTG planning was executed and synchronized within the staff; however, the NTC Ops GRP planning did not factor in the defensive preparations. These preparations should allow for additional supplies located within close proximity to the main defensive line and allocate ammunition quantities beyond that of a combat load, especially given the proximity to the Donovian international border.

Observations from BP1, BP2, and BP3 identified a critical requirement: staff functions must remain synchronized during the entire planning process. All the commanders and staff have a general understanding of DATE and the implementation of hybrid threat, but they lack the details and experience of working as a cohesive unit. If synchronization is improved, it will improve the OPFOR presented to the RTU and ensure that the RTU is receiving a World Class OPFOR that can fully test and stress the RTU staff and line units in the executing of wide area security, movement to contact, offense, and defense operations. The 11th DTG staffs all have a 65-70% understanding of threat actions, but they are not synched within the staff to plan and prepare an operation for the commander's decision. Even with a good plan, the OPFOR are restricted in conducting actions to assist in the survivability of and maintaining training objectives of the RTU.

In order to foster and build a World Class OPFOR, the 11th DTG should approach the planning cycle for a DATE rotation as a unit/team with detailed knowledge to operate efficiently and effectively as a hybrid threat, not as a US Force. This unit/team extends beyond the 11th DTG to the NTC Operation Center; for example, the training environment incorporation of guerrilla forces and criminals is not fully synchronized with the 11th DTG. This is partly due to scripted development within the NTC OPS Group (White Cell) of over 2,000 rolls with supporting threads for BFB, PAL, etc., but not for the DTG/BTG. This is good for the 11th DTG to maintain mission command and think outside the box, but bad when the staff and units are not communicating and are unfamiliar with all aspects of the DATE OE. This is but one area that desynchronizes the 11th DTG staff and causes the S2 to leave out the key collection assets internal to the organization or that may be controlled by the S3. Throughout the planning cycle, the S2 needs to provide the 11th DTG staff with RTU COAs that cover every warfighting function. This is a primary planning step for the 11th DTG staff to develop COAs designed to significantly challenge the RTU. When executing the planning cycle and developing COAs for the commander's decision, there are key differences in terms, symbols, and tactics (no phase lines, probable enemy locations vs. named areas of interest, integrated attack, etc.). To better understand and fight as an OPFOR will only increase a Soldier's value to the US Army fighting force at the next assignment.

# Guerrilla Tactical Actions: *Reconnaissance Attack*

**Irregular Forces as Hybrid Threat in a Rural Complex Environment**
by Jon H. Moilanen, CTID Operations (BMA Ctr)

**Guerrilla Reconnaissance Attack against a Coalition Force**

A *reconnaissance attack* is a tactical offensive action that locates moving, dispersed, or concealed enemy elements and either fixes or destroys them. It may also be used by an opposing force (OPFOR) commander to fight for information about the enemy's location, dispositions, military capabilities, and/or tactical intentions. (For information related to reconnaissance attack options, see TC 7-100.2, Opposing Force Tactics, Chapter 3 and Chapter 8.) A reconnaissance attack objective may be force-, terrain-, or facility-oriented with a force-oriented attack as the typical overarching objective.

Reconnaissance elements penetrate or circumvent the enemy's security elements, and can be directed to fix, defeat, and/or destroy enemy security elements. This may require additional security elements working in conjunction with reconnaissance elements. This type of offensive action can exploit a tactical situation with elements that continue the reconnaissance attack toward objectives. Support elements provide capabilities to sustain the combat power of the unit to accomplish the assigned mission task. The decision to conduct a reconnaissance attack is deliberate and requires detailed planning and significant resources.

**Reconnaissance Attack**

**A reconnaissance attack is a tactical offensive action that locates moving, dispersed, or concealed enemy elements and either fixes or destroys them…the purpose can be to find the enemy but not attack him….An attack to gain information is a subset of the reconnaissance attack.**

**TC 7-100.2, *Opposing Force Tactics***

Reconnaissance elements collect information by various methods. Gathering information within the framework of reconnaissance can use a number of standard methods including—

- Surveillance and Observation.
- Raids.
- Ambushes.

During the conduct of a reconnaissance attack, the commander or leader in charge of an element may transition from reconnaissance to another primary action task in order to accomplish his mission. The tactical vignette in this article incorporates mission tasks of reconnaissance, raid, and ambush as an *action* element or *enabling* element that support a reconnaissance attack.

**Action and Enabling Elements**

**At threat battalion and below echelon, one part of the unit conducting a particular action is normally responsible for performing the primary 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 force or element, 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 a Reconnaissance Attack**

Depending on the tactical situation, a guerrilla commander organizing a reconnaissance attack may designate various mission elements. There may be more than one of each type element. For example, the guerrilla battalion commander will use a term such as *ambush, fixing,* or *raiding* element to best describe an element's function. (See figures 1, 2, 3, and 4.)

***Reconnaissance Element(s)***

In this vignette, reconnaissance elements receive indications that enemy elements are entering the guerrilla battalion's area of responsibility (AOR). An initial task is to identify and report the location of enemy reconnaissance patrols and/or security observation posts (OPs) along the Budo river line. The guerrilla reconnaissance elements along the south bank of the Budo River are to monitor the movements of enemy roving patrols and/or OPs but not initiate contact with the enemy. The reconnaissance task shifts to security, on order, to fix identified enemy security forces along the Budo River from disrupting the reconnaissance attack exfiltration by guerrilla units returning from deep in the AOR.

Reconnaissance elements that precede other elements of the reconnaissance attack are task-organized platoon-size elements from guerrilla companies. Each element is self-contained for combat service support (CSS). These elements move and maneuver with preplanned indirect fire support of the guerrilla battalion. 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 guerrilla company commanders organize for one or more security elements north of the river line. Security elements can work in conjunction with reconnaissance elements or perform a reconnaissance role of their own. When a security element conducts these functions, the element is often described as a *fixing* or *ambush* element.

***Action Element(s)***

The guerrilla battalion commander orders his two company commanders to configure their guerrilla companies to accomplish designated functional tasks. The battalion had already allocated the remnants of its one combat ineffective company to each of the other companies. The guerrilla brigade commander augments the guerrilla battalion with a platoon-size unit for this mission. Guerrilla companies are the guerrilla battalion's primary *raiding* elements against what is suspected to be a logistics site and enemy soldiers conducting construction and repair activities near the Zang Bridge. (***Note***. For more information on guerrilla organization and operations, see TC 7-100.3, Ch. 3.)

***Support Element(s)***

Support elements perform various combat support (CS) and CSS tasks. The lack of trained subordinate guerrilla units in specific functional capabilities requires guerrillas to apply general tactical skills and active supporters in the civilian population. (***Note***. The threat uses CS and CSS as doctrinal terms.)

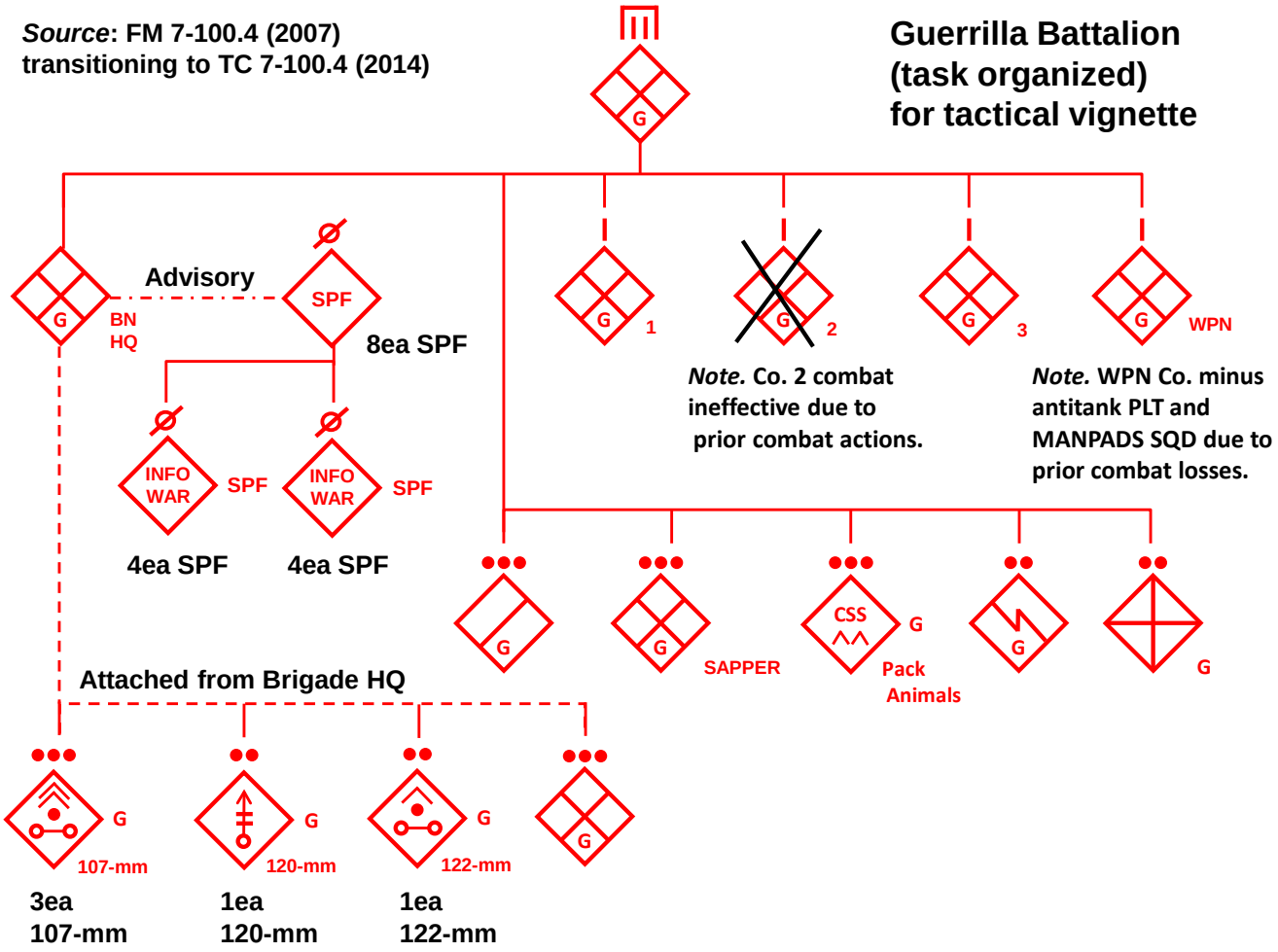



**Figure 1. Guerrilla battalion task organization-reconnaissance attack (example)**

**Functional Support for a Reconnaissance Attack**

A reconnaissance attack typically requires several types of support that can include reconnaissance, fire support, logistics, and information warfare (INFOWAR). Functions and tasks such as mobility, countermobility, and air defense may be performed by guerrillas with specialized skills. In this vignette, the rough terrain, dense vegetation, and season preclude use of armored or wheeled vehicles for guerrilla operations.

***Fire Support***

Due to prior battalion combat losses in indirect fires capability, the guerrilla brigade commander provides the guerrilla battalion with one 107-mm multiple rocket launcher (MRL) platoon, one 120-mm mortar section, and one section of a 122-mm rocket launcher (RL) with support assets to augment the one remaining 82-mm mortar section of the guerrilla battalion. Fire support in a reconnaissance attack focuses on—

- Fires in support of reconnaissance, security, and/or action elements in contact with enemy.
- Support maneuver of reconnaissance, security, and/or action elements.
- Defeat and/or destruction of a fixed enemy.

The guerrilla battalion commander has the 122-mm rocket launcher section and 120-mm mortar section infiltrate to firing positions near the southern bank of the Budo River. The 107-mm multiple rocket launcher platoon and 82-mm mortars position close to the southern river bank for maximum effective ranges that can hit the reported enemy locations near the Zang River and highway intersections.

***Air Defense***

The guerrilla battalion uses an all-arms air defense concept. Guerrillas plan to damage and/or destroy tactical enemy aircraft within the range of their available small arms weapons systems. There are neither man-portable air defense systems (MANPADS) nor any other specialized air defense weapons in the guerrilla battalion during this mission. No elements are to engage enemy aircraft unless receiving direct fires from an aircraft and needing to self-defend. (***Note***. For more information on the OPFOR all-arms air defense tactic, see TC 7-100.2, pp. 11-11 to 11-13.)

***Engineer***

Engineer support to the reconnaissance attack focuses on mobility and to improve security and/or freedom of maneuver. The guerrillas have no organic combat engineer units. Mobility and countermobility tasks are performed by guerrillas with specialized skills. Guerrillas with expertise from civilian engineering occupations and/or previous training by SPF teams concentrate on marking enemy minefields and other obstacles identified during reconnaissance. These guerrillas are prepared to emplace mines and improvised explosive devices (IEDs) along planned withdrawal routes to disrupt any pursuit by the enemy after the successful reconnaissance attack.

Guerrillas from the battalion's sapper platoon are task-organized with each reconnaissance element to assist in infiltrating through the enemy's disruption zone and support attacks on enemy positions. (***Note.*** Guerrilla sappers are not engineers; they are guerrillas trained to perform several typical raider and engineer functions. For detailed capability descriptions on guerrilla sappers, see FM 7-100.4, guerrilla battalion, sapper platoon, pp. 78-84.)

***Logistics***

Guerrillas carry supplies and materiel to be self-sufficient while north of the river. Pack animals are the norm of transportation to supplement man-carried systems along the trails and severe terrain. After the reconnaissance attack, those guerrilla units designated to remain north of the Buda River will subsist with active support from civilians in the local population. Several caches established along planned primary and alternate routes of withdrawal will resupply water, food, ammunition, and medical supplies. Caches south of the Buda River are stockpiled in assembly areas and near river crossing sites.

***Information Warfare***

INFOWAR activities in this reconnaissance attack are primarily executed to—

- Protect elements of the guerrilla battalion from being detected.
- Deceive enemy elements on guerrilla operations and intentions.
- Deceive enemy elements on guerrilla unit locations.
- Create a false sense of security in the enemy.

Deception activities ensure that the guerrilla battalion achieves tactical surprise and enhances guerrilla force survivability. The guerrilla commander deceives the enemy concerning the strength and composition of his forces, their current dispositions and orientation, and intended manner of employment with the support of information warfare (INFOWAR) deception.

Special purpose force (SPF) advisors support simulative electronic deception (SED) with two INFOWAR teams to mislead the enemy on current operations of the guerrilla battalion. With the assistance of the SPF INFOWAR teams, several guerrillas of the combat ineffective guerrilla company establish simulated unit command posts and subordinate stations with a network of radio emitters to emulate electronic activities found in guerrilla companies and a battalion headquarters. Locating the communications equipment at sites away from the actual guerrilla battalion complex battle position (CBP) and two company assembly areas, the INFOWAR team uses techniques such as several controlled breaches of radio security and unencrypted radio net traffic.

The deception story convinces the enemy that company-size or less guerrilla units are relocating to the south and have no elements north of the river. The INFOWAR deception succeeds in creating a false sense of security in the enemy.

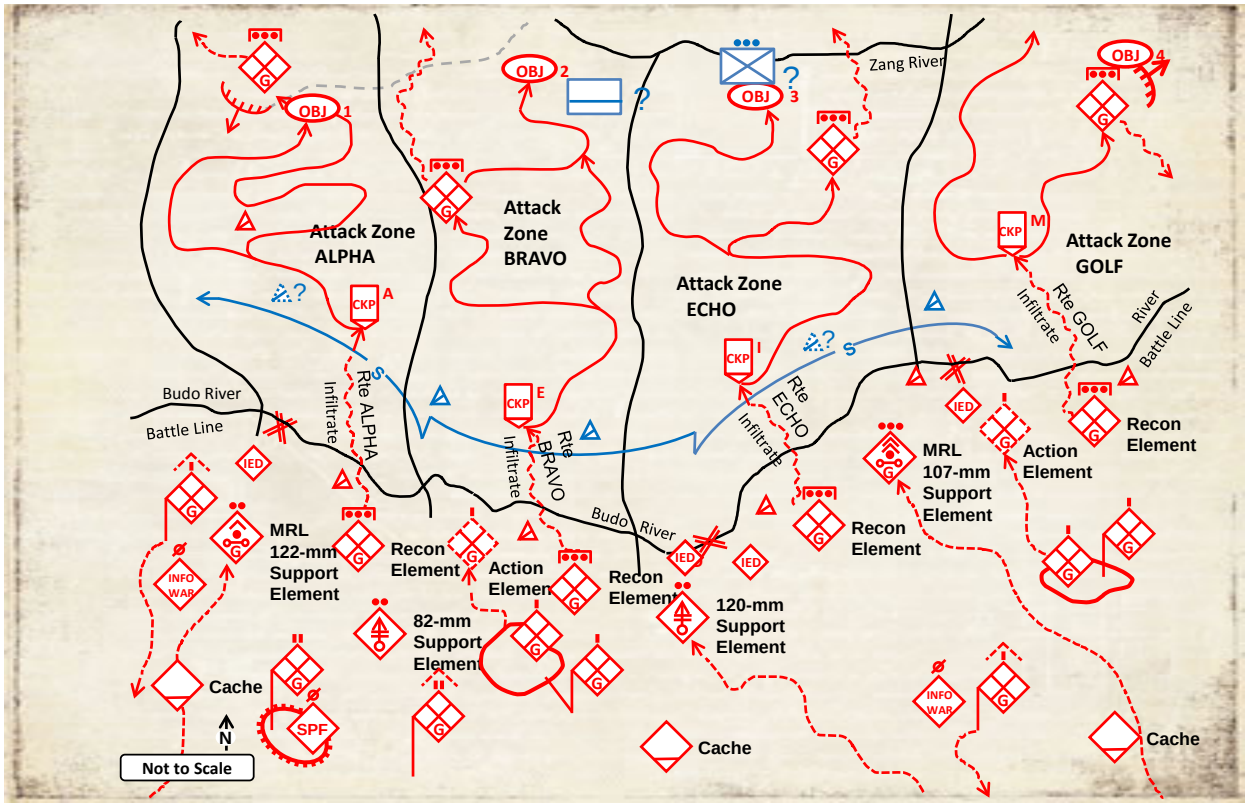



**Figure 2. Reconnaissance and security concept sketch (example)**

**Executing a Reconnaissance Attack**

Active supporters in the civilian population north of the Budo River report that security forces along the river are limited to several small team-size roving patrols and temporary OPs from West Creek to Dirt Creek. Based on their distinctive uniforms and equipment, civilians report that coalition forces are operating with the enemy forces of the repressive regional government. With this appearance of enemy forces with supporting forces from outside the region, the guerrilla battalion commander requires confirmation of enemy locations and activities in his AOR north of the Budo River.

The guerrilla battalion commander recognizes that the enemy is in an initial phase of area occupation. He knows that he must act quickly. He plans to attack these elements before additional enemy capability arrives and establishes larger operations in his area. Although the reconnaissance attack is the most ambitious and least preferred method to gain information, the guerrilla battalion commander determines that a reconnaissance attack is required and orders the attack.

As enemy elements are located, situation reports provide information updates on enemy disposition, actions, and probable intentions. The primary *kill zones* are the area occupied by enemy logistics along Highway 7 west of the Zang Bridge, and the construction site and bivouac near the Zang Bridge.

**Kill Zone**

**A *kill zone* is a designated area on the battlefield where the OPFOR plans to destroy a key enemy target. A kill zone may be within the disruption zone or the battle zone. In the defense, it could also be in the support zone.**

**TC 7-100.2, *Opposing Force Tactics***

The mission task is to destroy enemy forces at these two sites. The concept is to achieve this destruction with a combination of direct and indirect fires. There is no initial intention to capture enemy personnel or exploit enemy

equipment at the sites. When the guerrilla element leaders determine that their target is destroyed, they will conduct rapid exfiltration from the objectives areas and disperse using multiple withdrawal routes.

Guerrilla security elements are initially south of the river. There is no indication of an enemy advance south of the Buda River. However, civilian reports note an increase in coalition east-west motor vehicle traffic on Highway 7 and dismounted regional home guard and coalition forces doing construction work south of the Zang River near the Zang Bridge. Additional reports indicate a logistics site is being developed with tentage, construction materiel, and fuel blivets along Highway 7 west of the Zang Bridge.

The guerrilla battalion commander is supported with SPF that are advisors on rebuilding his organizational capabilities as he conducts ongoing missions. These actions complement the SPF INFOWAR teams in support of deception activities. Recent combat actions have severely reduced his organic battalion fire support. Only two guerrilla companies in his battalion remain as effective units. The guerrilla battalion commander coordinates with his guerrilla brigade commander for additional guerrillas, mortar, and rocket launcher support.

The reconnaissance elements receive a situational update from guerrilla security elements posted along the southern river bank prior to infiltrating north across the Budo River. Graphic control measures assigned by the guerrilla battalion orient the reconnaissance elements with routes and identify particular areas or points to observe and report on during their maneuver. Reconnaissance elements use control measures such as check points, terrain features, and orientation objectives. The reconnaissance elements have adequate combat power for their own limited security capability. They are to avoid contact in the disruption zone, reach their objectives, and report status updates to the guerrilla battalion headquarters.

The reconnaissance elements infiltrate past the enemy security screen to conduct reconnaissance, report, and maneuver along designated routes and check points. The reconnaissance element's tasks include–

- Infiltrate through the enemy's security elements.
- Report any enemy reconnaissance units and/or observation posts located along the north river bank and higher terrain.
- Locate and target enemy combat and artillery forces in assembly areas and/or temporary positions or facilities.
- Locate and target enemy logistics sites.
- Locate and target company and battalion command posts.
- On order, engage to fix and defeat designated enemy forces.

The guerrilla battalion commander retains the decision of when to attack enemy elements. He intends to conduct nearly simultaneous attacks on enemy units and/or activities. Based on the information and intelligence obtained from reconnaissance elements, the guerrilla battalion commander will announce the time of attack. If an individual reconnaissance element has an unexpected encounter and engagement with enemy elements, the element will break contact. Afterwards, the element will reestablish and maintain contact with the enemy through stealth and surveillance. Supporting mortar or rocket fires will be provided only on order of the guerrilla battalion commander.

***Route ALPHA***

As the reconnaissance elements infiltrates across the Budo River, it reconnoiters along the designated route, reports activity it observes, and clears multiple check points along the route. The element leader avoids an enemy roving patrol that appears to be moving toward the West Creek. He tasks a two-guerrilla team to keep the enemy roving patrol under observation, sends a situation report, and continues to conduct reconnaissance to the north.

No other enemy forces are observed as the reconnaissance element occupies an ambush site focused on the bridge crossing near Objective 1 and establishes an observation post (OP) to the northeast. The element leader continues to observe the bridge at West Creek. As an ambush element, the leader is prepared to block any enemy forces that attempt to escape to the west from the logistics site, and block enemy forces that attempt to reinforce from the west across the bridge. The patrol leader reports his readiness and continues to observe for any activity along Highway 7 and at the West Bridge.

***Route BRAVO***

The reconnaissance element encounters no enemy forces as it infiltrates across the Budo River to check point ECHO and moves north along its designated route. After clearing other check points, it approaches Objective 2. The forward reconnaissance team observes a logistics site in operation along the north side of Highway 7. No defensive positions are visible but camouflage nets conceal a number of wheeled vehicles, tents, and palletized supplies. Several bulk fuel vehicles are concentrated in a small area next to the road configured for rapid refueling operations.

After reporting the enemy forces and locations, the element leader prepares an *attack-by-fire* position as a raid element. This raid element guides the guerrilla company into an attack-by-fire position as the primary action element in zone. The guerrilla battalion commander directs that if conditions after the attack indicate that if the guerrillas can physically raid the logistics site, a platoon-size raid element will quickly collect information from the site and withdraw to the north. The guerrilla company will withdraw to the south and cross the Budo River.

***Route ECHO***

The reconnaissance element observes an enemy roving patrol on high ground at the river line near check point INDIA. The reconnaissance element maneuvers through a valley and along a major ridgeline after infiltrating past the enemy patrol. The element observes a combat outpost oriented south along Highway 2. The element leader reports the squad-size infantry element as stationary in a simple battle position (SBP). He establishes an attack-by-fire position on high ground to the north and rear of the enemy combat outpost.

The leader transitions his reconnaissance element to a *fixing* element. He sends a small reconnaissance team to continue north to observe the area at Objective 3. This reconnaissance team identifies a dismounted enemy force of about platoon-size strength doing road improvement and construction work near the Zang Bridge. This report causes the guerrilla battalion commander to shift his guerrilla company in the eastern part of his AOR to occupy an attack-by-fire position oriented on this enemy force. The reconnaissance element links up with the guerrilla company and provides an updated situation report, and returns to his platoon as part of a fixing element in the attack-by-fire task on the combat outpost.

***Route GOLF***

The infiltration by the reconnaissance element across the Budo River to check point MIKE occurs without incident. After crossing Dirt Creek, the element finds evidence of enemy dismounted traffic on the north-south trail but observes no enemy as it continues north along check points to Objective 4. Timely reports assist the rapid movement of the guerrilla company into position towards the enemy near Objective 3.

The reconnaissance element occupies an ambush position near Objective 4 as an *ambush* element along the trail system and orients to the northeast. The ambush element leader reports his readiness and continues to observe across both the Zang River ford to the north and the trails to the northeast for any enemy activity.

**Synchronizing the Reconnaissance Attack**

The guerrilla battalion commander coordinates the timing for indirect fires to impact on the designated target areas of the logistics site along Highway 7 and the dismounted enemy force near the Zang Bridge. The guerrilla companies and platoon-size action elements mass their direct fires when the first rockets and mortar rounds impact in the kill zones. Within minutes, the nearly simultaneous indirect and direct fires are devastating at the highway logistics site and construction location near the river.

Several fuel vehicles in the logistics site explode in flames from the first volley of incoming rocket and mortar fires. Large black clouds billow above the tree canopy. Confusion among the logisticians is obvious as many vehicles speed from the site in a reckless manner and head east along the highway and unimproved dirt trails. Several vehicles run into each other in the confusion near Highway 7 and partially block a road leading to the highway. Automatic weapons fire and rocket propelled grenades (RPGs) from the guerrilla company and platoon destroy other vehicles and soldiers as they approach the highway.

Concurrently, multiple rockets impact near the enemy bivouac near the Zang Bridge and cause similar damage to construction equipment and enemy soldiers. Much of the first volley of rockets land beyond and to the west of the bivouac as the company-size raiding element engages unprotected crews with direct fires and RPGs that damage or destroy several of the trucks. A second and third volley of adjusted rockets impact in the midst of the construction position and damage or destroy wheeled or towed equipment that were not affected in the first rocket volley. Enemy casualties are very evident in the bivouac and bridge site.

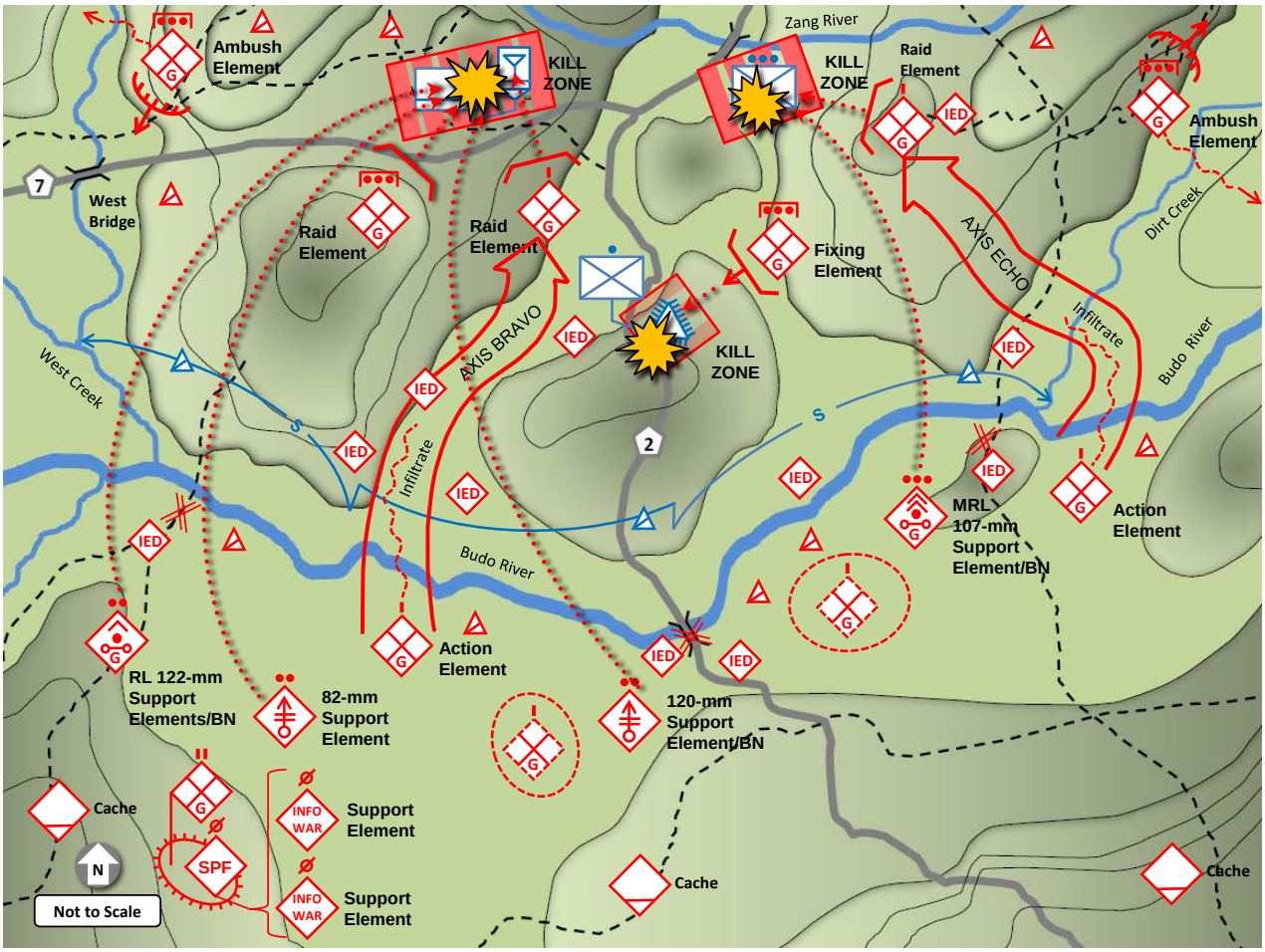



**Figure 3. Reconnaissance attack (example)**

Meanwhile, the platoon-size fixing element near the enemy combat outpost along Highway 2 initiates its attack-by-fire when guerrilla rocket and mortar fire is heard impacting on the enemy to the north. The fixing element's direct fires immediately pin the enemy soldiers in their shallow fighting positions. Direct fires coming from the enemy combat outpost are ineffective and sporadic. RPGs impacting in the outpost fighting positions cause additional enemy casualties.

The platoon-size ambush element near the West Bridge waits and focuses their attention primarily to the west. Surprisingly, no vehicles appear from the west. Although reports from guerrilla elements at the logistics site state that wheeled vehicles are moving out of the logistics site toward the bridge, no enemy vehicles appear. The guerrilla platoon leader at the West Bridge waits and continues to observe. A similar situation occurs in the northeast with the platoon-size ambush element ready to act against any enemy reinforcements. No enemy units appear.

**Assessing the Reconnaissance Attack**

The nearly simultaneous engagements on the Highway 7 logistics site and Zang Bridge site last approximately 20 minutes. Based on reports from his commanders, the battalion commander is satisfied that he has destroyed the

combat effectiveness of both enemy concentrations. He orders the guerrilla companies and other elements to disengage.

The guerrilla companies and platoon-size elements initiate their withdrawals along multiple routes to the south toward rally points near the Budo River. Designated platoon-size action elements participating in the attacks on the logistics site and combat outpost reorient to act as rear security for the withdrawing guerrilla companies as they exfiltrate to the south. (See figure 4.)

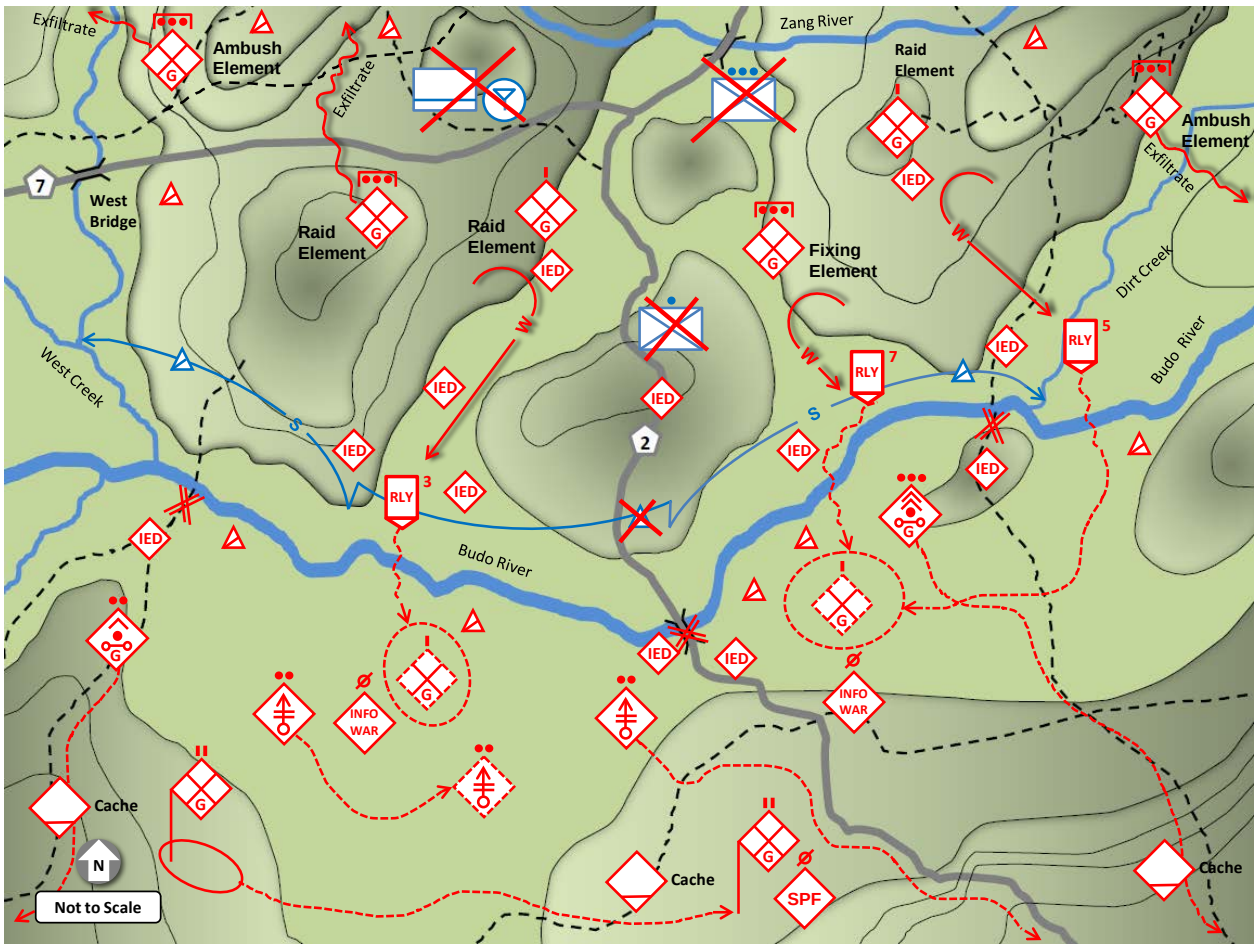



**Figure 4. Reconnaissance attack exfiltration and ongoing missions (example)**

The ambush element at the West Bridge disperses to the northwest and the ambush element near Dirt Creek moves to the southeast. Some guerrilla elements are designated to remain north of the Buda River after the attack and continue their reconnaissance and surveillance of enemy activity in the AOR while some elements will conduct ambushes. Other elements of the reconnaissance attack will return south of the Buda River and reorganize in company assembly areas.

South of the Buda River, indirect fire systems reposition and are prepared to support the guerrillas as they withdrawal. When guerrilla indirect fire support is no longer required, the guerrillas quickly displace their rocket launchers and mortars again to avoid possible counterbattery fires of the enemy.

The guerrilla companies and elements re-form in assembly areas south of the Budo River. Platoon-size elements complete rendezvous with their companies south of the river within three to five days. Two platoon-size elements continue to operate in zone in the West Creek area and conduct periodic harassment or annihilation ambushes along Highway 7 and the Zang River basin. The platoon in the vicinity of Dirt Creek conducts reconnaissance to the east and returns to its company south of the Buda River two weeks after the reconnaissance attack.

The guerrilla battalion commander achieves a tactical success with his timely decision to conduct a reconnaissance attack. Having previously deceived the enemy regarding his actual intentions, the guerrilla battalion commander completely surprised the enemy. The massed guerrilla battalion indirect fires, combined with guerrilla raiding and fixing element direct fires, were devastating on the enemy. Reports from local civilians after the attack confirm that the reconnaissance attack damaged or destroyed critical combat power and sustainment capabilities of an arriving enemy home guard battalion and coalition advisors.

The guerrilla battalion experienced minor losses in comparison to the enemy. When the platoon-size action elements report to their guerrilla companies, the total guerrilla battalion losses were four guerrillas killed in action, five seriously wounded, and seven lightly wounded. Three guerrillas were unaccounted for in unit after action reviews. These losses were insignificant compared to the casualties that the battalion commander was willing to accept in order to destroy the introduction of enemy presence in his AOR.

The guerrilla brigade commander was very pleased with how the battalion commander used his tactical initiative, deceived the enemy with SPF INFOWAR asset support, and stopped the enemy advance into his AOR. Major enemy operations south of the Zang River did not occur until the following dry season and provided a significant period of time for guerrilla recruitment and training in the guerrilla brigade AOR.

**Training Implications**

Hybrid threats can be simultaneous combinations of various types of activities by adaptive enemies and adversaries. This article presents a way in which future threats could operationally organize to fight US forces. A *hybrid threat* is the diverse and dynamic combination of regular forces, irregular forces, and/or criminal elements all unified to achieve mutually benefitting effects. For detailed discussions of HT operations, tactics, and organizations, the reader should consult other the TC 7-100 series and related TRADOC G2 supporting products in progress of update. (See figure 5.)


**Figure 5. TC 7-100 series of hybrid threat and operational environments for US Army learning**

# *CTID DAILY UPDATE*: MONTHLY RECAP

by LTC Shane Lee and CPT Ari Fisher, Training, Education, & Leader Development Team

CTID analysts produce a *CTID Daily Update* to assist our readers' focus on key current events and developments across the Army training community. Each *CTID Daily Update* is organized topically across the Combatant Commands (COCOMs). This list highlights key updates during the current month. An article's inclusion in the *Update* does not reflect an official US government position on the topic. CTID does not assume responsibility for the accuracy of each article.


## May 2014 Sampler

**2 May**

- **US:** Mexico Cartel-US Gang Ties Deepening as Criminal Landscape Fragments
- **Arctic:** Exxon Sticks With Russia Despite Ukraine Sanctions -- 2nd Update
- **Africa:** Diamonds, Ivory Fund War in Central African Republic: US Group
- **Egypt:** Army Accuses Brotherhood of Inciting Workers to Detain Ships
- **Israel:** "David the Nahal Soldier" goes viral. Army chief: Facebook is not a tool of command

**21May**

- **Technology:** 3-D Printing Companies See Growing Market in Unmanned Aircraft
- **Columbia:** Submarine carrying 2.3 tons of cocaine found close to Colombia's Pacific coast
- **Columbia:** Arrests Show Colombia's BACRIM Moving on Amazon Border Region
- **Yemen:** Pictures and video of Yemeni southern offensive
- **Montenegro:** Unholy Alliances - How Organized Crime, Government and Business Interact in Montenegro

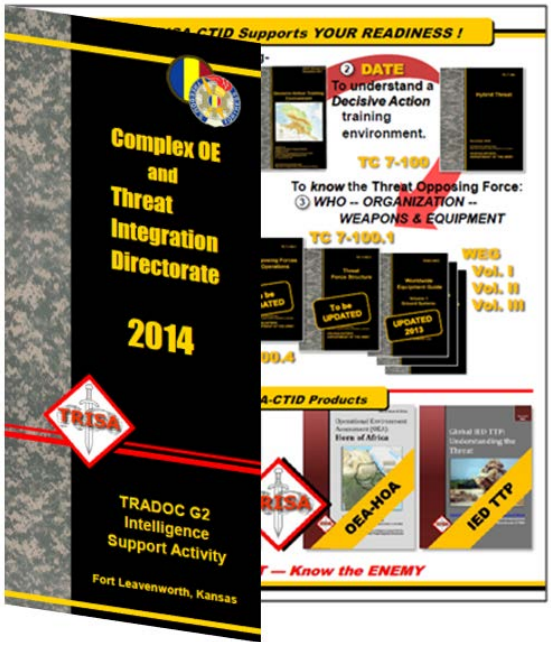
---

***Conditions in the Complex Operational Environment***
***…Now and for the Foreseeable Future***

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

# PRODUCTS SAMPLER FOR COMPLEX OPERATIONAL ENVIRONMENTS

by CTID Operations




**Sampler of Products:**

**TC 7-100** ***Hybrid Threat***
**TC 7-101** ***Exercise Design***
**TC 7-100.2** ***Opposing Force Tactics***
***Worldwide Equipment Guide*** **(WEG) (2013)**
**TC 7-100.3,** ***Irregular Opposing Forces*** **(2014)**
**DATE v. 2.1 (2014):** ***Decisive Action Training Environment***

***COMING spring-mid 2014!***

***RAFTE-North Korea: Regionally Aligned Forces Training Environment***

***RAFTE-Pacific: Regionally Aligned Forces Training Environment***

***CTID Threat Reports (TBD)***

***TC 7-102, Operational Environment and Army Learning***

## 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 |
| UK LNO | Warrant Officer Matt Tucker | |
| matthew.j.tucker28.fm@mail.mil | | 684-7994 |
| Operations–Military Analyst | Dr Jon Moilanen | |
| jon.h.moilanen.ctr@mail.mil | BMA | 684.7928 |
| Military Analyst | Steffany Trofino | |
| steffany.a.trofino.civ@mail.mil | | 684.7960 |
| Threat Assessment Team Lead DAC | | 684.7934 |
| Jerry England | jerry.j.england.civ@mail.mil | |
| Military Analyst DAC | Jennifer Dunn | |
| jennifer.v.dunn.civ@mail.mil | | 684.7962 |
| Military Analyst DAC | Kris Lechowicz | |
| kristin.d.lechowicz.civ@mail.mil | | 684.7922 |
| Worldwide Equipment Guide | John Cantin | |
| john.m.cantin.ctr@mail.mil | BMA | 684.7952 |
| Train-Edu-Ldr Dev Team Lead DAC | | 684.7923 |
| Walt Williams | walter.l.williams112.civ@mail.mil | |
| TELD Team/RAF LNO | LTC Shane Lee | |
| shane.e.lee.mil@mail.mil | | 684.7907 |
| TELD Team/CoE LNO | CPT Ari Fisher | |
| ari.d.fisher.mil@mail.mil | | 684.7939 |
| TELD Team/JMRC LNO | Mike Spight | |
| michael.g.spight.ctr@mail.mil | CGI | 684.7974 |
| TELD/MCTP LNO | Pat Madden BMA | |
| patrick.m.madden16.ctr@mail.mil | | 684.7997 |
| OE Assessment Tm Lead | BMA | 684.7929 |
| Angela Wilkins | angela.m.wilkins7.ctr@mail.mil | |
| Military Analyst | Laura Deatrick | |
| laura.m.deatrick.ctr@mail.mil | CGI | 684.7925 |
| Military Analyst | H. David Pendleton | |
| henry.d.pendleton.ctr@mail.mil | CGI | 684.7946 |
| Military Analyst | Rick Burns | |
| richard.b.burns4.ctr@mail.mil | BMA | 684.7897 |
| OE Assessment Team | Dr Jim Bird | |
| james.r.bird.ctr@mail.mil | Textron | 684.7919 |

### CTID Mission

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

### What We Do for YOU

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

***YOUR Easy e-Access Resource***

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