Operational Environment Enterprise
US TRADOC G2 Intelligence Support Activity

Red Diamond

Complex Operational Environment
and Threat Integration Directorate

Fort Leavenworth, KS Volume 5, Issue 12 DEC 2014

INSIDE THIS ISSUE

OEE *Red Diamond* published monthly by TRISA at CTID

Send suggestions to CTID
ATTN: *Red Diamond*
Dr. Jon H. Moilanen
CTID Operations
BMA Contractor
and
Angela Wilkins
Chief Editor and
Product Integration
BMA Contractor

READINESS IN COMPLEX OPERATIONAL ENVIRONMENTS

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

The TRADOC G2 OEE *Red Diamond* is a monthly newsletter that presents topics of interest on an opposing force (OPFOR) threat for training and observations from ongoing or historical conflicts in complex environments. The value of rigorous and realistic threats in Army training, professional education, and leader development is evident in the quality of performance by our Soldiers, Army leaders, and Department of Army Civilians (DACs) in the daily conduct of missions and mission support.

This December issue of the *Red Diamond* is a selective collection of TRISA articles from 2014 that addresses the diverse and challenging threats and related conditions of complex operational environments (OEs). These threats and conditions remain a significant factor in military missions today and for the foreseeable future.

Win in a Complex World

To win in a complex world….It requires a thorough understanding of the problem and the many facets, including cultural, economic, military, and political; an understanding of all the players and relationships between them; and an understanding of the variables that drive them.

General David G. Perkins (2014)

RED DIAMOND TOPICS OF INTEREST

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

This month's lead article details the many threat, opposing force (OPFOR), and operational environment (OE) products of the TRADOC G2 Operational Environment Enterprise and its Complex Operational Environment and Threat Integration Directorate (TRISA-CTID) that were released in 2014. Another article addresses a concept of functional tactics and its role in functional analysis. OPFOR training literature embeds these principles in threat conditions to live, virtual, constructive, and gaming (LVCG) venues that replicate conditions representative of an actual OE.

Articles range institutional and operational topics such as recent rotation activities at the National Training Center (NTC) and how the Decisive Action Training Environment (DATE) is fundamental to robust and relevant training. Other observations assess state and paramilitary actions in Crimea by one state against another sovereign state; vulnerabilities in unmanned vehicle system (UAS) tactics and techniques that could be applied by a threat; irregular forces' use of multiple improvised explosive devices (IEDs) in a complex urban environment; and anti-satellite (ASAT) technologies that could be used by state and non-state surrogates' plans to disrupt or negate potential enemy capabilities.

Many of these topics are covered in the instruction and practical exercises of the CTID Threat Tactics Course (TTC) and mobile training team (MTT) variants.

Email your topic recommendations to:

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

Director's Corner:
Thoughts for Training Readiness

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

The *Red Diamond* newsletter enters its fifth year of presenting threat and opposing force (OPFOR) conditions for training, professional education, and leader development by the Army, joint forces, and multinational partners. Produced by the TRADOC G2 Intelligence Support Activity (TRISA) as part of the US Army TRADOC G2 Operational Environment Enterprise (G2 OEE), this unclassified monthly newsletter provides information and unclassified intelligence of current events as well as historical perspectives. Analysis supports the situational awareness and understanding of threats in complex operational environments (OEs) today, as well as probable or possible near-term threat conditions.

The Complex Operational Environment and Threat Integration Directorate (CTID) is the OEE lead functional activity to review and approve *Red Diamond* article submissions from organizations across DoD, the Intelligence Community, and multinational partners. The *Red Diamond* charter is to assess real-time information and unclassified intelligence on worldwide threats and provide informed analysis to stakeholders that enhance rapid integration into exercise design, curricula development, other Army developmental venues, and training readiness. This threat integration is fundamental to creating realistic, robust, and relevant ***conditions*** at all Army Combat Training Centers (CTC), Centers of Excellence (CoE), and unit home stations for mission readiness.

CTID provides the oversight function, on behalf of the G2 and TRADOC Commander, to ensure a consistent threat representation across all US Army readiness venues in accordance with AR 350-2, *Opposing Force (OPFOR) Program*. The TRADOC G2 is the decision authority on behalf of the TRADOC Commander.

CTID is responsible for publishing threat doctrinal literature, tactics and techniques, organizational force structure, weapon systems and equipment capabilities and limitations, and emergent adaptations of a hybrid threat in today's complex OEs. The adjudication of any changes or updates to threat conditions for Army readiness is particularly critical as products such as the Army's *Decisive Action Training Environment* (v.2.1) or HQDA TC 7-101, *Exercise Design* are in use by Army active and reserve components, joint team members, and an expanding application by multinational partners in training, education, and leader development.

For subscription to *Red Diamond*, submit email address to CTID POCs jon.h.moilanen.ctr@mail.mil or angela.m.wilkins7.ctr@mail.mil. Article submissions are welcome for consideration and must comply with CTID standing operating procedures, available upon request.

JON

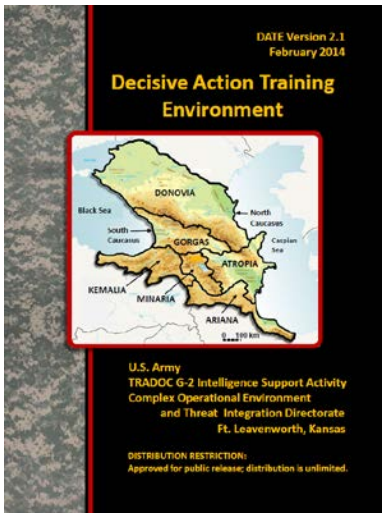
CTID Threat Integration Products: 2014

by Angela Wilkins, TRISA-CTID Product Integration (BMA Ctr)

The Complex Operational Environment and Threat Integration Directorate (CTID) provides the US Army and wider military training community with a multitude of products that enable trainers and others to gain a deeper understanding of the threats the US may face, their tactics, and their techniques. CTID analysts do this through studying new and enduring tactics, weapons, and actors. We apply this information to our doctrine and training products, and make that information accessible primarily through the Army Training Network (ATN). CTID products are designed for Combat Training Centers, home station training, and all others who find it valuable to understand the strategic environment. What follows is a descriptive list of the products CTID released in 2014. If you have questions or comments on any of the products, or would like to request something you do not see here, please contact Angela Wilkins or any CTID analyst directly. Contact information always appears on the last page of the *Red Diamond.*

Training Circular (TC) 7–102, *Operational Environment and Army Learning*, is a practical guide on how to integrate the conditions of an operational environment (OE) into robust, relevant, and realistic training, professional education, and leader development experiences. This TC presents critical design techniques and means that support the fundamental concepts of a continuously adaptive learner-centric model—the Army Learning Model (ALM)—for improved Army mastery to anticipate, understand, and adapt successfully to complex, uncertain, and/or ambiguous environments in decisive action.

Decisive Action Training Environment 2.1 **(DATE)** provides the US Army training community with a detailed description of the conditions of five operational environments (OEs) in the Caucasus region. It presents trainers with a tool to assist in the construction of scenarios for specific training events but does not provide a complete scenario. The DATE offers discussions of OE conditions through the political, military, economic, social, information, infrastructure, physical environment, and time (PMESII-PT) variables. The OE conditions represent a composite of real-world conditions of OE and threat actors identified through extensive and ongoing research.



The DATE is a tool for the training community to use across training events ranging from rotations at the Combat Training Centers (CTCs) to individual home station training (HST) events. It is the baseline document for all the conditions and characteristics of the five OEs in the region. Exercise planners should use this document for all exercise and scenario design requirements. DATE is updated/revised as needed.

A **Regionally Aligned Forces Training Environment (RAFTE)** is a COCOM-based supplement to DATE that describes important modifications to the DATE to increase OE condition fidelity with respect to conditions endemic to the identified region. This year, CTID released two RAFTEs, one for North Korea and one for the Pacific operational environment (OE). A RAFTE for Africa was previously published. RAFTE–North Korea, although not a region but a country, was developed in response to a specific request, but RAFTEs will typically focus on *regions.* RAFTEs have a unique format. They follow the PMESII-PT variable methodology, and within each variable, specific conditions are identified that are unique to that OE, meaning they are conditions not already present in DATE but that are relevant for training prior to deployment to that area of the world. The condition is identified and explained in its real-world context, then explanation on how to modify the DATE to add the condition to training follows. Many conditions include Events (DATE has an entire section of Events) which serve as an aid to scenario writers by providing a way to incorporate the condition into training. As a supplemental product, any RAFTE must be used in conjunction with the DATE; they are not stand-alone products.

Micro-OEAs [Operational Environment Assessments] are another DATE-based product developed in response to a specific request. Micro-OEAs focus in on the unique conditions of a small OE, typically a province or town, to provide a high degree

of fidelity needed for certain training exercised. Micro–OEAs are also specifically used in the development of training software. In 2014, CTID produced Micro–OEAs for these four OEs: Allar, Masalli, Prishib City, and Dzhallabad.

The ***Worldwide Equipment Guide*** (WEG)—The WEG was developed to support the TC 7-100 series and all OPFOR portrayal in training simulations (live, virtual, constructive, and gaming). The equipment portrayed in the WEG represents military systems, variants, and upgrades that US forces may encounter now and in the foreseeable future. The authors continually analyze real-world developments, capabilities, and trends to guarantee the OPFOR remains relevant. Published in three volumes—Ground, Airspace & Air Defense Systems, and Naval & Littoral Systems—the WEG is the approved document for OPFOR equipment data used in US Army training. Annual updates are posted on ATN, where it is available for downloading and local distribution.

Combating Terrorism Poster Series is an unclassified monthly poster on threat and opposing force (OPFOR) resources for US Army and joint training in complex operational environments with adversaries and enemies. The poster series supports the US Army's quarterly antiterrorism themes and related antiterrorism, terrorism, and complex operational environment topics for Army and joint training and mission readiness.

Threats Terrorism Team (T3) Advisory is an unclassified monthly one-page advisory on threat and opposing force (OPFOR) resources for US Army and joint training in complex operational environments with adversaries and enemies. The advisory supports the US Army's quarterly antiterrorism themes and related antiterrorism, terrorism, and complex operational environment topics for Army and joint training and mission readiness.

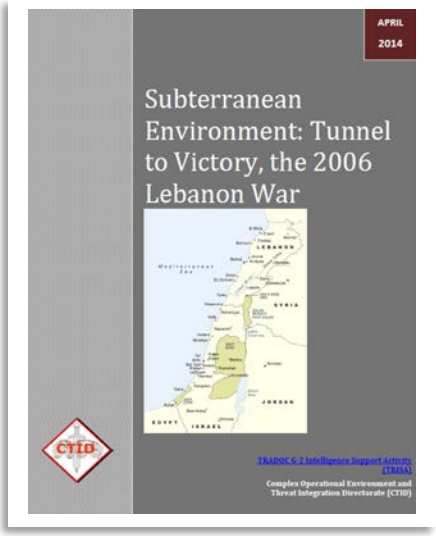
Operational Environment (OE) Threat Assessments provide a concise look at a potential OE for US forces through the lense of PMESII-PT variables [political, military, economic, social, information, infrastructure, physical environment, and time]. Using the PMESII-PT approach gives the user a holistic sense of the OE, but the OE Threat Assessments place greater emphasis on the military variable than the others. The military variable section provides information about weapons, equipment, threat force structure, recent actions (if applicable), and threat actor information. In 2014, CTID added two new OE Threat Assessments, one on Tajikistan and one on Kyrgyzstan. The primary threat actor operating inside Tajikistan is the Islamic Movement of Uzbekistan (IMU), which has known links with al-Qaeda. There are two primary threat actors operating throughout Kyrgyzstan: Hizb ut-Tahrir (HT) and IMU. HT operates in the Ferghana Valley region located in the southwest of the country. Though nonviolent, the group seeks to establish a caliphate centered on the Ferghana Valley and implement *sharia* law. The IMU has direct links with al-Qaeda, and at one time controlled more than half of the narcotics trafficked throughout Central Asia. The trafficking of narcotics through Kyrgyzstan's territory is a security concern for the current government.

Threat Reports focus on a specific threat *action* or group of related actions, and describe the tactics and/or techniques used by the threat actor. This product is an excellent resource to inform trainers on current threat actions occurring in multiple OEs. The threat action is explained in narrative text and typically accompanied by a graphic representation of the action. Appropriate background and contextual information is included, as well as a section on training implications so that users can clearly link the real world event to training scenarios. CTID released eight Threat Reports in 2014—

> ***Boot-Heel or Achilles Heel? Turkey's Hatay Province*** (January)—Ethnic Arab Alawites living in Hatay Province typically subscribe to an eccentric offshoot of Shia Islam that scorns Sunnis, especially including refugees from the ongoing Syrian civil war and supporters of the anti-Assad Free Syrian Army (FSA). Meanwhile, the current regime in Turkey is moderately pro-Sunni. Mihraç Ural, a Turkish-born Alawite long connected with militant leftist and separatist organizations, also leads a pro-Assad Shabiha militia unit that operates inside Syria. He has publicly advocated "cleansing" the Turkish-Syrian Alawite coastline of Sunni enclaves. Ural is suspected of perpetrating massacres of Sunnis in Banias Province, Syria on 2-3 May 2013, as well as twin car bombings in downtown Reyhanli, Turkey about a week later. His alleged involvement in both of these terrorist attacks underscores the danger that the Syrian civil war could jump international boundaries to enter a new phase characterized by a prolonged cycle of ethnic cleansing.

***If at First You Don't Succeed: 1 January 2014 Bombing of the Jazeera Hotel* [Somalia Hotel Bombing]** (March)—The Jazeera Hotel in Mogadishu, Somalia was the target of a complex attack on the evening of 1 January 2014. The attack consisted of a suicide vehicle-borne IED (SVBIED), two person-borne IEDs (PBIEDs), and a secondary vehicle-borne IED (VBIED) aimed at first responders. Al Shabaab, a Somali Islamist insurgent group that is associated with al-Qaeda, claimed credit for the attack. Al Shabaab's stated target was a meeting of senior intelligence officials. While Somali Federal Government and African Union forces have made significant progress against al Shabaab during the past three years, this event is a clear reminder that the group remains capable of performing major attacks using hybrid threat tactics.

Subterranean Environment: Key Player in 2006 Lebanon War (April)—In 2006, Hezbollah was able to achieve tactical, operational, and even strategic victory through its use of the subterranean environment. This report describes how Hezbollah created a complex integrated network of underground tunnel and bunkers throughout southern Lebanon as a key component of its planned defense.



South Sudan's Deep Divisions Surface (May)—On 9 July 2011, after years of fighting and political wrangling, South Sudan became the world's newest independent country. The excitement of the moment, however, hid the deep ethnic divisions within the new country. Relatively united while fighting to secede from Sudan, South Sudanese unity did not come with independence. Internal conflicts have added to the pressures of writing a new constitution and preparing to hold the first South Sudanese elections in 2015. The omnipresent problem in South Sudan is the growing and pervasive violence that manifests itself along ethnic fault lines. President Kiir is an ethnic Dinka, and his dismissed vice president is an ethnic Nuer, setting the stage for conflict on both the military and political fronts. These two largest ethnic groups have provided the impetus for the violence now plaguing South Sudan, with other ethnic groups playing contributing roles. South Sudan will remain an unstable and volatile area of the world for the foreseeable future. The hotspots will be defined by ethnic fault lines. Knowing where those fault lines are will be critical to anticipating where the next outbreak will likely be.

BRDM Scout Car (May)—This report is a contrast to a typical Threat Report in that its focus is on equipment versus a threat actor or tactic. The Army training community benefits from information about the proliferation of the BRDM (*Bronirovannaya Razvedyvatelnaya Dozornaya Mashina*) Scout Car throughout the world's militaries, and by understanding ways in which the hybrid threat may use the BRDM. The various BRDM variants have been used by Russia, former Soviet bloc countries, their partners, and currently non-aligned forces for over a half-century. Approximately 80 countries use BRDM variants in their armed forces. BRDMS are available for purchase—either by a country for military and/or law enforcement purposes, or even by individuals. Many countries will willingly sell their obsolete BRDMs to other countries that will still use them.

Serena Hotel Attack (September)—Aga Khan Development Network (AKDN) renovated the old Kabul Hotel at the request of Afghan President Hamid Karzai to be a secure place for foreigners and others working in Kabul. Despite being viewed as the most secure civilian compound in Kabul, four youth penetrated the multi-layered security perimeter on 20 March 2014. Hiding small guns in their socks, the four attackers moved through physical pat-downs and a metal detector to emerge inside the hotel where they killed nine people before Afghan Security forces killed them. The Taliban quickly took credit for the attack, but President Karzai also pointed accusations at Pakistan's Inter-Service Intelligence directorate. This attack points to the vulnerability of any place viewed as a target by an enemy. The facility was built and 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.

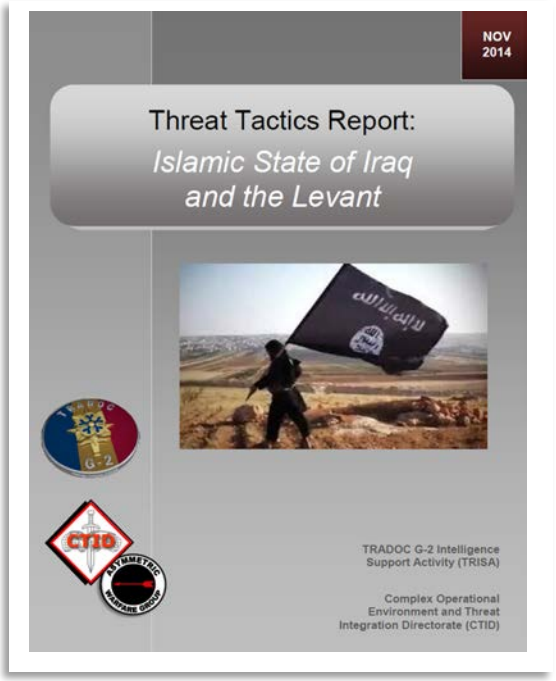
China Market Attack (October)—Historic ethnic tensions between minority Islamic Uighurs and majority Chinese Han in China's Xinjiang province have resurfaced, resulting in several recent terrorist attacks against Chinese Han. Radicalized Uighurs have increased terrorist attacks against majority Han within China, targeting larger crowds and adopting deadlier tactics. The Urumqi market attack is the most deadly, sophisticated attack within China to date.

The continued suppression and alienation of Uighur society closely resembles the fate of Baluchi separatists operating in Ariana, as depicted in DATE 2.1. Similar to the Baluchi separatists, Uighurs feel repressed by the Chinese government, a condition that reinforces and aggravates existing ethnic fault lines. A continuation of this suppression will likely result in an increase in violence targeting the majority Han population perceived as the enemy.

Crimea Crisis (October)—In less than a week after the pro-European protesters forced the resignation of pro-Russian President Viktor Yanukovych on 21 February 2014, and his subsequent hasty exodus to eastern Ukraine or Russia the following day, a large number of then-unidentified military personnel with support from local "self-defense" groups began to take control of strategic civilian and military facilities in the Crimean Peninsula. In early March 2014, multiple media sources reported these unidentified soldiers—most likely Russian troops—had taken control of Crimea. Over the next three weeks these organized units, with local militia assistance, took control of 189 Ukrainian military facilities and most of the Ukrainian naval fleet, and forced the Ukrainian military to leave Crimea for the mainland. Even more dramatically, the Russians did it with a slightly fewer military personnel on the peninsula than the Ukrainians had stationed there and with low casualty figures on both sides. The Russians used a combination of psychological operations, information warfare, coercion, bribery, naval and land blockades, and a limited amount of overwhelming force.

Threat Tactics Reports are a new type of product out of TRISA–CTID that serve to explain to the Army training community how an actor fights. Elements that contribute to this understanding may include an actor's doctrine, force structure, weapons and equipment, education, and warfighting functions. A Threat Tactics Report includes discussion of the actor's tactics and techniques, and recent examples of tactical actions will be described if they exist. An actor may be regular or irregular, and a TTR will have a discussion of what a particular actor's capabilities mean to the US and its allies. A TTR will also identify where the conditions specific to the actor are present in Decisive Action Training Environment (DATE) and other training materials so that these conditions can easily be implemented across all training venues.

TTR: Islamic State of Iraq and the Levant (ISIL) was published in November. ISIL is an evolution of an insurgent group that has changed its name to reflect an increasing geographic vision. ISIL's advantage to date has been an increasingly large number of fighters and deep cash reserves to fund its operations. This provides greater capacity to organize, train, and equip like a military organization. ISIL executes military tactics to the best of its capability. This is a greater capability than that shown by previous insurgencies in the area, but still not best practice in a number of warfighting functions and key tasks. High value targets for ISIL have included such infrastructure as dams and oil refineries, which also contribute to its cash flow.



More refined social media strategies capitalizing on readily available technology have given ISIL the means to advertise its successes to potential recruits worldwide and to threaten its enemies through graphic images. Finally, ISIL's rapid mobility, due to control of key lines of communication (LOCs) in Eastern Syria, is a key strength of the group.

In addition to the above products, the analysts at CTID conduct biannual training on threat tactics at Fort Leavenworth and other locations as requested, and are available to receive your phone calls and emails with requests for information about threat tactics, operational environments, DATE, orders of battle/threat force structure, and weapons and equipment.

CTID is part of the TRADOC G2 Intelligence Support Activity (TRISA) which is part of the G2 Operational Environment Enterprise (G2 OEE). Our monthly publications (*Red Diamond* newsletter, Combatting Terrorism Posters, and the Threat Team Advisory posters) are distributed through the OEE via email, and are also available on ATN along with most of our other products. Please contact us by phone or email with comments, questions, and requests for information.

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

Threat opposing forces (OPFOR) fight as a norm in a very practical manner. Threat OPFOR doctrine demonstrates a keen understanding and conduct of basic action fundamentals—*functional* tactics. The concept of *functional* tactics remains constant regardless of the echelon executing a mission. The core principle is to clearly understand the threat objective. Then, organizing by functional requirement and capability, the threat synchronizes the functional execution of combat power capabilities at a specific place and time in order to achieve its objective against an enemy. Whether conducting a small dismounted unit raid on an observation post (OP) or attacking across a broad front with large mechanized and supporting aviation formations—*function* is the underpinning of understanding and effectively applying "tactics is tactics is tactics."

Functional Tactics and Adaptive Application

The US Army's Training Circular (TC) 7-100 series describes OPFOR that exist for the purpose of training US forces for potential or known missions. OPFOR reflect a composite of the characteristics of military and/or paramilitary forces present in actual operational environments (OEs).

Hybrid Threat

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

Functional Tactics (Concept)
The conduct of primary and/or enabling actions by threat opposing forces (OPFORin order to achieve a task or mission objective.

OPFOR may replicate an enemy that US forces are currently in conflict with or might confront during near-term and midterm missions. Similar to actual or potential adversaries, threats, or enemies, opposing forces in training present robust challenges that often reflect the composition and capabilities of a hybrid threat.

TC 7-100.2, *Opposing Force Tactics*, is a basic reference on how an OPFOR commander specifies the initial organization or task organization of forces or elements within his level of command. At brigade or brigade tactical group (BTG)

echelon and above in task organization, subordinate threat OPFOR units and organizations performing tactical functions are referred to as *forces*, while at battalion or battalion detachment (BDET) echelon and below, the units and/or organizations are called *elements*.

Threat OPFOR Forces and Elements

At the brigade or brigade tactical group (BTG) echelon and above, the subordinate threat OPFOR units and organizations performing functions are referred to as *forces*, while at battalion or battalion detachment (BDET) echelon and below, the units and/or organizations are called *elements*.

TC 7-100.2, *Opposing Force Tactics*

Functions do not change dependent on the size of a unit or formation. However, a function of a particular threat OPFOR *force* or *element* may change during the course of an operation. While the various direct and support functions required to accomplish a given mission can be quite diverse in their combinations as capabilities are applied in sequence, series, or parallel actions, two general categories of function are *action* and *enabling* functions.

With a common threat OPFOR language and terms, each individual and leader—particularly in a hybrid threat—acknowledges a clear understanding of how the commander or organizational leader intends to functionally operate and/or fight each of his subordinate's capabilities. Subordinates that perform common tactical tasks such as disruption, fixing, assault, exploitation, security, deception, or main defense receive a clear designation as disruption, fixing, assault, exploitation, security, deception, or main defense forces or elements.

The use of precise functional designations for every force or element in a task organization minimizes any misunderstanding by subordinate units of the distinctive functions that the commander orders them to perform. These mission tasks are further confirmed during rehearsals, brief-backs, and backbriefs. This knowledge facilitates the threat OPFOR's ability to make quick adjustments and to adapt rapidly to unexpected conditions in a tactical situation.

Primary Functions: Action Forces and Elements

One part of the unit or organization conducting a particular offensive or defensive action is normally responsible for performing the primary function or task that accomplishes the overall mission goal or objective of that *action*. In general terms, that part can be called the *action force* or *action element*. In most cases, the higher unit commander identifies the action force or element with a more specific designation of its assigned mission or task.

For example, if the objective of the action at detachment level is to conduct a raid, the element designated to complete that primary action is called the *raiding element*. In offensive actions at brigade or BTG and higher echelon, a force that completes the primary offensive mission by exploiting a window of opportunity created by another threat OPFOR is called the *exploitation force*. In defensive actions, the unit or organizations that perform the main defensive mission in the threat battle zone is called the *main defense force* or *main defense element*. However, a maneuver defense at brigade or higher echelon uses a combination of two functional forces of *contact force* and *shielding force* in the main defensive actions.

Supporting Functions: Enabling Forces and Elements

In relation to the action force or element, all other parts of a unit or organization conducting an offensive or defensive action provide *enabling* functions of various capacities to an action force or element. Each of these units or organization can be called an *enabling force* or *enabling element*.

A specific functional title is assigned specific to the function or task to be performed. For example, a brigade-size force that enables by *fixing* enemy forces so they cannot interfere with the primary action is a *fixing force*. Similarly, an element that *clears* obstacles to permit an action element to accomplish a company detachment's tactical task is a *clearing element*.

Types of enabling forces or elements designated by their specific function may include—

- *Disruption force or element*. Operates in the disruption zone; disrupts enemy preparations or actions; destroys or deceives enemy reconnaissance; begins reducing the effectiveness of key components of the enemy's combat system.
- *Fixing force or element*. Fixes the enemy by preventing a part of his force from moving from a specific location for a specific period of time, so it cannot interfere with the primary threat OPFOR action.
- *Security force or element*. Provides security for other parts of a larger organization, protecting them from observation, destruction, or becoming fixed.
- *Deception force or element*. Conducts a deceptive action (such as a demonstration or feint) that leads the enemy to act in ways prejudicial to enemy interests or favoring the success of an OPFOR action force or element.
- *Support force or element*. Provides support by fire; other combat or combat service support; or command and control (C2) [the threat OPFOR uses the term "command and control"] functions for other parts of a larger unit or organization.

Tactics is Tactics

Large unit formations in offensive operations compared with a small unit assault illustrate the *functional* basis for actions and support as described in threat OPFOR doctrine. The historical vignette and assessment of major operations in an attack during *August Storm: The 1945 Strategic Offensive in Manchuria* by Glantz, presents a narrative of tactical actions and functions. This article summarizes offensive actions of the 2d Red Banner Army in the callout box below.

Large Scale Unit Tactics (Example WW II)

During the final phases of Russia's 1945 WW II combat actions in Manchuria, the 2d Red Banner Army conducted a supporting attack as part of the 2d Far Eastern Front in its strategic offensive operations. Three major subordinate organizations of the 2d Red Banner Army were an operational group comprised of two rifle divisions and two tank brigades; an operational group of one rifle division, one mountain rifle regiment, and one tank brigade; and a task-organized "fortified region" unit. The enemy in defensive positions along a major river line consisted of one infantry division and an independent mixed brigade of five battalions.

Artillery fires initiated the army attack that established multiple crossing sites across the river, but limited crossing equipment and bad weather conditions slowed Russian reinforcement of lead forces on the river's far banks. Gradually Russian momentum increased while supporting attacks focused on fixing and reducing enemy formations in their assigned zones. Other Russian units attacked and forced major penetrations on more than one axis in the army zone.

As enemy forces were defeated, contained in defensive positions in depth or were bypassed, Russian combined arms detachments task-organized from the operational groups exploited penetrations and continued to attack deep into the enemy rear areas. The enemy conducted strong resistance and conducted frequent localized sorties against Russian forces. Nonetheless, significant Russian artillery and aviation bombardment of enemy defenses and continued Russian ground maneuver attacks achieved enemy defeat and surrender.

The 2d Red Banner Army conducted successful offensive operations from 9-15 August 1945 over an area ranging 200 to 300 kilometers in width by 150 to 250 kilometers in depth. The army achieved its mission of fixing or defeating enemy forces in zone, and prevented their use against other major offensive actions of the 2d Far Eastern Front.

Summary from
August Storm: The 1945 Strategic Offensive in Manchuria **Glantz, D.M. (1983)**

This example of large-scale offensive actions and functions could be used in terms of how threat OPFOR brigade and task-organized higher echelon units could operate in training. The battle maps (see figure 1 and 2 below), for this article, of a corps-size area of operations with attack graphics and overlays of simplified symbols, control measures, and terms.

The small-scale unit sketches of an assault (see figure 1 and 2 below) focus also on function and tactical execution. The designations use OPFOR terms of *element* at battalion and subordinate echelons.

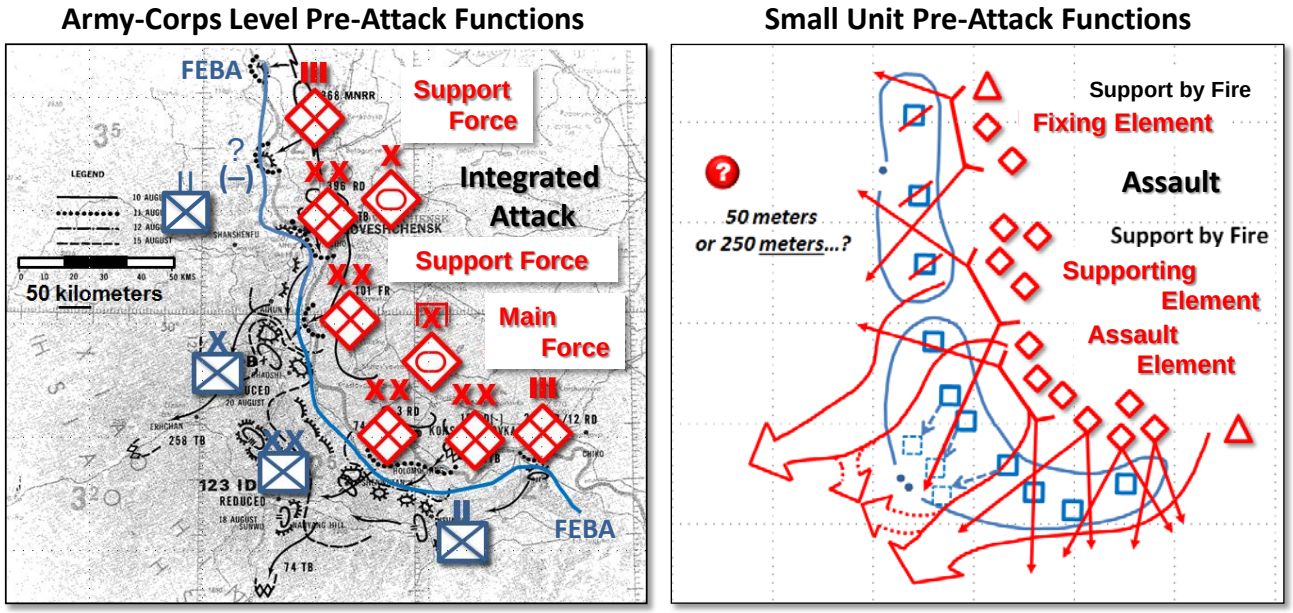


Figure 1. Echelon comparison of threat functions and terms (1 of 2) (example)

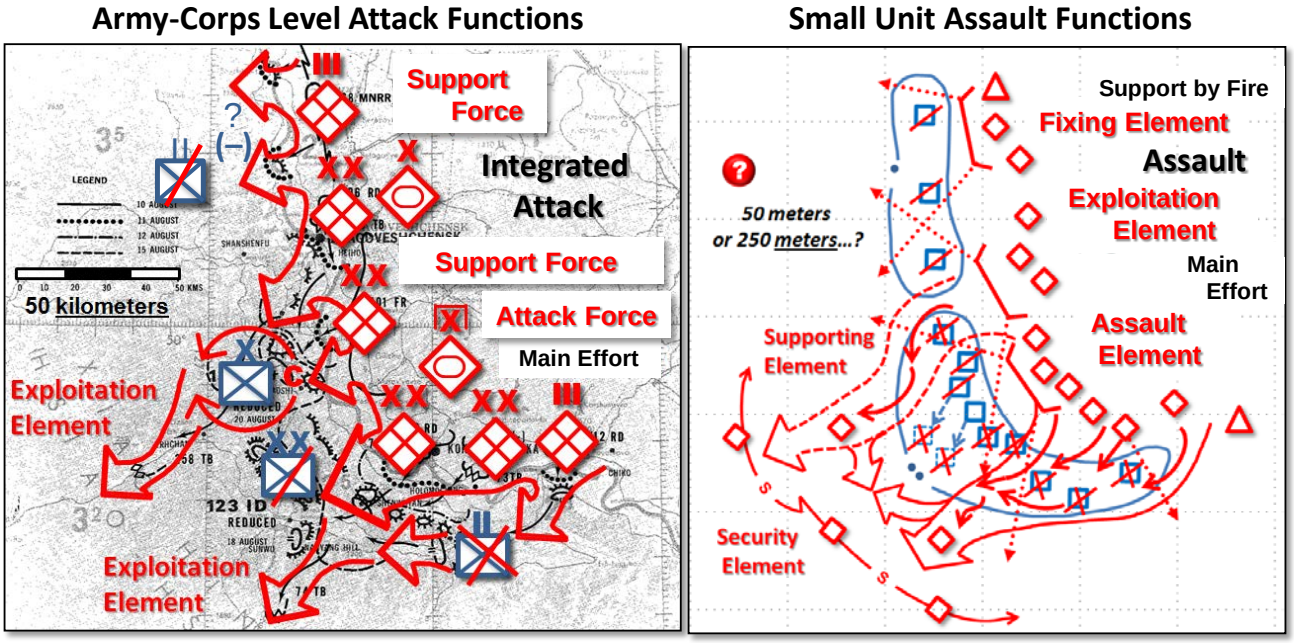


Figure 2. Echelon comparison of threat functions and terms (2 of 2) (example)

Other Threat Forces or Elements

In initial orders, some threat subordinates and capabilities are held in a status pending determination of their specific function. At the commander's or organizational leader's decision, some forces or elements may be withheld from initial actions, in *reserve*, so that this capability can influence unforeseen events or take advantage of developing opportunities. The designation of reserves is either a *reserve force* or *reserve element*. If and when such units are subsequently assigned a mission to perform a specific function, they receive the appropriate functional force or element designation. For example, a reserve force in a defensive operation might become a *counterattack* force. In another defensive action example, a particular unit or organization may require protection from enemy observation or fire. To ensure that it will be

available after the current action, the threat OPFOR commander designates that unit or organization as the *protected* force or element.

A unit or organization designated initially as a particular functional force or element may also be ordered to perform other or more specific functions during the course of an operation. In that case, the function of that force or element is more accurately described by that specific functional designation. For example, a disruption force generally disrupts enemy actions but also may need to conduct a fixing function during a period of a tactical operation. In that case, the entire *disruption* force could become the *fixing* force, or parts of that force could become *fixing* elements.

Implications for US Army Training and Education

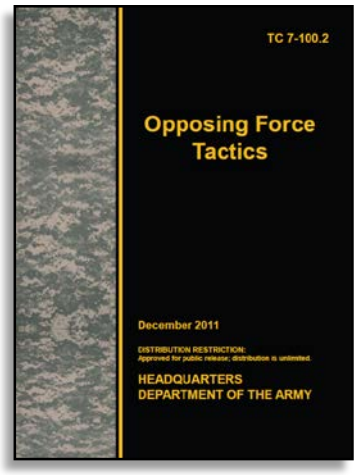
The Army provides several sources to describe opposing forces (OPFOR) for training. The training circular (TC) TC 7-100 series describes OPFOR within the conditions that exist for the purpose of training U.S. forces and achieving training objectives. A training objective consists of task, conditions, and standard. Readiness standards are identified by a unit commander and unit's mission essential task list and/or specified tasks for known or contingency operations. The *conditions* for Army training events must include a complex operational environment (OE) that is realistic, relevant, and challenging to the training unit, leaders, and Soldiers.

Condition. Those variables of an operational environment or situation in which a unit, system, or individual is expected to operate and may affect performance.

Department of Defense Dictionary of Military Terms

The threat in TC 7-100.2, ***Opposing Force Tactics***, reflects a composite of the characteristics of military and/or paramilitary forces that may be present in actual operational environments (OEs) in which US forces might become involved in the near-term and midterm. Like those actual threats or enemies, the OPFOR will continue to present new and different challenges for US forces. The overall nature of an OE is constantly changing and is an integral to situational awareness and understanding requirement for Army training.

TC 7-101, ***Hybrid Threat***, addresses an expanding category of threats and activities that do not fit into the traditional understanding of conventional and unconventional war. The focus is hybrid threats as simultaneous combinations of various types of activities by enemies and adversaries that will change and adapt over time.



This TC summarizes the manner in which future threats operationally organize to fight us. Description includes the strategy, operations, tactics, and organizations of the Hybrid Threat (HT) in training exercises.

Another training circular in the series is TC 7-100.3, ***Irregular Opposing Forces***, [soon to be released on the Army Publishing Directorate website] addresses irregular opposing forces (OPFOR) which represent individual and/or composite threats and enemies. The three primary categories of irregular forces portrayed by the OPFOR are insurgents, guerrillas, and criminals.

Actors may operate separately or in conjunction with one another and/or combined with regular military forces as a Hybrid Threat (HT). Other actors may be independent or may be affiliated or associated with irregular OPFOR through willing support or coercion, and/or be passive or unknowing supporters of the irregular OPFOR.

TRADOC G2 provides the threat conditions to live, virtual, constructive, and gaming (LVCG) training environments to replicate conditions representative of an actual OE. The CTID researches and sustains robust and realistic threat opposing forces for training. Requests for information and related training and education support can refer to subject matter experts and their contact information at the end of this newsletter.

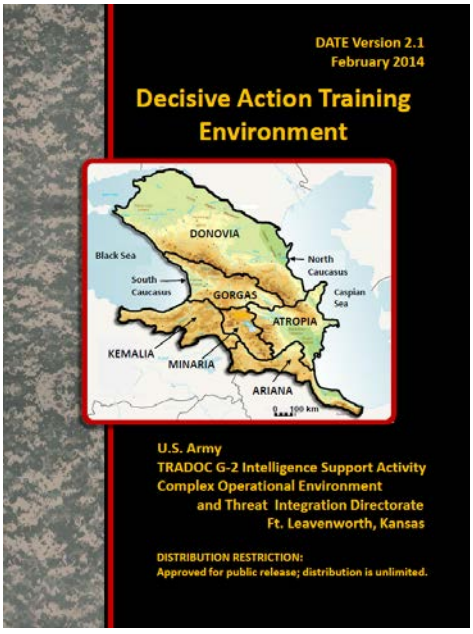
Opposing Force (OPFOR) Insights: DATE Rotation 14-04 at the National Training Center
by LTC Shane Lee, TRISA-CTID

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.

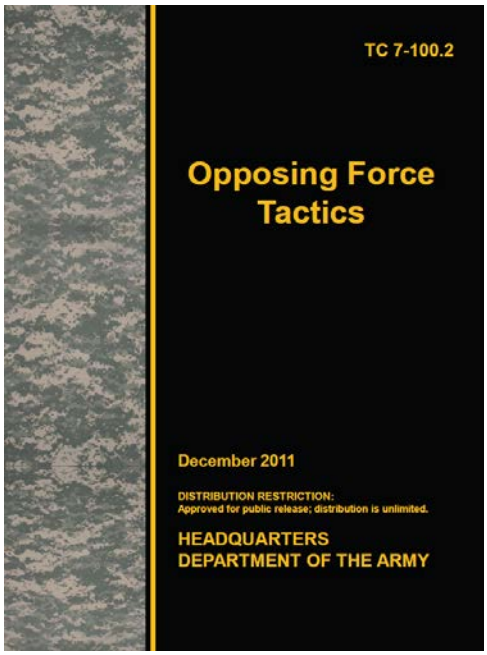
Commander's Intent: The purpose of our operation is to prevent US and Atropian forces from seizing key military and urban areas IVO the IB.

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.

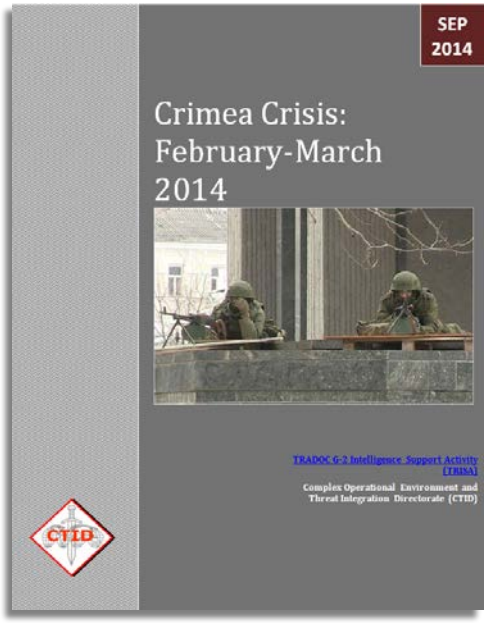
In order to foster and build a World Class OPFOR, the 11th DTG should approach the planning cycle for a DATE rotation as a unit/team with detailed knowledge to operate efficiently and effectively as a hybrid threat, not as a US Force. This unit/team extends beyond the 11th DTG to the NTC Operation Center; 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.

by H. David Pendleton, TRISA-CTID (CGI Ctr)

In less than a month's time starting in late February 2014, Russian and local militia elements took control of Crimea, defeated the approximately 25,000 Ukrainian military personnel stationed there, orchestrated the independence of the peninsula from Ukraine, and facilitated Crimea's eventual merger with the Russian federation. The lightning speed of the takeover caught the local Ukrainian military off guard. Seizure of strategic targets by pro-Russian paramilitary Crimean self-defense units augmented by highly-skilled and heavily-armed uniformed personnel of undeclared origin allowed the operation to run smoothly. Russian President Vladimir Putin later acknowledged these unidentified professional military augmentees to be Russian soldiers. Paralysis displayed by Ukrainian political leaders in Kiev resulted in only a token resistance by the country's military and contributed significantly to a successful Russian *fait accompli* in Crimea.

The Threat Report, *Crimea Crisis: February-March 2014*, (available soon on ATN) examines the events during the four-week run-up to the Russian seizure of Ukraine from strategic, operational, and tactical perspectives and provides historical context in analyzing the crisis.

Strategic Situation



At the strategic level, there are three major issues in play between Russia and Ukraine. First, historical friction between the two countries dates back many centuries. The area that now comprises Ukraine has been fought over by more powerful neighbors for at least 500 years. In the 14th century, Poland and Lithuania annexed most of what is now present-day Ukraine. In the 17th century, Russia and Poland divided most of Ukraine's territory lands between themselves. When Poland was subsequently partitioned, Russia appropriated almost all of Ukraine into its own empire.

After a short-lived period of independence following the end of World War I, the Soviet Union seized the eastern two-thirds of Ukraine, converting the country to a Soviet Socialist State (SSR). After Nazi Germany's defeat in World War II, the Union of Soviet Socialist Republics (USSR) re-appropriated not only the former Ukraine SSR, but also territory comprising what is today the western third of Ukraine. When both Russia and Ukraine belonged to the USSR, the leaders in Moscow and Kiev usually found common ground. When the Soviet Union collapsed in the early 1990s, the relationship between the two

former Soviet states became more strained as Ukraine found itself embroiled in a renewed competition for influence between Western Europe and Russia.

A second historical dimension of the present-day crisis is a longstanding language barrier that plagues Crimea's unique relationship with Russia. In order to foster a more cohesive bond between the heterogeneous peoples of the Soviet Union after World War II, the Soviet government decided that the Russian language should become the dominant vernacular throughout the USSR. For Ukrainians, this meant the suppression of the role played by their native tongue in sustaining the country's unique culture and traditions. In the eastern part of Ukraine, the predominance of the Russian language and culture resonated more among the local population than was the case throughout the western portion of the country.

In the two easternmost Ukrainian provinces, Donetsk and Luhansk, Russian is the primary instructional language in a majority of the schools. In Crimea, a part of Russia from the founding of Sevastopol in 1783 until 1954, only 8% of the students currently receive formal schooling imparted in the Ukrainian language. In the remainder of the country, Ukrainian is the primary language of education. Native Crimeans, reflecting the influence of a large indigenous ethnic Russian population as well as a sizeable Russian/Soviet military retiree population, tend to regard their province as part of Russia and not Ukraine. This attitude prevails despite 60 years of Ukrainian rule.

The final strategic problem affecting the current crisis is Ukraine's dependence on Russia for its hydrocarbon resources, especially natural gas. Ukraine produces no natural gas of its own, and imports 100% of its energy from Russia through the latter's gas company, GazProm. Since Ukraine became a nation-state in its own right in 1991, Russia has wielded the price of natural gas as both a carrot and a stick to keep its neighboring country in line politically. When Ukraine complies with Russian guidance or supports the Russian geopolitical party line, GazProm reduces the price of natural gas. Conversely, when Ukraine's leaders take exception to Russian policies or demonstrate support of policies tending to remove them from the Russian sphere of influence, GazProm raises the price of natural gas. Since Russian leaders believed that Ukraine supported Georgia in the 2008 Russo-Georgian Conflict, GazProm stopped all natural gas shipments to Ukraine before eventually striking an agreement that charged Ukraine a higher price.

After a former pro-Russian Donetsk provincial governor, Viktor Yanukovych, won the Ukrainian presidency in February 2010, GazProm gave Ukraine a 30% discount in return for allowing Russia to station its Black Sea Naval Fleet in Crimea until at least 2042. In November 2013 Ukrainian leaders refused to sign a trade agreement with the European Union (EU). The following month, GazProm cut its price of natural gas to Ukraine by an additional one-third. Yet almost immediately after the Ukrainian government impeached Yanukovych in February 2014, GazProm raised the price of natural gas sold to Ukraine by 80% through early April 2014, until GazProm finally halted all gas shipments to the country in June 2014.

Operational Level

At the start of the present crisis in late February 2014, Russia had about 16,000 military personnel stationed in Crimea, in comparison with Ukraine's 25,000-strong military establishment. Most of the personnel on both sides stationed in Crimea before mid-February 2014 were naval, with a few exceptions. Due to the treaty that allowed the Russian Black Sea Fleet to remain in Crimea, the Russians could station up to 25,000 military personnel in the province; these also enjoyed a freedom of movement that afforded them easy deployment from and redeployment to their home country.

Russia used the 25,000 strength level ceiling to bring in approximately 10,000 specialized military personnel, including airborne troops and special forces personnel just days prior to the military takeover that began on 27 February 2014. The Russians then invoked the treaty's freedom of movement clause to move their ground troops near strategic targets at the onset of the military maneuvers.

The Russians chose their targets thoughtfully, based on their experiences over the last 30 years, especially drawing from information gathered during their 2008 campaign in Georgia. Russians, in unmarked uniforms along with local defense groups that provided a front to create the impression of internal Crimean as opposed to external Russian involvement, captured 189 Ukrainian military facilities within a four-week period. Ukrainian military personnel either escaped to their country's mainland or defected; this was especially true for naval personnel. See figure 1 for selected targets.

Figure 1. Selected targets of Russian forces (Numbers correspond to actions as listed below.)

The numbers on the map above correspond to the following targets in the order listed. This is not a complete list. Details of each action are in the Threat Report:

(1) 27 February 2014: Crimean parliament building and cabinet of minister's building.

(2) 27-28 February 2014: Simferopol civilian airport.

(3) 27-28 February 2014: Sevastopol military airport.

(4) 28 February 2014: Krym State Television Company and Urktelecom facilities throughout Crimea.

(5) 6 March 2014: Naval blockade of Donuzlav Lake.

(6) 6 March 2014: Remaining Ukrainian media stations.

(7) 8 March 2014: Warning shots fired at the Organization for Security and Cooperation in Europe (OSCE) observation teams.

(8) 10 March 2014: Targets of opportunity such as the Simferopol military hospital.

(9) 13 March 2014: Pro-Ukrainian and anti-Russian websites by blocking.

(10) 15 March 2014: Natural gas pipeline station to the Crimean peninsula.

(11) 18 March 2014: More difficult targets using overwhelming force.

(12) 19 March 2014: Capture and subsequent release of the Ukrainian Navy Commander.

(13) 21 March 2014: Ukrainian 174th Air Defense Regiment base with S-300 surface-to-air missiles.

(14) 21 March 2014: Prevention of Ukrainian ships that attempted to run the naval blockade.

(15) 22 March 2014: Belbek Airbase territory not already in Russian possession.

(16) 24 March 2014: Ukrainian 1st Marine Battalion.

The Russians used no tanks during this time, and the most advanced armored personnel carriers (APCs) used in these operations were BTR-80s. (See *The BTR Handbook-The Universal APC* for details on this APC's capabilities). The Russians and the Crimean militia used a combination of naval blockades, barricades to prevent soldiers leaving their bases, psychological warfare, intimidation, and bribery to convince most Ukrainian units to surrender without offering resistance. In units whose commanders initially refused to surrender, a few well-placed shots and a couple of resulting casualties typically sufficed to quickly change the resistors' minds. On 17 April 2014, Russian President Vladimir Putin finally revealed the worst-kept secret of the entire operation: Russian troops had been present in Crimea during the February/March 2014 military action. The Ukrainian government in Kyiv, however, refused to respond to the crisis even when the Ukrainian military held the upper hand in terms of personnel and heavy weapons. By the time the Ukrainian government decided to have their forces in Crimea resist, it was too late as Russia then held the advantage in both quantity and quality of the ground forces on the peninsula.

Tactical

One of the best examples of a tactical action reported in open sources was the seizure of the Ukrainian command ship *Slavutych* (U-510) in the Sevastopol Harbor on 22 March 2014. On 3 March 2014, five Russian tugboats positioned themselves behind the *Slavutych* and a neighboring ship, the U-209 *Ternopil*, to prevent them from leaving the docks. The Russians and local militia quickly took control of the *Ternopil*, but the *Slavutych*'s commander backed his ship 10 meters away from the pier to prevent hostile forces boarding via the landward side. Over the next few weeks, the *Slvautych's* crew kept their ship from being boarded by the enemy, primarily by using water cannons.

Two small Russian warships eventually relieved the tugboats and positioned themselves about 50 meters seaward from the *Slavutych*. Over the next three weeks, naval and ground forces kept a 24-hour watch on the Ukrainian command ship. After the Russian Black Sea Fleet commander boarded the *Ternopil* to inspect the captured vessel, the Russians gave the *Slavutych* in Sevastopol Harbor and the rest of the Ukrainian navy bottled up at Donuzlav Lake until Friday, 21 March 2014, to either surrender or join the Russian Navy. Using various psychological techniques that included urging mothers of the sailors on board the *Slavutych* to call their sons' cell phones, up to 40% of the crew eventually deserted the ship.

On the day of the Russian boarding, fathers also called, urging sons to stay in their cabins, unlock their doors, and leave them open, since the attackers would probably break down the doors anyway. Many of those on board were native Crimeans and felt little allegiance to Ukraine. Some of the sailors were not technically members of the Ukrainian military, but working as civilian contractors. Several of the sailors simply jumped overboard to escape; their mothers came, fished them out of the water, and took them home. Many sailors chose to join the Russian Navy, fearing that Ukrainian sailors who offered no resistance would be treated as deserters once they returned to Ukrainian-controlled territory. This was due in part to rumors indicating that some sailors who abandoned other ships had been arrested and were facing trial and possible prison sentences ranging from five to seven years. Other sailors simply chose to join the Russian Navy because they were native Crimeans, ethnic Russians, or married to local Crimean women; for them loyalty to family, heritage, or ship trumped national allegiance to Ukraine. (See figure 2.)

Despite all the psychological and family pressure, the *Slavutych's* captain and some of the crew refused to surrender their ship and remained loyal to the Ukrainian government in Kiev. Shortly thereafter it became apparent that the local defense forces would attack the *Slavutych* on the evening of Saturday, 22 March 2014. That afternoon, several of the ship's crew—some in uniform and some in civilian clothes—left the *Slavutych*, carrying their possessions in black plastic bags. At approximately 1730 hours local time, a tugboat with a few dozen men approached the Ukrainian ship while bystanders watched from the pier. While it appeared to some onlookers that the attackers were members of the self-defense forces, at least one witness alleged that the tugboat carried Russian special operations personnel.

Sailors aboard the *Slavutych* used their loudspeaker system to warn the approaching vessel against illegally boarding the ship, but to no avail. The Ukrainian ship then began to play the patriotic song *Varyag,* a heroic composition dating back to the Russo-Japanese War.

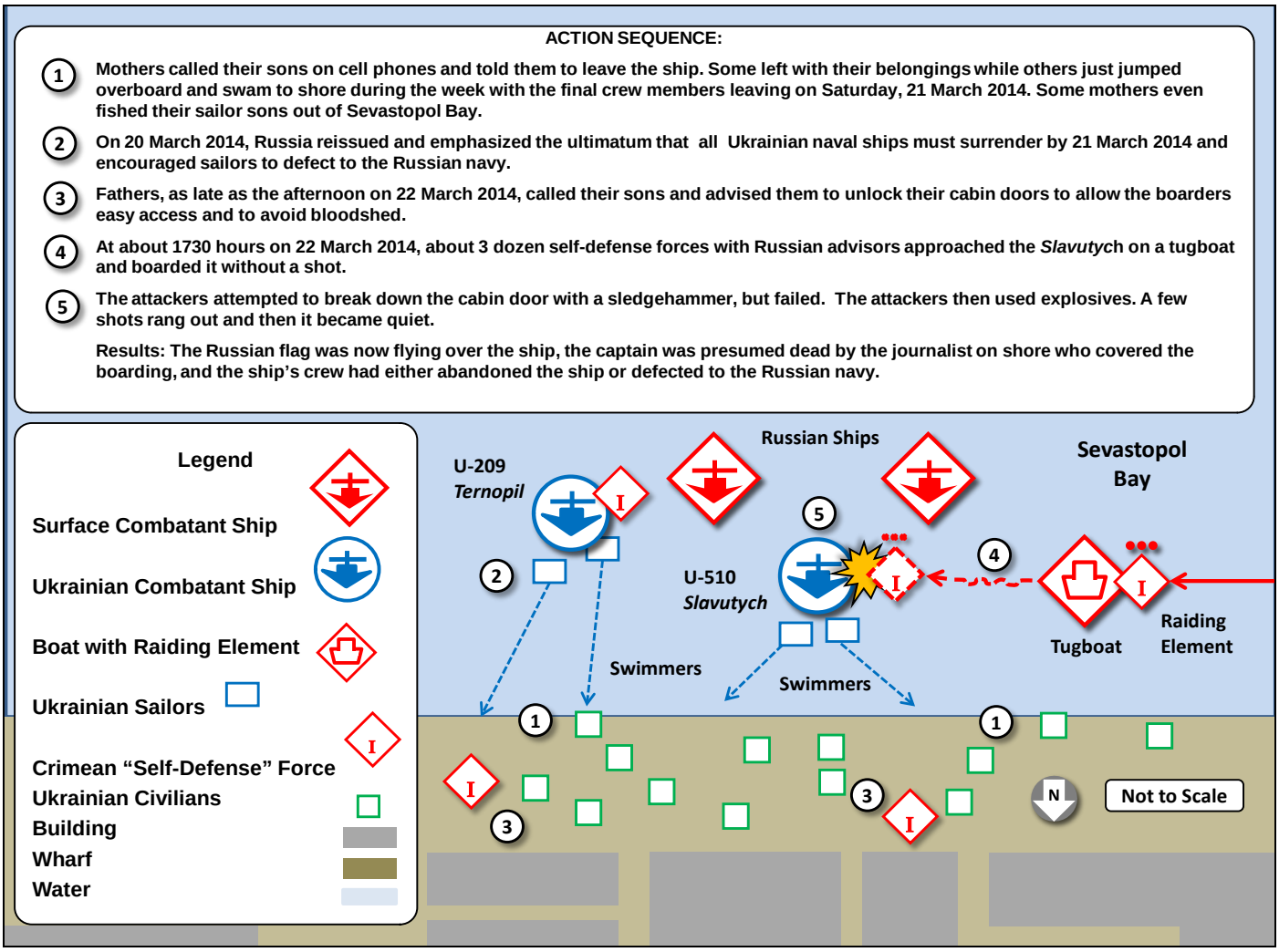


Figure 2. Storming of the Ukrainian command ship, U-510 *Slavutych*, on 22 March 2014

The attackers on the tugboat reached the *Slavutych* and then boarded it. By that time, almost everyone had surrendered except for the ship's captain, who had locked himself in his cabin. The attackers first tried to use a sledgehammer to break the door down. When that failed, they resorted to grenades. A few gunshots rang out after the sledgehammer echoes faded and the grenades exploded, but soon after the noise abated, the Ukrainian flag came down from the mast and the boarders raised a Russian flag in its place. The storming of the *Slavutych* was over in a matter of minutes.

The capture of the *Slavutych* is an excellent example of an attack to gain control of equipment, as described in Training Circular (TC) 7-100.2, Opposing Force Tactics. The only difference is that in this instance the attack occurred on water instead of land. While the Russians may call the units that participated in the attack by a variety of names, the attackers on the tugboat consisted of raiding, security, and support elements.

Summary

Since most of the Ukrainian military personnel stationed in Crimea were sailors as opposed to ground combat troops, there were few Ukrainian ground forces available to meet the military challenge posed by Russia and the local pro-Russian self-defense units. Although most of the Russian military personnel originally stationed in Crimea were sailors, sufficient ground forces entered Crimea by air and sea to convince most Ukrainian military personnel to surrender without a fight.

Once the pro-Russian forces seized selected strategic targets, the combination of Russian military and local self-defense forces systematically took control of the remaining military installations in Crimea. The Russians deployed soldiers in

uniforms that bore no identifiable markings in an attempt to afford themselves plausible deniability, but almost immediately observers external to Crimea discerned the true nationality of the well-trained and well-armed invaders.

To lend an indigenous flavor to operations, the Russians assigned their advisors to local militia units and allowed the self-defense forces to seize many of the softer targets. For the more difficult or important objectives, the disguised Russian forces either took the objectives themselves or heavily augmented the local self-defense units. Ultimately, the failure of the Ukrainian government in Kiev to react decisively with military action to the events in Crimea lost them their province as much as the Russian-led forces won. With the ongoing conflict in eastern Ukraine, it is highly unlikely that Ukraine will regain possession of Crimea in the foreseeable future.

by Pat Madden, TRISA-CTID (BMA Ctr)

Unmanned Aircraft System (UAS) development and proliferation have soared to new heights during the past decade and show little signs of significantly slowing in the near future. A 2013 market study by the Teal Group estimates that global UAS spending "will double over the next decade, rising from $5.2 billion in 2014 to $11.9 billion in 2023."[1]

Currently, approximately 50 nations employ UAS with estimates that the US could control approximately 60% of the market by 2020.[2] It goes without saying that UAS has proven its value to the US and its coalition partners in Iraq and Afghanistan.

Many lives have been saved by the ability of these robotic planes to conduct aerial reconnaissance and air-to-ground missile attacks on the insurgents operating in these countries. However, during these conflicts, vulnerabilities have surfaced that call into question their long term survivability in a highly kinetic, conventional war where the ground, sea, and airspace is contested.

Potential threat countries like China, Russia, and Iran are steadily building up their arsenals of weapons that could make the next military environment much more lethal and challenging than the conflicts we have been engaged in for over a decade.

UAS vulnerabilities observed, such as implications of high accidents rates, information warfare (INFOWAR), and integrated air defense systems (IADS) attacks make this relatively new aerospace asset potentially vulnerable in future conflicts. Even with known weaknesses being addressed, the ultimate issue for future UAS value is one of timeliness in resolving these vulnerabilities.

Implications of High Accident Rates

At first glance, high accident rates may not indicate a critical vulnerability other than lack of performance. However, high accidents rates can potentially contribute to more serious issues.

Many of the UAS deployed to Iraq and Afghanistan were not systems that had completed formal military development, testing and fielding processes. Often they were rushed into theater in an effort to provide valuable air surveillance, especially at the tactical level.

Assumed risk meant many shortcomings. Inadequate flight manuals, lack of enough trained pilots, sustainment issues, extreme physical environment variations, as well as design and system flaws were just a few of the problems initially contributing to these high rates of failure. As late as 2005, human error, combined with a harsh environment and other factors mentioned, including dependency on a constant navigational signal, all "contributed to a UAS accident rate 100 times greater than manned aircraft."[3]

By 2010, thirty-eight UAS MQ-1 Predators and MQ-9 Reapers had "crashed during combat missions in Afghanistan and Iraq."[4] Total UAS flight hours over Afghanistan and Iraq between 2006 and 2009 tripled, but tactical commanders claimed that only a third of their surveillance requests for coverage were executed.[5]

Losses due to accidents were highest at the Army tactical level. For example, during the early years of UAS RQ-7 Shadow deployments, accidents reached a rate of more than 400 per 100,000 flight hours.[6] This high rate of loss occurred even though the Shadow was a program of record. Much of these initial losses were due to communication and engine related failures. Despite recent improved accident rates and future engine/communications upgrades, these and other UAS mishaps negatively impacted the warfighters.

Figure 1. Armed MQ-1 Predator

Figure 2. RQ-7 Shadow UAS on catapult launcher

The results of growing pains with UAS platforms negatively affected ground forces in two ways. First, the high accident rates of theater, operational and tactical UAS meant a loss of timely intelligence from air surveillance coverage resulting in missed opportunities to attack/destroy fleeting targets. Second and most importantly, was that some UAS were never recovered. If not seriously damaged, UAS can potentially be stolen and then sold or traded to other countries which in turn could be reverse engineered and exploited. Some captured UAS as well as prototypes in Iran and China have either been displayed or are in the early stages of testing. The well-known seizure of a US RQ-170 Sentinel in Iran was lost by its CIA operators on the 29th of November 2011 and put on display the following month.[7] A more serious development was Iran's announcement that Russia and China were requesting access to the RQ-170.[8] Assuming the data on board was encrypted, valuable intelligence could still be gained such as design, propulsion, and radar resistant stealth coating.[9]

Additional UAS designs have shown up in threat countries, such as the Chinese Sharp Sword and the Wing Loong. The Sharp Sword is a stealth delta wing design powered by a jet engine. The Chinese government claims it is currently undergoing flight tests.[10] The Wing Loong is very similar in design to the Predator and is advertised as having a weaponized capability as well as being for sale.[11] This new UAS, like many other Chinese weapons, could easily be proliferated to other potential threat nations like North Korea. It is estimated that approximately 23 nations are in various stages developing armed UAS.[12] Even more troubling is if access to the RQ-120 was granted to Russia or China, what type of compensation agreement was made? If a deal was made it could have involved a technology exchange such as long range ballistics or sophisticated electronic warfare. The point of this discussion is that losing a UAS is not just a loss in dollars or surveillance. It also has the potential of ending up in the hands of threat nations that can exploit its technology against us in future conflicts.

UAS Vulnerabilities to Information Warfare

Two of the seven elements of INFOWAR discussed in TC 7-100.2, *Opposing Force Tactics*, are electronic warfare (EW) and information attack (IA). EW is defined as "activity conducted to control or deny the enemy's use of the electromagnetic spectrum, while ensuring its use by the OPFOR." IA is defined as focusing "on the intentional disruption or distortion of information in a manner that supports accomplishment of the OPFOR mission." UAS are especially vulnerable to EW jamming since many of them are dependent on navigational signals from the satellite based Global Positioning System (GPS). These signals are also used for armed UAS targeting as well as the uninterrupted communications with the associated ground control stations. Access to GPS jamming devices is readily available on the open market and relatively cheap. Vulnerabilities to GPS have been known since the Bosnia campaign of the 1990s but have recently been highlighted in the open press. On 19 June 2014, the Federal Communications Commission

(FCC) levied a historical fine of S34.9 million against a Chinese firm called C.T.S. for illegally selling GPS jammers in the US for as cheap as $25.[13] Many of the jammers have been used by truckers to prevent their GPS fleet tracking systems from monitoring their locations, as well as avoiding taxes and fees. The most infamous recent incident involved a trucker in New Jersey that inadvertently jammed the GPS ground signals at the Newark Liberty International Airport.[14] Several other countries like Russia also manufacture inexpensive commercial GPS jammers, all of which can be used against UAS GPS signals.

This capability is not missed by potential threat military forces or insurgents, as evidenced below. Beginning in August 2010, North Korea's military began a series of large-scale jamming efforts aimed at South Korean GPS signals, interrupting military exercises intermittently until the spring of 2012.[15] The transmitters were believed to have come from Russia and were positioned near the South Korean border. These attacks were only stopped after the South Korean president requested intervention from the Chinese government.[16] This example of large-scale barrage jamming can also have devastating effects on UAS whether or not the GPS signal is encrypted. Alternately, insurgent EW interests were demonstrated when recent reports leaked that that al-Qaeda in 2010 "was sponsoring research to develop jammers that could be used to disrupt both GPS signals and infrared tags used by drone (UAS) operators to guide missiles."[17] Also mentioned were efforts to build laser detectors to provide early warning of UAS air-to-surface missile strikes, and the testing of GPS jammers in North Waziristan.[18] Even more alarming were reports that senior al-Qaeda leaders have distributed "a 'strategy guide' to operatives around the world advising them how 'to anticipate and defeat' unmanned aircraft."[19] It is only a matter of time before these EW capabilities develop and spread to other insurgents across the globe.

Further EW and IA UAS vulnerabilities include passive interceptions of UAS video feeds from their sensors, and GPS spoofing. In 2008 it was revealed that a cheap software application called Sky Grabber was being used by an apprehended Shiite insurgent in Iraq to passively intercept and download full-motion video from UAS sensors onto his laptop.[20] The insurgent was able to purchase this software for approximately $26 and successfully intercept sensor videos being transmitted to ground control stations because the signals were unencrypted. In 2009 the US military also found evidence that other downloads "were being intercepted and shared with multiple extremist groups."[21] Information from the videos showed where and what the UAS were targeting, providing valuable information on US military surveillance patterns. The ability to determine the extent of this capability is limited because it is passive. However, it is not hard to imagine that this technique could be or is currently being applied with other insurgencies.

UAS GPS spoofing is an electronic IA attempt to deceive a GPS receiver by transmitting counterfeit navigational signals, or resending legitimate signals captured elsewhere or at a different time. These initial spoofed signals can force the receiver to synchronize with the spoofer's signal and then begin to accept false location signals. If successful, the UAS can then be flown, landed, or destroyed by these false navigational signals. While spoofing attacks against US military UAS have not been documented, there have been successful spoofing demonstrations against civilian UAS. On 19 June 2010, Associate Professor Todd Humphrey, from the University of Texas at Austin, led a research team that successfully performed a spoofing attack at White Sands, New Mexico.[22] They successfully demonstrated to observing Department of Homeland Security officials the ability to take control of a UAS by manipulating unencrypted GPS signals, diverting the UAS approximately one kilometer away from its scheduled flight path. The purpose for the demonstration was to raise awareness of our vulnerability to GPS spoofing attacks against domestic commercial and government UAS. Of further concern, the successful spoofing device used in this attack was made by engineering students at the university for less than $1,000.[23]

Both spoofing and the interception of sensor videos pose significant vulnerabilities to unencrypted satellite and radio frequency signals. The US military acknowledges this and has been working diligently to encrypt UAS signals. The challenges are complex and expensive. The current UAS have to be retrofitted, or new ones built, to carry the encryption. This means heavier payloads, which in turn means reduced operational ranges, unless other modifications such as wing span and engine power are increased. An equal encryption effort has to be applied to the associated ground control stations and remote video receivers.

UAS Vulnerabilities to Air Defense Artillery (ADA)

Depending on the level of a threat country's capabilities, the most significant vulnerability to UAS is a linked, cohesive, multi-layered integrated air defense system. Several threat countries like China, Russia, and North

Korea have significant IADS capabilities. IADS enables engagement of UAS at long stand-off ranges, with integrated engagement capabilities at low, medium, and high altitudes. This provides early warning and enables ADA units time to coordinate and acquire incoming targets. They will also focus on operating passively since most conventional armies know their ADA systems are vulnerable to associated target acquisition radars.

According to the 2013 Worldwide Equipment Guide (WEG), many IADS also have passive air detection capability. They include sensors such as high-power TV day sights, infrared or thermal night sights, acoustic triggered ground sensors, and radio frequency direction-finders. This capability is also augmented by other units, such as reconnaissance and artillery, which can enhance the IADS capability. Together these capabilities – combined with operating autonomously, relocating frequently, and remaining dispersed – provides a formidable threat to relatively slow moving UAS with continuous electronic signatures.

Training Implications at Combat Training Centers

The lethal effects on UAS from ADA are being played out at the majority of the CTCs during Decisive Action Training Environment (DATE) training exercises. The majority of the CTCs engage their opposing force (OPFOR) hybrid threat ADA and INFOWAR assets against rotational unit's UAS. Attacks include jamming of GPS downlinks, interception of optical sensors, ADA destruction of UAS, and ground attacks against launch and recovery sites**.** CTID CTC liaison officers (LNOs) routinely observe these training exercises which include ADA engagements.

CTC examples of recent exercises observed by these LNOs include the Joint Readiness Training Center (JRTC), National Training Center (NTC), and the Mission Command Training Center (MCTP) respectively. During JRTC DATE Exercise 13-09 in August 2013, the hybrid threat unit intercepted unencrypted UAS feeds and watched real-time video throughout the exercise. They also shot down one RQ-11 Raven and destroyed or damaged three RQ-7 Shadows and launchers by ground attack. During NTC DATE Exercise 14-04 in February 2014 multiple RQ-7 Shadows and MQ-1C Gray Eagles were shot down by ADA systems, including Russian SA-6s. The final example is a nine-hour extract of UAS losses during MCTP DATE Exercise 14-5B during the evening of 17-18 June 2014. Table 1 illustrates the UAS losses during this seven day competitive, simulated exercise. The losses could have been higher if it included high to medium altitude ADA which was limited due to simulation and artificial restrictions. It is acknowledged that the data cited above takes place in controlled environments which is not actual combat. However, these training examples extracted from competitive, highly kinetic hybrid threat OPFOR illustrate that UAS will sustain significant losses given their current vulnerabilities.

Table 1. UAS Losses in Seven-Day Simulation

ADA UAS Kill Report Form*	
Time	**Destroyed per ADA System**
Start: 170257Z 14	**SA-15 - 5**
Stop: 180801Z 14	**SA-17 - 3**
	SA-18 - 11
	2S6M1- 4
Total Destroyed	**23**
**** Note:*** **Numbers include other division/corps UAS assets**	

Summary

Despite significant challenges with tighter military budgets and force reductions, determined efforts are underway to develop more advanced UAS to combat known vulnerabilities. Better sensors, stealth technology, encryption, propulsion, "sense and avoid" radar, and integrated ground control stations are just some examples of ongoing developments to counter UAS threats.

The question is can these improvements be fielded fast enough in light of the projected downsizing of the defense budget? Since potential threat nations will continue to develop more sophisticated attacks against UAS technologies, will the US be able to counter these efforts in the ongoing battle for technology supremacy? Are the UAS testing, training, encryption and navigation efforts now, and in the future, sophisticated enough to withstand the challenges of non-permissive air, land, and sea environments?

All these factors must be considered, as well as over a decade of lessons learned in Iraq and Afghanistan. Current and future UAS vulnerabilities indentified must continue to be quickly and efficiently corrected if we hope to successfully remain competitive and meet future challenges in an ever changing, increasing complex, and hostile environment.

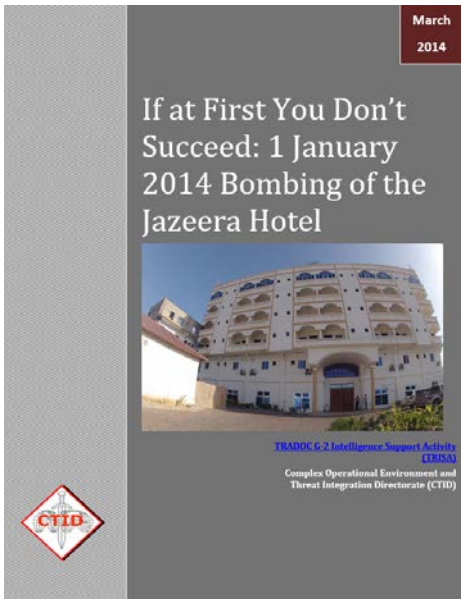
Endnotes

[1]John Keller, "Teal: worldwide spending for unmanned aerial vehicles (UAVs) to double over next decade," Military & Aerospace, 15 August 2013.
[2] Derrick Maple, "Briefing: Global UAV market forecasts to 2020 Jane's Global Market forecasts to 2020," Jane's Defence Industry, IHS Jane's, 6 February 2012.
[3] Jaysen A. Yochim, "The Vulnerabilities of Unmanned Aircraft System Common Data links to Electronic Attack," Master of Military Art and Science, US Army Command and General Staff College, Fort Leavenworth, Kansas, 11 June 2010.
[4] David Zucchino, "War Zone Drone Crashes Add Up," Los Angeles Times, 6 July 2010.
[5] David Zucchino, "War Zone Drone Crashes Add Up," Los Angeles Times, 6 July 2010.
[6] "Shadow UAV Defies Gravity With Success," DefenceTalk," 9 March 2011.
[7] Scott Shane and David Sanger,"Drone Crash in Iran Reveals Secret US Surveillance Effort," The New York Times, 7 December 2011.
[8] "Russia, China seek info on US drone held by Iran," Fox News, 19 April 2012.
[9] Dave Majumdar, "Iran's captured RQ-170: How bad is the damage?," Air Force Times, 9 December 2011.
[10] "China Tests First Stealth Combat Drone," Business Insider, 22 November 2012.
[11] "China's Mysterious Predator Clone Is Finally Out In The Open," Business Insider, 8 November 2012.
[12] Patrick Tucker, "Every Country Will Have Armed Drones Within Ten Years," Defense One, 6 May 2014.
[13] Bob Brewin, "FCC Hits Chinese GPS Jammer Vendor With Record $34.9 Million Fine," Next Gov, 19 June 2014.
[14] Bob Brewin, "FCC Hits Chinese GPS Jammer Vendor With Record $34.9 Million Fine," Next Gov, 19 June 2014.
[15] Shaun Waterman," North Korean jamming of GPS shows system's weakness," The Washington Times, 23 August 2012.
[16] "NK stops jamming satellite signals in South Korea," The Dong-A Ilbo, 16 May 2012.
[17] "Al-Qaeda reportedly targeting US drones," Defense Systems, 5 September 2013.
[18] "Al-Qaeda reportedly targeting US drones," Defense Systems, 5 September 2013.
[19] Craig Whitlock, Barton Gellman," US documents detail al-Qaeda's efforts to fight back against drones,"The Washington Post, 3 September 2013.
[20] Siobhan Gorman, Yochi J. Dreazen, August Cole, "Insurgents Hack US Drones," The Wall Street Journal, 17 December 2009.
[21] Siobhan Gorman, Yochi J. Dreazen, August Cole, "Insurgents Hack US Drones," The Wall Street Journal, 17 December 2009.
[22] "University of Texas at Austin researchers demonstrate first 'spoofing' of UAVs," Space Daily, 11 July 2012.
[23]"University of Texas at Austin researchers demonstrate first 'spoofing' of UAVs," Space Daily, 11 July 2012.

IF AT FIRST YOU DON'T SUCCEED: 1 JANUARY 2014 BOMBING OF THE JAZEERA HOTEL

An example of IED Tactics, Techniques, and Procedures

by Laura Deatrick, TRISA-CTID (CGI Ctr)



During the evening of 1 January 2014, the Jazeera Hotel in Mogadishu, Somalia, sustained its second complex attack involving improvised explosive devices (IEDs) in as many years. Initiating with a suicide vehicle-borne IED (SVBIED), the attackers then stormed the hotel compound in an unsuccessful attempt to gain entrance to the main building. The attack concluded with the detonation of a nearby vehicle-borne IED (VBIED) aimed at first responders. The new OEA Team Threat Report, *If at First You Don't Succeed: 1 January 2014 Bombing of the Jazeera Hotel*, examines the details of the attack and possible training implications.

On the evening of 1 January 2014, a number of Somali Federal Government senior officials were at the Jazeera Hotel. Popular with both foreigners and members of government, the facility possessed two restaurants, an equal number of conference rooms, and excellent security. The group was likely either holding a meeting at the hotel or enjoying dinner.

Around 7:30 p.m. local time an attacker rammed an SVBIED into a police car located next to the main gate, detonating his explosives and killing four security force personnel. Using the explosion as a diversion, two attackers wearing person-borne IEDs (PBIEDs) attempted to penetrate the compound; they were shot and killed by security forces before reaching the hotel entrance. Emergency personnel and additional security forces responded within minutes, and were assisting the wounded when a second VBIED, possibly an SVBIED, detonated only yards from the first explosion, killing at least four. The number of people wounded during the complex attack was at least 37.

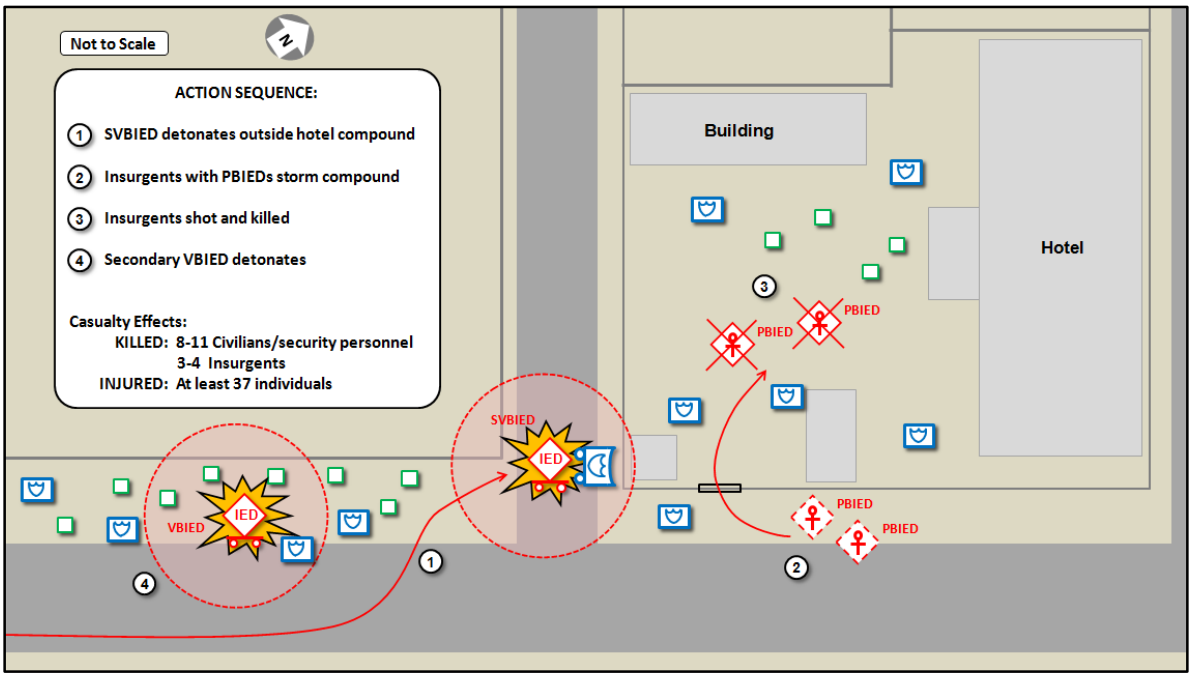
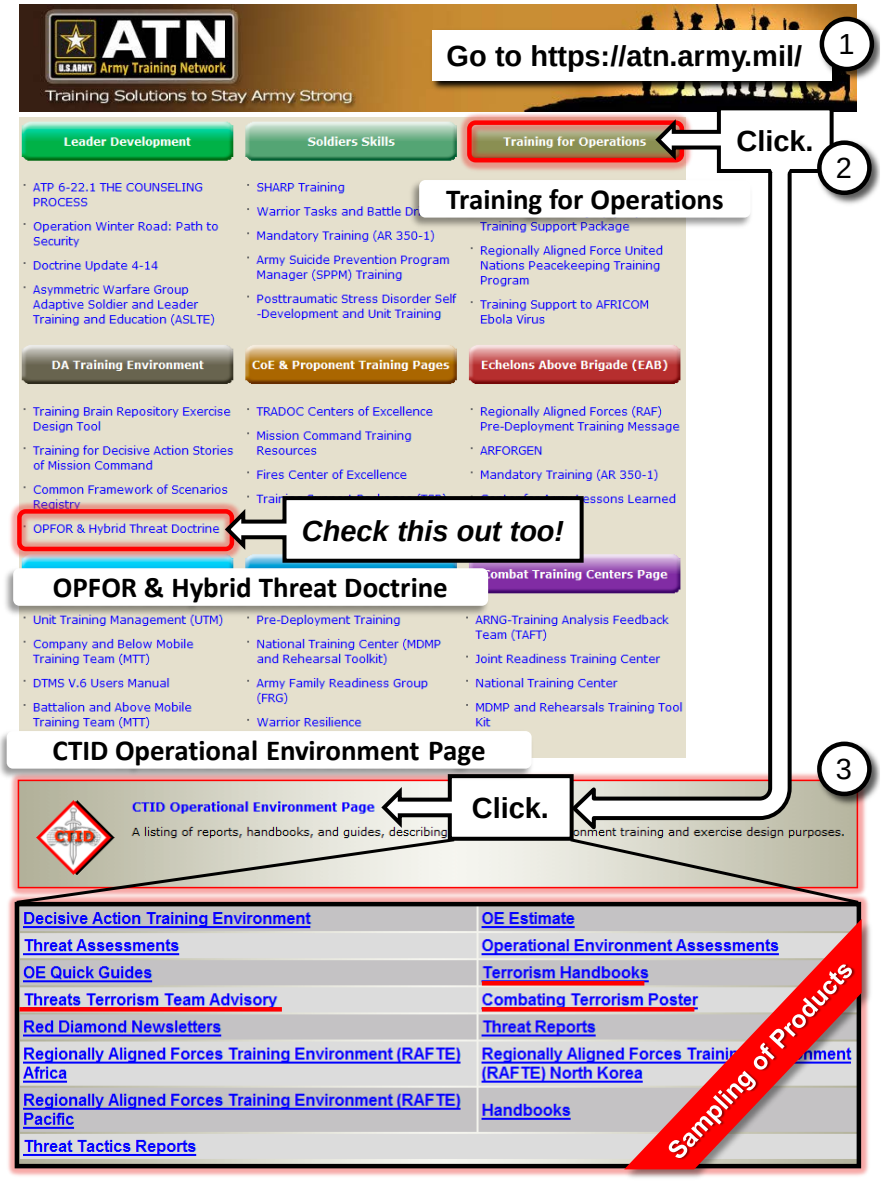


Figure 1. January 2014 Attack on the Jazeera Hotel

Several aspects of this event will make it of interest to trainers and scenario writers. First, it would be easy to mimic in the home-training environment, and the small number of attackers allows for efficient use of role players. Conflicting reporting regarding the second IED and the sequence of events makes the scenario particularly challenging for MI units. Finally, complexity is added due to the two-pronged attack and use of multiple types of IEDs.

The *If at First You Don't Succeed: 1 January 2014 Bombing of the Jazeera Hotel* Threat Report provides information to the Army training community on the January attack. It contains an event review and accompanying diagram, discusses recent threats and security, and considers the likely actors and their motives. In addition, the report provides an analyst assessment and examines training implications.

Threats and OE Awareness Products on Army Training Network (ATN)



Find-Use TRISA-CTID Threats and OE Awareness Products

Three Clicks to Threats/OE

Army Training Network (ATN) hosts threats and operational environment products of the Complex Operational Environment and Threat Integration Directorate (CTID) at two easy-to-reach locations at their website front page.

The front page of the ATN website changes its spotlight notices as new resources are entered in the website. Nonetheless, three "clicks" and you can find CTID resources in ATN.

CTID coordinates regularly with ATN to post new research on a number of topics focused on current threats, the opposing force (OPFOR), and variables of an operational environment (OE).

As displayed in the illustration (left), CTID products are within the two ATN front-page links of:

Training for Operations

or

OPFOR & Hybrid Threat Doctrine (under DA Training Environment)

1-2-3 and you're there!

What Happened to my GPS? Anti-Satellite (ASAT) Threats to US Systems
by Marc Williams, TRISA-CTID (CGI Ctr)

Imagine this: your brigade combat team goes to the field for an extended field training exercise (FTX) in preparation for a combat training center (CTC) rotation. Two days into the FTX, all long range communications suddenly cease, global positioning systems (GPS) go blank, and the S2 cannot pull up any weather data for upcoming operations planning. Impossible? Not really. This is the real-world scenario the US faces with the loss of its satellites. Your problem is how to find a "work around" to continue combat operations.

The US military uses satellites for long range communications (voice, data, and video), intelligence (enemy surveillance, electronic signals intelligence [ELINT], and signals intelligence [SIGINT]), electronic monetary transactions, targeting (precision guided munitions [PGM]), navigation services (GPS), detection of ballistic missile launches, arms control verification, and weather data collection.

The US Air Force maintains a "constellation of satellites in medium Earth orbit to ensure availability of at least 24 satellites 95 percent of the time. The current constellation consists of 31 operational satellites, along with three or four decommissioned satellites that can be reactivated if needed."[1]

The US Navy uses satellites extensively for ocean surveillance. Commercial satellites provide secure communications, high-resolution imagery, and news services. "Some wireless services cannot operate without it," and "nearly all new military assets—from vehicles to munitions—come equipped with GPS."[2]

Non-Military Use of Satellites

Multiple industry and government use of satellites extends to communications, energy, financial services and transportation industries/agencies, including the Department of Homeland Security (DHS) and Department of Transportation (DOT). "GPS is the backbone for NextGen, the Federal Aviation Administration's next-generation air traffic control system, and because of its use for navigation, DOT is the lead civilian agency for GPS reliability efforts. The department was charged in a 2004 national security directive with developing backup capabilities for government and industry, with the assistance of DHS."[3]

Techniques for ASAT

ASAT techniques include "kinetic kills," destruction of earth stations, directed electromagnetic energy weapons, satellite jamming, maneuvering satellites, and hijacked signals—

Kinetic kills: Kinetic kills include "hit to kill" vehicles or use of nuclear and non-nuclear missiles. "The act of destroying a satellite can damage the space environment by creating dangerous amounts of space debris. What's more, the impairment or loss of an important satellite, such as one used for reconnaissance, can quickly escalate a conflict or generate other unpredictable and dangerous consequences."[4]

Destruction of earth stations (launch, tracking, telemetry, and control facilities): Compared to launching an ASAT missile or shooting a satellite with lasers, conducting a ground raid or air strike against a satellite earth station is relatively simple and effective.

Directed electromagnetic energy weapons: Directed-energy weapons utilize lasers, high-powered microwaves, and particle beams. Projects in development by the US have names like Airborne Laser, the Active Denial System, and the Tactical High Energy Laser (THEL). Twenty-three countries are currently part of the International Satellite Laser Ranging effort. This is the ability to bounce laser signals off cooperating satellites to make precise measurements on earth. "This equipment could be used—without permission—to illuminate satellites that are not part of the network."[5]

Satellite jamming: "Interfering with radio communications between a satellite and users on the ground—can be attempted with either the uplink (ground-to-satellite transfer of data to be broadcast) or the downlink (satellite-to-ground data transfer), which are more vulnerable than the command-and-control link between ground stations and satellites."[6] GPS jamming is already being used at the Combat Training Centers to enhance realism. Both state and non-state actors use this capability.

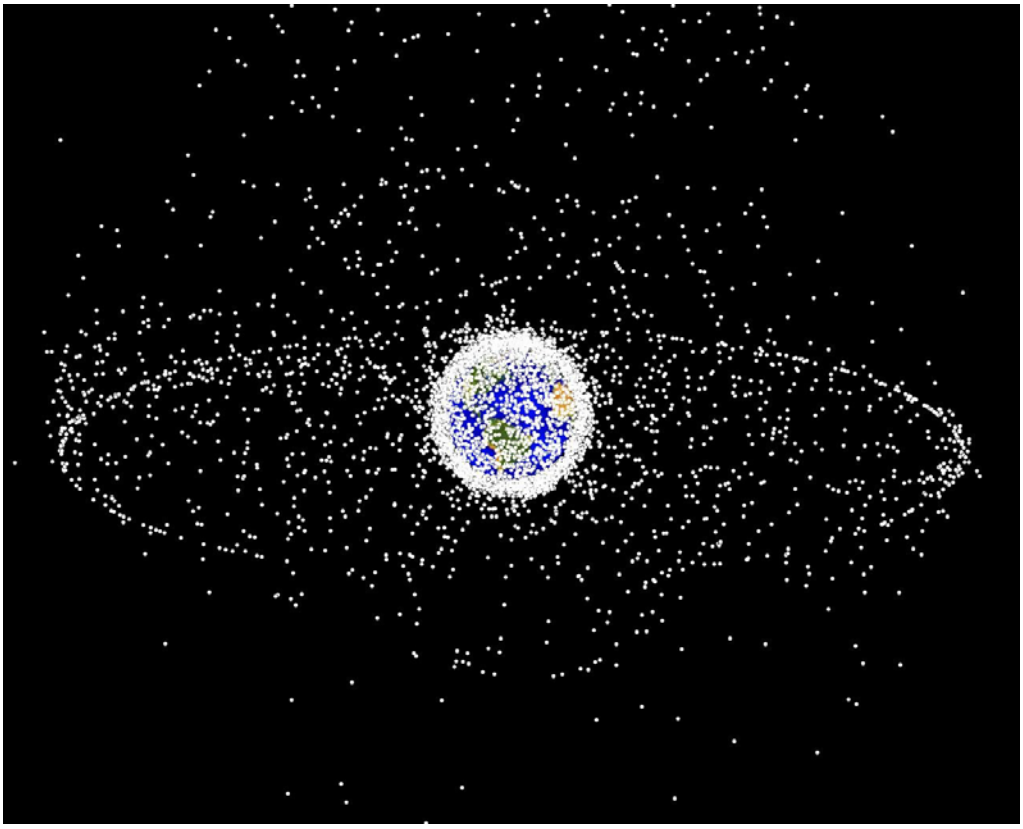


Figure 1. GEO image of earth space debris (not to scale). Only 5% of these objects are functional satellites. Graphic from the NASA Orbital Debris Program Office

Maneuvering satellites: These are satellites that could approach and potentially touch target satellites without the target's cooperation. This capability is being developed by multiple countries and organizations including the US, Russia, Japan, China, Sweden, and the European Space Agency. The Swedish maneuverable satellites are called Mango and Tango. The US program named "Phoenix" is designed to pick apart dead satellites for spare parts.[7]

Hijacked signals: This capability includes "spoofing," or deliberately providing incorrect coordinates with GPS. Destruction of satellites is not a new phenomenon. Just as new armor generates new armor piercing weapons, new satellites provoke new ways to interfere with their functions.

"For countries that could never win a war by using the method of tanks and planes, attacking the US space system may be an irresistible and most tempting choice…"

Al Santoli, *China Reform Monitor*, 10 October 2000

In the 1950s to 60s, both the US and the USSR developed megaton-class nuclear interceptors as ASAT weapons. In 1973, the USSR developed a "co-orbital strategy, in which a weapon armed with conventional explosives is launched into the same orbit as the target satellite and moves near enough to destroy it."[8] In October 1985, the US used the Air Launched Miniature Vehicle (ALMV) to destroy a Solwind satellite at 555 kilometers altitude, generating 250 pieces of persistent space debris that stayed in orbit until 2002.[9]

China began work on hit to kill technology in the 1980s. Russia developed an ASAT platform called Naryad as both anti-satellite and anti-ballistic missile missions.[10] Through the 1990s, the US began developing directed energy weapons of both lasers and microwaves. These were intended to either dazzle (temporarily overwhelm), blind (permanently damage), or destroy satellites. The first successful "dazzle" of a satellite took place in testing at an altitude of 420 kilometers.[11]

In the 2000s, the US withdrew from the Anti-Ballistic Missile (ABM) treaty and deployed satellite jamming systems. In September 2002, non-state actor Falun Gong hijacked satellite signals from SINOSAT to broadcast its own message to remote areas of China.[12] On 16 July 2003, Iran successfully jammed the "Telestar-12, a commercial communications satellite orbiting at 15 degrees west, 22,000 miles above the Atlantic, which carries programs by the American government as well as by Iranian radio and television stations based in the US aimed at mainland Iran."[13] This was done from a compound owned by the Iranian Embassy in Havana, Cuba.

"The illumination of somebody else's satellite for destructive purposes would be a huge provocation and could lead to war."

Michael Krepon, Henry L. Stimson Center, 27 September 2006

In 2006, a ground-based laser in China illuminated at least one American satellite, as confirmed by the US National Reconnaissance Office (NRO).[14] A year later, China successfully launched a homing vehicle from a mobile ground-based missile to directly destroy one of its own satellites. "This destructive ASAT test, the first by any country in 20 years, caused a great deal of international concern because it created more persistent debris than any previous event in space."[15] In July 2013, China launched three maneuvering satellites which conducted unusual maneuvers in space. "One of the satellites was equipped with an extension arm capable of attacking orbiting satellites that currently are vulnerable to both kinetic and electronic disruption."[16]

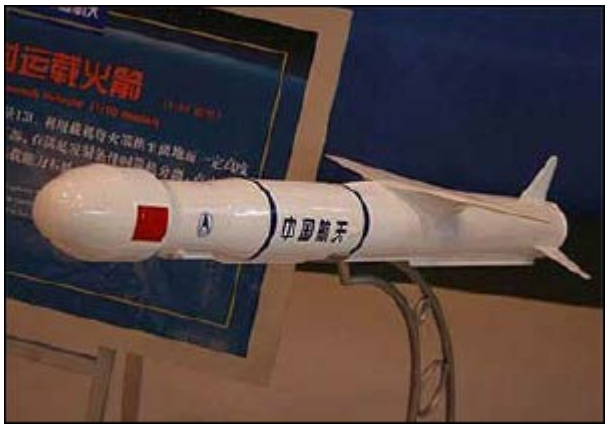


Figure 2. Chinese anti-satellite missile; photo from Congressional Research Service Report for Congress 7-5700, "Proliferation of Precision Strike: Issues for Congress" 14 May 2012 by Randy Huiss

Future Trends

State and non-state actors will actively pursue ASAT technologies to negate potential enemy capabilities. "Because entire constellations of valuable satellite systems rotating the Earth could be destroyed quickly if indeed an adversary is targeting them, military commanders with expertise and responsibilities in the space domain will press for an immediate presidential grant of authority to take action."[17]

The ***European Space Agency*** (ESA) is developing an unmanned re-entry vehicle named the Intermediate Experimental Vehicle (IXV). Its capabilities will include capturing items in space and returning them to Earth.

India intends to develop anti-satellite weapons following its successful Agni-V intercontinental ballistic missile (ICBM) test. Apart from adding a new dimension to its strategic defense, India has opportunities in building ASAT weapons and launching mini/micro satellites on demand.[18]

Japan is developing space robots to work in space. Missions for these robots will include assembly and maintenance of satellites.[19] By 2019, Japan intends to have the capability to maneuver satellites and capture debris in space in an attempt to clean up orbiting debris.[20]

Sweden is investing in maneuvering satellites which can conduct "1) Autonomous formation flying, 2) homing and rendezvous, 3) proximity operations or RV (Rendezvous) tests, including final approach and recede operations."[21]

Russia is currently building a new cosmodrome in the Amur Oblast, in the Russian Far East and Outer Manchuria. The new facility will have its first launch by 2015 and its first manned mission by 2018.[22] Russian sources promised to add ASAT capabilities to the S-400 and S-500 ground-to-air systems.[23]

China's space and missile capabilities are growing and will be directed against the use of space-based assets by potential adversaries during times of conflict. China's space launch vehicle industry is expanding to support satellite launch services and the manned space program. China's ASAT programs have significant implications for anti-access/area-denial efforts against the United States in Taiwan Strait contingencies. "Citing the requirements of its manned and lunar space programs, China is improving its ability to track and identify satellites—a prerequisite for effective, precise counter-space operations."[24]

China is developing a growing range of satellites, a new heavy-lift space launcher, and a fourth launch site on Hainan Island. "In addition, China's improving space capabilities, coupled with its steadily advancing conventional capabilities, will provide the increased ability to seek space superiority or space dominance (*zhitian quan*) through a combination of space offensive and defensive operations."[25] Many US experts now consider China's counterspace capabilities to be on par with its offensive cyber operations.[26]

Impacts

Loss of satellites will have severe impacts to both military and non-military actions. It could mean no financial transactions, no mid- or long-range communications, no GPS support, and/or no use of precision guided munitions. The US is a digitized, web-based army dependent on satellite support. This is a weakness the US can expect future adversaries to exploit.

Training Implications

Replicating the ASAT threat may be difficult but must be addressed. The Combat Training Centers are already taking steps to incorporate some of this into their scenarios. Use of GPS jammers causes real challenges to rotational training units (RTU) even when used for a limited time. Opposing Forces (OPFOR) are already targeting and overrunning unmanned aerial systems (UAS) launch sites. It is only a matter of time before they begin to do the same to satellite earth stations. Future training events may include forcing the RTU to shut down tactical satellite communications to replicate satellite loss. Training developers will have the responsibility for coming up with solutions to this challenge. RTUs will have the challenge of working in alternate ways to complete their mission.

Training materials already exist to help trainers plan exercises which address ASAT capabilities. The *Decisive Action Training Environment (DATE) 2.0* addresses this threat. Donovian ASAT assets include "ground-based radar and visual sensors cueing air-launched missiles carried by specially-equipped interceptor aircraft. It is likely that ASAT efforts would attempt to neutralize enemy space-based surveillance and communications efforts early in any potential conflict."[27]

OPFOR doctrine (FM 7-100.1, *Opposing Force Operations*) calls for units to use both lethal and non-lethal attacks to disrupt satellite communications and supporting infrastructure. At a minimum, the OPFOR will jam or monitor satellites. Training units can also find information about counter-satellite systems in the *Worldwide Equipment Guide (WEG),* Volume 2, Airspace and Air Defense Systems, August 2013. The WEG can be downloaded from the Army Training Network at https://atn.army.mil/dsp_template.aspx?dpID=311.

Notes

[1] William Jackson, The serious side of GPS, where timing is everything, GCN, 12 November 2013.
[2] William Jackson, The serious side of GPS, where timing is everything, GCN, 12 November 2013.
[3] William Jackson, Critical infrastructure not prepared for GPS disruption, GCN.com, 8 November 2013.
[4] Laura Grego, A History of Anti-Satellite Programs, Union of Concerned Scientists (UCS) Global Security Program, January 2012.
[5] Laura Grego, A History of Anti-Satellite Programs, Union of Concerned Scientists (UCS) Global Security Program, January 2012, page 11.
[6] Laura Grego, A History of Anti-Satellite Programs, Union of Concerned Scientists (UCS) Global Security Program, January 2012, page 9.
[7] Robert Beckhusen, China's mystery satellite could be a dangerous new weapon, War is Boring, 22 August 2013.
[8] Laura Grego, A History of Anti-Satellite Programs, Union of Concerned Scientists (UCS) Global Security Program, January 2012, page 3.
[9] The Air-Launched Miniature Vehicle (ALMV) consisted of a two-stage missile launched from an F-15 aircraft flying at high altitude. The missile would ascend to a target satellite in low earth orbit and destroy or disrupt the satellite in a high-speed collision" known as a "kinetic kill" or "hit-to-kill."
[10] Anatoly Zak, The Naryad System, Russianspaceweb.com, 1 November 2013.
[11] Laura Grego, A History of Anti-Satellite Programs, Union of Concerned Scientists (UCS) Global Security Program, January 2012, page 7.
[12] Experts condemn Falun Gong TV hijacking, Xinhua News Agency, 26 September 2002.
[13] Safa Haeria, Cuba blows the whistle on Iranian jamming, Asia Times Online, 22 August 2003.
[14] Warren Ferster and Colin Clark, NRO confirms Chinese laser test illuminated U.S. spacecraft, Space News, 3 October 2006.
[15] Laura Grego, A History of Anti-Satellite Programs, Union of Concerned Scientists (UCS) Global Security Program, January 2012, page 13.
[16] China launches three ASAT satellites, Missile Threat, A Project of the George C. Marshall and Claremont Institutes, 26 August 2013.
[17] Michael Krepon and Julia Thompson, Editors, Anti-Satellite Weapons, Deterrence, and Sino-American Space Relations, Stimson Center, September 2013.
[18] India developing anti-satellite weapons, Space Daily, 23 April 2012.
[19] Pioneering research for future space missions, Japan Aerospace Exploration Agency (JAXA), 2012.
[20] J.T. Quigley, Japan will cast a "magnetic net" for space junk, The Diplomat, 16 January 2014.
[21] PRISMA (Prototype Research Instruments and Space Mission technology Advancement), Earth Observation resources, Fall 2013.
[22] Ilya Arkhipov, Putin builds space-arms defense as Russia targets Mars, Moon, Bloomberg.com, 12 April 2013.
[23] Anatoly Zak, The Naryad System, Russianspaceweb.com, 1 November 2013.
[24] Departments of Defense and State, *Report to Congress* Section 1248 of the National Defense Authorization Act for Fiscal Year 2010 (Public Law 111 - 84), Risk Assessment Of United States Space Export Control Policy.
[25] Dean Cheng, China's space program: A growing factor in US security planning, The Heritage Foundation, 16 August 2011.
[26] Marcia S. Smith, HASC Told China's Counterspace Capabilities "Extremely Serious", spacepolicyonline.com, 28 January 2014.
[27] Decisive Action Training Environment 2.0 dated December 2011, page 2E-5-4.

—What CTID Does for YOU—

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

CTID Points of Contact

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