Red Diamond
Threats Newsletter

TRADOC G2 Operational Environment Enterprise
ACE-Threats Integration

Fort Leavenworth, KS Volume 6, Issue 3 MAR 2015

INSIDE THIS ISSUE

OEE *Red Diamond* published monthly by TRADOC G2 OEE ACE-Threats Integration

Send suggestions to:

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

by TRADOC G2 ACE-Threats Integration, Operations

The TRADOC G2 Operational Environment Enterprise (G2 OEE) is transitioning a series of army field manuals-training literature into the HQDA Training Circular 7-100 series. *Threat Force Structure*, TC 7-100.4, will be released soon as an unclassified document on the Army Publishing Directorate. The TRADOC G2, as the responsible official for the development, management, administration, and approval functions of the OE concept across the army, addresses a flexible baseline of regular forces and irregular forces that can be adapted to meet a variety of different training, professional education, and leader development requirements.

These force structures and associated online organizational directories represent a realistic composite of known enemies and/or adversaries the army might encounter in near- and midterm OEs. These units and organizations apply to OE conditions and variables, except when mission rehearsal or contingency training requires maximum fidelity to a specific real-world threat.

The online organizational directories are living documents, and are updated by the TRADOC G2 ACE-Threats Integration directorate to ensure relevance in OE conditions in assessing and evaluating army readiness in live, virtual, constructive, and gaming simulation experiences.

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

Red Diamond Topics of Interest

by Jon H. Moilanen, TRADOC G2 ACE-Threats Integration, Operations and Chief, *Red Diamond* Newsletter (BMA Ctr)

This month's lead article spotlights examples of hybrid threat with pro-Russian separatists in eastern Ukraine combat actions of intelligence, special purpose forces, information warfare, and local militias quickly seizing key infrastructure. Another article discusses TRADOC G2 OEE support to conversion of the current Network Integration Evaluation (NIE) scenario to an operational environment based on the Decisive Action Training Environment (DATE).

Current threats/OPFOR symbology in the HQDA Training Circular 7-100 series applies the recent update to ADRP 1-02, the army standard for terms and military symbols. A complementary part 2 to this article will be published in the April *Red Diamond*.

An article on threat model analysis supports intelligence preparation of the battlefield (IPB) and situational understanding of tactical tasks. In this first article of a series, functional analysis and tactical skill determine Threat/OPFOR actions in construction and defense of a simple battle position.

An article surveys major changes in North Korean leadership since Kim Jong Un became the DPRK supreme leader upon the death of his father.

Observations of Syrian army reconnaissance and Hezbollah in current operations provides insight for required OPFOR capabilities in training US forces.

Email your topic recommendations to:

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

Red Diamond Disclaimer

The *Red Diamond* presents professional information but the views expressed herein are those of the authors, not the Department of Defense or its elements. The content does not necessarily reflect the official US Army position and does not change or supersede any information in other official US Army publications. Authors are responsible for the accuracy and source documentation of material that they reference. The *Red Diamond* staff reserves the right to edit material. Appearance of external hyperlinks does not constitute endorsement by the US Army for information contained therein.

U.S. Army TRADOC G2 Operational Environment Enterprise
TRADOC G2 ACE-Threats
Know the Enemy
Know the Threats
TRADOC G-2
We are Combating TERRORISM
TC 7-100.2
TC 7-100.2
Opposing Force Tactics
December 2011
HEADQUARTERS DEPARTMENT OF THE ARMY
Training Antiterrorism Awareness in Units
Combating Terrorism (CbT)
Poster No. 06-15
(DOD Photo: Senior Airman Richardson)
Go to https://atn.army.mil/
Click "Training for Operations"-"CTID OE Page"-"Terrorism"
See multiple resources: training-education-leader development.
ATN Army Training Network

Director's Corner

Thoughts for Training Readiness

by Jon Cleaves, Director, TRADOC G2 ACE-Threats Integration

The TRADOC G2 recently hosted an Opposing Force Conference to plan for the continued quality of Training and Doctrine Command intelligence support to US Army readiness. One of the central aspects to TRADOC G2 Operational Environment Enterprise (G2 OEE) support in unit, activity, and leader readiness is identifying realistic, robust, and relevant opposing forces (OPFOR) for training, professional education, and leader development.

Once requirements are validated, resourcing OPFOR is always a matter of priorities to provide the best possible conditions to the US Army unit commander in order for him or her to evaluate tasks-missions to an army standard. This mission task is even more problematic in an era when the Secretary of the Army and the Chief of Staff of the Army acknowledge compromises to army modernization and force reductions underway, and warn of risk to operational readiness and army responsiveness. Enemies and adversaries continue to flex intent and capabilities in current events throughout US combatant commands worldwide. Recent examples include expanding paramilitary insurgencies and state sponsors promoting separatist movements and combat into neighboring sovereign states.

With the army requirement to represent or replicate Threat/OPFOR capabilities for the dynamic capabilities of a hybrid threat (HT)—regular forces, irregular forces, criminal organizations, active and/or passive supporters in a relevant population, and acts of terrorism unrestrained by extremist actors—knowing "what right looks like" as requirements is a prime mission task. Confronting the combined arms task organizations of army brigade combat teams (BCTs), and their augmentation from division-corps echelons and Joint or partner forces with realistic, robust, and relevant OPFOR is already a training operational environment (OE) challenge. Identifying and validating critical requirements remains particularly challenging in live, constructive, virtual, and/or gaming simulations. The TRADOC G2 ACE-Threats Integration Directorate serves as army lead for designing, documenting, and integrating threat or OPFOR and OE conditions in support of all army training, education, and leader development programs. We also review, analyze, and provide recommendations for the integration of OE and its critical variables into training, education, and leader development.

In the coming months of 2015, the TRADOC G2 ACE-Threats Integration Directorate will conduct a series of internal tactical vignettes and threat assessments—*Threats Integration Wargame 2025*—to study possible and probable threats in near-term and midterm OEs that a regionally aligned force (RAF) could confront in decisive action missions. The resulting sets of conditions will assist in identifying threat capabilities and limitations as a basis to update flexible and dynamic OPFOR force structure requirements. One concept among several concepts to be considered is a more adaptable task organization such as a guerrilla brigade tactical group (BTG) with affiliated or associated regular forces, and state actors and/or other irregular actors. These options may prove more effective in threats representation than a traditional use of heavy BTG OPFOR and/or lesser irregular OPFOR affiliates.

Evaluation of these wargame outcomes will guide revision of OPFOR equipment requirements in the TRADOC *Operational Environment Master Plan* (OEMP). The OEMP states the high and medium fidelity requirements for current and future, realistic, and viable training conditions at the Combat Training Centers (CTCs), home station training (HST) sites, institutions and Centers of Excellence (CoEs), and Enduring Mobilization Training Centers (EMTC). Validated requirements of the OEMP are essential to army senior leader decisionmaking on fiscal priorities and allocation programs of army resources. The ACE-Threats Integration Directorate will keep the *Red Diamond* readership apprised of OEMP developments on revised requirements and implementations as they occur toward supporting US Army readiness now and into the immediate future.

JON

Pro-Russian Separatists: Crisis in the Eastern Ukraine

by John Cantin, TRADOC G2 ACE-Threats Integration (BMA Ctr)

In May 2014, pro-Russian separatists in eastern Ukraine were able to seize control of parts the Donetsk and Luhansk oblasts (areas similar to US counties) with assistance from Russian Special Operations Forces (SPF), Russian intelligence operatives, and a limited number of regular Russian troops. This was an example of the Russian concept of hybrid warfare: the use of intelligence, SPF, information warfare (INFOWAR), and indigenous local militias and fighters to quickly seize key infrastructure as well as civil and military facilities.

The use of SPF and intelligence operatives is not a new concept for the Russians. In Afghanistan, 700 Russian Spetsnaz paved the way for the main invasion in 1979. During the 1990s, the Russians used Spetsnaz extensively in the First and Second Chechen War. In 2008, Russia used these highly trained troops to set the conditions for success in Georgia. This article will discuss Russian tactics and strategy for hybrid warfare.

With Euromaidan protests in early 2014, the pro-Russian Ukrainian government fled and was replaced with the pro-Western/European Union government. To the ethnic Russian minority in the eastern section of Ukraine, this was an intolerable situation. The Crimean port of Sevastopol (home to the Russian Black Sea naval fleet) was seized by Russian troops and the Donetsk and Luhansk oblasts were soon overrun by pro-Russian separatists. These separatists seemed to be receiving intelligence, logistical, and manpower assistance from Russia, although they vehemently denied this when pressed on the issue.

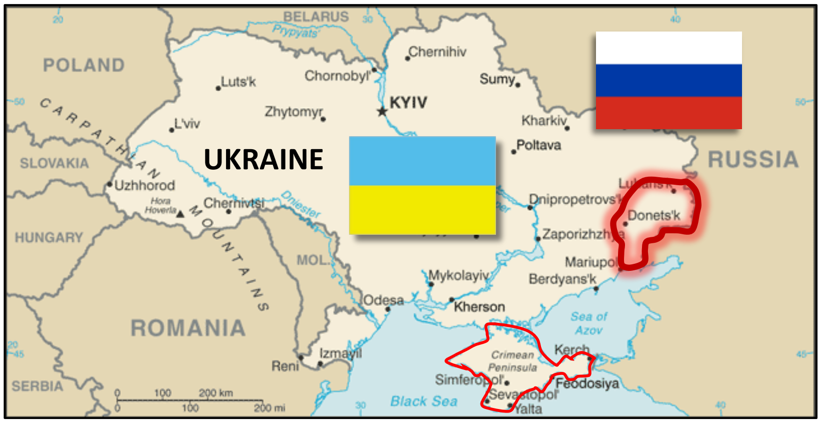


Figure 1. Map of Ukraine and addition of flags with highlight of disputed areas 2014-2015

Separatists in Donetsk and Luhansk had several advantages over the civil authorities that they wished to replace. First, most Ukrainian males have some military training due to conscription or service in the Soviet or Ukrainian armed forces. Secondly, Russia and Ukraine share a porous border that aided the infiltration of Russian advisors and operatives. Finally, Russian intelligence operatives have been active in eastern Ukraine since the dissolution of the Soviet Union in 1991.

These three factors combined with an unstable situation throughout the country gave the separatists an opportunity to take advantage of a chaotic situation and seize control of the government in these areas.

The first tactic employed was to use INFOWAR to spread anti-Ukrainian and pro-Russian propaganda. This was done masterfully, portraying the support for the separatists on a much bigger scale than it actually was. Stories of alleged atrocities against the Russian minority in eastern Ukraine were disseminated, as well as information that portrayed Kiev government as anti-Russian.

Many separatists used the ouster of President Yanukovych as the justification for rebellion and separation from Kiev. By attempting to cast the current Ukrainian government as illegitimate, the separatists could justify their actions as a legal and proper rebellion against an illegal government. This also allowed for more overt Russian assistance and intervention in the Crimean peninsula and the port of Sevastopol. The Russians declared that they were merely protecting the Black Sea Fleet from an illegal and rogue government in Kiev.

Figure 2. Separatists in tactical actions

The media was also used to rally supporters to go to various locations to protest or show support for the separatists. Television and radio stations were seized and began broadcasting Russian newscasts. The Internet and social media were also employed to spread the pro-Russian message and to notify citizens of rallies, protests, and other events. Separatists also used this medium to assist civilians with administrative and legal tasks once the pro-Russian governments were in place. Television and Internet services were also transferred to Russian ownership and management, assuring that they would continue to broadcast Russian and separatist messages.

Russian electronic warfare (EW) systems were used to jam Ukrainian military and civilian communications. The Russians were also able to jam or disrupt Ukrainian unmanned aerial vehicle (UAV) and drone operations by severing the links between control stations and the vehicles. Separatists often placed EW assets near schools and hospitals to hinder Ukrainian targeting of these assets. This put the Ukrainians in a no win situation. If they targeted the EW systems, they risked civilian casualties that would be exploited by the rebels, but doing nothing allowed these systems to continue to disrupt Ukrainian army operations.

Figure 3. Separatist column repositioning near Donetsk

Russian separatists teamed up with Russian advisors during the confusing and chaotic initial days of the rebellion. This was done without difficulty as the border between Russia and eastern Ukraine is easy to cross. The high number of separate rebel groups and the various uniforms and equipment that the rebels used was an advantage. The rebels and their advisors simply blended into the population when needed, only to reappear at another time and place.

Many rebels also had skills that could be used by the separatists to run and administer government and infrastructure. Rebels moved swiftly to take charge of supplying the power, water, police and civil service functions to solidify their hold on the local populace. Advisors assisted with the command and control of all of the disparate rebel groups and brought in men and materials as needed to help with the consolidation of these groups into a coherent and viable military and police force.

The rebels used a long term strategy of infiltrating local police, civil service, and paramilitary groups in Ukraine. It is believed that Russian operatives were in eastern Ukraine for years prior to the open hostilities of 2014. This allowed the separatists to develop relationships with Russian advisors and become familiar with the terrain and infrastructure of

Donbass and Luhansk oblasts. By using this prepositioned force of fighters, police, organizers, and media assets, the rebels were able to quickly seize territory, dominate and control of the news and information cycle, and set conditions for the follow-on forces that would soon enter the conflict.

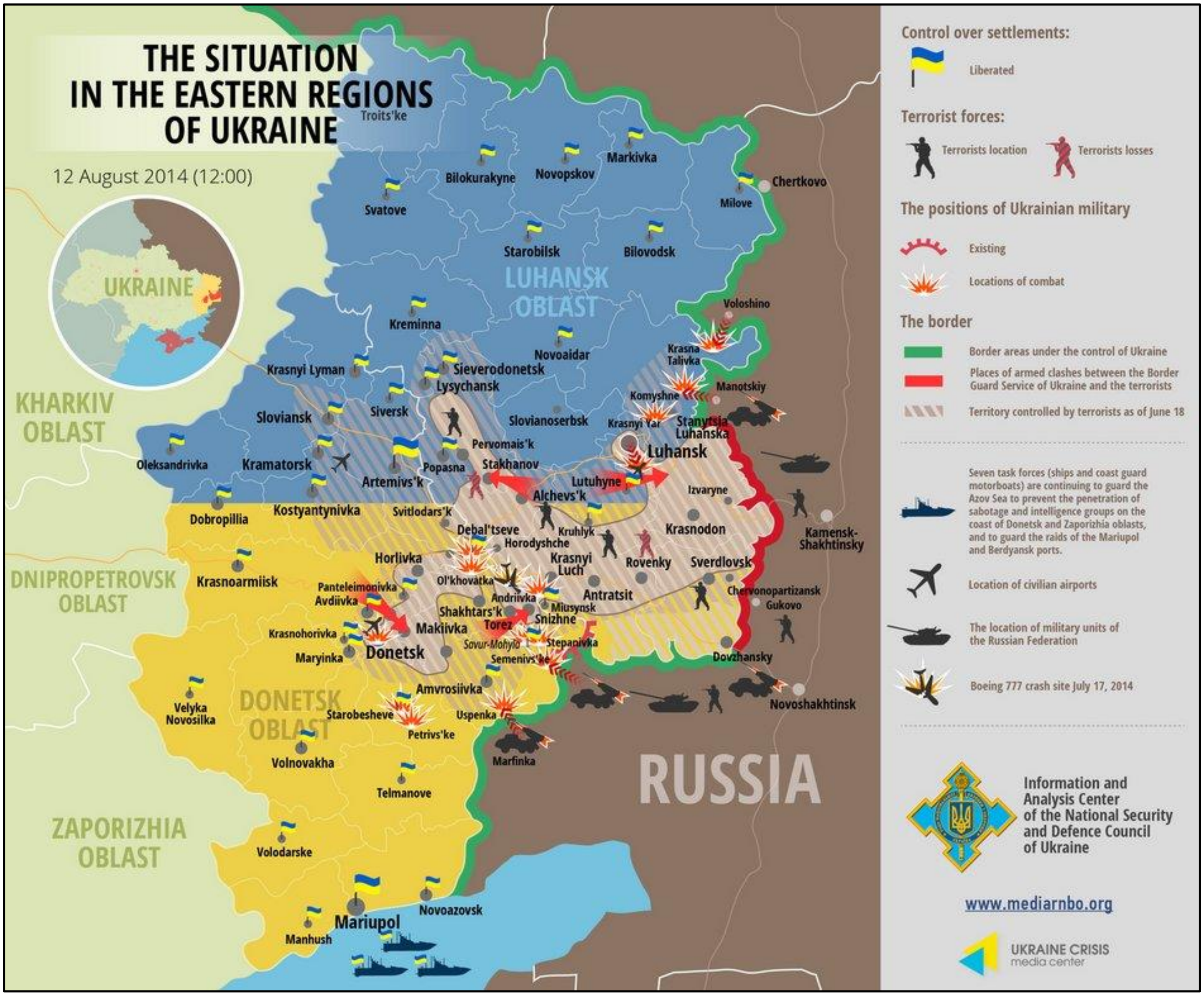


Figure 4. Situation in eastern Ukraine, 12 August 2014

After the initial seizure of Donbass and Luhansk, the rebels prepared for the inevitable counter attack by Ukrainian forces. The rebels were augmented by Russian forces who provided command and control, and most importantly, military equipment. Russian mechanized infantry vehicles, artillery pieces, and air defense artillery were reported in eastern Ukraine.

The rebels used their information and media outlets to claim that these vehicles were seized from Ukrainian army garrisons and depots. This equipment was then used to reinforce defensive positions on key roads, border checkpoints, airports, government buildings, and cities.

As the Ukrainian army attempted to take back lost territory, the rebels used social media to rally supporters to key military and civilian sites. These supporters were used by armed rebels as human shields by the separatists and succeeded in blocking key roads and intersections. In some cases the rebels not only repelled Ukrainian troops, but convinced some to defect to their side or simply surrender their equipment and retreat back to their lines. See table 1 for a chronology of several events in the crisis.[1]

As the rebels held on to conquered territory, provided and maintained municipal and police services, the Russians continued to resupply the separatists with equipment, ammunition, and personnel. The Russians did this in a piecemeal fashion to avoid detection. One or two tanks, APCs, or IFVs were infiltrated to avoid a large signature. The vehicles and men were also spread around for the same reasons. This served two purposes. One is to solidify existing territorial gains, and the second is to create a de facto autonomous state bordering Russia. This gave the separatists leverage to negotiate a ceasefire with Ukraine in late February 2015. As the ceasefire was being negotiated, the Russians moved equipment into place to solidify gains and reinforce current positions. This gives them a permanent presence in in the disputed region and allows the illusion of legitimacy for the insurgents and Russian troops.

Table 1. Ukrainian Crisis Timeline

1 December 2013	Ukrainian police break up student protest camp in Kiev's Independence Square over President Viktor Yanukovych's failure to sign trade deal with EU.
20 February 2014	More than 100 people reportedly die in 48 hours as protesters and police clash in Kiev, with government snipers opening fire.
22 February 2014	Viktor Yanukovych, president of Ukraine, flees Kiev.
27 February 2014	Pro-Russian gunmen seize government buildings in Simferopol, the capital of Ukraine's Crimea peninsula.
16 March 2014	Ninety seven per cent of people in Crimea are said to have voted to join Russia in a referendum condemned as a sham in the West. Two days later, Vladimir Putin, Russia's president, signs a law incorporating Crimea into Russia.
7 April 2014	Protesters seize government buildings in Kharkov, Donetsk and Luhansk in eastern Ukraine.
11 May 2014	The Donetsk and Luhansk "People's Republics" declare independence after referendums.
25 May 2014	Petro Poroshenko is elected president of Ukraine.
27 June 2014	The EU signs a landmark trade deal with Ukraine – Viktor Yanukovych's refusal to sign the deal sparked the original protests in Kiev in late 2013.
17 July 2014	Malaysia Airlines Flight MH17 is shot down in eastern Ukraine, allegedly by pro-Russian rebels, with the loss of 298 lives.
31 July 2014	EU agrees punishing economic sanctions, restricting access of Russian banks and oil companies to long-term western financing.
5 September 2014	The rebels, Ukraine, Russia and the Organization for Security and Cooperation in Europe sign a peace deal in Minsk, Belarus.
22 January 2015	Ukrainian troops are overrun by the rebels at the long-fought-over Donetsk airport.
23 January 2015	After repeated failed attempts at reviving the peace process, Alexander Zakharchenko, the separatists' leader, says his forces are going on the offensive.
31 January 2015	The latest peace talks of the contact group (representatives of the rebels, Ukraine, Russia and OSCE) in Minsk collapse.
5 February 2015	John Kerry, the US Secretary of State, travels to Kiev for talks amid debate over whether the US should arm Ukrainian government forces. Francois Hollande and Angela Merkel announce a surprise "new peace initiative."
12 February 2015	The leaders of Ukraine, Russia, Germany and France agree a deal to end fighting in eastern Ukraine at talks in Minsk, Belarus.
2 March 2015	United Nations warns that an estimated 6,000 people have been killed in eastern Ukraine since April 2014, as violence continues despite ceasefire.

Russia has used the concept of hybrid warfare to assert itself militarily and achieve long term strategic goals in their former Soviet territories. Because of the decline in the size and strength of the Russian Armed Forces, the hybrid warfare strategy compensates for the lack of men and material. By using intelligence operatives, local insurgents, and information operations, Russia can project power beyond its borders with smaller, tailored forces and proxies and still achieve their military and political objectives. The Russians view hybrid warfare as a viable strategy to control events and policy in its former Cold War provinces and allied states. Russia will continue to use this strategy as it attempts to influence governments and policy in Eurasia, the Baltic States, and the Balkans.

Sources

Kevin Brent. "Russian Spetsnaz Arrested In Ukraine." Examiner.com. March 2014.

Rueben F. Johnson. "UPDATE: Russia's Hybrid War In Ukraine 'is working'." IHS *Jane's Defence Weekly.* February 2015.

Eli Lake. "U.S. Eyes Russian Spies Infiltrating Ukraine." *The Daily Beast*. March 2014.

Eli Lake and Anna Nemstova. "Russia's Special Ops Invasion of Ukraine Has Begun." *The Daily Beast*. March 2014.

Alexander J. Motyl. "The Myth of The West's Threat To Russia." *New Atlanticist*. March 2015.

Ishaan Thoroor and Gene Thorp. "Maps: How Ukraine Became Ukraine." *The Washington Post*. 9 March2015

Mark Urban. "How Many Russians Are Fighting In Ukraine." BBC Newsnight. 25 March 2015.

Notes

[1] Foreign Staff Writers. Ukraine crisis: Timeline of major events. The Telegraph. 5 March 2015.

Doctrinal Corner: Hybrid Threat and DATE Support to Network Integration Evaluation (NIE)

by Kristin Lechowicz, TRADOC G2 ACE-Threats Integration (DAC)

During 17-18 February 2015, ACE-Threats Integration, along with a number of entities, participated in the first in a series of collaborative efforts to support the Network Integration Evaluation (NIE) 16.1 at the Training Brain Operations Center (TBOC) in Oyster Point, Virginia. ACE-Threats Integration's primary objectives during this session were to provide support to the conversion from the current NIE scenario to a Decisive Action Training Environment (DATE)-based construct while providing insight into the correct hybrid threat composite. Numerous organizational entities took part in this collective effort that included Army Capabilities Integration Center's (ARCIC's) Brigade Modernization Command (BMC) (which included 2nd Brigade 1st Armor Division), Army Test and Evaluation Command, the TRADOC G-2's Operational Environment Enterprise (OEE), which included the TBOC and ACE Threats Integration. The DATE and hybrid threat doctrine has supported US Army and coalition partners' training community for over four years with constructs that are flexible enough to sustain the rigorous capabilities-based exercises that are NIE requirements.

Overview of the NIE

ARCIC's BMC supports the US Army by providing the evaluation, recommendations, and conclusions extracted from the NIE exercises. NIE's exercises combine the elements of live, virtual, and constructive simulations in order to create a complex operational environment supporting dynamic assessments for each exercise. "NIEs serve as a principal driver of change in the Army evaluation and integration events that drive requirements, procurement, and fielding recommendations."[1]

1st Armored Division's 2nd Brigade bi-annually supports the requirements for NIE that "assess the operational utility, maturity and technical readiness, integration and interoperability with tactical systems from Soldier to Brigade and higher levels."[2] New systems and equipment are stress-tested during the exercise to allow for firsthand observations of the effects in a simulated combat environment. The realistic conditions set forth in NIE allow for critical observations and feedback from participants and/or observers on systems' performance that could determine future army capabilities development and requirements. The NIE relies on an adaptive threat and complex operational environment to create the precise conditions that challenge US Army leadership and stress systems capabilities in a field environment.

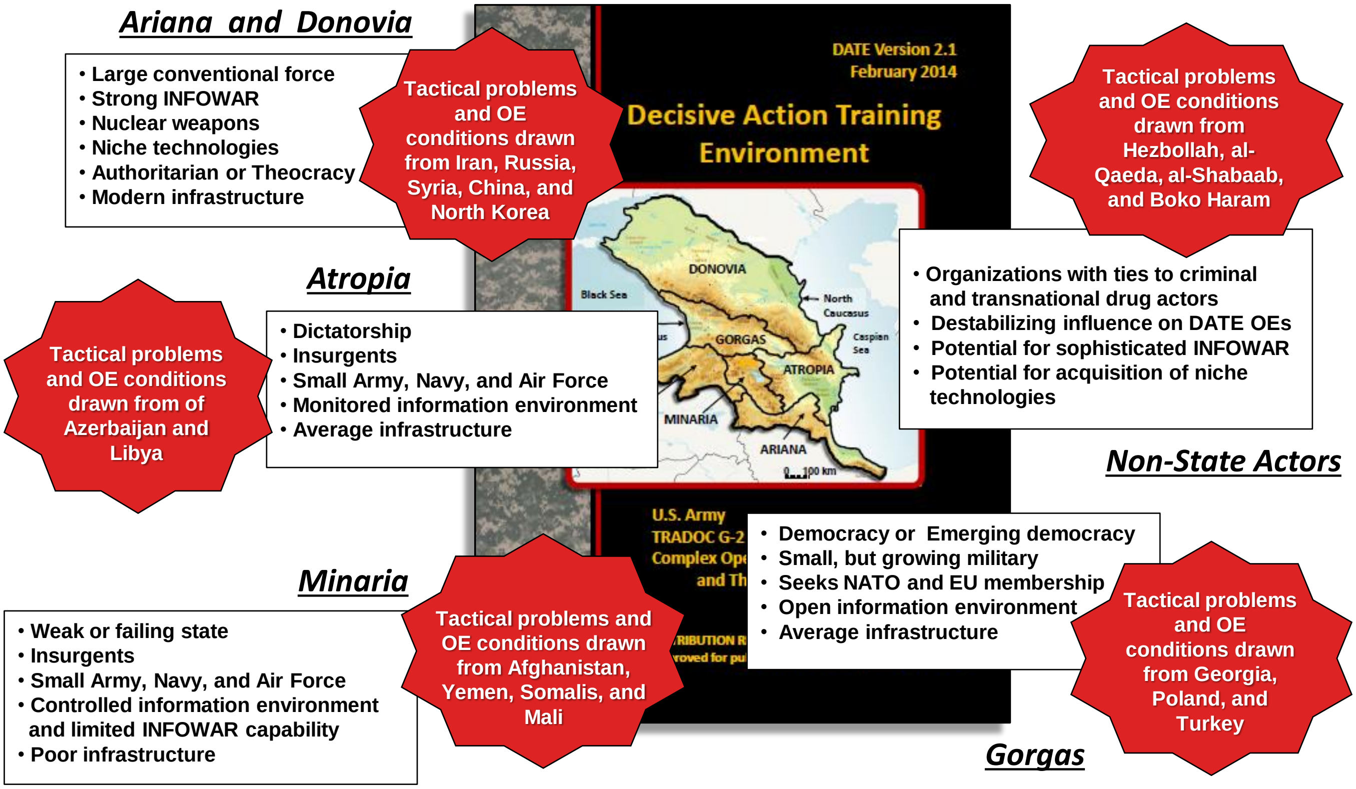
How Can the DATE and Hybrid Threat Support NIE?

DATE 2.1 is a flexible and comprehensive OE for training that contains material which can be adapted to support the NIE's challenging requirements. The DATE and hybrid threat doctrine also permit scenario development to remain at an unclassified level, which allows for coalition involvement and transparency for the scenario audience. The DATE and hybrid threat doctrine are proven concepts that have supported numerous successful combat training center (CTC) decisive action rotations and have been embedded in Centers of Excellence (COEs) along with home station training in support of the US Army's training agenda.

The DATE 2.1 describes a complex OE (much like the demanding OE required for NIE) using the PMESII-PT [Political, Military, Economic, Social, Information, Infrastructure, Physical Environment, and Time] construct which includes the capabilities for the five countries within DATE's framework. The DATE countries of Ariana, Atropia, Gorgas, Minaria, and Donovia present a wide range of characteristics and conditions that would be applicable for NIE scenario requirements. The DATE allows the flexibility for scenario developers to change the specific type of threats in order to present the correct construct for NIE's mission. See figure 1.

The DATE provides NIE with a flexible and complex threat that is based on the TC 7-100 series. TC 7-100 states that the "hybrid threats will use an ever-changing variety of conventional and unconventional organizations, equipment, and tactics to create multiple dilemmas…hybrid threats are networks of people, capabilities, and devices that merge, split, and coalesce in action across all of the operational variables."[3] The DATE captures these concepts in an OE for the scenario developer to leverage. The DATE provides the following additional items for scenario development in support of the military variable:

- Provides a high intensity dynamic regular near-peer force with niche capabilities. (NIE partners should train to face a near-peer force to better evaluate future capabilities development).
- Noncombatants on the battlefield and irregular forces such as insurgent, guerrilla, or criminal elements add to the complexity of the scenario and stress leadership and the military decision making process.
- Details about types, purposes, and general locations of underground facilities (UGFs).
- Details about nuclear capabilities and facilities.
- Information on satellite capabilities for each country has been expanded.



Ariana and Donovia

- Large conventional force
- Strong INFOWAR
- Nuclear weapons
- Niche technologies
- Authoritarian or Theocracy
- Modern infrastructure

Tactical problems and OE conditions drawn from Iran, Russia, Syria, China, and North Korea

Tactical problems and OE conditions drawn from Hezbollah, al-Qaeda, al-Shabaab, and Boko Haram

Atropia

- Dictatorship
- Insurgents
- Small Army, Navy, and Air Force
- Monitored information environment
- Average infrastructure

Tactical problems and OE conditions drawn from of Azerbaijan and Libya

- Organizations with ties to criminal and transnational drug actors
- Destabilizing influence on DATE OEs
- Potential for sophisticated INFOWAR
- Potential for acquisition of niche technologies

Non-State Actors

Minaria

- Weak or failing state
- Insurgents
- Small Army, Navy, and Air Force
- Controlled information environment and limited INFOWAR capability
- Poor infrastructure

Tactical problems and OE conditions drawn from Afghanistan, Yemen, Somalis, and Mali

- Democracy or Emerging democracy
- Small, but growing military
- Seeks NATO and EU membership
- Open information environment
- Average infrastructure

Tactical problems and OE conditions drawn from Georgia, Poland, and Turkey

Gorgas

Figure 1. DATE and hybrid threat application in NIE

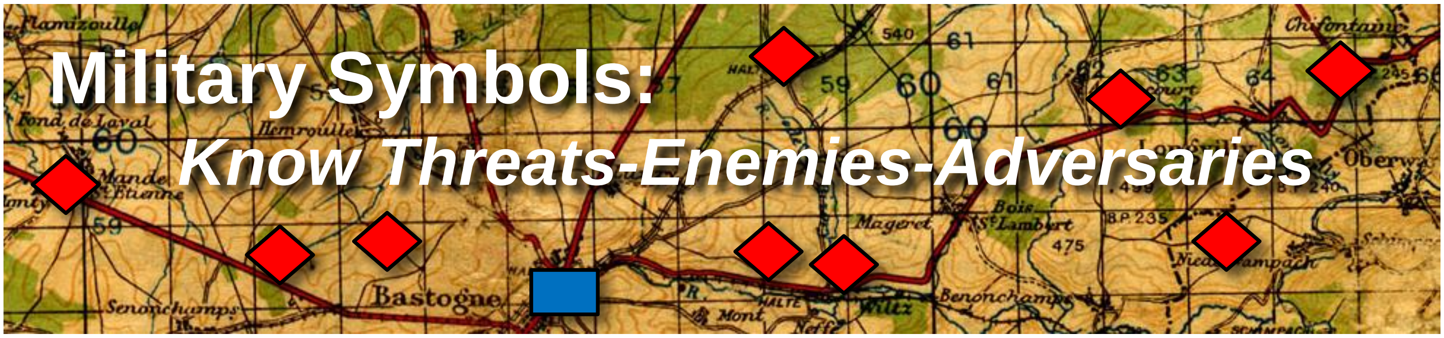
Elements such as ACE-Threats Integration and TBOC from the OEE will continue to support the NIE 16.1 usage of DATE OEs and hybrid threat concepts. The NIE is an important enduring requirement for the US Army's future capabilities development that requires a demanding OE with a persistent threat. The DATE provides complex OEs and adaptive threats, which remain a key piece of the US Army's training community.

Notes

[1] Army Capabilities Integration Center. Network Integration Evaluation. 18 March 2015.

[2] Army Capabilities Integration Center. Network Integration Evaluation. 18 March 2015.

[3] Headquarters, Department of the Army. Training Circular 7-100, Hybrid Threat. TRADOC G-2 Intelligence Support Activity (TRISA)-Threats, Complex Operational Environment and Threat Integration Directorate (CTID). November 2010.



Military Symbols:
Know Threats-Enemies-Adversaries

by Jon H. Moilanen, TRADOC G2 ACE-Threats Integration, Operations (BMA Ctr) Part 1 of 2 Parts

Know the Threat—Know the Enemy

Representing threats and enemies effectively in visual presentations requires standardized symbology and graphics to provide for a common and cogent understanding of a threat, adversary, or enemy in operational environments (OEs). For army training, professional education, and leader development, this professional understanding uses an opposing force (OPFOR). Several particular aspects of threats and/or OPFOR representation, primarily in types of irregular forces, remain to be standardized for symbols and graphics for common army use.

This article spotlights ongoing actions within the HQDA Training Circular 7-100 series and TRADOC G2 training literature to provide common symbology and graphics measures from a threats/OPFOR perspective.[1] Figure 1 provides an overview of the linkages among the TC 7-100 series.

A fundamental recognition is threat actors in current persistent conflicts and various regions of the world do not necessarily think, act, or appear as do US military forces in the conduct of military operations. Correspondingly, the threat/OPFOR in training, professional education, leader development, and other venues must represent these characteristics differently from US military forces.

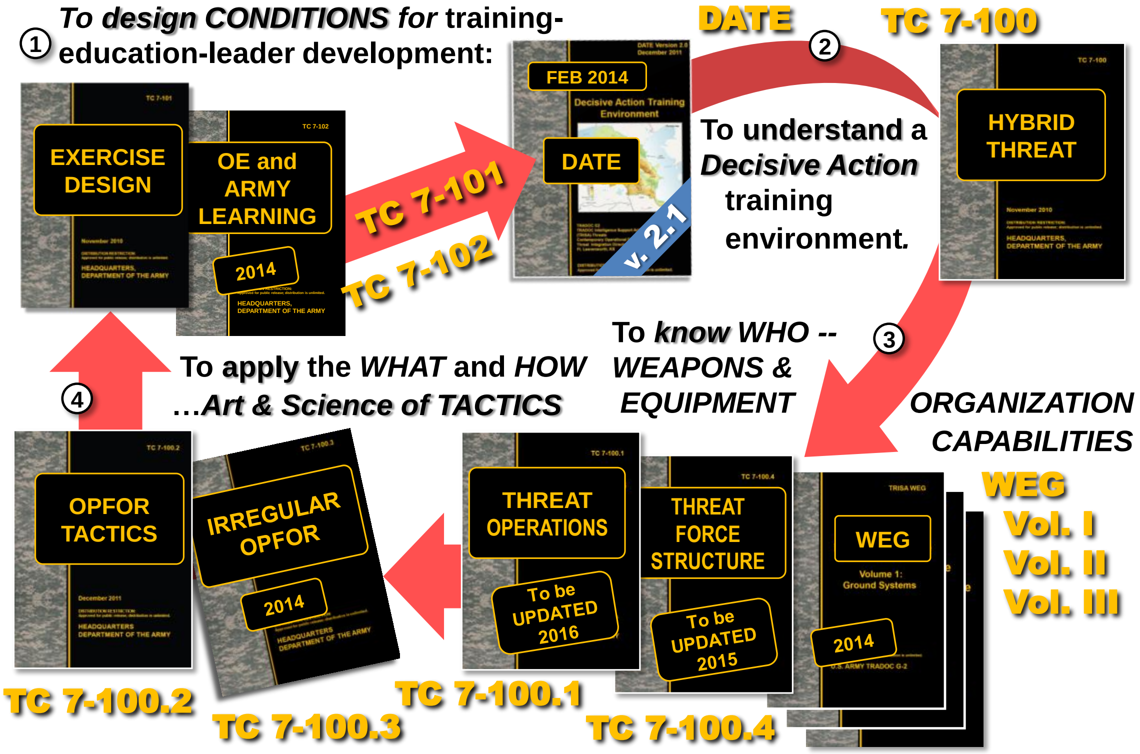
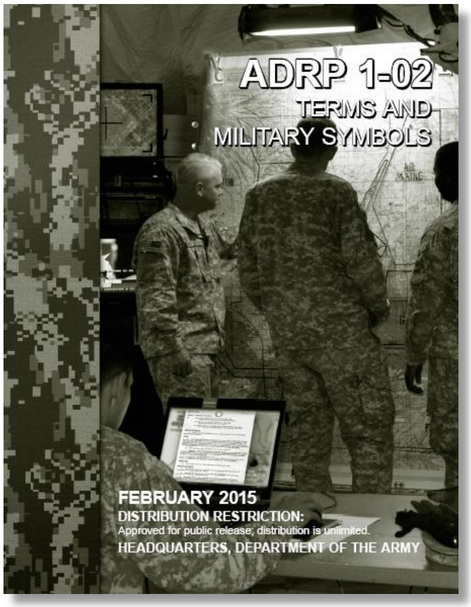


Figure 1. Overview of analysis and product integration into Threats/OPFOR training literature

The US Army describes an OPFOR for training as "a plausible, flexible military and/or paramilitary force representing a composite of varying capabilities of actual worldwide forces (doctrine, tactics, organization, and equipment) used in lieu of a specific threat force for training and developing US forces."[2] When an Army unit is preparing for deployment or is deployed in an OE with known threats, adversaries, and/or enemies, those actual OE conditions and force capabilities and limitations are used rather than an OPFOR.

The Training and Doctrine Command (TRADOC) G2—as the responsible intelligence official to the TRADOC Commanding General—develops, manages, administers, integrates, and approves the functions of the *Opposing Force (OPFOR) Program* (AR 350-2) across the army.[3] Functional areas include OE conditions and threats/OPFOR doctrinal, organizational, and equipment capabilities used for army training, military operations, and other army concepts and scenarios developmental efforts.



ADRP 1-02
TERMS AND
MILITARY SYMBOLS

FEBRUARY 2015
DISTRIBUTION RESTRICTION:
Approved for public release; distribution is unlimited.
HEADQUARTERS, DEPARTMENT OF THE ARMY

Current US Army Doctrine for Symbols-Control Measures

The US Army recently updated Army Doctrine Reference Publication (ADRP) 1-02, *Military Terms and Symbols*, in February 2015. This publication constitutes approved army doctrinal terminology and symbology for use in army operations, and builds on foundational doctrine established in Army Doctrine Publication (ADP) 1-02.[4] This army publication complies with Department of Defense (DOD) Military Standard (MIL-STD) 2525C, *Common Military Symbology,* and does acknowledge some differences in standards among consideration of US Army, US Joint Forces, and the North Atlantic Treaty Organization (NATO).

Nonetheless, several threat/OPFOR capabilities are not currently represented in ADRP 1-02 symbology. Examples illustrated later in this article include types of regular and irregular force symbols such as Threat/OPFOR motorized infantry units, insurgent cells, and guerrilla units.

To provide selected standardized threats/OPFOR symbols and graphics in support of ADRP 1-02, the TRADOC G2 Analytical and Control Element-Threats Integration Directorate (ACE-Threats Integration) identifies and updates threats/OPFOR symbols and graphics in the HQDA TC 7-100 series and associated TRADOC G2 training literature. This TRADOC G2 directorate "serves as Army lead for designing, documenting, and integrating threat (or OPFOR) and OE conditions in support of all army training, education, and leader development programs."[5] This directorate also reviews, analyzes, and provides recommendations for the integration of an OE and its critical variables into training, education, and leader development events.

ADRP 1-02 provides the single standard for developing and depicting hand-drawn and computer-generated military symbols for situation maps, overlays, and other graphics displays for all types of military operations. The ACE-Threats Integration directorate constructs threats/OPFOR symbols and graphics within this guidance and flexibility allowed by ADRP 1-02 to meet training, educational, and operational needs.[6] For example, within or adjacent to the standard diamond-shape symbol frame for a hostile entity—a threat or OPFOR—appropriate icons, modifiers, and/or free text areas identify primary functions, capability, mobility, and/or other critical information.

When representing unorthodox framed symbols, ACE-Threats Integration selects the most appropriate icon or modifier from ADRP 1-02. US Army TC 7-100.2 describes use of amplifiers for organizational echelon or task-organized status of threat/OPFOR units and organizations. For threat/OPFOR echelon designation, the echelon amplifier is centered above the symbol frame but does not touch the symbol frame. Other symbol construction norms such as for a threat/OPFOR guerrilla unit or insurgent organization are presented in TC 7-100.3.

Threats/OPFOR Symbology for Training and Readiness

A military symbol is a graphic representation of a unit, equipment, installation, activity, control measure, or tactical task relevant to military operations that is used for planning or to represent a commonly understood operational picture on a map, display, or overlay.[7] Military symbols include unit, equipment, installation, and activity symbols, and control measure and tactical symbols.

The icon, as the innermost part of a symbol, typically has three internal sectors to display information within a symbol frame. A central icon is normally not so large as to exceed the dimensions of the central sector or touch the interior border of the frame as presented in ADRP 1-02. However, there are exceptions to this size rule. In those cases, icons occupy the entire frame and touch the interior border of the symbol frame.[8]

From a threats and OPFOR viewpoint, a diamond-shape frame is a friend or assumed friendly entity or equipment of a threat/OPFOR and uses the color red. An enemy or assumed hostile entity of a threat/OPFOR uses the color blue with a rectangle frame for a unit and a circle frame for equipment.

A square frame is a neutral identity, and a quatrefoil frame denotes an unknown and pending identity. The color green is neutral, and the color yellow is for unknown or pending symbols.[9] The color purple is typically not used in Army presentations; however, some exceptions can exist when operating with joint or multinational conditions for civilian units, equipment, and/or installations. Notwithstanding, threat/OPFOR civilian units, equipment, and/or installations will use the color red.[10] Table 3-1 of ADRP 1-02 (2015) illustrates threat/OPFOR installation and activity frames.

Indicating whether an operational object exists at a location is identified as either present or planned. The symbol frame is a solid line when indicating a present status, and the frame is a dashed line when indicating a planned or anticipated location. See figure 2 for basic threat/OPFOR [friendly forces]-type symbols and locational information.

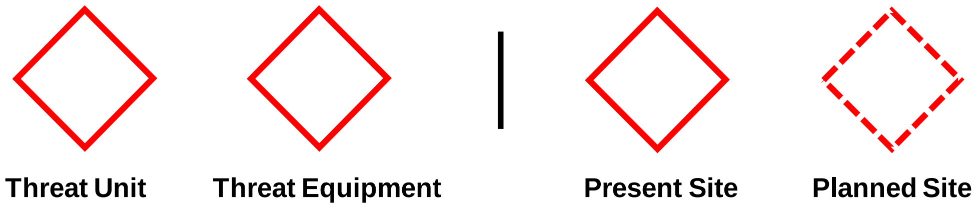


Figure 2. Threat symbol frame types and present or planned location

In a case of a suspected location or other assumed status, a threat/OPFOR technique can make use of special amplifiers such a question mark character icon and/or word "SUSPECTED" as a free text modifier inside or next to the symbol.[11] See figure 3 with sample symbol frames used by threats/OPFOR for enemy [blue] units and equipment, as well as suspected enemy [blue] units or unknown entities with as much information as known.

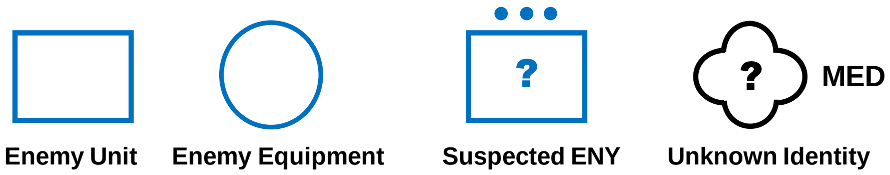


Figure 3. Threat symbol frames for enemy, suspected enemy, and unknown

Threat/OPFOR Units and Organizations

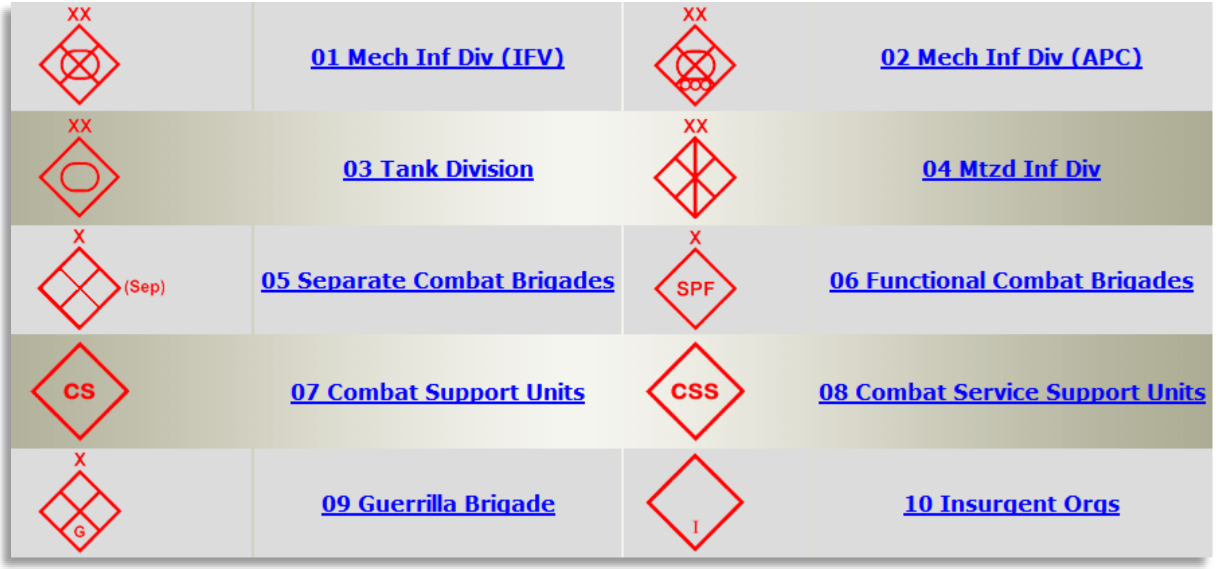
The threat/OPFOR identifies two main groupings of military forces: regular forces and irregular forces. A unit or organization symbol is often not enough information to visualize organizational capability. In such cases, threat/OPFOR symbols use the free text area primarily to the right of a frame; however, free text is allowable to the left, right, or below in order to adequately communicate a unit, equipment, activity, or installation capability.

Regular Forces

Table 1 displays an introduction screen in the Army Training Network (ATN) website of several threat/OPFOR regular force unit and irregular force unit and organization structures. These e-folders are within the "Training for Operations" button on the ATN front-page, and its subordinate e-folder "ACE-Threats Integration Operational Environment Page." Click Threat Doctrine and Force Structure.

The TRADOC G2 ACE-Threats Integration Directorate updates these e-folders with representative capabilities. Additional information in other e-folders provides detailed unclassified organization, weapon system, and equipment data.[12]

Table 1. Sample of Threat/OPFOR regular and irregular force structures in ATN website



XX	01 Mech Inf Div (IFV)	XX	02 Mech Inf Div (APC)
XX	03 Tank Division	XX	04 Mtzd Inf Div
X (Sep)	05 Separate Combat Brigades	X SPF	06 Functional Combat Brigades
CS	07 Combat Support Units	CSS	08 Combat Service Support Units
X G	09 Guerrilla Brigade	I	10 Insurgent Orgs

Unit symbols often use free text to identify primary weapon systems and/or indicate the level of modernization and capabilities that exist in a particular unit. A norm considers that almost all units have a mix of tiered or varied modernization, even when a state-of-the art weapon system is displayed as free text next to a unit symbol. Other mobility modifiers can also be added when appropriate.

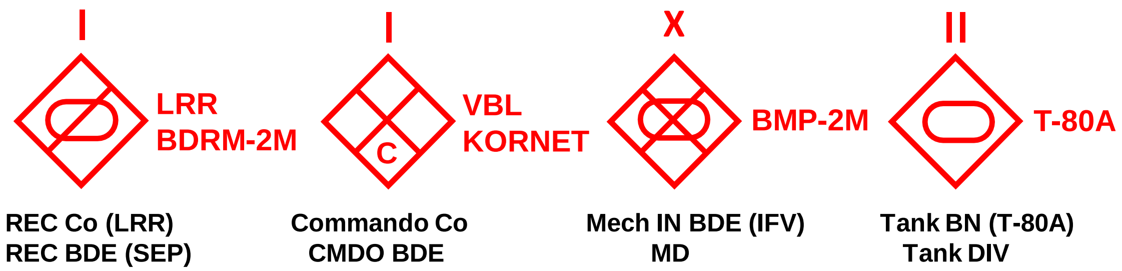
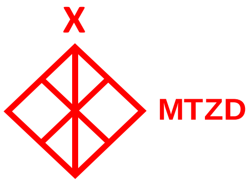


Figure 4. Sample of Threat/OPFOR regular units and free text amplifiers

Capability is more than just organizational structure. For example, the threat/OPFOR motorized division may be quite different from how some nation-states organize and equip motorized force. The US Army uses the term “Stryker” in lieu of “motorized” when referring to US Army forces, but does allow the term “motorized” to be used in doctrine when referring to other than US Army forces.[13] As an example of distinct differences, a motorized threat/OPFOR infantry unit uses its wheeled vehicle fleet primarily to move and transfer units, personnel, equipment, and logistics to support operations. Its wheeled utility vehicles are transportation rather than fighting vehicles. Symbology may also be different.[14] The infantry of a threat/OPFOR motorized infantry unit are dismounted when conducting tactical combat tasks in an operation. OPFOR uses the DOD motorized symbol.



Irregular Forces

TC 7-100.3 describes three main categories of irregular forces: guerrilla units, insurgent organizations, and criminal organizations. To better understand an OE, this training circular also addresses elements within a relevant population such as noncombatants and/or who may be an active supporter or passive supporter of regular and/or irregular forces. The threat/OPFOR does not describe itself as a terrorist force, group, or element. Acts of terrorism are addressed as a tactic applied with diverse techniques.

The guerrilla unit uses the basic infantry icon and adds the letter "G" in the lower sector of the symbol frame to identify this type of irregular paramilitary element or force. The hunter-killer (HK) task organization configures guerrilla force structure into multiple small groups, sections, and teams to optimize dispersed tactical operations.

An insurgent organization places the capital letter "I" in the lower sector of the organization or cell symbol, and usually does not have other icons within the symbol frame. Insurgent and criminal symbols do not have an echelon amplifier above the symbol. However, when clarity requires an icon and/or modifier, they are placed inside or next to the symbol frame, as in the information warfare cell of an insurgent organization. Figure 5 displays a sample of unit and organizational symbols with concise descriptions. Additional information is available on the ACE-Threats Integration page on the ATN site.

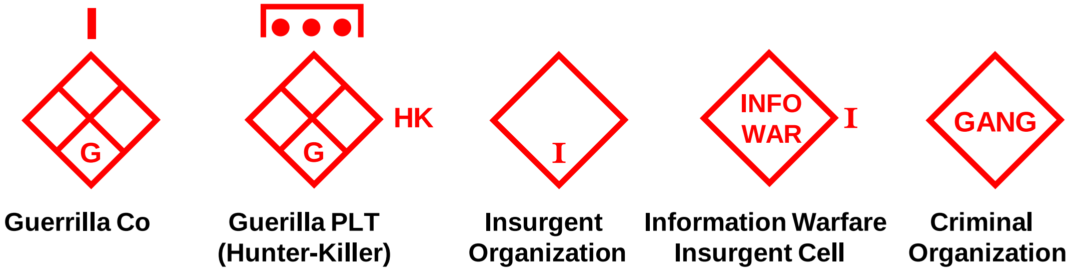


Figure 5. Sample of Threat/OPFOR irregular units, organizations, and cells

What Next for Part 2 in the April 2015 *Red Diamond*

This March *Red Diamond* part 1 of a two-part article accents ADRP 1-02 as the army standard and how the HQDA TC 7-100 series complements military symbols and terms for threats and an OPFOR. The part 2 article in the April 2015 *Red Diamond* newsletter will provide examples of selected threat/OPFOR equipment and weapons systems and how they are displayed as symbols and/or amplifying terms. Selected threat/OPFOR activities and installations receive similar attention as symbols and descriptions. Several examples of threat/OPFOR individual, group, or cell identities such as assassin, coerced recruit, and/or freedom fighter use modified symbols and are different from the types of killings or criminal activity victim symbols presented in ADRP 1-02.

Most mission tasks for threat/OPFOR use symbols consistent with ADRP 1-02; however, several threat/OPFOR symbols appear different and/or have different definition. Similarly, some threat/OPFOR symbols and control measures are different for types of movement and maneuver, fires, and defensive positions.

Implications for Army Training and Readiness

Training readiness can be evaluated in the context of at least two distinct conditions. When a specific threat force is not identified or known for mission readiness, a robust, realistic, and relevant OPFOR provides a composite of varying capabilities of actual worldwide forces in doctrine, tactics, organization, and equipment. However, when an army unit is preparing for a specified mission or contingency operation deployment in an OE with known threats, adversaries, and/or enemies, training replicates those actual OE and force capabilities and limitations to the optimum extent possible. In both cases, the conditions are created to provide a challenging environment for the US Army commanders to evaluate and confirm their mission essential or specified tasks to an army standard.

ADRP 1-02 is the US Army doctrinal source for terms and military symbols. The *Army Dictionary online* augments this ADRP due to changes to terminology that occur more frequently than traditional publication media can be updated. See https://www.milsuite.mil/book/docs/DOC-40298. This terminology and symbology database, known as the *Army Dictionary*, is updated monthly to reflect the latest editions of army publications. (With a common access card, access the dictionary database at https://jdeis.js.mil/jdeis/index.jsp?pindex=207.) This database is an official Department of Defense (DOD) website, maintained by the Combined Arms Doctrine Directorate (CADD) at the US Army Combined Arms Center (USACAC) and in collaboration with the US Joint Staff.[15]

The HQDA TC 7-100 series, as produced by the TRADOC G2 ACE-Threats, is the US Army source for tailoring a realistic, robust, and relevant array of threats to challenge designated training tasks, and is a key complement to preparing for and understanding known threats, enemies, and adversaries in operational missions. The TRADOC G2 Operational Environment

Enterprise (G2 OEE) recognizes and supports the comprehensive readiness mission of focused training, progressive professional education, and a continuum of army leader development.

Notes

[1] This HQDA training circular (TC) series is in final transition in 2015 from army field manuals to training circulars. The currently published TC 7-100 series is on the Army Publishing Directorate (APD).

[2] Headquarters, Department of the Army. Army Regulation 350-2. *Opposing Force (OPFOR) Program*. 9 April 2004. Para. 1-5.

[3] Headquarters, Department of the Army. Army Regulation 350-2. *Opposing Force (OPFOR) Program*. 9 April 2004. Para. 1-13.

[4] Headquarters, Department of the Army. Army Doctrine Reference Publication 1-02. *Terms and Military Symbols*. 2 February 2015. p. v. *Note*. Department of Defense (DOD) Military Standard (MIL-STD) 2525C, *Common Warfighting Symbology.* 17 November 2008 remains in effect. *Note*. This DOD standard is in revision with a probable publication update in late 2015.

[5] Headquarters, United States Army Training and Doctrine Command. TRADOC Regulation 10-5-1, *Headquarters, United States Army Training and Doctrine Command*. 20 July 2010. para. 18-8, 1c(a). Note. TR 10-5-1 is in revision with TRADOC publication due in 2015.

[6] Headquarters, Department of the Army. ADRP 1-02. *Military Terms and Symbols*. 2 February 2015. Para. 3-15.

[7] Headquarters, Department of the Army. ADRP 1-02. *Military Terms and Symbols*. 2 February 2015. Para. 3-1.

[8] Headquarters, Department of the Army. ADRP 1-02. *Military Terms and Symbols*. 2 February 2015. Para. 3-14.

[9] Headquarters, Department of the Army. ADRP 1-02. *Military Terms and Symbols*. 2 February 2015. Para. 3-4.

[10] US Department of Defense. Military Standard (MIL-STD-2525C). *Common Warfighting Symbology*. 17 November 2008. P 20.

[11] US Department of Defense. Military Standard (MIL-STD-2525C). *Common Warfighting Symbology*. 17 November 2008. p. 15.

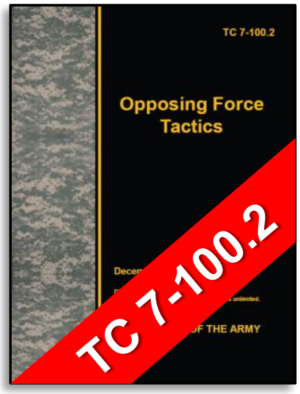
[12] Headquarters, United States Army Training and Doctrine Command. Deputy Chief of Staff G-2. *Worldwide Equipment Guide*. (Volumes I, II, and III) 1 December 2015.

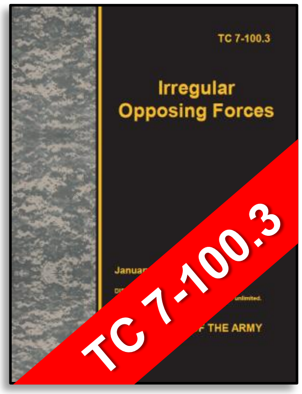
[13] US Army Combined Arms Center. Combined Arms Doctrine Directorate (CADD). Army Doctrine Term Changes Historical Database (as of 10 MAR 2015). Term "motorized." See also, Introductory Table-2, ADRP 3-90. *Offense and Defense*. 31 August 2012.

[14] US Department of Defense. Military Standard (MIL-STD-2525C). *Common Warfighting Symbology*. 17 November 2008. p. 129. *Note*. Threat/OPFOR uses the DOD symbol for motorized elements-forces, and can use a "MTZD" amplifier.

[15] Headquarters, Department of the Army. ADRP 1-02. *Military Terms and Symbols*. 2 February 2015. p. vii.

Training for Readiness





Operational Environments
with
Realistic-Robust-Relevant
Threats

Irregular Force

Threat Model Design: Simple Battle Position (SBP)

by LTC Shane E. Lee and CPT Ari Fisher, TRADOC G2 ACE-Threats Integration

A threat model is a "three-part analytical work aid designed to assist in the development of situation templates during step 4 of the IPB process." Threat models provide graphical representations of threat doctrine, describe the threat's tactics, and identify high-value targets (ATP 2-01.3).[1] The threat will have obvious, as well as subtle, differences in how it approaches situations and problem solving. Understanding these differences is essential in understanding how a threat force will react in a given situation.

The intelligence staff conducts threat evaluation and develops threat models as part of the generate intelligence knowledge task of support to force generation. Using this information, the intelligence staff refines threat models, as necessary, to support intelligence preparation of the battlefield (IPB). When analyzing a well-known threat, the intelligence staff may be able to rely on previously developed threat models. When analyzing a new or less well-known threat, the intelligence staff may need to evaluate the threat and develop models. (For information related to IPB, see ATP 2-01.3 *Intelligence Preparation of the Battlefield/Battlespace,* Chapter 5.)

Threat Model design requires the following steps:

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

This article will discuss threat model design steps 1-4 by demonstrating an irregular force prosecuting defending a *simple battle position* with the mission to delay enemy force follow on and pursuit.

Simple Battle Position

A *simple battle position* (SBP) is a defensive location oriented on the most likely enemy avenue of approach. SBPs may or may not be tied to restrictive terrain, but use camouflage, concealment, cover, and deception (C3D) measures, and employ as much engineer effort as possible to restrict enemy maneuver. SBP defenders conduct all actions to prevent enemy penetration of their position and/or defeat a penetration once it has occurred.

TC 7-100.2 *Opposing Force Tactics*

A *simple battle position* (SBP) is a defensive location oriented on the most likely enemy avenue of approach. SBPs are not necessarily tied to complex terrain. However, they often employ as much engineer effort and/or camouflage, concealment, cover, and deception (C3D) measures as time allows. Defenders of SBPs will take actions required to prevent enemy penetration of their position or defeat it once it has occurred. Likely, an SBP is not singular in nature and is linked to other positions in a larger integrated defensive array. (For information related to simple battle positions, see TC 7-100.2, *Opposing Force Tactics*, Chapter 4.)

Opposing Force (OPFOR) commanders of detachments, battalions, and below select the tactical action best suited to accomplish their mission. Units at this level and below are typically called upon to execute one combat mission at a time; both offense and defensive actions associated with this echelon are designated as Detachment Tactics.

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

Simple Battle Positions are characterized by:

- **Control** of key terrain and/or an enemy avenue of approach
- **Gain Advantage** over the enemy by use of terrain, C3D, and survivability

> **Action and Enabling Functions**
>
> **At threat battalion and below echelon, one part of the unit conducting a particular action is normally responsible for performing the action function or task that accomplishes the overall mission objective of that action. At battalion and below echelon that part can be called the *action* element.**
>
> **In relation to the action function or force, all other parts of the organization conducting an action provide enabling functions of various kinds. These parts can be called an enabling element.**
>
> **TC 7-100.2, *Opposing Force Tactics***

Functional Organization for a Simple Battle Position

Depending on the tactical situation, a commander organizing a simple battle position may designate various mission elements. There may be more than one of each type element. For example, the guerrilla platoon commander will use a term such as *disruption, fires, reserve,* or *main defense* element to best describe an element's function. (See figures 1 and 2.)

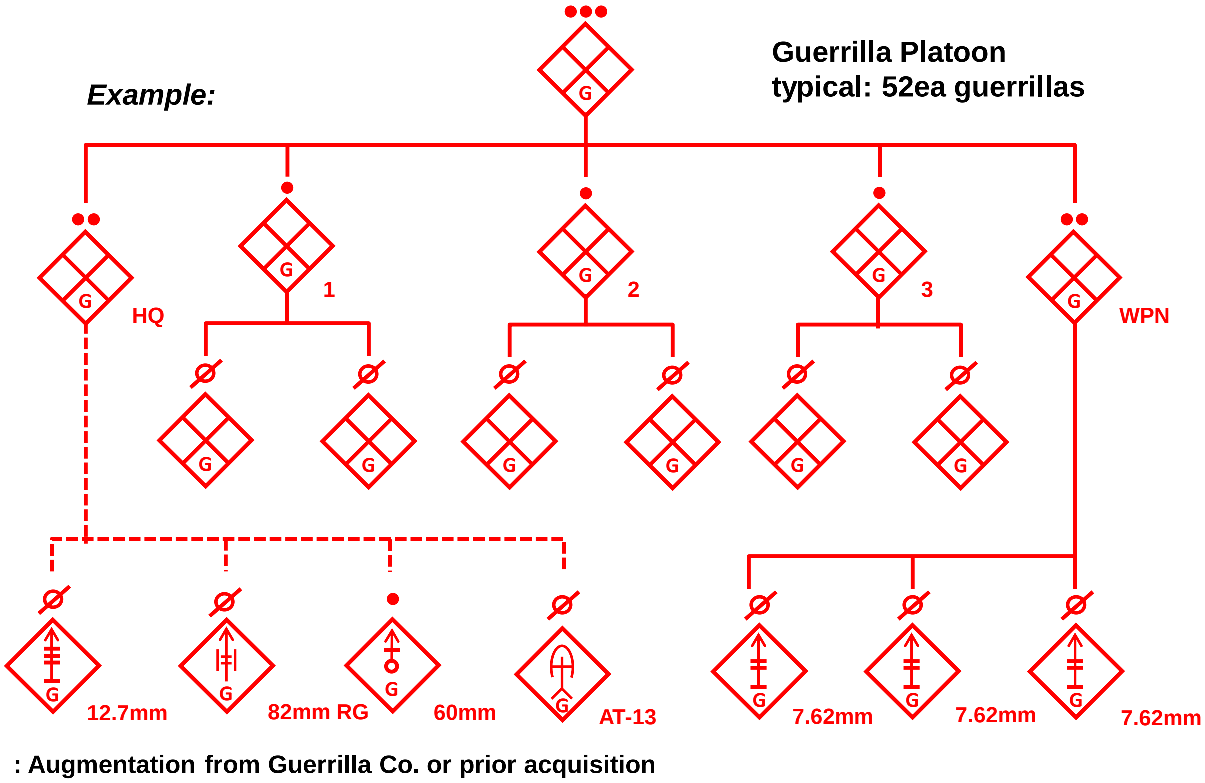


Figure 1. Simple battle position (order of battle example)

When constructing a threat model with the threat mission identified, during steps two and three it is imperative to begin with what success looks like on the objective with the action function and work backwards toward the assembly area. This is done for one primary reason: the threat prioritizes commander's intent and mission accomplishment over capability possessed and will determine what types of actions have to occur before allocating resources.

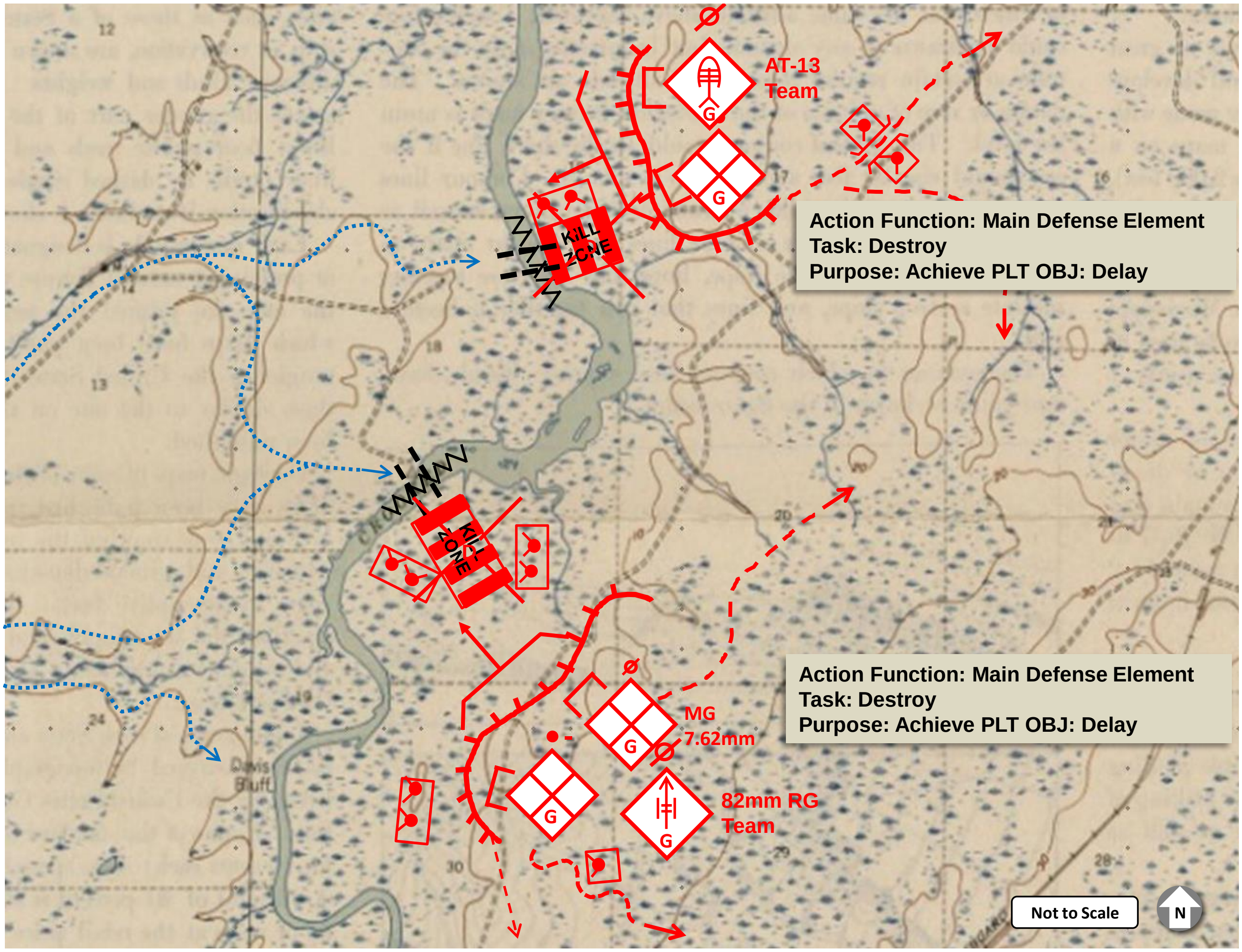

AT-13 Team
G
G
KILL ZONE
Action Function: Main Defense Element
Task: Destroy
Purpose: Achieve PLT OBJ: Delay
KILL ZONE
Action Function: Main Defense Element
Task: Destroy
Purpose: Achieve PLT OBJ: Delay
MG 7.62mm
G
G
82mm RG Team
G
Not to Scale
N

Figure 2. Simple battle position (main defense example)

If the threat is not in possession of a capability to accomplish a tactical mission task required in time and space, it will either devise an adaptive means to do so or attain assistance from a higher command or another threat actor to augment their order of battle providing them the capability required. Conversely, if we prioritize in the reverse and articulate threat tactics under an assumed constraint of their capability, we are likely to be surprised. The following discussion begins with the action function achieving success on the objective with enabling functions following in order of how to place them on a threat model to support and ensure success.

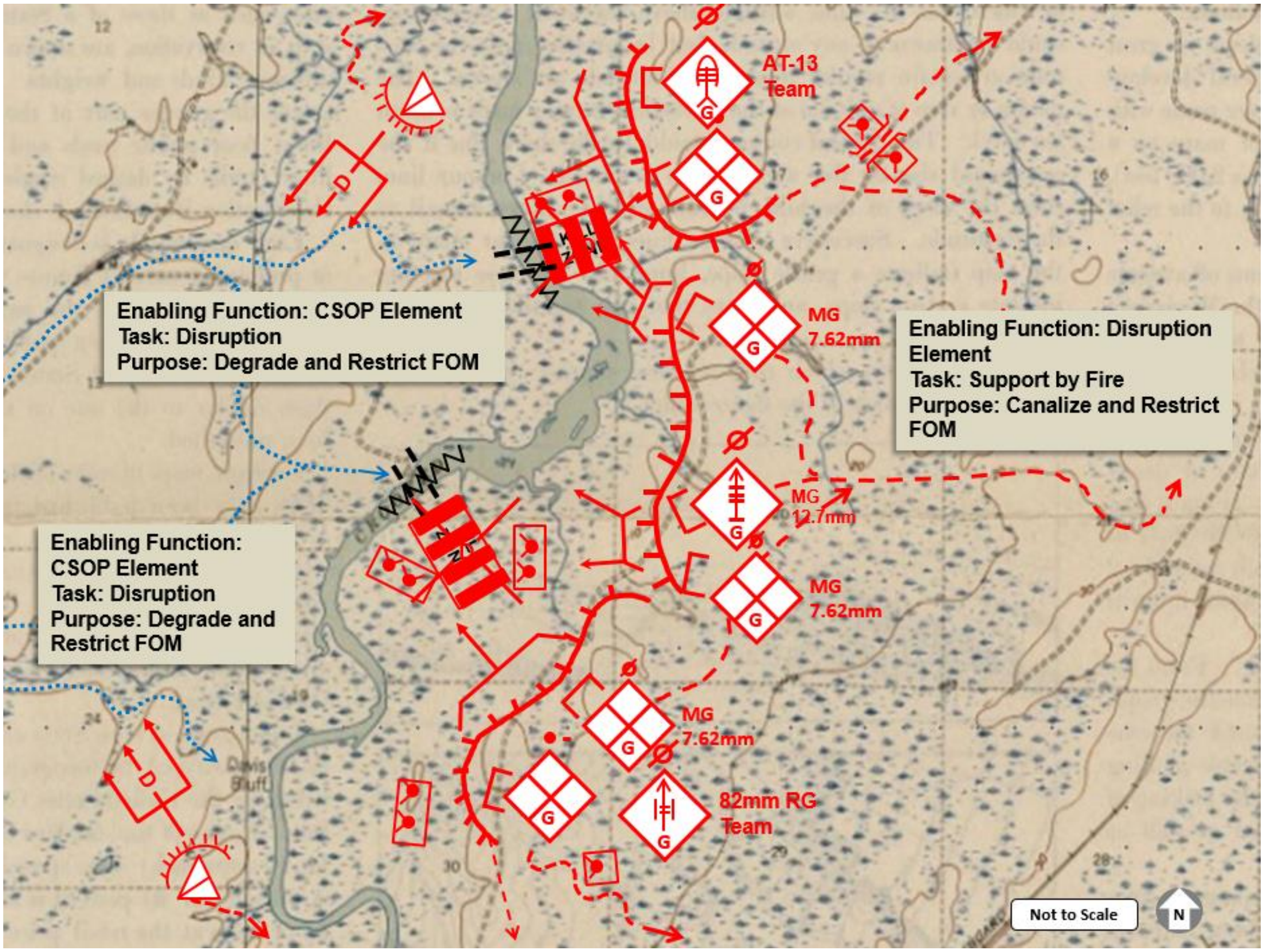
Action Function—*Main Defense Element(s)*

The guerrilla platoon commander orders the one squad to the north, augmented by an anti-tank capability, and a squad in the south, augmented with a heavy machine gun and recoilless gun capability, to accomplish the designated tactical mission tasks to *defeat* an enemy attack in order to enable other threat elements the time to reposition, and allow the guerrilla platoon to trade space for time. These locations are the most likely avenue of approach for enemy forces attempting a gap crossing in that vicinity. For synchronization purposes, these elements identify the likely crossing points as kill zones and employ obstacles to further canalize and hinder enemy movement and action. In order to ensure the success of these elements, the platoon commander identifies enabling functions to assist these main defense elements. In the case of this guerrilla platoon, use disruption and fires elements.

Enabling Functions

Disruption Element—Combat Security Outpost(s)

In this vignette, disruption elements receive indications that enemy elements are within the platoon's area of responsibility (AOR). The guerrilla platoon commander requires counterreconnaissance to identify and report the location of enemy reconnaissance patrols, main attack elements, and/or subsystems of the enemy's combat system, and subsequently seeks to engage designated elements with direct fires. Therefore, the threat establishes two combat security outposts (CSOP) forward of identified kill zones to support each main defense element. Once complete with their counterreconnaissance task, the OPFOR performs the tactical mission task of *disruption* to degrade the enemy's pursuit or attack by forcing them to commit prematurely, break apart their combat formation and systems, or desynchronize their plan. Should the enemy not be able to locate these positions once contact occurs, it is possible for these elements to break contact and reposition to be re-missioned, attack by fire or ambush, for instance, to prosecute a counterattack continuing to service the main defense elements in another form.



Enabling Function: CSOP Element
Task: Disruption
Purpose: Degrade and Restrict FOM

Enabling Function: Disruption Element
Task: Support by Fire
Purpose: Canalize and Restrict FOM

Enabling Function: CSOP Element
Task: Disruption
Purpose: Degrade and Restrict FOM

Figure 3. Simple battle position (disruption example)

Disruption Element(s)

The guerrilla platoon commander also identifies a terrain gap between the two main defense forces that requires attention. To support the main defense force in canalization of the enemy, the platoon places a disruption element with fighting positions oriented to provide direct fires over kill zones and associated obstacles that overlap in the center sector should the enemy contemplate the least likely approach avenue and challenging gap crossing. This element executes the tactical mission task of *support by fire* to restrict enemy freedom of movement and enable main defense force freedom of movement to best remain or attain a position of advantage to achieve effects associated with their task of defeat.

Fires Element(s)

Due to the importance of a successful delay, the guerrilla platoon leader's commander coordinates to ensure the platoon has a local indirect fires capability and provides a 60-mm mortar team. Fire support to support the defense of an SBP desires to—

- Attrit attackers along avenues of approach.
- Defeat attackers in the battle zone.
- Defeat penetrations of battle positions.
- Support counterattacking forces.

The guerrilla platoon commander prioritizes first to attrit attackers, second, to assist the main defense element defeat task in the kill zones, and finally support CSOP elements who may be re-missioned as an element performing a counterattack.

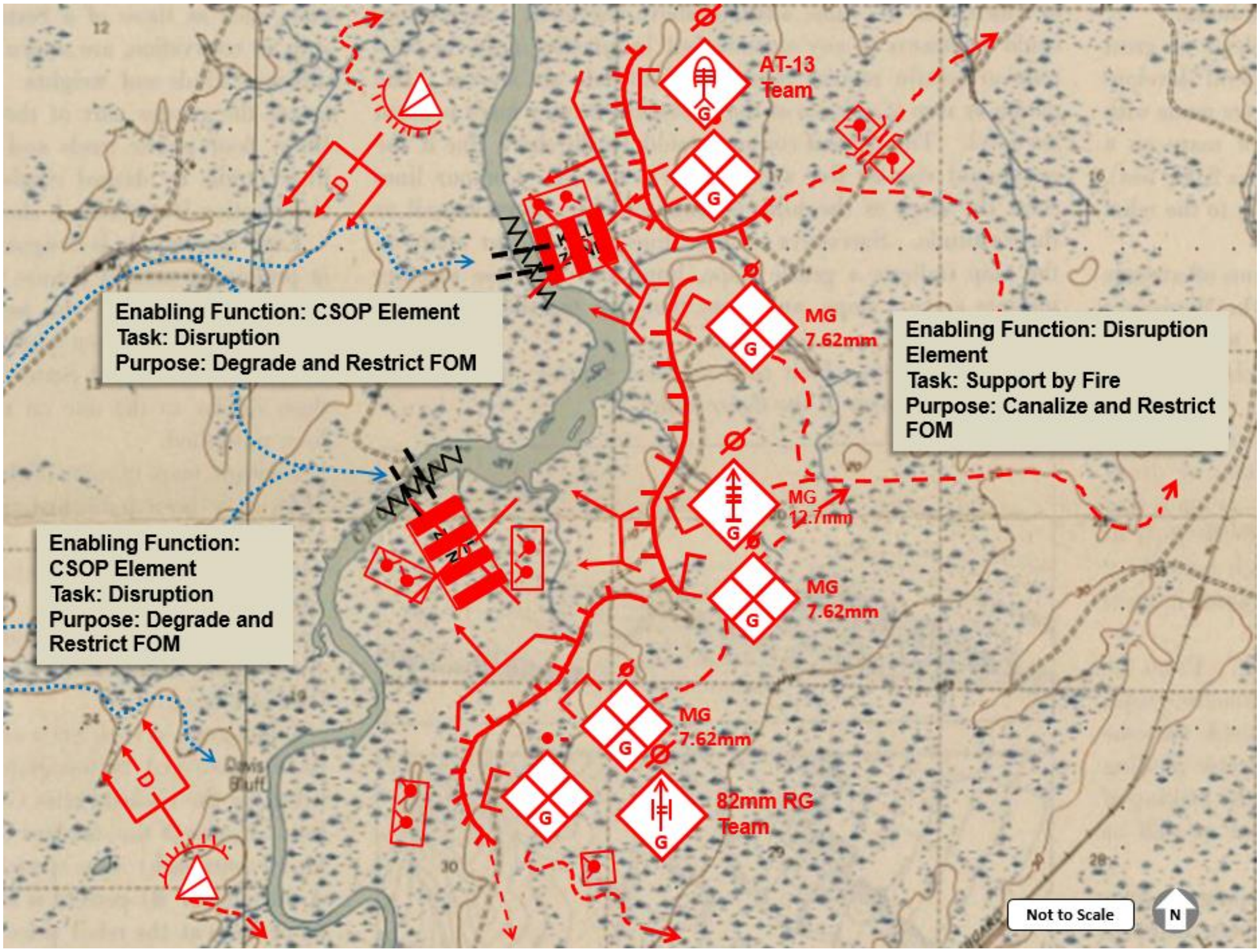

AT-13 Team
D
G
KILL ZONE
Enabling Function: CSOP Element
Task: Disruption
Purpose: Degrade and Restrict FOM
MG 7.62mm
Enabling Function: Disruption Element
Task: Support by Fire
Purpose: Canalize and Restrict FOM
MG 12.7mm
Enabling Function: CSOP Element
Task: Disruption
Purpose: Degrade and Restrict FOM
MG 7.62mm
MG 7.62mm
82mm RG Team
Not to Scale
N

Figure 4. Simple battle position (fires example)

Conclusion

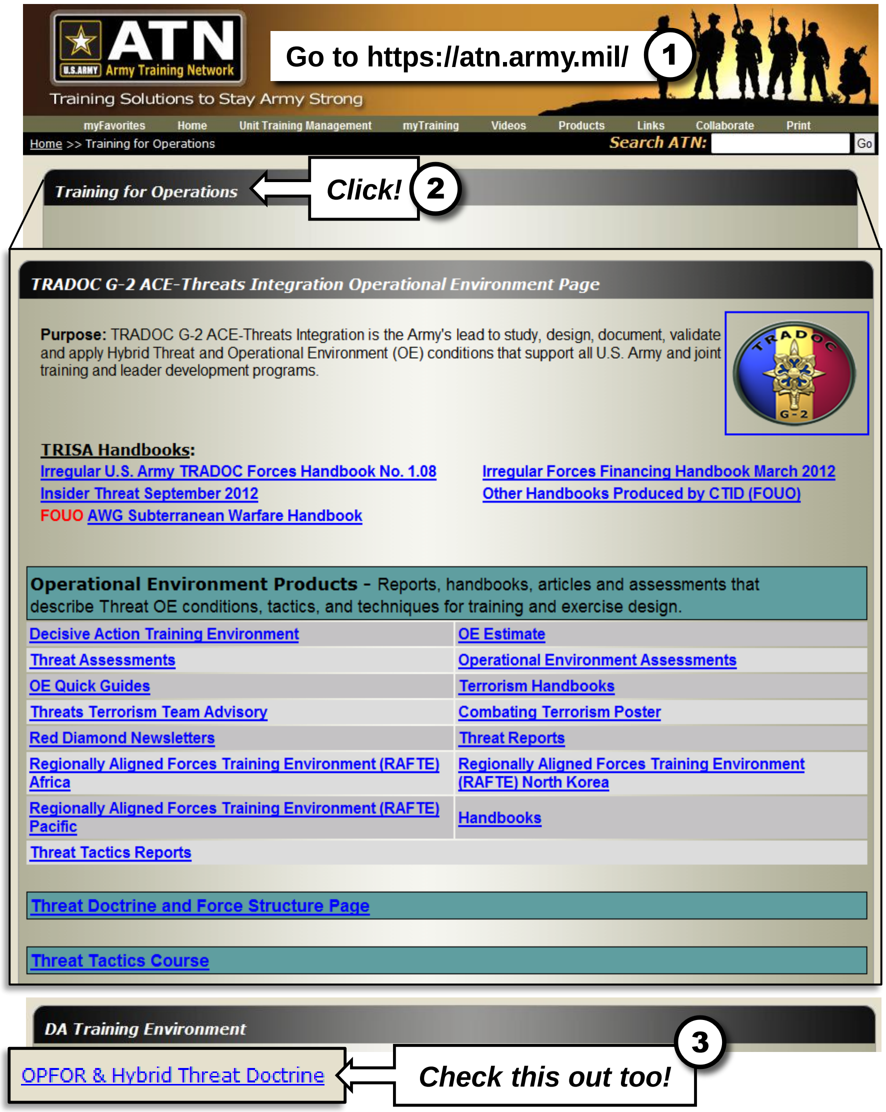
As a building block, simple battle positions are an important aspect of defensive tactics. Like with all threat models, they are constructed by first visualizing victory and then identifying what functions must be performed to support that success. In this vignette of a SBP defense, the main defense elements performed the action function complemented by elements performing an enabling function. It is important to remember that the threat seeks to culminate engagements by searching for enemy single points of failure. While the main defense elements seek victory in the kill zone, other elements that have broken contact are actively looking to destroy a critical node forcing enemy culmination. Likewise, disruption elements hope to expose those enemy nodes through disruption causing premature committal of forces. Inherently then, even when the threat is prosecuting a defensive action, the threat thinks and acts offensively.

Notes

[1] ATP 2-01.3, Intelligence Preparation of the Battlefield/Battlespace. 10 November 2014.

____

Threats Integration on ***Army Training Network***



Go to https://atn.army.mil/ 1

Home >> Training for Operations

Training for Operations

Click! 2

TRADOC G-2 ACE-Threats Integration Operational Environment Page

Purpose: TRADOC G-2 ACE-Threats Integration is the Army's lead to study, design, document, validate and apply Hybrid Threat and Operational Environment (OE) conditions that support all U.S. Army and joint training and leader development programs.

TRISA Handbooks:

Irregular U.S. Army TRADOC Forces Handbook No. 1.08
Insider Threat September 2012
FOUO AWG Subterranean Warfare Handbook
Irregular Forces Financing Handbook March 2012
Other Handbooks Produced by CTID (FOUO)

Operational Environment Products - Reports, handbooks, articles and assessments that describe Threat OE conditions, tactics, and techniques for training and exercise design.

Decisive Action Training Environment	OE Estimate
Threat Assessments	Operational Environment Assessments
OE Quick Guides	Terrorism Handbooks
Threats Terrorism Team Advisory	Combating Terrorism Poster
Red Diamond Newsletters	Threat Reports
Regionally Aligned Forces Training Environment (RAFTE) Africa	Regionally Aligned Forces Training Environment (RAFTE) North Korea
Regionally Aligned Forces Training Environment (RAFTE) Pacific	Handbooks
Threat Tactics Reports	

Threat Doctrine and Force Structure Page

Threat Tactics Course

DA Training Environment

OPFOR & Hybrid Threat Doctrine

Check this out too! 3

North Korean Leadership Turmoil

by H. David Pendleton, TRADOC G2 ACE-Threats Integration (CGI Ctr)

Who actually are the primary government leaders in North Korea? The secretive nature of the Democratic People's Republic of Korea (DPRK, also known as North Korea) and its reluctance to reveal information about its officials makes it is difficult to obtain background on the country's leadership. Additionally, a number of changes have occurred in the governmental and military leadership since Kim Jong Un took control of North Korea in 2011, including four different heads of the military. The latest changes were the February 2015 execution of General Pyon In Son for expressing an opinion different than that of Kim Jong Un and the removal of Ma Won Chun for alleged corruption. In all, Kim Jong Un ordered the execution of about 50 government officials and military officers in 2014. While a new head of state will inevitably make some changes upon the assumption of power, there has also been a series of shakeups on an irregular basis since Kim Jong Un assumed power upon the death of his father, Kim Jong Il, on 17 December 2011. This article will cover some of the major changes in the DPRK leadership since then and review the biographies of some major North Korean influencers.[1]

April 2012

Figure 1. KIM Jong Un

On 14 April 2012, four months after Kim Jong Il's death, Kim Jong Un was formally elected as the DPRK's supreme leader at the fifth session of the 12th Supreme People's Assembly (SPA). While some new leaders emerged at a meeting of the Korean Workers' Party (KWP) held prior to the SPA session, most of the leaders selected were a holdover from Kim Jong Il's regime. Of note, the KWP and SPA membership are often identical. The Presidium of the KWP Central Committee is the highest governmental power in the country and holds legislative power when the SPA is not in session, which is most of the year. The newly-elected Presidium included three holdovers: Kim Yong Nam and Choe Yong Rim from their appointments in September 2010 and Jang Song Taek—Kim Jong Un's uncle by marriage—from an appointment in November 2012. As the country's supreme leader, Kim Jong Un was appointed to the Presidium along with Vice Marshal Choe Ryong Hae at the April 2012 SPA. Eleven regular members of the KWP Central Committee remained as holdovers from the previous year with only three new members added at that time: Pak To Chun, Vice Marshal Hyon Chol Hae, and General Kim Won Hong. Of the twelve alternate (more secondary in power) Central Committee members, five were installed at this April 2012 event: Kwak Pom Gi, Jo Yon Jun, Ro Tu Chol, General O Kuk Ryol, and Colonel General Ri Pyong Sam. While there were new names added to all three bodies, the majority of the leaders maintained their positions due to past relationships with the former supreme leader, Kim Jong Il, as opposed to the current North Korean leader.[2]

April 2013

Now with over 15 months in power, Kim Jong Un began to put some distance between himself and those leaders who had supported his father. Kim Jong Un oversaw the installation of national leaders who owed their allegiance to him rather than Kim Jong Il. While the Presidium remained the same as the previous year, Kim Jong Un restructured the size of the Central Committee, reducing it from 19 members to 17. While the reduction would diminish Kim Jong Un's ability to express favor, it is not known whether the 10% cut was to instill fear, demonstrate the new leader's power, eliminate those he did not like, attempt to get the others to pay more attention, or resulted from the advice of others. What is known is that there was a slight de-emphasis on the military, as those members affiliated with the KWP or holding a civilian position in the government rose from 11 to 12 while those with a military or a security background dropped from eight to five. The number of alternate Central Committee members rose from 12 to 15, with an increase of one with primarily KWP/civilian experience and three with military/security backgrounds. With the exception of the Presidium, more Central Committee members and alternates still rose to their positions before the accession of Kim Jong Un than after his elevation to supreme leader. Those leaders in bold were still listed as holding a leadership position in the North Korean government as of September 2014. The number of changes—17 of 32 positions—indicates over a 50% change in Central Committee membership in less than a 18-month window since Kim Jong Un joined the Presidium in April 2013.[3]

Table 1. Central committee positions and membership

Korean Workers' Party Central Committee Membership: April 2013[4]		
NAME	**Position**	**First Appointed**
KIM Jong Un	**Presidium**	**April 2012**
KIM Yong Nam	**Presidium**	**September 2010**
CHOE Yong Rim	**Presidium**	**September 2010**
CHOE Tae Bok	**Member**	**September 2010**
YANG Hyong Sop	**Member**	**September 2010**
Vice Marshal RI Yong Mu	**Member**	**September 2010**
Colonel General PAK To Chun	**Member**	**April 2012**
General KIM Won Hong	**Member**	**April 2013**
PAK Pong Ju	**Member**	**April 2013**
KIM Yang Gon	**Alternate Member**	**September 2010**
THAE Jong Su	**Alternate Member**	**September 2010**
General O Kuk Ryol	**Alternate Member**	**April 2012**
RO Tu Chol	**Alternate Member**	**April 2012**
General HYON Yong Chol	**Alternate Member**	**April 2013**
Colonel General CHOE Pu Il	**Alternate Member**	**April 2013**
Vice Marshal CHOE Ryong Hae	Presidium	April 2012
JANG Song Taek	Presidium	November 2012
General KIM Kyong Hui	Member	September 2010
KIM Ki Nam	Member	September 2010
KIM Kuk Tae	Member	September 2010
KANG Sok Ju	Member	September 2010
Vice Marshal KIM Yong Chun	Member	September 2010
Vice Marshal Hyon Chol Hae	Member	April 2012
KIM Yong Il	Alternate Member	September 2010
KIM Pyong Hae	Alternate Member	September 2010
MUN Kyong Dok	Alternate Member	September 2010
JU Kyu Chang	Alternate Member	September 2010
Colonel General KIM Chang Sop	Alternate Member	September 2010
KWAK Pom Gi	Alternate Member	April 2012
JO Yon Jun	Alternate Member	April 2012
Colonel General RI Pyong Sam	Alternate Member	April 2012
General KIM Kyok Sik	Alternate Member	April 2013

November/December 2013

In December 2013, a competition for power between Kim Jong Un and his uncle, Jang Song Taek, came to a head and eventually concluded with the execution of the latter. Many analysts at the time considered Jang Song Taek as the second most powerful person in North Korea behind his nephew, and his appointment in November 2012 to the Presidium was a method Kim Jong Il planned to use as a means to provide support to the relatively young 30-something Kim Jong Un by his soon-to-be deceased father. Jang Song Taek had met Kim Kyong Hui, the younger sister of Kim Jong Il, while they were both students at Kim Jong Il University in the early 1970s. After their marriage, the family ties gave Jang Song Taek the connections to become an SPA member in 1986, a KWP Central Committee member in 1995, and First Vice-Director of the KWP Organization and Guidance Department in 1995.

In 2003, Jang Song Taek attempted to seize too much power and Kim Jong Il banished him from the government with no public appearances for three years. In 2006, Kim Jong Il reinstated Jang Song Taek, possibly to assist Kim Jong Un when the transition of power upon Kim Jong Il's death, and Jang Song Taek started to move up through the KWP ranks once again. In April 2009, Jang Song Taek received a promotion to the DPRK National Defense Commission and then was eventually assigned the responsibility of advisor to the young Kim Jong Un.[5]

In the fall of 2013, Kim Jong Un and Jang Song Taek both sought the profits from North Korea's most lucrative exports, namely clams, crabs, and coal. Kim Jong Un ordered North Korean military forces to take physical control of the fishing grounds and the coal mines from his uncle's associates. The uncle had the better-trained men and after several North Korean soldiers died, Kim Jong Un backed off from using further military force to seize the productive assets.

In retaliation, Kim Jong Un ordered guards to drag Jang Song Taek out of an SPA session in November 2013 and placed him under arrest. Kim Jong Un also had his uncle's two main lieutenants, Ri Ryong Ha and Chang Su Kil, arrested at approximately the same time and then immediately had the prisoners executed by firing squad using anti-aircraft machine guns.

On 12 December 2013, Jang Song Taek went to trial on a number of charges, many likely trumped up by the Kim Jong Un regime, primarily related to the mismanagement of his economic portfolio. After one day of testimony, the three-man tribunal found Jang Song Taek guilty, probably on Kim Jong Un's order, and the court carried out the sentence immediately—this time, however, with a normal firing squad instead of an anti-aircraft machine gun—in deference to his relationship to the ruling family. It is speculation on why Jang Song Taek could not have been banished again, but the verdict seemed to be a surprise to some Kim family members. During a heated phone conversation between Kim Jong Un and Kim Kyong Hui after the arrest of her husband, the 68-year old aunt of the current supreme leader suffered a severe stroke. Reports indicate that Kim Kyong Hui later died at a hospital even though the North Korean government has made no official announcement. The execution of Jang Song Taek eliminated Kim Jong Un's economic rival and possibly his only rival to wrest control of the DPRK from him at some future date.[6]

June 2014

The shakeups in the North Korean government did not end with the death of Kim Jong Un's uncle, but continued into the next year. In June 2014, Jane's Information Group published a study of the major influencers in the North Korean government. The ink was barely dry on the report before the information became obsolete. The diagram (figure 2, next page) portrays the structure as the Jane's analysts wrote their report in June 2014 and, less than three months later, the CIA's website showed an almost completely different organization. More than half of the individuals changed duty positions or were no longer active in the North Korean government leadership or military circles. During this reshuffling, Kim Jong Un remained firmly in control of power and the changes were not due to instability in the regime.[7]

Fall 2014

Kim Jong Un disappeared from public view for approximately six weeks with his last public appearance on 3 September 2014, before a photo of him supposedly on official state business was published by North Korean sources on 14 October 2014. Conjecture flooded the international media on Kim Jong Un's location and status as, during his absence, a high-level DPRK delegation flew to Seoul on short notice to hold negotiations with South Korean government officials.

Hwang Pyong So, who many external analysts consider the number two man in North Korea after Kim Jong Un, led the delegation to its southern neighbor. Also in the entourage to South Korea were Choe Ryong Hae and Kim Yang Gon. The former is a Vice Marshal and one of the five Presidium members. The latter served in the North Korean intelligence community, previously visited South Korea on another state visit in 2009, and is currently a KWP secretary.

One theory was that Kim Jong Un was demonstrating he was still in charge and everything was stable in the DPRK because he was comfortable with the unaccompanied, high level personnel visiting South Korea despite the internal shakeups in the North Korean leadership. The other theory of a possible coup proved unfounded as Kim Jong Un's seclusion was eliminated when DPRK sources released the news that the DPRK leader needed recovery time from foot surgery. Initially, the North Korean supreme leader walked with a cane, but by early November 2014, Kim Jong Un had recovered enough to walk without assistance and resumed making public appearances on a regular basis.[8]

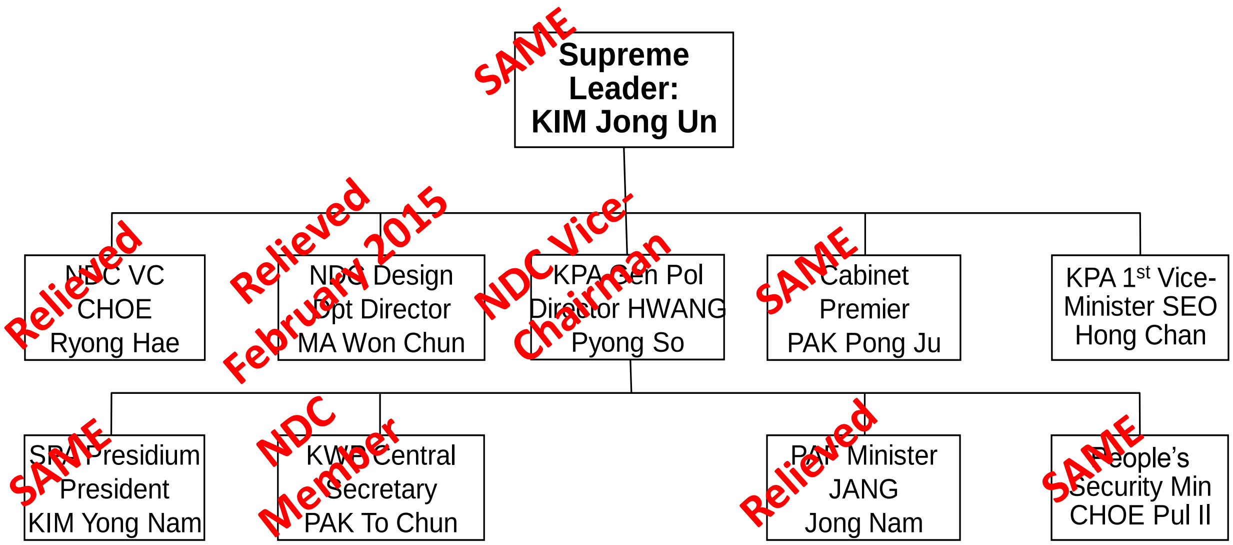

SAME
Supreme Leader: KIM Jong Un
Relieved
NDC VC CHOE Ryong Hae
Relieved February 2015
NDC Design Dpt Director MA Won Chun
NDC Vice-Chairman
KPA Gen Pol Director HWANG Pyong So
SAME
Cabinet Premier PAK Pong Ju
KPA 1st Vice-Minister SEO Hong Chan
SAME
SPA Presidium President KIM Yong Nam
NDC Member
KWP Central Secretary PAK To Chun
Relieved
PAF Minister JANG Jong Nam
SAME
People's Security Min CHOE Pul Il

Figure 2. North Korean senior leadership positions in turmoil (mid-2014 assessment)

Assumptions about no change in Kim Jong Un's status as the DPRK leader were premature. On 28 November 2014, North Korea announced that Kim Yo Jong, Kim Jong Un's younger sister, received a promotion to a department vice-director's position in the KWP Central Committee. Reports indicate that the DPRK supreme leader's younger sister is approximately 26 years old and was only first seen at the funeral of her father, Kim Jong Il, in 2011. Kim Yo Jong routinely joins her elder brother at public appearances and at one time managed Kim Jong Un's schedule as part of her work in the executive office.

In March 2014, the DPRK state media reported her as a senior official for the first time as she voted in her first SPA elections. Speculation on the appointment of such a youthful woman to such a powerful position is rampant. Some reports suggest that the appointment demonstrates that Kim Jong Un exercises so much power in North Korea that he can do anything he desires, while others speculate that the appointment demonstrates that her older brother is in dire need of allies and family associates in the government after the execution of his uncle the previous December and the subsequent disappearance and likely death of his aunt.

While the elimination of Kim Jong Un is unlikely because of the North Korean myth's dependence on the Kim family, the DPRK's political future could suffer continued challenges to regime legitimacy and authority, unlike anything that occurred during his father's and grandfather's reigns.[9]

Current Leadership

The most current information on the political and military leaders in North Korea is in the chart below. Selected individuals in *italics* are then profiled after the chart.[10]

Table 2. North Korean political, military, and cabinet senior leaders

North Korean Leaders[11]					
Political		**Military**		**Cabinet**	
Eternal President	KIM Il Sung (Deceased)	National Defense Committee (NDC) First Chairman	*KIM Jong Un*	Cabinet Premier	PAK Pong Ju
Korean Workers' Party (KWP) Eternal General Secretary	KIM Jong Il (Deceased)	Korean People's Army (KPA) Supreme Commander	*KIM Jong Un*	Cabinet Vice Premier	KIM Tok Hun
KWP First Secretary	*KIM Jong Un*	NDC Vice Chairman (KPA General Political Department Director)	*Vice Marshal HWANG Pyong So*	Cabinet Vice Premier	KIM Yong Jin
Supreme People's Assembly (SPA) Presidium Vice President	KIM Yong Dae	NDC Vice Chairman (Foreign Intelligence Director)	*General O Kuk Ryol*	Cabinet Vice Premier	RI Chol Man
SPA Presidium Vice President	YANG Hyong Sop	NDC Vice Chairman	*Vice Marshal RI Yong Mu*	Cabinet Vice Premier	RI Mu Yong
SPA Presidium Honorary Vice President	CHOE Yong Rim	NDC Member	*CHO Chun Ryong*	Cabinet Vice Premier	RO Tu Chol
SPA Presidium Honorary Vice President	KIM Yong Ju	People's Security Minister (NDC Member)	*General CHOE Pul Il*	Cabinet Secretariat Chief	KIM Yong Ho
SPA Presidium Secretary General	HONG Son Ok	People's Armed Forces Minister (NDC Member)	*General HYON Yong Chol*	Agriculture Minister	RI Chol Man
SPA Presidium Member	HYON Sang Ju	State Security Minister (NDC Member)	*General KIM Won Hong*	Atomic Energy & Industry Minister	RI Je Son
SPA Presidium Member	JON Kyong Nam	NDC Member (Munitions Industry Department Chairman)	*Colonel General PAK To Chun*	Chemical Industry Minister	RI Mu Yong
SPA Presidium Member	JON Yong Nam	NDC Member (Korean People's Air & Air Defense Forces Commander)	General RI Pyong Chol	Coal Industry Minister	MUN Myong Hak
SPA Presidium Member	KANG Myong Chol	People's Armed Forces Vice Minister	Lieutenant General KIM Su Gil	Commerce Minister	KIM Kyong Nam
SPA Presidium Member	KANG Su Rin	General Staff Department Chief	General RI Yong Gil	Construction & Building Materials Industries Minister	TONG Jong Ho
SPA Presidium Member	KIM Jong Sun	Operations Bureau Director	General PYON In Son: Executed Feb 2015	Crude Oil Industry Minister	PAE Hak
SPA Presidium Member	KIM Wan Su	Korean People's Navy Commander	General (Admiral) CHONG Myong To	Culture Minister	PAK Chun Nam
SPA Presidium Member	KIM Yang Gon	West Sea Fleet Commander	Rear Admiral HAN Sang Soon	Electric Power Industry Minister	KIM Man Su
SPA Presidium Member	RI Myong Gil	East Sea Fleet Commander	Rear Admiral	Electronics Industry Minister	KIM Jae Song

North Korean Leaders[11]

Political		Military		Cabinet	
			PARK Won Shik		
SPA Presidium Member	RYU Mi Yong	Strategic Rocket Force Commander	Lieutenant General KIM Rak Gyom	Finance Minister	CHOE Kwang Jin
SPA Presidium Member	THAE Jong Su	KPA General Political Department Deputy Director	Lieutenant General RYOM Chol Song	Fisheries Minister	RI Hyok
SPA Chairman	CHOE Thae Bok	Security Guard Commander	General YUN Jong Rin	Foodstuffs & Daily Necessities Industry Minister	JO Yong Chol
SPA Vice Chairman	AN Tong Chun	NDC Reconnaissance General Bureau Commander	Lieutenant General KIM Yong Chol	Foreign Affairs Minister	RI Su Yong
SPA Vice Chairman	RI Hye Jong			Foreign Trade Minister	RI Ryong Nam
				UN Representative	JA Song Nam

The current DPRK supreme leader was born on 8 January 1983, but DPRK officials may have falsified the year to make it coincide with a special anniversary year in North Korea's history. Kim Jong Un is most likely the second child fathered by Kim Jong Il with his common-law wife Ko Yong Hue. While not initially groomed to take over power, he was chosen after Kim Jong Il's other two sons failed to demonstrate the prerequisites for the highest DPRK leadership position. Between 1991 and 1994, Kim Jong Un traveled to the People's Republic of China, Japan, and Europe with family. From 1996 to 2001, he studied in Berne, Switzerland under an assumed name where he learned to speak German, French, and English. Upon his return to North Korea, he continued his education at Kim Il Song Military University with his military studies concentrating on artillery. In 2007, with his father's assistance, Kim Jong Un became active in the KWP leadership. He was rushed through a grooming process having received a promotion to KPA General in 2010, while at virtually the same time being elected to the KWP Central Committee and the Party Central Military Commission (CMC). On 17 December 2011, Kim Jong Un succeeded his father in the DPRK leadership. This KWP and SPA ratified his appointment in April 2012. Following a struggle with his uncle by marriage, Jang Song Taek, Kim Jong Un continues to put his personal mark on the North Korean leadership by favoring younger and more loyal supporters KWP, SPA, and the military in order to build a personal base of support.[12]

HWANG Pyong So

In May 2014, Hwang Pyong So became the second most powerful person in North Korea with his promotion to Vice Marshal—his second promotion in a month—and his assignment as a National Defense Committee (NDC) Vice Chairman. He came from the KWP Organization and Guidance Department (OGD), where he oversaw Kim Jong Un's physical and political protection, North Korea's military and defense industry, and the country's weapons of mass destruction (WMD) programs. It is likely that Hwang Pyong So played a major role in the downfall of Jang Song Taek and the previous NDC Vice Chairman, Choe Ryong Hae. Hwang Pyong So is said not to harbor any political ambitions, but will continue to promote Kim Jong Un's agenda as a military hardliner. This may be far from the truth as anyone associated with the senior leadership in North Korean must become a good politician to survive.[13]

Figure 3. HWANG Pyong So

O Kuk Ryol

Like Hwang Pyong So, O Kuk Ryol is also an NDC Vice Chairman and likely responsible for North Korean intelligence operations. He was born in 1931 and is the son or nephew of O Jung Hup, who fought the Japanese during World War II with Kim Il Sung, the DPRK founder. O Kuk Ryol grew up with Kim Jong Il and, despite the age difference, served as an advisor to Kim Il Sung. He also advised his childhood friend, Kim Jong Il, and now his friend's son, Kim Jong Un. O Kuk Ryol's son, O Se Won, grew up with Kim Jong Un and now also serves as an advisor to the DPRK supreme leader. O Kuk Ryol studied at the Mangyongdae Revolutionary School in Pyongyang and the Kim Il Sung University. He later studied air power and learned Russian at the Frunze Military Academy in the Soviet Union. North Korean pilots including O Kuk Ryol secretly trained Egyptian pilots in Cairo throughout the 1973 Arab-Israeli War. O and the other North Korean pilots flew combat air patrols to defend Egyptian airfields from Israeli attacks. After the fall of the Soviet Union in the early 1990s, O Kuk Ryol survived the purge of most of the North Korean officers who had trained in Russia and contaminated by a "decadent" lifestyle there. Still, he disappeared from public view in the 1990s, and speculation abounds on whether it was due to a disagreement with the North Korean leader or if O Kuk Ryol was performing some clandestine operation for the regime. There is some evidence that both he and his son, O Se Won, were both heavily involved in the counterfeiting of American dollars used by the DPRK to pay overseas debts. The counterfeiting operation may be a more likely scenario as he not only survived the elimination of Soviet-trained officers from the DPRK military, but continued to serve despite another one of his sons, O Se Uk, defecting to the United States in 2004. Most families of North Korean defectors suffer when their loved ones escape from North Korea. In this case, no negative consequences seem to have occurred. Despite his age of 83, however, it is likely that O Kuk Ryol will continue to serve for several more years as he is not the oldest current NDC member. Moreover, O provides a link to Kim Il Sung, whose style Kim Jong Un is known to emulate for legitimacy purposes.[14]

Figure 4. O Kuk Ryol

RI Yong Mu

At about the age of 90, Vice Marshal Ri Yong Mu is one of the oldest leaders in the DPRK government and an NDC Vice Chairman since 1998. He is the husband of one of Kim Jong Il's aunts. Ri Yong Mu became a Lieutenant General and KPA political commissar in 1964 and has served in the DPRK government almost continuously since that date. The only exception is a short period in the 1970s when Kim Jong Il forced him into exile, likely due to the influence of the latter's wife at the time, who attempted to get rid of those associated with one of Kim Jong Il's former wives. In the 1980s, Ri Yong Mu was rehabilitated by the regime and reentered civil service at about the same time that Jang Song Taek returned from his hiatus from government circles. With his advanced age and Kim Jong Un's zeal to restructure the upper levels of the DPRK government, it is possible that Ri Yong Mu will leave office in the not too distant future.[15]

Figure 5. RI Yong Mu

CHO Chun Ryong [No photo available]

One of the newest members of the NDC is Cho Chung Ryong, and not much is known about him other than he joined the NDC in April 2014. Speculation by the media makes his background likely either the Second Economic Commission Vice Chairman or the head of the North Korea Missiles Bureau. Cho Chun Ryong replaced Paek Se Bong, the Second Economic Commission Chief and at one time rumored son of the former leader, Kim Jong Il. Cho Chun Ryong ran for the SPA from the Kangdong No. 76 electoral district where the Second Economic Commission maintains its offices in Pyongyang.[16]

CHOE Pul Il

Born in 1944, General Choe Pul Il not only serves as the Minister of the People's Security, but as an NDC member. He also serves as an alternate member of the KWP Political Bureau, the Party CMC, the KWP Central Committee, and as an SPA delegate. From his portfolio of positions, it is easy to ascertain that the lines between politics and the military in North Korea are not easily distinguishable. After attending Kim Il Sung University, Choe Pul Il joined the Korean People's Navy in 1961 before moving into the KPA Sports and Physical Culture Guidance Committee. As a former basketball player, Choe Pul Il formed an elite DPRK team that practiced and played with Kim Jong Il's sons, Kim Jong Un and Kim Jong Chol. Choe Pul Il served as a brigade commander, army corps chief of staff, and a corps commander while working his way to the rank of Lieutenant General in 1995. He received his promotion to Colonel General in 2006 and became the KPA General Staff Vice Chief in 2009. In September 2010, just before the 3rd Party Conference and KWP Central Committee plenary meeting, Choe Pul Il became a full general and for a short time served as the KPA General Staff Operations Bureau Chief. In 2012, he lost one star for unknown reasons and reverted to the rank of Colonel General. Choe Pul Il took over as the People's Security Minister in February 2013 and was elected to the NDC two months later. In June 2013, he returned to four-star rank shortly before leading a delegation to Mongolia three months later. At the age of 70, Choe Pul Il is one of the younger generals on the NDC. With his position placing him in charge of internal security procedures, it is likely that Choe Pul Il will remain a major influence in the DPRK government for the foreseeable future.[17]

Figure 6. CHOE Pul Il

HYON Yong Chol

Hyon Yong Chol serves as the Minister of the People's Armed Forces, a position equivalent to the US Secretary of Defense. Born in 1949, he joined the military in 1966. As an army officer, Kyong Yong Chol served as a battalion commander, brigade commander, infantry training center chief of staff, Reconnaissance Bureau chief, the VIII Army Corps Commander (2006-2010), and KPA General Staff Vice Chief. In 2009, he began his political career as a deputy or delegate to the SPA. He received his promotion to general in September 2010, skipping the three-star rank completely, and promoted to vice marshal in July 2012 when Vice Marshal Ri Yong Ho was relieved as the KPA General Staff chief. Hyon Yong Chol later returned to the lower rank of general for unknown reasons before his election as a KWP Political Bureau alternate member in March 2013 and an SPA rostrum member the following month. In May 2013, he was removed as the Chief of the General Staff after only serving approximately ten months. With a reduction to the rank of colonel general, Hyon Yong Chol became the V Army Corps Commander. About a year later, in June 2014, he received his appointment as the Minister of the People's Armed Forces with an NDC position. Hyon Yong Chol is the fourth person to serve as the Minister of the People's Armed Forces since Kim Jong Un took power in December 2011. His up-and-down career demonstrates either the fickleness of North Korean leadership for several decades or the inability of the DPRK leadership to hold grudges. Hyon Yong Chol's ability to fall out of favor, receive a demotion, but then rebound to a more powerful position can be used to justify either interpretation. The promotions may be just as likely rewards for supporting the right regime members as they are for the demonstration of competence in one's duties.[18]

Figure 7. HYON Yong Chol

KIM Wong Hong

Born in 1945 and a member of the KPA since 1962, Kim Won Hong currently serves as the North Korean Minister of State Security, the KWP Political Bureau, the Party CMC, and the NDC. Since 2009, he has been a strong public supporter of Kim Jong Un and sat next to him during the 3rd Party Conference in September 2010. Kim Won Hong is one of the four senior KPA officials who prominently supported and assisted Kim Jong Un during the transition of power after the death of Kim Jong Il. He served from 2004 to 2010 as the head of the Military Security Command (MSC) that watches and investigates military officers and facilities. Other notable assignments included KPA

Figure 8. KIM Wong Hong

General Political Department Director, VII Army Corps Commander, and IX Army Corps Commander. Kim Wong Hong received his promotion to general in April 2009 and was appointed Minister of State Security in April 2012. As an early supporter of Kim Jong Un, Kim Won Hong should continue to hold an important role in the DPRK government.[19]

PAK To Chun

While he holds the title of colonel general, Pak To Chun has spent more time in the civilian sector than with the military. Besides his position in the NDC, he serves as the KWP Secretary with a portfolio of military and machine-building industries as well as a KWP Political Bureau member. A second-generation government leader, Pak To Chun first served as an SPA deputy in 1998. In the late 1990s, he served as the Chagang Province KWP Committee Secretary before his elevation in 2005 to the Chief KWP Secretary for the same province. In April 2011, Pak To Chun received election to the NDC and was given the perfunctory rank of general despite little actual active military service. He was heavily involved in the North Korean rocket program, where he supervised the failed launch of the Unha-2 rocket with its Kwangmyongong-3 satellite in 2012 and the second Unha-3 launch later that same year. Pak To Chun also supervised the technical preparations and oversaw operational management of North Korea's third experimental nuclear test in February 2012. Despite the setbacks that the North Koreans have encountered in their rocket program, Pak To Chun continues to maintain his influential position because North Korea has succeeded in launching a satellite. Pak To Chun often accompanied Kim Jong Il on tours of factories, and this public relationship with the previous North Korean leader seems to have carried over to his relationship with Kim Jong Un.[20]

Figure 9. PAK To Chun

Summary

There appears little doubt that Kim Jong Un is still in charge in North Korea. He has spent the past three years ridding himself of his rival and the most significant potential threat to his power, his uncle, while slowly changing the face of the DPRK government with the appointment of younger leaders. Still, many senior DPRK leaders cannot remain in their positions forever. Kim Jong Un's ultimate aim may be the establishment of his legitimacy as the DPRK leader rather than exerting raw power. The trend toward younger leaders who owe their allegiance to the current supreme leader and not Kim Jong Il will endure as Kim Jong Un continues to mold the DPRK leadership to execute his personal vision for North Korea.

Notes

[1] Kim Sam, "Kim Jong Un executes army general in latest purge of officials," Bloomberg News Via Stars and Stripes, 4 February 2015; BBC, "Timeline: North Korean attacks," 1 April 2013.

[2] Michael Madden, "Kim Jong Un's Pyongyang Shuffle," 38 North, 5 April 2013.

[3] Michael Madden, "Kim Jong Un's Pyongyang Shuffle," 38 North, 5 April 2013.

[4] Michael Madden, "Kim Jong Un's Pyongyang Shuffle," 38 North, 5 April 2013.

[5] North Korea Leadership Watch, "Jang Song Taek," 28 January 2011; Choe Sang-hun and David E. Sanger, "Korea Execution Is Tied to Clash Over Businesses," The New York Times, 23 December 2013; BBC, "Profile: Chang Song-thaek," 12 December 2013; BBC, "What does purge say about North Korea's stability," 12 December 2013; BBC, "What is known about North Korea's brutal purge?," 13 December 2013.

[6] Choe Sang-hun and David E. Sanger, "Korea Execution Is Tied to Clash Over Businesses," The New York Times, 23 December 2013; North Korea Leadership Watch, "Jang Song Taek Dies By Execution," 13 December 2013; Christof Lehmann, "North Korea's Execution of Jang Song Taek, Peace in the Korean Peninsula and National Sovereignty," NSNBC International, 13 December 2013; Chris Irvine, "Rare images show Kim Jong-un's uncle being dragged away,' The Telegraph, 9 December 2013; BBC, "Profile: Chang Song-thaek," 12 December 2013; BBC, "What does purge say about North Korea's stability," 12 December 2013; BBC, "What is known about North Korea's brutal purge?," 13 December 2013.

[7] Central Intelligence Agency, "Chiefs of State and Cabinet Members of Foreign Governments: Korea, North – NDE," 25 September 2014; Neil Ashdown, Nick Hansen, and Sean O'Connor, "Stability In North Korea? Assessing the impact of recent elections," June 2014.

[8] Hyung-Jin Kim and Foster Klug, "Top North Korea Officials Make Rare Visit to South Korea," Association Press (AP) Via The World Post, 6 October 2014; Dana Ford, "North Korea says leader has reappeared," CNN, 15 October 2014; Choe Sang-Hun, "North Korea Chief Walks Minus Cane," The New York Times, 5 November 2014.

[9] Scott Smith, "Kim Jong Un's little sister named to top leadership post in North Korea," UPI, 28 November 2014; North Korea Leadership Watch, "Kim Yo Jong," 10 March 2014.

[10] Koreans put their family name before their given name and last names are depicted in all capital letters.

[11] Jane's Sentinel Security Assessment, "Korea, North > Armed Forces," 2 July 2014; Jane's Sentinel Security Assessment, "Korea, North > Army," 1 September 2014; Jane's Sentinel Security Assessment, "Korea, North > Air Force," 1 September 2014; Jane's Sentinel Security Assessment, "Korea, North > Navy," 1 September 2014; Central Intelligence Agency, "Chiefs of State and Cabinet Members of Foreign Governments: Korea, North – NDE," 25 September 2014.

[12] BBC, "Profile: Kim Jong-un," 14 October 2014; North Korea Leadership Watch, "Kim Jong Un," Undated; North Korea Leadership Watch, "Jang Song Taek," 28 January 2011; Choe Sang-hun and David E. Sanger, "Korea Execution Is Tied to Clash Over Businesses," The New York Times, 23 December 2013; BBC, "Profile: Chang Song-thaek," 12 December 2013; BBC, "What does purge say about North Korea's stability," 12 December 2013; BBC, "What is known about North Korea's brutal purge?," 13 December 2013.

[13] Martin Sieff, "Hardliner Hwang Pyong-so is North Korea's second in command," Asia Pacific Defense Forum, 28 May 2014; James Pearson and Jack Kim, "North Korea Official Hwang Pyong So Rises Ranks Amid Speculation Over Kim," The World Post, 14 October 2014.

[14] Elites et economie de la Coree du Nord, "O Kuk Ryol: The Old Guard Never Dies," 11 April 2013; Hot Air, "O Kuk-ryol: The Power Behind the Throne," 3 June 2009.

[15] North Korea Leadership Watch, "VMAR Ri Yong Mu," Undated; North Korea Leadership Watch, "Ri Yong Mu," Undated.

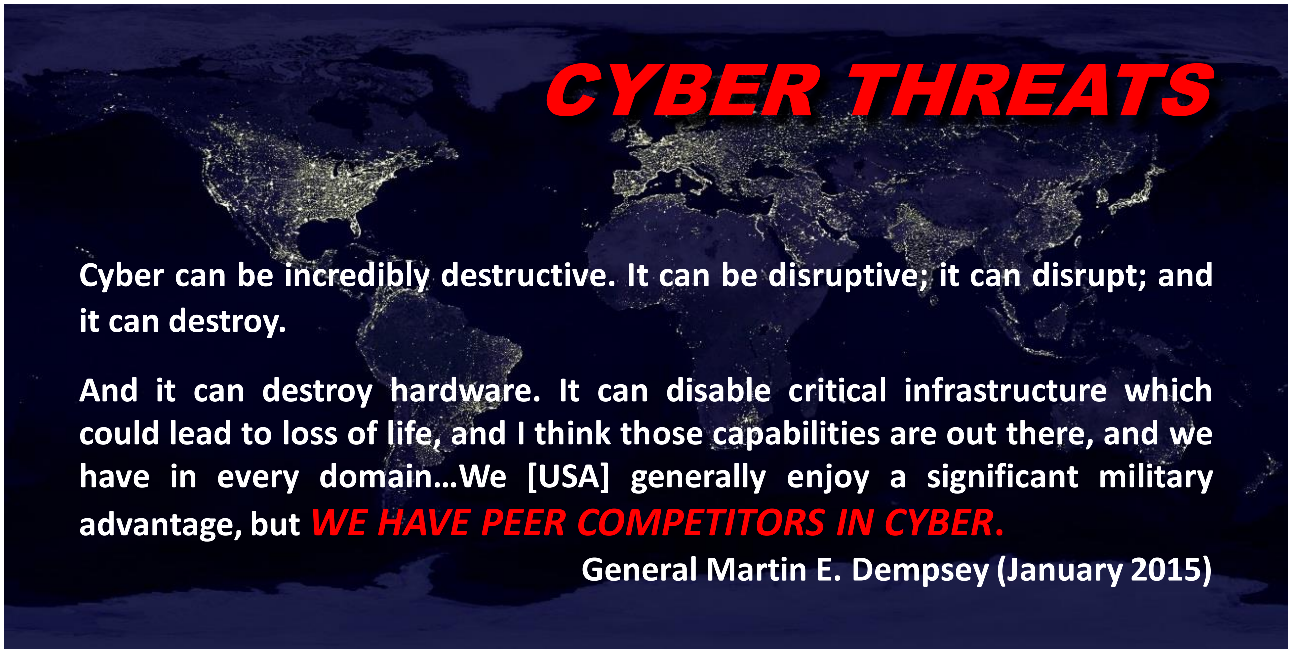
[16] Fortuna's Corner, "The New Face In the North Korean Regime," 11 April 2014.

[17] North Korea Leadership Watch, "Gen. Choe Pul Il," 27 September 2013.

[18] Brian Kim, "Impact Players: Hyon Yong Chol," Center For Strategic & International Studies (CSIS), Undated; The World Post, "Hyon Yong Chol Named North Korea's New Military Chief," 16 July 2012; North Korea Leadership Watch, "Gen. Hyon Yong Chol," 25 June 2014.

[19] North Korea Leadership Watch, "Gen. Kim Won Hong," 12 April 2012.

[20] North Korea Leadership Watch, "Pak To Chun [Pak To-ch'un]," 14 August 2013.

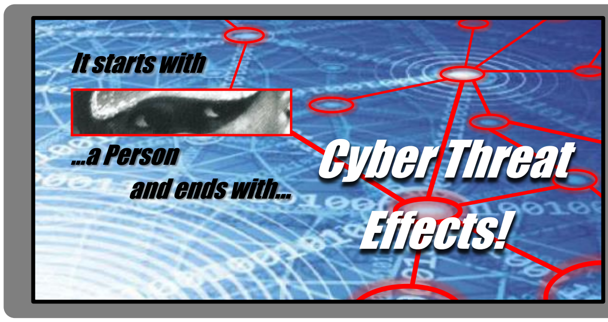


CYBER THREATS

Cyber can be incredibly destructive. It can be disruptive; it can disrupt; and it can destroy.

And it can destroy hardware. It can disable critical infrastructure which could lead to loss of life, and I think those capabilities are out there, and we have in every domain…We [USA] generally enjoy a significant military advantage, but WE HAVE PEER COMPETITORS IN CYBER.

General Martin E. Dempsey (January 2015)



ANTITERRORISM AWARENESS IN FIELD UNITS—TERRORISM *T3 ADVISORY*

by TRADOC G2 ACE-Threats Integration, Operations

U.S. Army Training and Doctrine Command G2

Operational Environment Enterprise

TRADOC G2 Intelligence S

Complex Operational E

Threat Integratio

Terrorism T3 Advisory

Survive an Active Shoot! –

1 Evacuate 2 Hide 3 Take Action

What to do whe

ACTIVE SH

Law Enforcement

When Law Enforc

Follow In

Dro

Rais

Do N

See Defense Security Service

http://www.cdse.edu/s

See Related Threats Trai

Front Page = CLICKs

ATN

JAN 2015 No. 4-15

U.S. Army Training and Doctrine Command G2

Operational Environment Enterprise

TRADOC G2 Intelligence Supp

Complex Operational Environ

Threat Integration Dir

Terrorism T3 Advisory

Antiterrorism Awareness

1 Police 2 Prevent 3 Protect 4 Preserve 5 and Safeguard

What to do when c

Identif

Lea

Police training support in

See Related Threats Training M

Front Page = CLICKs

ATN

FEB 2015 No. 5-15

U.S. Army Training and Doctrine Command G2

Operational Environment Enterprise

TRADOC G2 Analytical and Control Element

ACE-Threats Integration

TRADOC G-2

Terrorism T3 Advisory

Situational Understanding in Field Units

1 Prepare 2 Plan 3 Practice 4 Perform 5 and Safeguard

Identify the Threats

Apply ROE

Lead with Action

TC 7-100.3

Irregular Opposing Forces

Antiterrorism Awareness in Field Units

See Related Threats Training Materials at https://atn.army.mil

① "Training for Operations"

② "CTID Operational Environment Page"

③ "Terrorism Handbooks"

Front Page = CLICKs

ATN

MAR 2015 No. 6-15

JAN-FEB-MAR 2015 Antiterrorism Theme Support: *T3 Advisory*

The TRADOC G2, ACE-Threats Integration, publishes a monthly ***Threats Terrorism Team (T3) Advisory*** to promote antiterrorism themes announced by the Antiterrorism (AT) Branch of the Army's Office of the Provost Marshal General (OPMG). These advisories are in support of the *Army Antiterrorism Strategic Plan, Phase III 2013-2016* (2013) and it's January 2015 Amendment and Responsibilities.

TRADOC G2 Handbook No. 1.07 C3

A Soldier's Primer to

Terrorism TTP

Tactics, Techniques, and Procedures in

Complex Operational Environments

TRADOC G2 Intelligence Support Activity (TRISA)

Fort Leavenworth, Kansas

August 2012

As part of several topic areas for training awareness such as antiterrorism doctrine, pre-deployment vulnerability assessments, specific training requirements for in-transit forces deploying to or redeploying from an area of responsibility (AOR), and resources from the Army Threat Integration Center (ARTIC), the OPMG AT Branch also spotlights the use of Threats and Opposing Force (OPFOR) products such as HQDA TC 7-100, Hybrid Threat, and TC 7-100.2, Opposing Force Tactics.

Other resources include TC 7-100.3, *Irregular Opposing Forces*, and TRADOC G2 Handbook 1.07 C3, *A Soldier's Primer to Terrorism TTP,* as a hip-pocket resource (5" x 7") for Soldiers and tactical unit leaders.

Comparison of OPFOR and Syrian Reconnaissance Techniques

by Jerry England, TRADOC G2 ACE-Threats Integration (DAC)

To the threat, the single most important component of military action is reconnaissance.[1] Reconnaissance is part of the threat military function called RISTA [reconnaissance, intelligence, surveillance, and target acquisition]. The Syrian army is adapting the way its military operates because of an ongoing conflict between the forces of Syrian President Bashar al Asad and Sunni rebels. This article will discuss how the Syrian military has changed its reconnaissance techniques, from a regional focus to an internal one by highlighting those reconnaissance assets most in demand for conducting counterinsurgency operations.

The RISTA units use specialized assets to complete their reconnaissance mission. At times, the threat goes beyond using only RISTA units for reconnaissance. The threat will employ a variety of hybrid threat actors to perform the reconnaissance function, including aerial units, regular and irregular forces, and INFOWAR activities to perform reconnaissance operations, including:

- Ground Reconnaissance
- Reconnaissance by Fire
- Aerial Reconnaissance

The reconnaissance techniques used for the hybrid threat are based on a composite model that includes techniques and forces observed in past and current operational environments (OE). This modeling allows exercise designers the flexibility to create formations with a wide range of capabilities able to match many different levels of proficiency across the spectrum of warfighting functions.

The emphasis among the Syrian army reconnaissance assets is changing as a result of ongoing combat operations. The civil war forced the Syrian army to focus on the internal threat and accept risk on maintaining situational awareness on external threats from Israel. This has led to some atrophy of security and surveillance systems that are designed to stop an air attack from the Western powers. The heavy investment in air defense and early warning systems has been redirected, at least temporarily, to the acquisition of systems such as UAVS and long range optics designed to win the ground war against these rebel groups. The situation has caused the Syrian regime to seek assistance from its allies and their proxies to locate and destroy an enemy that is familiar with the government forces' tactics, techniques, and procedures (TTP).

Ground Reconnaissance

The Syrian army is mainly a heavy ground force and is not suited for urban combat. Conducting population and resource control operations from an armored vehicle is difficult and sends the wrong message when the intent is to influence the population to reject rebel narratives and accept government authority. Syrian forces attacked population centers using anti-aircraft guns and tanks to destroy suspected enemy positions with little regard for the civilians in the area. This type of heavy handedness isolated populations and increased their resolve to fight against Syrian regular forces. Additionally, heavy weapons lacked the maneuverability to pursue lightly armed insurgents in an urban battlefield. Hezbollah provided experienced fighters with recent combat experience against Israel to assist the Syrian army in areas where they were lacking the ground forces necessary to root out rebels in complex battle positions and safe havens throughout the cities of Syria. This included reconnaissance, snipers, and light infantry to augment Syrian heavy forces.

All Syrian maneuver units have the ability to execute a reconnaissance mission to support the overall objective. The reconnaissance force could include a mix of elements from any of the regular divisional or independent infantry and armored brigades, the border guard brigade, or Special Forces regiments.[2] Tactical units may also send out independent reconnaissance patrols (IRPs) to perform ground reconnaissance. The size of such patrols can vary, but in today's fight, the Syrian army usually opts for a reconnaissance or combat arms platoon often augmented with Hezbollah or other irregular light infantry and engineers.

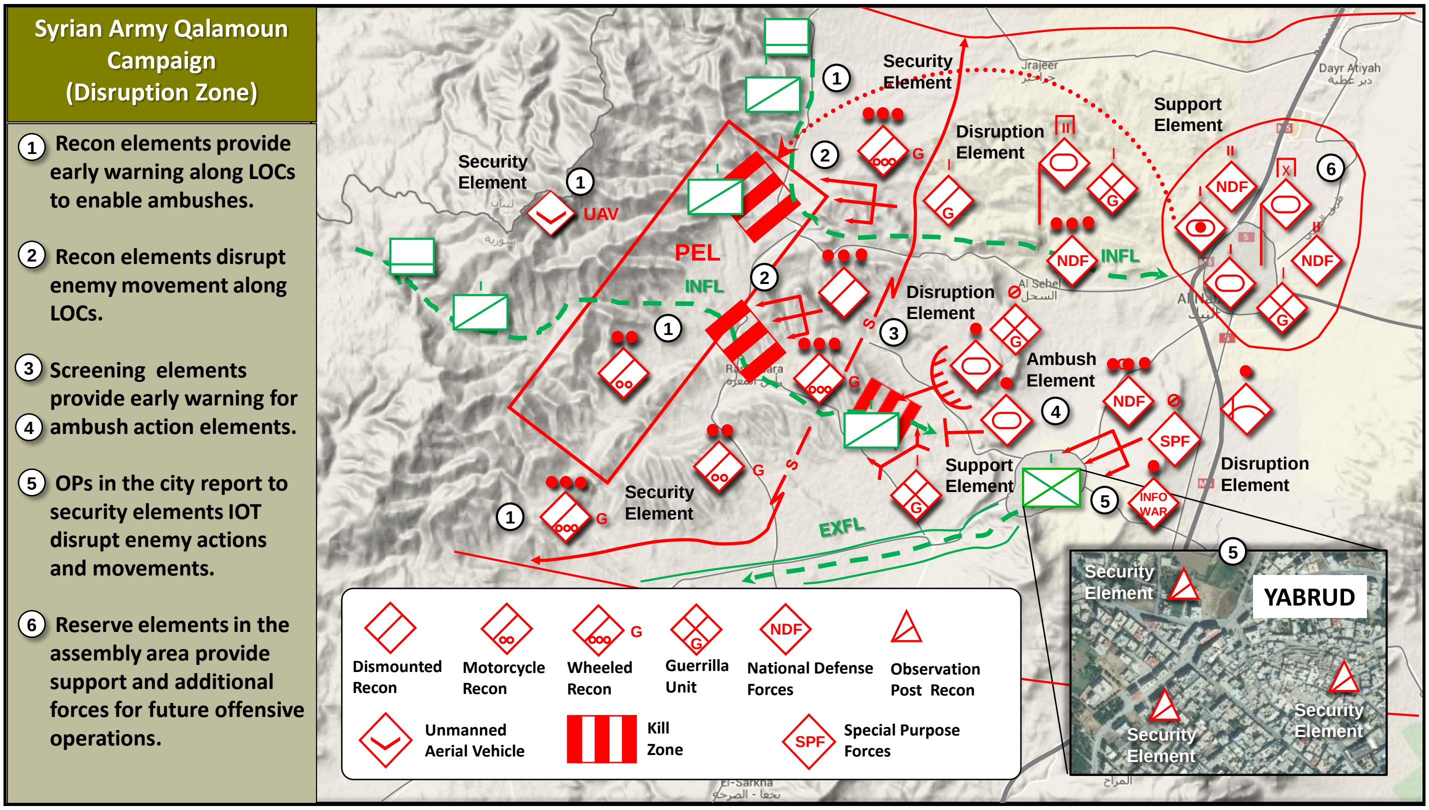
The Syrian Special Forces (SF), may form additional IRPs, or their personnel and vehicles can supplement patrols formed by the other reconnaissance or combined arms units. Many SF personnel are specially trained for insertion in small reconnaissance teams forward of the battle line. In the early days of the current Syrian conflict, Syrian SF patrols located and eliminated opposition leaders suspected of radicalism within contested areas. Before the civil unrest began, however, the Syrian SF units supported border security operations and guarded sensitive defense facilities throughout the country.[3] While many SF units provided intelligence and information on external threats to Syria, some SF units were not prepared to conduct counterinsurgency operations against their own populations. This led to a number of defections not just among the ranks of the Special Forces in the regular forces as well. Most of the SF were considered among the most loyal of the Syrian armed forces and President Assad allocated the best weapons to them as well as support from the Syrian security apparatus. Reconnaissance forces geared for border security such as the 14th Special Forces Division received the mission of canalizing attacking forces into conventional forces' engagement zones.[4]

Irregular Support to Syrian Operations

Ground reconnaissance in Syria is not only conducted by regular forces and the SF, it includes a large and growing number of irregular forces and fighters from Hezbollah, and technical advisors from Syrian allies Iran and Russia. Additionally, militia fighters from the National Defense Force (NDF), which is composed of regime loyalists trained by the Syrian army and or its proxies, joined the ranks of the government forces and provided a wide range of security support including reconnaissance. For example, intelligence gathered by loyalist volunteers for the Syrian regime targeted radicalized individuals throughout the country. Reconnaissance operations along the Syrian and Lebanese border conducted by the guerrilla forces of Hezbollah shaped the battle for al Qusayr in 2013 and were refined for other battle zones from Qalamoun to Damascus. These forces were not only able to disrupt rebel troops and supplies as they moved into Syria, but also acted as forward observers for missile attacks on rebel strongholds inside the town and surrounding villages. Their safe havens in the Lebanese border areas provided sanctuary while conducting surveillance on rebel lines of communications.

Throughout Syria, Hezbollah forces deployed sizeable formations of troops in an effort to fill in the gaps for Syria's regular military. As many as 1,700 troops were deployed to retake al Qusayr in support of the Syrian army. These units operated in small 2 to 5-man teams to conduct surveillance on rebel positions and provide support to the Syrian army. Syrian commanders assigned designated sectors within the area of operations. The Hezbollah fighters methodically cleared booby traps and tunnels on their objectives and cleared the path for regular Syrian army units.[5] Additionally, reconnaissance units acted as forward observers and were instrumental in calling in airstrikes and artillery.[6] Command and control was enhanced by using a system of code words for each of the city sectors in order to provide interoperability between Hezbollah and Syrian Regime Forces.[7]

These techniques were refined as the Syrian regime maintained a disruption zone in the Anti-Lebanon Mountains of the Qalamoun province, south of al Qusayr. There Hezbollah fighters also used Iranian unmanned aerial vehicles (UAVs) and enhanced optics to locate and engage rebel fighters traversing the border area between Sunni support zones in the Lebanese Bekaa valley and the village of Yabrud in Syria.[8] In addition to the disruption efforts in the hills and villages, Hezbollah forces also conducted reconnaissance operations within the population centers to locate suspected improvised explosive devices (IEDs) destined for Hezbollah strongholds in Lebanon. See figure 1.



Syrian Army Qalamoun Campaign (Disruption Zone)

1 Recon elements provide early warning along LOCs to enable ambushes.

2 Recon elements disrupt enemy movement along LOCs.

3 Screening elements provide early warning for

4 ambush action elements.

5 OPs in the city report to security elements IOT disrupt enemy actions and movements.

6 Reserve elements in the assembly area provide support and additional forces for future offensive operations.

Figure 1. Reconnaissance and disruption actions in a disruption zone (example)

Reconnaissance by Fire

Reconnaissance by fire is a method of reconnaissance in which fire is placed on a suspected enemy position to cause the enemy to disclose his presence by movement or return fire. This technique is used to provoke a reaction from the other side. The threat also uses a similar tactic in which individuals may brandish weapons or purposely draw suspicion, in order to learn more about their enemy's rules of engagement. The Syrian regime is known to use artillery and armor to attack rebel positions before ground troops move in to clear and hold contested areas.[9] This technique is designed to preserve ground troops and mass firepower on suspected enemy locations.

At the platoon and squad level, reconnaissance by fire may also be called cover or drake shooting. This is a technique employed to quickly reveal and kill concealed enemy riflemen. Using two- to three-round bursts, the threat riflemen deliberately aim and fire low on the ground immediately to the front of the cover, raking it with fire from the one flank to the other. Ricochets, fragments, earth, rocks, and wood either injure the hidden enemy soldiers and/or force them to react. Additionally, snipers engage enemy observers as a counterreconnaissance technique. Snipers also have the ability to gauge the enemy response contact which exposes battle positions and support zones when targets attempt to evacuate wounded.

Aerial Reconnaissance

Aerial reconnaissance includes visual observation, imagery, and signals reconnaissance from airborne platforms. These platforms may be either piloted aircraft or UAVs. Syrian forces are known to use UAVs to provide intelligence on enemy locations and to assist in locating targets for artillery and air strikes.[10] Additionally, Hezbollah forces used UAVs to patrol potential enemy mortar point of origin sites aimed at security outposts. The use of UAVs provides situational awareness and preserves combat power that can otherwise be used for decisive operations. Iran supported the Syrian regime by providing a wide array of UAV technology. Relatively advance platforms such as the Shahed-129, with a possible range of 200 km and an endurance of 24 hours appear in insurgent videos.[11]

Syrian Strategic Reconnaissance Assets

The Syrian military originally organized itself for defense against Israel. Syria prepared to defend its airspace against an Israeli aerial attack. As such, the most significant investments in the years leading up to Syria's current conflict were in air defense assets. An insurgent video of a captured Syrian SIGINT site shows how the Syrian regime supported its allies by providing access to its SIGINT capabilities in exchange for military technology.[12] Many of these assets degraded as the priority in Syria has shifted to the current conflict which is primarily a ground-based counterinsurgency.

The reconnaissance elements of Syria were reorganized for the current civil war and now target rebel fighters. Hezbollah a key ally is assisting the Syrian army by providing units of combat veterans and training the national defense forces. The Syrian military shifted, to some extent, away from the defense of its borders with Israel and has moved SF recon assets to support the counter insurgency effort inside the country. Syria acquired a number of UAVs, believed to be from Iran, which provide reconnaissance support throughout the country. The UAVs provide tactical units the ability to maintain situational awareness around military bases and security outposts. The UAVs also provide support for targeting and battle damage assessments. Rebel videos posted on the Internet show the wreckage of a number of UAVs including the Iranian Mohajer and Yasir.[13] The list below is not an exhaustive account of all the available reconnaissance assets used in Syria but gives an idea of what is prominent in the current conflict. Of note are the technical capabilities allocated to both Syrian army as well as Hezbollah. See table 1.

Table 1. Syrian army and Hezbollah reconnaissance assets comparison (sample)

Syrian Reconnaissance[14]					
Ground		**Aerial[15]**		**Cyber**	
Thermal Night Viewer Sadad 201 T	UNK	SU-22	50	Internet Surveillance Suite	
BMP / BTR[16]	200	SU-24	20		
BRDM	50	MIG-21	179		
PT-76	UNK	MIG-23	146		
		MIG-25	38		
		MIG-29	40		
		Shahed 129 UAV (MALE)	UNK		
		Ghods Mohajer UAV (Tactical)	UNK		
		Ababil-3 UAV (Tactical)	UNK		
		Yasir UAV (Mini)	UNK		

Hezbollah Reconnaissance				
Ground[17]		**Aerial**		**Cyber**
Thermal Night Viewer Iranian IRLRSP	UNK	Ghods Mohajer UAV (Tactical)	UNK	
Improvised Tactical Vehicles (Technical)	UNK	Ababil-3 UAV (Tactical)	UNK	
Noncombatants	UNK	DJI Phantom Commercial of the Shelf (COTS) UAV (hand Launched)	UNK	
		Yasir UAV (mini)	UNK	

As a proxy of Iran, Hezbollah forces may possess RISTA capabilities that equal those of the regular Syrian army. Due to the expeditionary nature of Hezbollah forces, however, those technologies that require extensive logistical support are controlled by Syrian and Iranian government forces along with technical advisors. Militia forces such as the National Defense Forces would probably have the same capabilities associated with lower tier forces. This is due to the level of trust the Syrian government and its supporters put in the NDF and its ability to conduct complex operations.

A list of comparable assets available in the Threat Force Structure is provided to allow exercise designers to build an OPFOR that would closely resemble the capabilities of the Syrian regime. The hybrid threat has traditionally used tier 3 and 4 systems to outfit guerrilla forces for training purposes. In light of the current conflict in Syria, however, it is conceivable that advanced systems (tier 1- and 2) are fielded to these forces as they support regular forces for a particular exercise. See table 2.

Table 2. Opposing force reconnaissance assets for training (sample)

Threat Force Structure (BTG)[18]				
Ground[19]		**Aerial[20]**		**Cyber**
Thermal Night Viewer DHY-307	323	SU-24	50	
Ground Surveillance Radar Fara-1	128	Hermes 450 UAV (MALE)	20	
Tactical Utility Vehicle	40	ASN-105 UAV Low Altitude)	179	
BMP-2M	129	Fox AT-2 UAV (Tactical)	146	
		Skylite-A UAV (manportable)	38	
		Zala 421 UAV (Hand Launched)	40	

INFOWAR as a Reconnaissance Enabler

INFOWAR operations enable the reconnaissance mission. INFOWAR elements—including electronic warfare, computer warfare, and information attack—represent the exploitation of information and information infrastructure for the purpose of achieving an advantage that affects the enemy's decision making while retaining the ability to employ friendly information-based systems.[21] Given today's advancements in information and communications technology (ICT), the importance of INFOWAR activities for threat operations is growing in scope, impact, and sophistication. Computer warfare assets such as computer worms, sniffers, and advanced persistent threats designed to collect information on high-value and high-priority targets. They enhance the reconnaissance effort as they offer a high informational payoff for a comparatively low risk to personnel and assets.

Threat organizations that are a part of a reconnaissance function recognize the importance of ICT to the extent that they integrate telecommunications infrastructure into the reconnaissance plan. INFOWAR assets can assist in this process by infiltrating computer-based social networks such as blogs and forums to gain more information on the level of interconnectivity between adversarial groups. Syria has actively pursued software packages designed to censor and monitor Internet traffic. The package includes tools that enable intelligence agencies to monitor targets on the Internet, traffic to opposition websites, and to shut down these sites when appropriate.[22] The Syrian regime implemented strict censorship policies in order to control the information environment.

Implications

The hybrid threat uses a variety of organizations to conduct reconnaissance operations including non-state actors and non-combatants. The presence of these actors on the battlefield will make it difficult to distinguish between friends or foes. Also, the increased use of UAVs to provide early warning and targeting support reflects the ubiquitous nature of UAV technology throughout an OE. Cover, concealment, camouflage, and deception is required for forces faced with a large UAV presence. Information operations will be disrupted by sophisticated censorship and monitoring of Internet traffic by threat actors who procure or develop the capability. Traditional notions of threat capabilities as it relates to regular and irregular forces may need to be reevaluated as irregular forces are allotted more advanced technology than their regular counterparts.

Sources

Al Jazeera English. "Al-Qaeda says it shot down Syria drone." YouTube. December 2013.

The Arkenstone. Iranian Battlefield Surveillance. August 2010.

Headquarters, Department of the Army. Training Circular 7-100.2. Opposing Force Tactics. TRADOC G-2 Intelligence Support Activity (TRISA)-Threats. Complex Operational Environment and Threat Integration Directorate (CTID). 9 December 2011.

US Army, TRADOC G-2 Intelligence Support Activity (TRISA)-Threats. Complex Operational Environment and Threat Integration Directorate (CTID). Worldwide Equipment Guide – Volume 1: Ground Systems. August 2014.

US Army, TRADOC G-2 Intelligence Support Activity (TRISA)-Threats. Complex Operational Environment and Threat Integration Directorate (CTID). Worldwide Equipment Guide – Volume 2: Airspace and Air Defense Systems. August 2014.

Bennet, Richard. "The Syrian Military: A Primer." Middle East Intelligence Bulletin. September 2001.

Binnie, Jeremy. "New UAV spotted over Damascus". Jane's. April 2013.

Blanford, Nicholas. "Hezbollah marks major triumph as Qusayr tips back into Assad camp." Christian Science Monitor. June 2013.

Blanford, Nicholas. "The Battle for Qusayr: How the Syrian Regime and Hizb Allah Tipped the Balance." CTC Sentinel. August 2013.

Holliday, Joseph. "The Assad Regime From Counterinsurgency to Civil War." Middle East Report 8. Institute for the Study of War. 2013.

Holliday, Joseph. "The Syrian Army Doctrinal Order of Battle." Institute for the Study of War. February 2013.

Rogin, Josh and Eli Lake. "Syrian Rebels Seize Russian Spy Station Near Israeli Border." The Daily Beast. October 2014.

Sullivan, Marissa. "Middle East Security Report 19. "Hezbollah in Syria." Institute for the Study of War. 2014.

World Tribune. "Assad using drones from Iran. Russia against Syrian rebels." June 2013.

YouTube. "Syrian freedom fighters display a downed Ghods Mohajer UAV Damascus Governate." Posted June 2013.

Notes

[1] Headquarters, Department of the Army, Training Circular 7-100.2, Opposing Force Tactics, TRADOC G-2 Intelligence Support Activity (TRISA)-Threats, Complex Operational Environment and Threat Integration Directorate (CTID), 9 December 2011.

[2] Richard Bennet, "The Syrian Military: A Primer," Middle East Intelligence Bulletin, September 2001.

[3] Richard Bennet, "The Syrian Military: A Primer," Middle East Intelligence Bulletin, September 2001.

[4] Joseph Holliday, "The Assad regime From Counterinsurgency to Civil War," Middle East Report 8, Institute for the Study of War, 2013.

[5] Nicholas Blanford, "Hezbollah marks major triumph as Qusayr tips back into Assad camp," Christian Science Monitor, June 2013.

[6] Marisa Sullivan, "Middle East Security Report 19, "Hezbollah in Syria," Institute for the Study of War, 2014.

[7] Nicholas Blanford, "The Battle for Qusayr: How the Syrian Regime and Hizb Allah Tipped the Balance," CTC Sentinel, August 2013.

[8] Nicholas Branford, "Hezbollah close to cutting off key route for Syrian rebels, refugee," Christian Science Monitor, March 2014.

[9] Joseph Holliday, "The Assad regime From Counterinsurgency to Civil War," Middle East Report 8, Institute for the Study of War, 2013.

[10] World Tribune, "Assad using drones from Iran, Russia against Syrian rebels," June 2013.

[11] Jeremy Binnie, "New UAV spotted over Damascus", Jane's, April 2013.

[12] Josh Rogin, Eli Lake, "Syrian Rebels Seize Russian Spy Station Near Israeli Border," The Daily Beast, October 2014.

[13] YouTube, "Syrian freedom fighters display a downed Ghods Mohajer UAV Damascus Governate," Posted June 2013; Al Jazeera English, "Al-Qaeda says it shot down Syria drone," YouTube, December 2013.

[14] Joseph Holliday, "The Assad regime From Counterinsurgency to Civil War," Middle East Report 8, Institute for the Study of War, 2013.

[15] Richard Bennet, "The Syrian Military: A Primer," Middle East Intelligence Bulletin, September 2001

[16] Richard Bennet, "The Syrian Military: A Primer," Middle East Intelligence Bulletin, September 2001.

[17] Joseph Holliday, "The Assad regime From Counterinsurgency to Civil War," Middle East Report 8, Institute for the Study of War, 2013.

[18] Headquarters, Department of the Army. Field Manual 7-100.4, Opposing Force Organization Guide. TRADOC G-2 Intelligence Support Activity (TRISA)-Threats, Complex Operational Environment and Threat Integration Directorate (CTID). May 2007.

[19] US Army, TRADOC G-2 Intelligence Support Activity (TRISA)-Threats, Complex Operational Environment and Threat Integration Directorate (CTID). Worldwide Equipment Guide – Volume 1: Ground Systems. August 2014.

[20] US Army, TRADOC G-2 Intelligence Support Activity (TRISA)-Threats, Complex Operational Environment and Threat Integration Directorate (CTID). Worldwide Equipment Guide – Volume 2: Airspace and Air Defense Systems. August 2014.

[21] Headquarters, Department of the Army. Training Circular 7-100.2, Opposing Force Tactics. TRADOC G-2 Intelligence Support Activity (TRISA)-Threats, Complex Operational Environment and Threat Integration Directorate (CTID). 9 December 2011.

[22] Jennifer Valentino-Devries, Paul Sonne, Nour Malas, "US Firm Acknowledges Syria Uses Its Gear to Block Web," Wall Street Journal, October 2011; Bloomberg News, "Syria Crackdown Gets Firm's Aid With US Spy Gear," November 2011.

What ACE-Threats Integration Supports for YOUR Readiness

- Determine Operational Environment (OE) conditions for Army training, education, and leader development.
- Design, document, and integrate hybrid threat opposing forces (OPFOR) doctrine for near-term/midterm OEs.
- Develop and update threat methods, tactics, and techniques in HQDA Training Circular (TC) 7-100 series.
- Design and update Army exercise design methods-learning model in TC 7-101/7-102.
- Develop and update the US Army *Decisive Action Training Environment (DATE)*.
- Develop and update the US Army *Regionally Aligned Forces Training Environment (RAFTE)* products.
- Conduct Threat Tactics Course resident at Fort Leavenworth, KS.
- Conduct Threat Tactics mobile training team (MTT) at units and activities.
- Support terrorism-antiterrorism awareness in threat models and OEs.
- Research, author, and publish OE and threat related classified/unclassified documents for Army operational and institutional domains.
- Support Combat Training Centers (CTCs) and Home Station Training (HST) and OE Master Plan reviews and updates.
- Support TRADOC G-2 threat and OE accreditation program for Army Centers of Excellence (CoEs), schools, and collective training at sites for Army/USAR/ARNG.
- Respond to requests for information (RFIs) on threat and OE issues.

ACE-Threats Integration POCs

DIR, ACE-Threats Integration	Jon Cleaves	jon.s.cleaves.civ@mail.mil	913.684.7975
Dep Director DSN:552	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
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 & CoEs 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
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-Analyst	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
JMRC & JRTC LNO-Analyst	Mike Spight	michael.g.spight.ctr@mail.mil	CGI 684.7974
Intel Specialist-Analyst	(TBD)		
Intel Specialist-Analyst	(TBD)		
Intel Specialist-Analyst	(TBD)		