Operational Environment Enterprise
US TRADOC G2 Intelligence Support Activity

Red Diamond

Complex Operational Environment
and Threat Integration Directorate

Fort Leavenworth, KS | Volume 5, Issue 10 | OCT 2014

INSIDE THIS ISSUE

UK DATE Exercise..... 4
INFOWAR in Ukraine .. 6
CAR Part 3..... 11
HAMAS 17
A2AD Overmatch..... 23
Counterrecon..... 26
CTID POCs 33

OEE *Red Diamond* published monthly by TRISA at CTID

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

THREAT TACTICS COURSE (TTC): TRAINING FOR COMPLEX OES

by CPT Ari Fisher, TRISA-CTID

The Threat Tactics Course (TTC) is the next step in the evolution of CTID's academic curricula experience. This resident course will occur 9-13 March 2015. Course content, presented in an unclassified classroom environment, is significantly modified and updated from previous courses to include a more in-depth analysis of functional tactics, new threat models of mission task execution, and a revised capstone exercise for the five-day course. Course material emphasizes tactical offensive and defensive actions as well as threat warfighting functions employed at Brigade Tactical Group (BTG) and subordinate unit levels. Students will obtain a credible threat tactics foundation to understand and apply threat tactics and techniques as critical to realistic, robust, and relevant conditions in training, professional education, and leader development.

The foundation for the TTC is the HQDA TC 7-100 series that includes TC 7-100, *Hybrid Threat*, TC- 7-100.2, *Opposing Force Tactics,* and Army TC 7-100.3 *Irregular Opposing Forces,* and related training literature such as *Decisive Action Training Environment 2.1 (DATE)*. For TTC enrollment opportunities, contact Ms. Steffany Trofino (913)684-7943, DSN 552-7943, or Steffany.A.Trofino.civ@mail.mil.

RED DIAMOND TOPICS OF INTEREST

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

This month's cover article provides a brief explanation of TRISA-CTID's week-long course focused on threat tactics to be offered in March 2015. Please contact us for more information or to register for this free course.

The UK conducted a successful DATE-based exercise with support from TRADOC G2 elements from TRISA-CTID and the Training Brain Operations Center (TBOC). A collaborative articles describes the exercise.

Two articles describe different types of threat actor tactics: one on the use of information warfare in the Ukraine and another article on various tactics employed by HAMAS in Israel.

The final installation (Part 3) in the series of articles on the Central African Republic (CAR) describes the January 2013 peace talks and the rebel offensive of February–March 2014 that resulted in the country's fifth successful coup d'état.

The concept of overmatch in the realm of anti-access/area denial (A2AD) is explained with examples of how the threat can employ low-tech yet highly effective techniques to achieve its objectives.

Finally, the threat's use of counterreconnaissance to achieve tactical success is described in Part 1 of a two-part article.

Email your topic recommendations to:

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

Director's Corner:
Thoughts for Training Readiness

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

The Combat Training Centers (CTCs) are critical to the success of Army training and support to the implementation of The Army Campaign Plan. CTCs must be able to support and replicate decisive action operations across the range of military operations in an ever-changing and complex operational environment.

As designated by the DA G3 and the TRADOC CG, and in compliance with AR 350-50 and AR 350-2, the OE/OPFOR pillar of the CTC program is supervised and managed day to day by a team comprised of the Combined Arms Center's CTC Directorate (CTCD), and the TRADOC G2's TRADOC Program Office–OPFOR (TPO–OPFOR) and TRADOC G2 Intelligence Support Activity (TRISA). With respect to requirements and acquisitions, CTCD manages the whole program with a staff supervisory function. TPO–OPFOR, through the Council of Colonels (CofC) and the General Officer Steering Committee (GOSC), seeks and obtains program decisions that support OPFOR personnel and material acquisitions. The Complex OE and Threat Integration Directorate (CTID) sets the overall OPFOR requirements on behalf of the TRADOC G2 and TRADOC CG. Said more simply: CTID determines what is needed to replicate a hybrid threat at the CTCs, TPO–OPFOR guides the determination of training risk and which requirements will become authorizations, and CTCD integrates those efforts into the CTC program as a whole. The collaborative document used to identify and track requirements and authorizations is the OE Master Plan (OEMP).

As an illustrative example, see Table 1 below. This table is an excerpt from the OEMP and shows the total non-hand-launched OPFOR UAV requirement. CTID has determined that the appropriate strength for these systems in an OPFOR Brigade Tactical Group designed to provide realistic challenges to a rotational unit at NTC is four. It has also determined that the type of UAVs that presents the correct realistic capability is the Camcopter S100. Note that this does NOT mean that only this system will do. This means that tactical UAV replication at NTC should include this level of capability, however this replication is accomplished—live, virtually, or constructively.

Table 1. UAV required equipment (excerpt)
(Source: TRADOC G2. *Operational Environment Master Plan*, Chapter 3, Total NTC System Requirements, p. 3-27.)

Equipment	Req	Auth	OH	Comments
Camcopter S100	4	3	3	70%, Boeing Hummingbird/ Fire Scout UAV

Note that with TPO–OPFOR as the lead, the GOSC has determined that three systems will be authorized for use. The determination has also been made that live analogs will be used to replicate the capabilities of the Camcopter. And this is where you come in. These requirements determinations do not occur in a vacuum. It is important to us here at CTID that trainers and training developers at the CTCs, at the Centers of Excellence, and at unit home stations are aware that they may nominate to us systems, personnel, and organizations to serve as requirements for replication. If you feel that your training objectives are best challenged by capabilities that do not appear in the OEMP, CTID is your one stop shop. There is no formal requirement to simply nominate the system or capability. While we may need to come back to you and gain additional information to support the requirement as we move through the process, the staff work is ours to do, along with our TPO and CTCD partners. Contact me or any of my leadership with your request and let us champion this change on your behalf. Our contact information is always presented in the back of every *Red Diamond* issue.

Camcopter S-100 UAV
(Source: Worldwide Equipment Guide, vol. II. "Austrian Unmanned Aerial Vehicle Camcopter S-100." 2013. p. 4-13.)

Observations on Complex Conditions and Hybrid Threats

by LTC Shane Lee (TRISA-CTID), WO2 Matt Tucker (UK LO to TRISA-CTID), and Mike Clark, Training Brain Operations Center (TBOC)

Introduction

In October 2014, elements of US Army TRADOC G2—TRADOC G2 Intelligence Support Activity (TRISA)–Complex Operational Environment and Threat Integration Directorate (CTID) and the G2 Training Brain Operations Center (TBOC)—supported Exercise IRON RESOLVE, as the first British Decisive Action Training Environment (DATE) exercise written and delivered solely by British Army forces. The training event was to validate a new divisional structure and integrate staff procedures in a warfighting role against a hybrid threat, the first exercise of this nature under a new construct. TRADOC G2 representatives provided observations, insights, and perspectives to assist the British Land Scenario Centre (LSC) on delivery of the DATE-based scenario in IRON RESOLVE.

The Land Scenario Centre (LSC) is the lead proponent for the use of DATE in the United Kingdom and Exercise IRON RESOLVE offered the opportunity showcase the capability. The 3rd (UK) Division chose to use the DATE and Lieutenant Colonel Steve Williams, the LSC commander, took the lead for the planning and execution. The LSC Operations Officer Captain Sandy Gill coordinated the exercise design and supported Lt-Col Williams' role as commander of the Opposing Forces (OPFOR). TRADOC G2 through TRISA coordinated with the LSC during the planning phase, and supported the execution directly by sending two representatives.

TBOC has a long-standing relationship of support and cooperation with the UK Land Scenario Center dating back several years. TBOC support to LSC and 3rd (UK) Division's Exercise IRON RESOLVE was discussed and consisted of data enrichment and delivery, but the LSC later decided to test their capability to provide the exercise support in-house. Exercise IRON RESOLVE was conducted in the Warminster, UK local area and the TBOC Team was hosted/based out of the LSC offices at Warminster. The LSC requested TBOC representatives attend the exercise 5-14 October to deliver an observer/mentor capability.

The Exercise

The LSC produced an outstanding corps-level (Allied Rapid Reaction Corps [ARRC] was the Corps Command) DATE scenario that was complex, rich with information from all PMESII variables, and absolutely compliant with DATE 2.1 as defined by TRISA. In fact, this is the purest form of a DATE scenario in existence today largely because the LSC did not allow capability—outside the TRISA definitions—to be included in their scenario. Good "ideas" were not allowed to water down the operational environment (OE).

The LSC delivered their DATE scenario to the 3rd UK Division with precision from well before STARTEX, then throughout the exercise using a combination of voice and digital transition means (MAGPIE—data and BOWMAN—voice and data). The Road to War, INTSUMs, and OPSUMS were delivered to the division HQ from March to late September 2014 to set the conditions to allow staff planning. The LSC MSEL management and dynamic scripting processes during the exercise were mature and seamless. Exercise control (EXCON) capability is usually judged by the amount of confusion the scenario generates for the training audience, and in the case of the LSC-led EXCON, that confusion was minimal.

The exercise scenario saw the Armed Forces of ARIANA and MINARIA invade ATROPIA. The 3rd (UK) Division formed part of a United States-led Coalition Joint Task Force and was tasked to restore the sovereignty of ATROPIA to pre-conflict boundaries and governing authority within its boundaries.

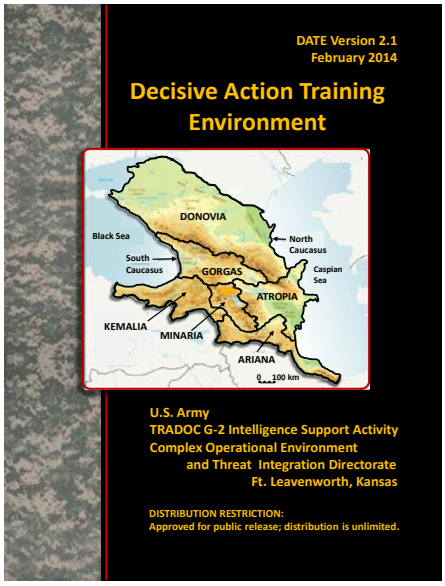
The OPFOR was hybrid in nature, the regular element consisted of a MINARIAN Operational Strategic Command (OSC) with six brigades supported by an ARIANIAN T-90 Tank Brigade. The irregular actors were made up by the insurgent organizations of Southern Atropian People's Army (SAPA) and Sadvol, the Bocyowicz crime family, and a complex political and humanitarian situation.

The OPFOR was deployed in a disruption zone, a defensive zone, and a reserve commitment zone; their plan was to conduct an area defense. The units were identified with a given task and purpose to achieve the overall strategic goal of negotiating the seizure of land for increased oil revenue. Irregular force actors' objectives developed as the exercise progressed and opportunities for them arose.

Due to 3rd (UK) Division's focus on the regular force fight, the irregular forces were downplayed in the rear areas from both an exercise design standpoint and by EXCON. This was counteracted by a more robust and developed irregular portrayal in front of the division. When this situation was underestimated there was an increase in the murder rate, a split among the insurgent groups, and a state within a state emerged to fill the void in uncontrolled territory.

Figure 1. Exercise IRON RESOLVE and Complex Conditions

The understanding of DATE and the hybrid threat exceeded the expectations of the TRADOC G2 observers. The LSC is to be complemented on the implementation, especially as this was the first attempt. The exercise design clearly outlined the conditions, thereby giving subject matter experts the ability to work Political-Economic (grey), Military-Insurgent-Criminal (red-orange-black), social-infrastructure-information (white), and host nation (green); the level of detail developed remained consistent within the condition set for DATE.



Overall, it was a very impressive effort by the LSC and the many training enablers tasked to support IRON RESOLVE 2014. The final analysis of any scenario used under any OE is the amount of time the training unit spends fighting the scenario instead of the enemy.

3rd UK Division fought the enemy and there were virtually no comments throughout the exercise related to the scenario or the underlying DATE. This is proof positive that the LSC delivered a world-class DATE scenario.

Future DATE Implementation

UK, Canadian, Australian, and Danish senior leader representatives were briefed on the use of DATE during Exercise IRON RESOLVE as well as the benefits for incorporating DATE into the ARRC, the British-led NATO corps. The Assistant Director, Capability Training-Army, from the United Kingdom Army Headquarters will identify resource requirements for continued use of DATE in future training in the British Army.

by Jerry England, TRISA-CTID (DAC)

Hybrid threats are distinguished by a combination of regular and irregular forces with skilled information warfare (INFOWAR) capabilities. Recent operations in Ukraine have highlighted the importance of information warfare by pro-Russian forces in a series of complex, layered attacks across multiple sectors of the Ukrainian information environment. While the use of INFOWAR as an asymmetric tactic is not a new concept, the ways in which the hybrid threat is evolving its use of technology and tactics requires some attention when analyzing the current situation in the Ukraine and what it means for future conflicts.

INFOWAR capabilities such as cyber operations, electronic warfare (EW), propaganda, and disinformation are hybrid threat force multipliers that support tactical and operational advantages by providing increased situational awareness and degrading the decisionmaking ability of friendly forces. INFOWAR activities are particularly useful when faced with circumstances that are politically sensitive or when the need to restrain lethal force is present. INFOWAR operations can buy time for threat actors to consolidate tactical gains and control events on the ground through misdirection and disinformation. The purpose of this paper is not to provide an exhaustive list of all Russian political and military INFOWAR capabilities in the Ukrainian operational environment (OE), but to highlight the activities that appear to be emerging trends.

Physical Destruction and Seizure of Media and Information Communication Technologies

The isolation of the Crimean peninsula by Russian forces and pro-Russian irregulars displayed how quickly regional operations can be executed when the objectives are defined and obtainable. Regional operations attempt to achieve strategic, political, or military decision by destroying the enemy's will and capability to fight.[1] The isolation of Ukrainian military targets by Russian forces was due in many ways to a compliant pro-Russian population who willingly accepted Russian themes and narratives portraying themselves as liberators. In order to make the operations successful even with a supportive majority, Russian forces had to control the information environment and reduce the risk of unaligned views getting into the open. This was done in part by destroying components of the Ukrainian command and control (C2) systems by physically attacking key nodes of the telecommunications infrastructure. The result was a confusing situation in which intermixed Ukrainian and Russian military forces were unable to contact policy makers and first responders for guidance and assistance.

As Ukrainian installations were being surrounded by Russian troops and other "unspecified" units, Soldiers acquiesced to Russian demands with little influence from Kiev.[2] The lack of communication prevented any units that were still loyal to Kiev from disrupting Moscow's coordination with the more than 15,000 Russian forces already stationed in the area. This enabled Russian forces to easily consolidate and secure installations on the peninsula with the help of an active pro-Russian population and to control the message about events on the ground to suit their purposes.

As tensions escalated, a Ukrainian authority confirmed that mobile phones and other forms of communication were cut, isolating Ukrainian leadership from the region.[3] Additionally, media outlets were seized by pro-Russian protestors and forced to either shutdown or rebroadcast Russian news media.[4] The region's information environment thus came under influence of Russian INFOWAR and the chance for any dissent among pro-Ukrainian outlets was actively discouraged.

Ukrainian defenders in Crimea were unable to receive guidance from Kiev regarding whether to surrender their bases or to stand and wait for reinforcements.[5] According to General Philip Breedlove, NATO Supreme Allied Commander, "The incursion into Crimea went very much like clockwork, starting with almost a complete disconnection of the Crimean forces from their command and control via jamming and cyber attacks and then a complete envelopment by the Russian forces inside of Crimea."[6]

The ease with which attacks on the information infrastructure in Ukraine were executed can be partially attributed to the fact that Ukraine was a former member of the Soviet block and thus had much of its network installed by Russian enterprises during the cold war. Ukrtelecom, Ukraine's largest telecom provider, was privatized after Ukraine gained its independence in the 1990s.

The network was most likely designed and installed by Soviet communications providers, thus accounting for the Russians' intimate knowledge of key nodes and trunk lines.[7] This intimate knowledge of the network and the help of a large number ethnic Russians who welcomed the change gave Moscow the ability to monitor communications and to contact persons of interest within the network for exploitation and disruption through a variety of cyber and electromagnetic attacks.

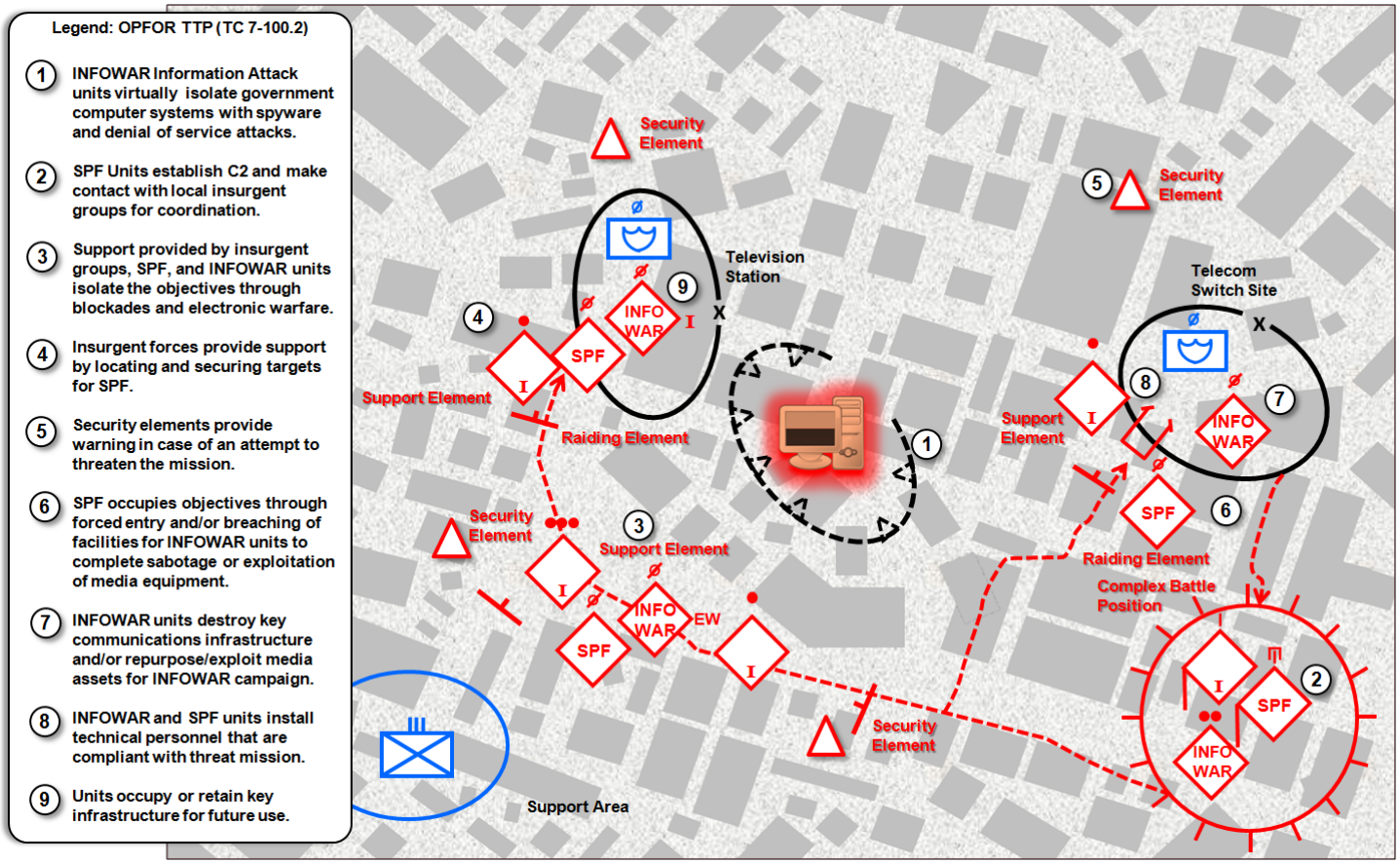


Figure 1. INFOWAR attack
(Source: TRISA-CTID, 2014)

Russian Electronic Warfare in Ukraine

The targeting of information technology and communications assets through physical destruction can be counterproductive if the threat wants to use these same systems at a later time for their own purposes or for intelligence and situational awareness purposes. The use of electronic warfare capabilities to collect data in transit and to disrupt the flow of information allows the threat to gain intelligence on enemy activity without the risk associated with physically destroying a target. Electronic warfare capabilities will sniff out communications and locate the source for further actions.

Electronic warfare assets that jam communications can also assist the threat in isolating objectives and disrupting friendly forces' ability to effectively exercise command and control. The systems employed included both communications intelligence and electronic countermeasures equipment. Examples are the R-330 jammer that can jam space-based communications and navigation systems.[8] The family of R-330 jammers has been in use in the Russian military since the Soviet days and recent upgrades have increased the capabilities of these systems for use on the modern battlefield. Additionally, a number of tactical EW systems were also witnessed in the early stages of the conflict, such as the Leer-2 direction-finder/jammer constellation and the Lorandit direction-finding constellation.[9] EW capabilities allow an actor to exploit, deceive, degrade, disrupt, damage, or destroy sensors, processors, and C2 nodes.

Figure 2. Russian electronic warfare vehicles Tigr-M (Leer-2 systems)
(Source: Twitter FdeStV@Marsattaqueblogv, 2014)

Malware and Large-Scale Data Breaches

Recent breaches against large commercial databases illustrated a new norm in the evolving cyberwar between hacker gangs in Ukraine and the financial sector. The release of financial and banking data from primarily US credit card holders by a pro-Russian Ukrainian cyber collective shows that countries that dare to take a stand in the struggle between Ukraine and Russia are at risk for cyber attacks. The financial information that was sold on the black market increases the threat's ability to conduct criminal activity, expand espionage efforts, and instill doubt in the private sectors' ability to secure financial data.[10] A spokesperson from Risk Based Security and the Dataloss DB project says that the activities of such hacktivist organizations are designed to have an impact on the international financial system.[11]

Researchers at a number of computer security firms have discovered a sophisticated malware platform that has noticeably targeted chiefly Ukrainian government targets.[12] This platform, known as "Snake" to researchers, bears a number of hallmarks that tie it to Russian-speaking malware developers. The unique ways in which it replicates itself indicates that the malware is designed to target large corporations or government agencies.[13]

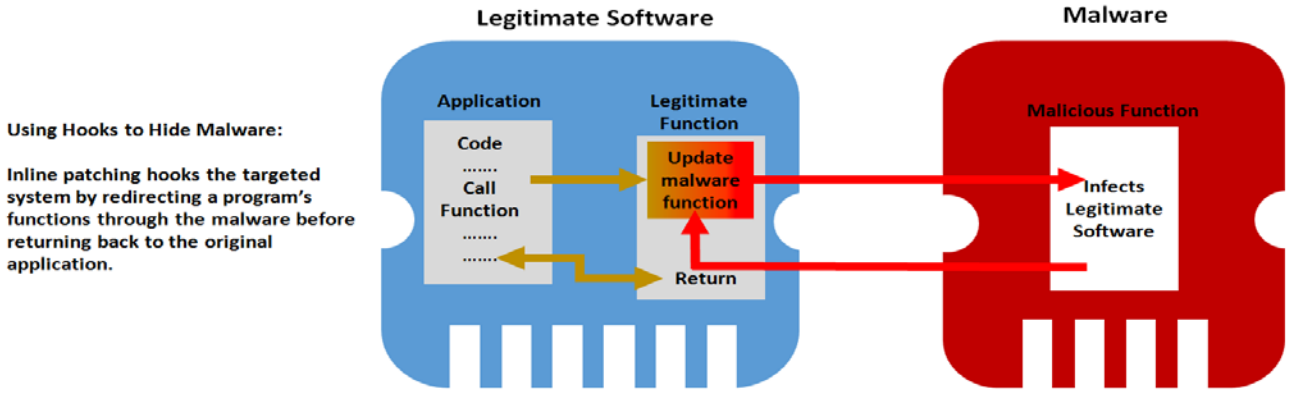


Figure 3. Inline patching model
(Source: TRISA-CTID, 2014)

By using a function that copies malware onto portable media devices such as thumb drives, Snake malware is able to move over the so-called air gap to unconnected networks. Snake is also said to bear some similarities to a previously-discovered malware known as agent.btz, which was identified as being of Russian origin.[14] The main qualities of the Snake malware make it a rootkit that covertly installs on compromised systems and communicates with command and control servers via a backdoor that exfiltrates data surreptitiously.[15] The ability to stay dormant when not in use makes locating the malware very difficult.

Spyware is just one tool of many being used in the current conflict. Many actors on both sides are using advanced service-denial applications to block websites and to prevent effective C2 among their respective enemies. One example is the Dirt Jumper DDoS kit that targeted pro-Ukrainian government websites and media sites. Dirt Jumper is a well-known distributed denial of service (DDoS) family with many servers located in both Ukraine and Russia.[16] The service can be rented for $30–70 a day through hacker community online markets.[17] Dirt Jumper is an advanced DDoS attack and appears to use volumetric user datagram protocol flood to cause targeted systems to become unreachable.[18]

Russian Propaganda in the Ukraine

Russia's sophisticated propaganda machine has developed into an effective combat force multiplier for its "fifth column" operations in the Ukraine. The use of social media is a key component to Russia's ability to control the message and undermine world opinion through use of radical rhetoric and disinformation. Unlike terrorist organizations who seek to intimidate through the use of extremely gruesome images, the Russian perspective is to control the truth and to deny its enemies the ability to make decisions through a program of disinformation and hyperbole.

The Russians do this by hiring professional bloggers known as "trolls" to seed popular websites with information supportive of the Russian foreign policies, an activity known as "astroturfing."[19] Although paying propagandists to plant stories is not a new technique, the scale and integration of the plan within the larger strategy and the Russians' use of the Internet are.

Opinions are provided by the Russian government and bloggers are paid by the number of comments they post, the number of accounts they create, and the number of websites they establish.[20] Russia's activities in the Ukraine are justified by the professional commenters in a variety of influential blogs that establish the protection of ethnic Russians as a legitimate reason. The section of southwestern Ukraine in which Russian supporters and Ukrainian forces are contesting for power is known in the Russian press as Novorossiya—"New Russia"—and is used to manipulate world opinion of Moscow's claims to the region.[21]

The message is less about the truth and more about influence and opinions, according to Russian media leaders who claim that ratings are what drive the stories and that these are more important than accuracy and truth in reporting.[22] Fabricated stories and the use of actors to provide "realism" to media reports of violence suggest that manipulation of the media is more about buying time than providing unbiased information to the public. Use of disinformation in Russian media provides a window of opportunity for threat forces to conduct operations before the public fully understands the situation. This tactic buys time for threat forces to act, free from the influence of public opinion.[23]

It is worth mentioning that Russian information warfare operations had been in effect in South East Ukraine months before the events of spring 2014. Many of the themes that were used to garner influence over the region were designed to reassure the majority of ethnic Russians living in the area that the annexation of Crimea was a forgone conclusion. For units still loyal to Kiev, the inevitability of Russian possession of Crimea convinced them of the futility of resisting. For those individuals who already considered themselves Russian, the support was given freely and the messages coming from Moscow only reassured them that they would be better off under a new regime with closer ties to Russia.

Raid in the Information Operational Environment: Implications for Training

The complex, layered INFOWAR attack by Russian forces in the Ukraine is not necessarily a new tactic, but represents the capability of an upper-tier threat that chooses to leverage not just military might but all of the tools available to an interconnected, information-driven society. For many threat actors, controlling the messages coming out of an area of operations is enabled by denying the enemy the means to communicate across a wide spectrum of media and technologies. The Russian technique has been to leverage a regional competitor's infrastructure in order to isolate key communications nodes both in terms of telecommunications and media outlets. The comparison of the current conflict

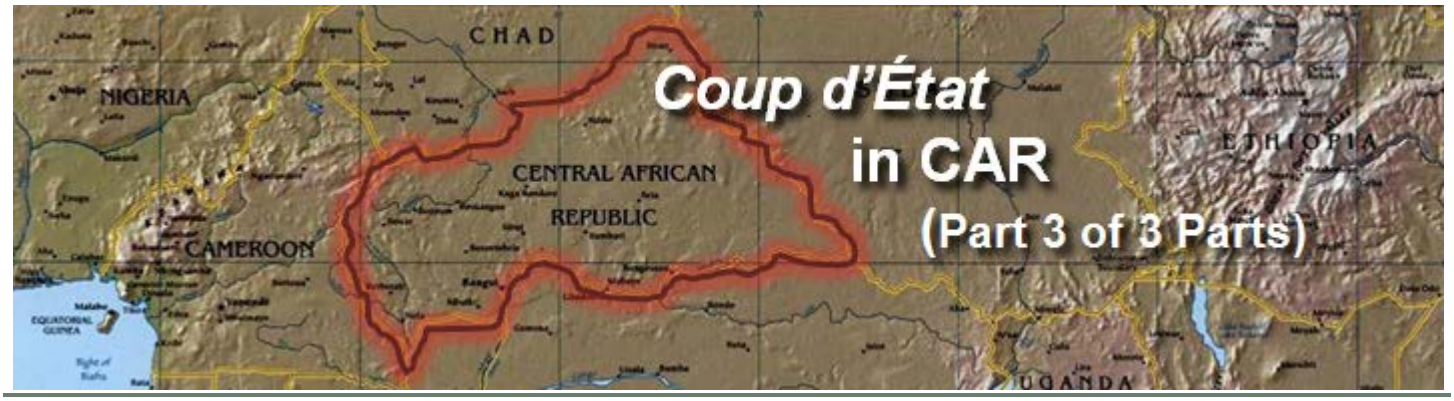
with Russia's recent history of cyber activity suggests that a more restrained approach is being used in order to minimize damage to infrastructure and possibly maintain economic stability. However, the risk of more-intense cyber activity is apparent in recent denial of service attacks which have the ability to target specific organizations and reduce the threat of collateral damage.

The TC 7-100.2, *Opposing Force Tactics* describes a raid as "an attack against a stationary target for the purposes of its capture or destruction that culminates in the withdrawal of the raiding force to safe territory." It goes on to say that, "Raids can also be used to secure information and to confuse or deceive the enemy." The events described above open the door for a new way to view a raid that not only includes the physical seizure of equipment for threat use, but also explores the exploitation and repurposing of existing telecommunications and media equipment (generally known as information communications technology [ICT] systems) in the information environment. ICT systems should be considered key terrain along with the other elements of the information environment, including the physical, informational, and cognitive dimensions, and must be secured according to their nature. Securing these resources will mean not only physically securing them but also shielding them from other forms of INFOWAR activities, such as cyber attacks and propaganda. Additionally, understanding the information environment enough to recognize when an information outlet has been compromised by threat forces could ensure that friendly forces can maintain access to an unhindered use of the information environment, as well as being a key indicator of an area of operations falling to the opposition.

"[Russia], is waging the most amazing information warfare blitzkrieg we have ever seen in the history of information warfare."
General Philip Breedlove, Supreme Allied Commander

Notes

[1] Headquarters, Department of the Army, FM 7-100.1, Opposing Force Operations, TRADOC Intelligence Support Activity, December 2004, p 3-1.
[2] Charles Miranda, Ukrainian military abandoning bases in Crimea after being warned they are now "enemy combatants," 7 March 2014; Associated Press, President Obama warns Russia not to intervene militarily in Ukraine, 1 March 2014.
[3] BBC, Russia and Ukraine in cyber 'stand-off', 5 March 2014.
[4] CNN, Ukraine says it retakes building seized by protesters, 7 April 2014.
[5] Charles Miranda, Ukrainian military abandoning bases in Crimea after being warned they are now "enemy combatants," 7 March 2014.
[6] Laurence Norman, NATO's Top Commander Reflects on Crimea, Wall Street Journal, 23 March 2014.
[7] Patrick Tucker, Why Ukraine Has Already Lost The Cyberwar, Too, April 2014.
[8] James Hasik, It's Time for a Backup to GPS, The Atlantic Council, 14 April 2014.
[9] Live leak, Russian army military electronic warfare vehicles arrives in Crimea Ukraine, 4 October 2014; Russian army's communication, jamming and Electronic Warfare systems, Asian Defence News, 5 April 2014.
[10] Steve Ragan, AMEX customers were part of a data dump by Anonymous Ukraine earlier this year, June 2014.
[11] Jeffery Roman, Anonymous Ukraine Posts 7 Million Cards, March 2014.
[12] Defense Update, The Ukrainian crisis – a cyber warfare battlefield, April 2014; Mark Clayton, Christian Science Monitor, Massive cyberattacks slam official sites in Russia, Ukraine, March 2014.
[13] G Data, Uroburos Highly complex espionage software with Russian roots, February 2014, p 3.
[14] BAE Systems, Snake Campaign & Cyber Tool Kit, March 2014.
[15] BAE Systems, Snake Campaign & Cyber Tool Kit, March 2014.
[16] Mark Clayton, Christian Science Monitor, Massive cyberattacks slam official sites in Russia, Ukraine, March 2014.
[17] Radware, 2012 Global Application and Network Security Report, January 2013.
[18] Radware, Threat Alert - Ukraine-Russia Global Conflict, July 2014.
[19] Chris Elliot, The readers' editor on… pro-Russia trolling below the line on Ukraine stories, The Guardian, 4 May 2014; Yazan Boshmaf, et al, The Socialbot Network: When Bots Socialize for Fame and Money, University of British Columbia, 9 December 2011.
[20] Olga Khazan, Russia's Online-Comment Propaganda Army, The Atlantic, 9 October 2013.
[21] Peter Pomerantsev, Russia and the Menace of Unreality, The Atlantic, 22 September 2014.
[22] Peter Pomerantsev, Russia and the Menace of Unreality, The Atlantic, 22 September 2014.
[23] Lucy Crossley, The 'aggrieved housewife', the 'soldier's mother' and the 'Kiev resident': Did Russian television 'use actress to portray FIVE different women' as it reported normal Ukrainians backed Kremlin, Daily Mail, 5 March 2014.
[24] Headquarters, Department of the Army, TC 7-100.2, Opposing Force Tactics, TRADOC Intelligence Support Activity, December 2011, p 3-36.



by Laura Deatrick, TRISA-CTID (CGI Ctr)

A former French colony, the Central African Republic (CAR) has had a stormy history since gaining independence in 1960. Power has primarily been transferred via coup d'état, with the only peaceful transition occurring in 1993. Rebel groups form often and easily, and CAR has had nearly continual foreign troop presence—French, African Union, and UN—in ongoing international attempts to stabilize the country and keep peace. This is the third and final article in a series that explores the most recent coup d'état in CAR, which occurred on 24 March 2013 when the Séléka rebel group overran the capital.

Background

From independence until the rebel takeover in 2013, the country was ruled by only five different men, with all but one taking power via coup d'état. The most recent of these was François Bozizé, who seized control in a 2003 coup with the support of neighboring country Chad. Opposed by many in the country – including those loyal to the man he deposed – Bozizé has been the target of various rebel groups since seizing power, the most recent of these being Séléka. The rebel group Séléka CPSK-CPJP-UFDR (Séléka) was created in 2012, and was formed as a coalition of three existing rebel groups. Two other groups subsequently joined Séléka, though one of these left shortly thereafter. Rebel groups that have belonged to Séléka include the following:

- A faction of the Union of Democratic Forces for Unity (*l'Union des Forces Démocratiques pour le Rassemblement*; UFDR), founding member, led by Michel Djotodia and Damané Zakaria
- A faction of the Convention of Patriots for Justice and Peace (*la Convention des Patriotes pour la Justice et la Paix*; CPJP), founding member, led by Noureddine Adam
- The Patriotic Convention for National Salvation (*la Convention Patriotique du Salut du Kodro*; CPSK), founding member, led by Dhaffane Mohamed-Moussa
- The Alliance for Rebirth and Reforging (*l'Alliance pour la Renaissance et la Refondation*; A2R), coordinated by Salvador Edjezekane and later renamed the Movement for Rebirth and Reforging (*Mouvement pour la Renaissance et la Refondation*; M2R)
- The Democratic Front of the Central African People (*le Front Démocratique du Peuple Centrafricain*; FDPC), led by Martin Kountamaji, aka Abdoulayé Miskine. This group later withdrew from the Séléka coalition. Michel Djotodia, leader of the UFDR faction, became Séléka's de facto leader.

Figure 1. Location of the Central African Republic

The First Offensive

As of 9 December 2012, CAR was experiencing an uneasy peace. Rebel groups that had signed peace agreements with the government during the previous five years were still awaiting the fulfillment of many of the promises made, including the release of political prisoners and the completion of the demobilization, disarmament, and reintegration process for former members. Only a few weeks earlier, threats of an attack made by a breakaway faction of the UFDR, led by Michel Djotodia, had caused many residents of the northern city of Ndélé to flee. The expected attack did not materialize, however, and the townspeople eventually returned to their homes. Then in late November, armed rebels had attacked the northern town of Kabo, but Central African Forces (*fr: Forces Armées Centrafricaines*; FACA) troops had been able to repulse them.[1]

Séléka began its first offensive on 10 December 2012 by attacking three northern towns: Ndélé, Sam Ouandja, and Ouadda. From there, the rebel group proceeded rapidly to take over a large portion of the country, capturing Bamingui (15 December), Mbrès (17 December), Bria (18 December), Kabo (19 December), Batangafo (20 December), Ippy and Ndassima (22 December), Bambari (23 December), Kaga Bandoro, (25 December), Sibut (29 December), and Alindao and Kouango (5 January 2013). FACA troops were ineffective in stopping the Séléka advance, and the Economic Community of Central African States (ECCAS), of which CAR was a member, sent in additional troops to augment those of the Central African Multinational Force (*fr: Force Multinationale de l'Afrique Centrale*; FOMAC) that were already on the ground. It was these forces in conjunction with non-ECCAS troops—notably those of South Africa—that finally convinced Séléka to negotiate for peace. On 7 January 2013, representatives of the CAR government and the Séléka rebels arrived in Libreville, Gabon, to begin peace talks.

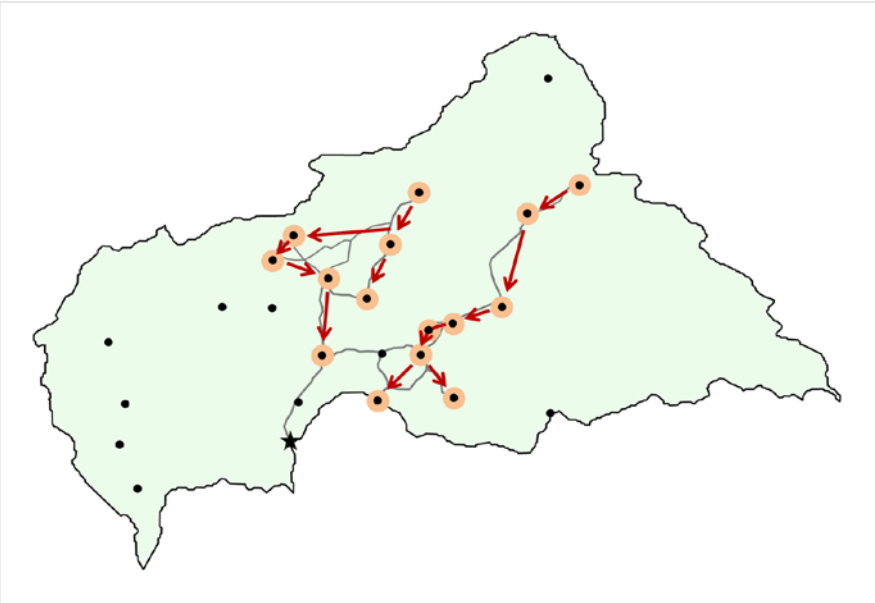


Figure 2. First offensive

Note. Distances mentioned and routes shown on graphics are most likely scenarios based on CAR's road system. Only select roads are shown on graphics for purposes of clarity.

8-17 January 2013

The peace process got off to a rocky start. The day before negotiations commenced, President Bozizé refused Séléka's continued calls to relinquish his position. He instead claimed the rebels represented foreign interests and referred to them as "terrorist mercenaries."[2] The beginning of peace talks was then delayed by two hours the following day (9 January), as Séléka representatives did not arrive to the negotiations on time. ECCAS, who was hosting the talks, desired to base a new peace agreement on previous, failed accords, and immediately sued for a ceasefire. Bozizé's representatives sought a unity (power-sharing) government, while Séléka demanded that Bozizé be removed from the presidency and tried for war crimes before the International Criminal Court. The rebels and CAR government agreed to a temporary ceasefire on 10 January, but no other progress was reported that day.

On 11 January, the CAR government and Séléka came to an agreement and signed a peace deal and permanent ceasefire, to go into effect 14 January. The agreement contained the following main points:

- Power-sharing government: Bozizé would remain president until the end of his term in 2016, while an opposition member would be named as prime minister and head of government. The current National Assembly would be dissolved and a transitional council would take its place until new legislative elections, to be held January 2014.
- Prisoners: The government would release prisoners held for political reasons—a promise that had been included in previous agreements but was never honored by Bozizé.
- Foreign troops: All foreign forces not associated with FOMAC/MICOPAX were to leave the country. This item was specifically aimed at the removal of South African forces, which had supported Bozizé.
- Captured towns: Séléka would relinquish the territory conquered during its December 2012- January 2013 offensive.

Bozizé quickly implemented part of the agreement. Within days, he had removed the prime minister from office and appointed Nicolas Tiangaye, an opposition leader, in his place. However, there were no immediate moves to either release political prisoners or to remove South African troops from the country.

18-30 January 2013

The peace agreement was in force for only days before it was violated. During 20-21 January, a group of Séléka members attacked the town of Dimbi, which lies 75 km southeast of Alindao, then traveled an additional 20 km east to Kembé, which they also captured. The group destroyed homes and government buildings, destroyed telephone infrastructure, and broke into the prison at Kembé, releasing prisoners in the process. There were also reports that they had killed a police brigade commander at Kembé, though it was later revealed that the commander had successfully gone into hiding.[3] They were then reported to be heading east toward Bangassou, a major regional city. Séléka originally denied the attacks, claiming that their members had only performed security duties in the area, but then later blamed the attacks on "uncontrolled elements."[4]

Only a few days later, on 25 January, Séléka members raided the town of Satema, just 35 km south of Dimbi. They entered the town on the weekly market day and proceeded to plunder goods from both vendors and local residents. They left the following day, but not before many residents had fled across the Oubangui River into the Democratic Republic of Congo (DRC).

Things were going no smoother on the political front. Both sides repeatedly accused the other of not abiding by the peace agreement, with Séléka threatening to renew its offensive if Bozizé did not hold up his end of the bargain. On top of this, newly-appointed Prime Minister Tiangaye was busy negotiating the minefield of determining which posts in the transitional council would go to each party. Supporters of the president made this task no easier, claiming that Bozizé had the right to name people to key ministries by himself.[5]

February 2013

The new transitional government was announced on 3 February 2013. It would be composed of the Prime Minister, two Deputy Prime Ministers, twenty-three Ministers, and seven Deputy Ministers. These positions were parceled out among five main parties: Séléka, the presidential majority, the democratic opposition, non-armed political-military groups, and the civil society. Of the twenty-three ministries, only four went to Séléka members: Defense, Communications, Forestry, and Geology—with Djotodia appointed as both Defense Minister and First Deputy Prime Minister.[6] This was well short of Séléka's request for seven ministries, which had included those of Finance and Mining.

Séléka members struck again on the morning of 7 February, this time attacking the city of Mobaye, 85 km south of Alindao. FACA forces were on the ground and fought the rebels briefly—killing one—then fled. The attackers looted government and security buildings, stole weapons from the police station, and took out the local telephone infrastructure. Thousands of local residents fled across the river to the DRC, just as those of Satema had done only two weeks prior. When they were done, the raiders left the city and headed back to Alindao. Séléka admitted the attack the next day, but laid the blame on "uncontrolled elements" and "bad communication."[7] A week later, around 12 February, Séléka attacked the town of Dékoa—70 km north of Sibut—and burned at least 100 homes.

The government began the process of demobilizing militants in late February. As with other aspects of the peace agreement, this one did not go smoothly. While Djotodia himself addressed some Séléka members about the process, others felt that they were ignored. Reports of members on the ground ignoring orders from Séléka leaders surfaced, as did complaints that the new government had yet to act regarding political prisoners and the presence of South African troops in the country. When all these complaints reached the ears of high government officials, the response was basically "we're discussing it."[8]

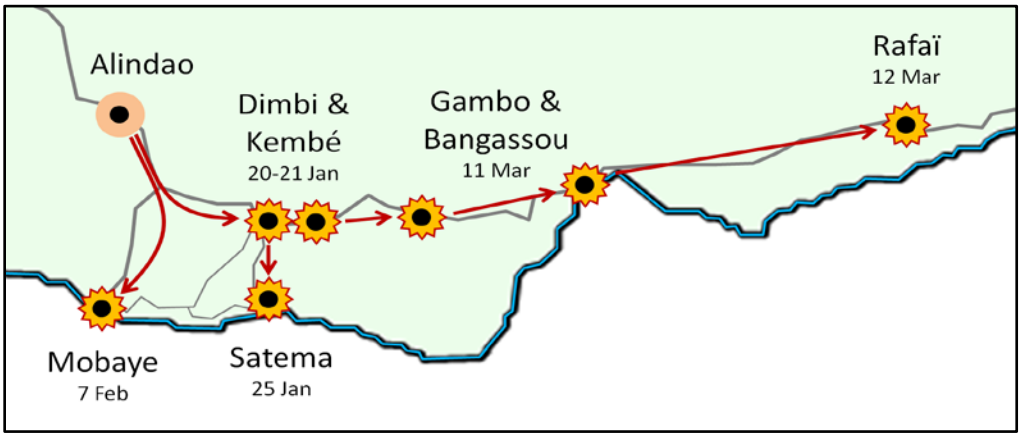


Figure 3. Second offensive–Eastern towns

1-16 March 2013

Séléka members struck again on the night of 28 February–1 March, capturing the town of Sido that lay 65 km north of Kabo on the Chadian border. Arriving in 4–6 vehicles mounted with heavy arms, the group attacked government offices—including the army base and the police station—and pillaged the town. Over 4,000 people, both FACA troops and local residents, fled across the border to Chad.[9] The attack was blamed on Noureddine Adam's CPJP faction, with reports indicating that Chadian soldiers also participated. Communications Minister and Séléka member Christophe Gazam-Betty immediately condemned the move and stated that the CPJP had chosen to leave Séléka.[10] He was contradicted on 4 March and again on 8 March, when Séléka issued two separate statements; first rejecting responsibility for the attack, then subsequently claiming that Séléka members had been ambushed by FACA troops near Sido in a "minor incident." [11]

During the pre-dawn hours of 11 March, Séléka elements traveling in seven vehicles attacked the town of Gambo, which lay only 45 km east of Kembé. Facing no resistance, the group then drove the additional 65 km east to Bangassou, which they also attacked.[12] FACA troops were stationed at the latter and fought the rebels, but subsequently retreated. Residents fled the city and Séléka severed the telephone lines, just as in other recent attacks. The following day the group took the town of Rafaï—130 km farther east—without a fight and took out its telephone lines.[13] The blame for these attacks was again laid at the feet of Noureddine Adams and his faction of CPJP.

During this time, Séléka continually complained that Bozizé was not acting in accordance with the peace agreement: he had not yet released political prisoners, and South African troops remained in the country. Rebel members continued to object to demobilizing until he acted on these issues. Séléka also accused Bozizé of setting up a shadow government to bypass the one selected by Prime Minister Tiangaye, and released a communiqué demanding that ministry positions be reassigned to comply with the group's previously-expressed wishes.[14]

17-24 March 2013

On 17 March, a delegation from the CAR government and the international community journeyed from the capital of Bangui to the nearby town of Sibut, where they planned to discuss implementation of the peace accords with Séléka rebel leaders. Instead of the dialogue the representatives expected, they received an ultimatum: the CAR government

had 72 hours to release political prisoners, remove South African troops from the country, lift the curfew that was in effect in Bangui, and begin to integrate rebel fighters into FACA. If these demands were not met within the specified time period, the rebel group would renew its offensive. To emphasize their demands, Séléka leaders forbade their four government ministers, who had accompanied the delegation to Sibut, from returning to Bangui.

Bozizé partially conceded to Séléka's demands on 20 March, lifting the curfew in Bangui and declaring the release of prisoners that had been "arrested, detained, or condemned" on or after 15 March 2012.[15] This was not enough for Séléka, who declared the measures insufficient and announced an end to the ceasefire agreement. The same day, the group issued a communiqué taking credit for the capture of Bangassou, Gambo, and Rafaï the previous week, claiming the attacks had been a defensive measure to prevent the "capture and control" of Bangassou by non-FOMAC foreign forces.[16]

Séléka recommenced its offensive the next day, recapturing Batangafo, 60 km south of Kabo, which it had taken during the first offensive and subsequently vacated. The group also captured Bouca – 85 km further south – on the morning of 21 March after overcoming resistance by FACA forces. As with previous incidents, the group reportedly severed communication lines to the area, then headed west toward Bossangoa.[17] Séléka raised the political stakes that day as well, calling for Bozizé's resignation and declaring that the group would remove him by force if he did not comply.

On the morning of 22 March, a group of Séléka fighters captured Bossangoa, 95 km west of Bouca, with little resistance and cut telephone lines to the town.[18] That same day, a second contingent attacked the town of Damara, 100 km south of Sibut and only 75 km north of the capital city of Bangui. Despite the presence of FOMAC troops and a helicopter attack by FACA, the rebels succeeded in taking control of the town. The CAR government denied the capture of Damara but many residents of Bangui took no chances, closing shops early and fleeing the city.

Séléka began its attack on Bangui on 23 March. The contingent that had taken Bossangoa the day before traveled south, capturing the towns of Bossembélé and Boali – 145 km and 240 km south of Bossangoa, respectively – and cutting electricity to the capital before entering Bangui from the west. The group that had captured Damara entered the city from the north. FACA troops fought back, but were consistently defeated by the rebel forces. Local residents fled southward, the UN began to evacuate all non-essential staff, and Bozizé sent his family out of the country. France called for an emergency meeting of the UN Security Council, but it was too late for diplomatic action. Séléka captured the presidential palace on 24 March. The next day, Séléka leader Michel Djotodia took power, suspending the constitution and dissolving parliament. The fifth coup d'état in the Central African Republic's history was now complete.

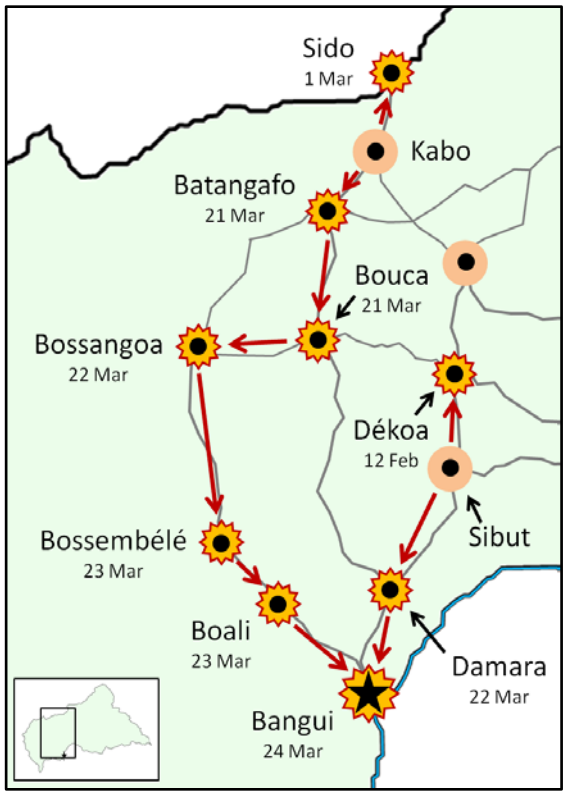


Figure 4. Second offensive – Western towns

Conclusion

Political tensions, rebel groups, and forceful regime changes are standard fare in the Central African Republic. Part One of this series focused on political events leading up to the beginning of the Séléka rebellion and the composition of the rebel group. Part Two reviewed the rebel offensive of December 2012–January 2013. This article examined the January 2013 peace talks and the rebel offensive of February–March 2014 that culminated in the country's fifth successful coup d'état.

References

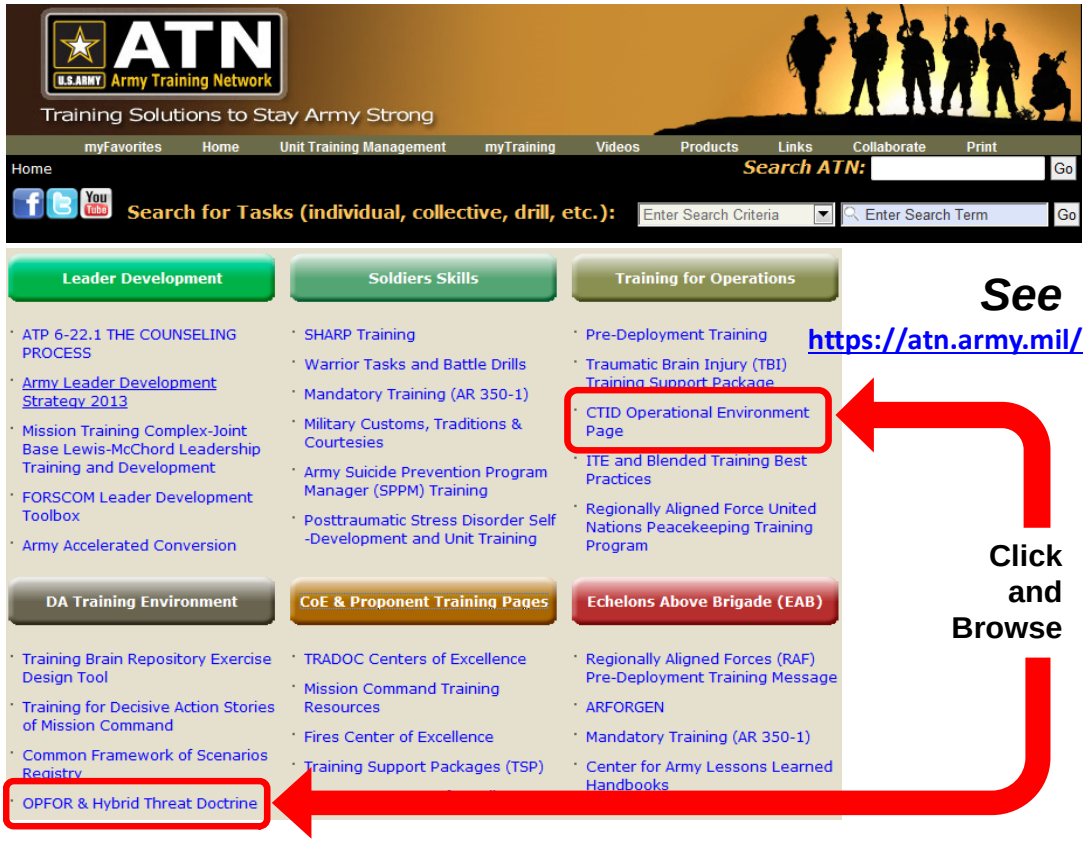
For source questions and a complete list of sources, please contact the author.

Notes

The sources listed below are not a complete listing of those consulted; rather, they portray unique information not included in other reports.

[1] Radio Ndéké Luka, "Attaque rebelle, panique générale à Ndele," 10 December 2012; RFI, "RCA: l'armée tchadienne en renfort des troupes centrafricaines face à la rébellion," 19 December 2012.
[2] Al Jazeera, "CAR war of words heats up amid talks," 10 January 2013.
[3] RJDH-RCA, "Bangassou: Le Calme Semble Revenir," Centrafrique-Presse, 23 January 2013.
[4] Radio Ndéké Luka, "Centrafrique: Séléka fait porter la responsabilité de la conquête de Dimbi et Kémbé à ses éléments incontrôlés," Afrique News Info, 24 January 2013.
[5] Reuters, "Opposition, rebels take key posts in new Central African Republic government," 3 February 2013.
[6] Xinhua, "Central African Republic's national unity gov't formed," People's Daily Online, 4 February 2013.
[7] Pacôme Paba, "Centrafrique: Séléka contrôle la ville de Mobaye," Journal de Bangui, 8 February 2013; Agence France-Presse, "Centrafrique: la rébellion reconnait un incident mais dit y avoir mis fin," Centrafrique-Presse, 8 February 2013.
[8] Jane's, "Séléka," 11 October 2013; Nouvelle Centrafrique, "Centrafrique: Accords de Libreville la Seleka s'impatiente," 28 February 2013; Nouvelle Centrafrique, "Centrafrique : Les principaux chefs de la rébellion contestés par leur base," 28 February 2013; Radio Ndéké Luka, "Ndjotodia sensibilise ses troupes pour leur cantonnement," 22 February 2013.
[9] RJDH-RCA, "Sido: Plus de 4 000 déplacés centrafricains enregistrés au Tchad," 5 March 2013.
[10] RFI, "RCA: scission de la Séléka et reprise des hostilités," 1 March 2013.
[11] Xinhua, "Centrafrique : Séléka rejette la responsabilité de l'attaque contre Sido, une localité du Nord," Centrafrique-Presse, 4 March 2013; Séléka, "Centrafrique: Seleka Communiqué de Presse 005/SG/08/03/13," Afrique News Info, 8 March 2013.
[12] Vincent Duhem, "Centrafrique : des éléments de la Séléka attaquent deux villes," Jeune Afrique,11 March 2013.
[13] Agence-France Presse and Journal de Bangui, "Centrafrique: La ville de Rafaï dans la tourmente," 13 March 2013.
[14] Séléka, "Centrafrique : Séléka rejette la responsabilité de l'attaque contre Sido, une localité du Nord," Centrafrique-Presse, 2 March 2013.
[15] RFI, "RCA: la rébellion exige le départ pur et simple du président Bozizé," 21 March 2013.
[16] Séléka, "Déclaration de la Coalition Séléka No_037/SG/RCA/20/03/13," Centrafrique-Presse, 20 March 2013.
[17] Pacôme Pabandji, "Centrafrique : Probables affrontements en cours à Bouca," Nouvelle Centrafrique, 21 March 2013; Nouvelle Centrafrique. "Centrafrique: La Seleka en Plein Deploiement." 21 March 2013.
[18] Gaëtan Barralon, "Centrafrique: les rebelles de la Séléka approchent de Bangui," 45e Nord, 22 March 2013.

TRADOC G2 THREAT Resources on Army Training Network



HAMAS: CONTINUING CONFLICT WITH ISREAL

by Steffany A. Trofino, TRISA-CTID (DAC)

On 12 June 2014, three Israeli teenagers were kidnapped in Gush Etzion, in the West Bank, as they were hitchhiking on their way home from school. One of the victims, Gilad Shaer, used his cell phone to call a police emergency hotline and told authorities he had been kidnapped along with two of his friends. The official heard Arabic shouting in the background and automatic gunfire before the call went dead. Israeli Defense Forces (IDF) launched Operation Brother's Keeper in search of the teens. During the 11-day operation, five Palestinians were killed, increasing tensions throughout the region. In addition to the five fatalities, IDF arrested nearly 350 Palestinians, including most of HAMAS' West Bank leaders. On 15 June 2014, Israeli Prime Minister Benjamin Netanyahu stated the teens had been kidnapped by HAMAS, which HAMAS promptly denied.[1] On 30 June, a search team located the three teens, bound and deceased, in an open field near Khirbet Aranava in the Wadi Tellem area of the West Bank.

In retaliation, on 2 July 2014, 16 year old Mohamed Abu Khdeir—a Palestinian living in East Jerusalem—was kidnapped outside his home. Israeli police found his burned body in a secluded forest later that evening. Three Israelis were charged with his murder.

Reacting to Abu Khdeir's murder, between 3 and 5 July 2014, 72 rockets and mortars were fired into Israel from Gaza, resulting in property damage but no fatalities. In response, on 6 July Israel launched a full-scale air assault into Gaza, specifically targeting and killing nine HAMAS leaders in the Khan Younis region. On 7 July, HAMAS launched several rockets into Israel, claiming full responsibility and publically stating that all Israelis had now become legitimate targets of HAMAS.[2]

Figure 1. Map of Israel depicting Gaza Strip and the West Bank
(Source National Counterterrorism Center, 2014)

As a result of the escalation of tensions, on 8 July Israel officially launched Operation Protective Edge, with the specific objective of militarily neutralizing HAMAS' capabilities to launch strikes against the State of Israel. This operation included targeting HAMAS' tunnel network throughout Gaza and stretching into Israeli territory. The group uses the network to target Israel and to transport needed supplies and weapons within the barricaded enclave.

HAMAS is identified by the US Department of State as a foreign terrorist organization. This article will describe some of the history and recent conflict between HAMAS and Israel as a framework for viewing the weapons and capabilities of HAMAS.

HAMAS' High-Value Targets Attacked

With the onset of Operation Protective Edge, a series of air strikes initially focused on high-value targets inside Gaza. The first phase of the operation concentrated on known HAMAS rocket launch sites, weapons storage facilities, and the organization's command and control (C2) elements.[3] The 50 sites initially targeted included several homes belonging to HAMAS officials, three known militant compounds, 18 concealed rocket launchers, and specific infrastructure sites, all of

which were destroyed.[4] In response, HAMAS launched a volley of rockets into Israel, escalating tensions in the region. Over the course of a nine-day period leading up to Israel's ground offensive, both Israel and HAMAS launched multiple air strikes against each other. By the evening of 16 July 2014, 2,053 strikes had been launched by the IDF against HAMAS militants, resulting in 241 Palestinian fatalities. By that time Israel had incurred 1,436 rockets launched into its territory, resulting in one fatality.[5]

During the early morning of 17 July 2014, thirteen HAMAS militants used a tunnel to infiltrate Israeli territory near the city of Sufa, in close proximity to an Israeli kibbutz. Israeli forces were able to stop the militants as they exited the tunnel shaft. As a result of this incident, IDF began preparations to launch a ground offensive into Gaza with the military objective of neutralizing Gaza tunnels and degrading HAMAS' capabilities to target and strike Israeli soldiers and citizens.

During the afternoon of 17 July 2014, IDF began dropping leaflets in various cities throughout the north and south of Gaza, warning Palestinians to seek shelter in the larger urban centers of Gaza City, Khan Younis, and Rafah.[6] As night fell, Israeli forces cut the electrical power in large areas of the north and Gaza City, in preparation of the first phase of the ground operation. The offensive began with air, sea, and tank bombardments striking targets on a band of northern coastal areas including the cities of Sudaniya, Attatra, Salateen, Beit Lahia, and Jabaliya. Later in the evening, IDF began striking targets in the southern regions of Khan Younis and Rafah.

At 2200 local time, Israeli tanks, infantry, and engineer units entered Gaza, formally launching the first ground offensive into the region in five years.[7] Specific units used by IDF during the assault included infantry, armored corps, engineer corps, artillery, and intelligence units. Detailed information describing the Israeli order of battle, beyond what is reported here, is unavailable via open sources at this time.

IDF officials recalled 48,000 reserve soldiers to active duty prior to the ground operation and authorized an additional 18,000 reservists, if needed. During the initial hours of the operation, 11 Palestinians and one Israeli soldier were killed. Ending its ground operation in Gaza the week of 4 August 2014, Israeli officials declared it tactically successful in neutralizing all known tunnels originating in Gaza and terminating in Israeli territory.[8]

Tactics and Techniques Used by HAMAS

HAMAS' Use of Human Shields

Though no fatalities were reported on the first day of Operation Protective Edge, three weeks into the campaign Gaza representatives stated that 797 Palestinians had been killed and an additional 5,100 civilians injured. The Israeli government claimed 32 Israeli soldiers had been killed along with three civilians during this same time period.[9] In addition to the fatalities, by 24 June 2014, Israel had targeted three UN schools in Gaza that provided shelter to Palestinian refugees. IDF representatives indicated the UN buildings were being used to conceal militants and store weapons, suggesting HAMAS was using the tactic of human shields to mask militant activity. Upon investigation, UN representatives found large stockpiles of weapons in three of its facilities, which it promptly condemned.[10] Israeli officials state that it is common practice for HAMAS to use human shields to mask terrorist activity; they further indicate that not only are UN schools used to store weapons, but mosques and hospitals are as well.[11]

HAMAS' use of Tunnels

During the mid-1990s, Israel blockaded Gaza when it built the Gaza/Israel wall, isolating Gaza completely. This was in response to the multiple suicide attacks Israel incurred during the mid-1990s, which killed several Israelis. Israel blamed HAMAS for the attacks. In an effort to control goods and services traveling into or out of Gaza that may be used against Israeli citizens, the wall was built to barricade the enclave. Through the use of checkpoints, the Israelis permitted goods and services to flow into and out of Gaza.

Adapting to the blockade, Palestinians developed an extensive network of underground tunnels along the edge of the Israeli/Egyptian border. Originally the tunnels were used to smuggle weapons and needed supplies into the barricaded enclave. However, in more recent years the tunnels were also used to target and kidnap Israeli soldiers. Today, the most prevalent and persistent tactic HAMAS employs against Israel is its use of this tunnel network.

HAMAS utilizes three types of tunnels: defensive tunnels used as command centers and for weapons storage; offensive tunnels used to infiltrate Israeli territory, targeting and attacking Israeli soldiers and citizens; and smuggling tunnels that run into Egypt and are used to transport supplies, personnel, and currency into the barricaded enclave. The network of tunnels is extensive, and, contains multiple entrances and exits, though the tunnels are not of a uniform construction. Some have electricity, ventilation, and concrete walls, while others have dirt walls braced with wood beams.

The significance of a tunnel to HAMAS' operations may be gauged by the manner in which it has been constructed, as many vary in degree of sophistication. For example, if a tunnel is fortified with concrete or equipped with electricity and ventilation, this may indicate it is used to protect something of significant value, such as weapons or personnel. If it appears relatively crude in design with simple dirt walls and timber, it may be used to transfer dry goods or supplies, but not necessarily to protect personnel or weapons.

Israel's main effort during Operation Protective Edge focused on destroying HAMAS' offensive tunnels. While these were not the only targets (as IDF officials also targeted HAMAS' capability to launch rockets into Israel), offensive tunnels remained a primary focal point of IDF ground operations. Israeli officials indicate they have identified 32 to 35 offensive tunnels. Though more than half have been destroyed, it is believed that several tunnels still remain undiscovered.[12]

Many of the tunnels originate inside covered, protected structures such as home basements, schools, or hospitals. Additionally, foliage and creative landscaping provide natural camouflage for tunnel entrances, as shown in Figure 2.

On 16 June 2013, Egyptian President Abdel Fattah el-Sisi ordered that all known tunnels running from Egypt into Gaza be sealed, ultimately shutting off this vital supply link to HAMAS. In early September 2013, the Egyptian military began shuttering a dozen known tunnels along its border with Gaza.[13] This, however, has not closed all tunnels, as there may still be several operating covertly, allowing smuggling of weapons and needed supplies into the enclave.

HAMAS' weapon smuggling routes

As the only country (other than Israel) that shares a contiguous land border with Gaza, Egypt has been the primary transport link HAMAS relies on to smuggle needed weapons and supplies into the Palestinian enclave. Gaza's only seaport is the Port of Gaza, located in Gaza city. With only one pier, it is quite small compared with other international shipping ports. After HAMAS became the ruling power in Gaza, the Israeli Navy imposed a naval blockade of the port, and used inspections as a pretext for diverting international ships. As a result, HAMAS' smuggling routes are limited.

On 2 March 2014, the Israeli Navy intercepted the Klos-C cargo ship carrying 40 Syrian-manufactured M-302 rockets intended for delivery in Gaza.[14] Originating in Syria, the rockets were first flown to Iran. Once inside Iran, they were shipped from Bandar Abbas sea port to Port Sudan, located on the border of Eritrea and Sudan in the Red Sea. Had the ship not been intercepted prior to entering Port Sudan, the rockets could have been unloaded, taken by land through Egypt into Sinai, and from there smuggled into Gaza through tunnels. Israeli officials state this is a commonly known route.[15] Though speculative as to which route the weapons would have traveled to enter Gaza, public mention of this known route suggests that some Egyptian tunnels may still be in use, as the incident occurred after Egypt's declaration that all known tunnels had been sealed. Thus, some links to Gaza from Egypt may remain active.

Sudan has become another suspected support link to HAMAS. On 18 July 2014, a warehouse at a military base north of Khartoum exploded. Sudanese officials stated the warehouse caught fire with ammunition inside, which caused the explosions. However, there were reports that Israel struck the warehouse, believing the government of Sudan was storing Sudanese-manufactured weapons inside the facility with the intent to transfer them to HAMAS in the Gaza Strip.[16] Rumors circulating inside Sudan indicate that Israeli officials believe Sudanese-manufactured weapons are currently being used by HAMAS against Israel from the Gaza Strip, though specifics as to weapon types remain unknown at this time.[17]

HAMAS' use of Kidnapping

Kidnapping is another effective tactic HAMAS uses against Israel. Once an Israeli is kidnapped, the victim becomes a bargaining chip in negotiations to trade for Palestinians who have been taken into custody by Israeli officials. The fate of IDF Sergeant Major Gilat Shalit provides a significant case-in-point.

On 25 June 2006, members of HAMAS infiltrated Israel near Kerem Shalom via an underground tunnel and attacked a nearby IDF post, killing two Israeli soldiers. Gilat Shalit, the only IDF survivor of the attack, was captured and taken through the tunnels to Gaza. He remained in HAMAS' custody for over five years. On 11 October 2011, a deal was struck between HAMAS and Israel, reached mainly through Egyptian mediation. Shalit was released in exchange for Israel's release of 1,027 Palestinians held inside Israeli prisons.

Figure 2. HAMAS tunnel for kidnapping

The most recent kidnapping of an Israeli soldier took place 1 August 2014 near the city of Rafah, Gaza. Early that morning, Israeli Forces moved in on a home identified as an entry point of a tunnel leading into Israel. As IDF moved in, a HAMAS militant exited a tunnel and opened fire, killing two IDF soldiers and capturing a third, Lieutenant Hadar Goldin. It is unclear whether Goldin was captured alive or dead.

This prompted Israel to enact a measure referred to as the Hannibal Directive: bombarding the last-known location of personnel in an attempt to stop militants from kidnapping the soldier.[18] A week later, Israeli officials stated Goldin was deceased though they did not indicate whether he was killed during the initial phases of Israeli bombardment, or killed after being captured.

Recent seizures of HAMAS tunnels by Israeli Forces have uncovered large bags, handcuffs, and tranquilizer guns that officials claim are used by HAMAS operatives during kidnapping attempts.[19] Recognizing the effectiveness of kidnapping, HAMAS continues to implement this strategy to achieve its objectives.

HAMAS' Weapons

HAMAS' Projectile Arsenal

Over the years, HAMAS' stockpile of projectiles has steadily increased in range, the majority of which are based on tier-two, Soviet-era technology. While HAMAS has relied on smuggled weapons through its extensive network of underground tunnels, it does possess the capability to indigenously manufacture smaller, short-range rockets using facilities throughout Gaza, though parts and components may still need to be smuggled into the enclave. With Egypt taking a more hardline approach to sealing known tunnels running from Gaza into Egypt, the replenishing of HAMAS' weapons used against Israel may become increasingly more challenging.

On 8 July 2014, HAMAS launched a long-range rocket for the first time, which landed outside the city of Hadra, almost 113 km from the Gaza Strip and twice the distance to Tel Aviv. On 9 July, HAMAS again launched a long-range rocket, this time targeting the northern area of Zichron Yaakov, 19 km north of Hadra.[20]

The current stockpile of weapons HAMAS has been using against Israel varies but can be divided into four categories: Mortars that can travel up to 7 kilometers; short-range rockets (up to 20 km); medium-range rockets (up to 80 km); and long-range rockets (up to 160 km).[21]

Mortars

Typical HAMAS heavy mortars are indigenously manufactured in Gaza with a range up to 9.3km.[22] For HAMAS, mortars are tactically significant as they are immune to Israel's Iron Dome air defense system. The vulnerability of the weapon is its limited range. At less than 10 km, mortars need to be placed in close proximity to Gaza borders for optimal reach into Israel. This renders the weapon vulnerable to ground forces. Mortars are, however, highly mobile and require little time or knowledge in deploying them against designated targets.

Short-Range Rockets

Short-range rockets in HAMAS' arsenal include the Qassam and Grad rockets with ranges of 17 and 20 km, respectively. Upgraded versions of the Grad are capable of extending the range up to 40 km. Additionally, there are several types of the Qassam missile, which include the one, two, and three variants. Both the Qassam and Grad rockets primarily threaten the southern Israeli cities of Ashkelon, Sderot, Beersheba, and the Israeli port of Ashdod, as all are within the weapon systems' ranges. The Qassam rocket is an indigenously-manufactured steel rocket developed by the al-Qassam Brigades.

Figure 3. Rocket ranges

Increasing HAMAS' short-range capabilities, the Iranian- and Chinese-manufactured Grad rocket enables greater range between 20 and 40 km (depending on if an upgraded variant is used) with a payload weight of 18 kilograms.[23] Distances and payload weight may vary based primarily on how HAMAS modifies the weapon. While both the Qassam and Grad are classified as short-range, neither rocket is precise or holds specific targeting capability, rendering both unpredictable when deployed. As such, the weapons are considered problematic and remain a viable threat to the southern periphery of Israeli territory.

Medium-Range Rockets

Significantly improving the lethality and range capabilities of the Grad rocket, an upgraded variant HAMAS is known to possess is the Chinese-manufactured WS-1E, a variant of the Chinese Weishi multiple rocket launcher systems. The WS-1E is claimed to have a range of 45 km with an expanded warhead of 22 kilograms, which increases the weapon's lethality from that of its predecessor. At the onset of Operation Protective Edge, HAMAS was suspected of having an estimated 1,200 WS-1E; it is thought 80% of these weapons were smuggled into the enclave from abroad.[24]

Long-Range Rockets

The most significant observations IDF officials made during Operation Protect Edge were advancements to HAMAS' long-range rocket arsenal. True capabilities of an adversary are never known with any specific degree of accuracy until weapons are used against opposing forces during times of war. HAMAS' first use of the suspected long-range M-302 on 8 July 2014 was a significant increased threat to Israel, as the weapon nearly doubled the range of HAMAS' previously-known long-range rocket, the Fajr-5.

The Fajr-5 is a 333-mm Iranian-manufactured rocket with a maximum range of 75 km utilizing a 90 kg warhead. During the Gaza/Israel conflict of 2012, a Fajr-5 rocket was reportedly deployed toward Tel Aviv for the first time.[25] While IDF officials indicated at the time that they militarily destroyed all known weapon caches of Fajr-5 missiles, they did not indicate how the missile was smuggled into the blockaded enclave. It is known that the system was proliferated to Lebanon from Iran, but definitive links of the transfer from either Iran or Lebanon into the enclave remain speculative. Also proliferated to Lebanon was the Syrian-manufactured M-302 that is a variant of the Chinese designed W-1. However, with Israel's interception of the Klos-C cargo ship in March 2014 carrying 40 Syrian-manufactured M-302s onboard and reportedly bound for Gaza, it was believed that the M-302 threat posed by HAMAS had been neutralized. With the suspected M-302 landing outside Hadra on 8 July, this may not be the case.

The M-302, also referred to as Khaibar-1, is the Syrian-manufactured variant of the more sophisticated Chinese W-1 and was first used by Hezbollah against Israel in 2006. The M-302 rocket has a maximum reported range of 100km, though modified versions may provide enhanced range capabilities.[26] Additionally, the weapon has a payload weight of up to 175 kg.[27]

Taking into account all rocket capabilities HAMAS currently possesses, none have advanced guidance systems or target acquisition capabilities. Due to the blockade of the enclave, most rockets are suspected of being indigenously manufactured inside Gaza using smuggled parts.

Training Implications

- When fighting against a larger, better-equipped force, opposing forces will revert to hybrid threat tactics such as the use of kidnapping to gain an advantage.
- Large military land forces are not always necessary to achieve quick results across fairly short distances. Small groups of well-trained soldiers can sometimes be just as effective.
- Weapon caches can always be hidden in public facilities such as hospitals, schools, or mosques.

Notes

[1] Tohav Lazaroff and Yaakov Lappin, "Netanyahu blames HAMAS for the kidnapping of the three Israeli teens," The Jerusalem Post, 15 June 2014.
[2] Khaled Abu Toameh, "HAMAS: All Israelis now targets for missile attacks," *The Jerusalem Post*, 8 July 2014.
[3] Jonathan Marcus, "What weapons are being used in the Israel-Gaza conflict," *BBC News*, 10 July 2014.
[4] "Operation Protective Edge: Israel bombs Gaza in retaliation for rockets," *The Guardian*, 8 July 2014.
[5] Karen Yourish and Josh Keller, "The Toll in Gaza and Israel, Day by Day," *The New York Times*, 8 August 2014.
[6] Jodi Rudoren, and Anne Barnard, "Israeli Military Invades Gaza, With Sights Set on HAMAS Operations," The New York Times, 18 July 2014.
[7] Peter Beaumont, "Israeli forces enter Gaza in ground assault after ceasefire talks fail," *The Guardian*, 17 July 2014.
[8] Janine Zacharia, "Tunnel mapping could have neutralized HAMAS threat without fatalities," *The Washington Post,* 11 August 2014.
[9] Karl Penhaul, Ed Payne, and Ashley Fantz, "U.N. shelter in Gaza hit, 16 dead," *CNN*, 24 July 2014.
[10] Terrence McCoy, "Why HAMAS stores its weapons inside hospitals, mosques and schools," *The Washington Post,* 31 July 2014.
[11] Anne Barnard and Jodi Rudoren, "Israel Says That HAMAS Uses Civilian Shields, Reviving Debate," *The New York Times,* 23 July 2014.
[12] Harriet Sherwood, "Inside the tunnels HAMAS built: Israel's struggle against new tactic in Gaza war," *The Guardian,* 2 August 2014.
[13] William Booth and Abigail Hauslohner, "Egypt shutting economic lifeline for Gaza Strip, in move to isolate HAMAS," *The Washington Post*, 8 September 2013.
[14] Yaakov Lappin, "Final inventory of Iran arms ship: 40 rockets, 180 mortars, 400,000 bullets," *The Jerusalem Post*, 9 March 2014.
[15] Yaakov Lappin, "Israel Navy intercepts Gaza-bound Iranian rocket ship near Port Sudan," *The Jerusalem Post*, 3 May 2014.
[16] Roi Kais," Report: IAF struck Sudan weapons stockpile headed for HAMAS," *Ynetnews*, July 21, 2014.
[17] "Sudan taking precautions against possible Israeli strike: spokesman," *Sudan Tribune*, 5 August 2014.
[18] Ruth Margalit, "Hadar Goldin and the Hannibal Directive," *The New Yorker*, 6 August 2014.
[19] Sudarsan Raghavan, William Booth and Ruth Eglash, "HAMAS shows resilience in face of Israeli ground incursion," *The Washington Post*, 19 July 2014.
[20] Christa Case Bryant, "HAMAS unveils bigger, better rocket arsenal against Israel," 9 July 2014.
[21] David Morgenstern, "Gaza's Arsenal," Military Periscope, 8 August 2014.
[22] David Morgenstern, "Gaza's Arsenal," Military Periscope, 8 August 2014.
[23] Jeremy Bender, "These Are The Rockets HAMAS Has Been Shooting At Israel," *Business Insider*, 10 July 2014.
[24] David Morgenstern, "Gaza's Arsenal," Military Periscope, 8 August 2014.
[25] Ian Black, "Fajr-5 missile gives Palestinians rare if short-lived advantage," *The Guardian*, 16 November 2012.
[26] Yaakov Katz, "'Hezbollah has long-range surface-to-air missiles," *The Jerusalem Post*, 19 January 2012.
[27] Mark Perry, "Gaza's Bottle Rockets," Foreign Affairs, 3 August 2014.

POTENTIAL FOR OVERMATCH: ANTI-ACCESS/AREA DENIAL

by Walter L. Williams, TRISA-CTID (DAC)

Potential US adversaries or hybrid threat forces may employ various conventional or unconventional strategies or operational tactics to challenge the US and/or their coalition partners conducting military operations in response to threatened US security and vital interests. There are five characteristics of a future operational environment that are likely to have significant impact on land force operations:

- Increased velocity and momentum of human interaction and events
- Potential for overmatch
- Proliferation of weapons of mass destruction
- Spread of advanced cyberspace and counter-space capabilities
- Demographics and operations among populations, in cities, and in complex terrain

This article briefly discusses an aspect of the second characteristic, potential for overmatch. Anti-access/area denial (A2AD) is an aspect of potential for overmatch in which an adversary establishes control and dominance in a specific area and denies an opponent the ability to conduct operations in that area. The hybrid threat doctrine refers to this concept as access limitation. However, for this article the term A2AD is used for ease of understanding and consistency.

A2AD is not a new concept and it includes the domains of air, sea, land, space, and the relatively new dimension of cyber. A2AD operations can be employed at the strategic, operational, and tactical levels. For example, at the strategic level, the hybrid threat may employ diplomatic or economic initiatives in their engagement of a sympathetic country to deny overflight or forward deployed sea and air basing rights. The strategic goal is to force US forces to conduct combat and logistical operations from distant bases. Table 1 provides a quick overview of a hybrid threat's A2AD mission or task, objectives, and targets that a US brigade combat team (BCT) may encounter during a combat training center (CTC) rotation or home station training (HST) event.

Table 1. A2AD Mission or Task, Objectives, and Targets

Hybrid Threat Anti-Access/Area Denial Operations		
Mission or Task	**Objectives**	**Targets**
Deception or to deceive	Mislead enemy decision makers Cause confusion and delays in the decision-making process Persuade the local population and/or international community to support hybrid threat objectives	Key military decisionmakers General population and international media sources and Internet sites
Disrupt or deny intelligence, surveillance, and reconnaissance	Exploit, disrupt, deny, and degrade the BCT's use of the electromagnetic spectrum	C2 and RISTA assets and networks.
Disrupt or destroy mission command and other network systems	Exploit, disrupt, deny, and degrade the BCT enemy's use of the electromagnetic spectrum	C2 nodes and links, RISTA assets, telecommunications, and power sources
Protection and security measures against an attack	Protect critical friendly assets	Attack enemy RISTA to include ground based space control centers or assets
Disruption of US airfields and forward area refuel rearm points (FARRPS)	Degrade or destroy US capability to conduct fixed wing and/or rotary wing air refueling and rearming operations	Attack enemy RISTA to include ground based space control centers or assets
Disruption of US sea and river approaches	Degrade or destroy US capability to conduct riverine and amphibious operations (to include logistics)	Attack coastal facilities, personnel, and naval vessels

At the operational to tactical level, a hybrid threat may employ capabilities or weapons systems such as cruise missiles, cyber attacks, air defense systems, or unmanned aerial vehicles (UAVs). Regardless of the level of operation, the hybrid threat seeks to use the operational variable of time to set favorable conditions for their conventional forces to remain on par with US or coalition forces, selectively disrupt or destroy enemy forces, or to simply survive to fight another day.

A2AD Weapon Systems and Technologies

The hybrid threat uses the technique of identifying critical weapon or mission command system components and attack to either degrade or destroy their use or importance of the system. This is commonly referred to as a systems approach to combat. The hybrid threat use of the systems approach to combat during A2AD operations can lead to the desired end state of either disrupting or destroying key components of a BCT combat system. Ideally, the hybrid threat uses niche weapons such as precision-guided munitions and electronic warfare capabilities combined with simple tactics to disaggregate enemy combat systems. Artillery-delivered high precision munitions such as the 152/155-mm Krasnopol laser-guided projectile can be used to attack stationary rotary and fixed wing aircraft on airfields and FARRPS. They can also be used to attack pilot and crew billeting facilities as a method of disaggregating an aircraft combat system.

Figure 1. Aviaconversia, GNSS jamming transmitter

At the tactical level, a BCT can expect the hybrid threat to apply electronic warfare capabilities to exploit, deceive, degrade, disrupt, damage, or destroy sensors, processors, communications, and command and control (C2) nodes. Global positioning system (GPS) jammers such as the Russian Aviaconversia, GNSS Jamming Transmitter (figure 1) and the Belarusian Optima-3, GNSS Jamming Complex are designed to affect the enemy's capability to exercise C2 as well as conduct maneuver and fire support activities. The use of the GPS jammer can force a maneuver unit to use traditional navigation techniques, thus slowing their mobility. In certain cases, jammers may affect high-precision munitions.

Radio jamming operations can be conducted in various means that can range from ground vehicle and airborne mounted platforms to artillery delivered (cannon projectile and rockets). For example, the Bulgarian artillery projectile, Starshel, is advertised in three different calibers—122-mm, 152-mm, and 155-mm. The projectile has two different spellings that denote two different Bulgarian manufacturers. Samel 90 uses the spelling Starshel while Kintex uses the spelling Sturshel. Recent marketing literature claims the jammer is capable of jamming both fixed and frequency hopping radios. Table 2 provides an overview of the projectile's parametric data.

Table 2. Bulgarian 152-mm RF Projectile

Parametric Data	
Jamming Frequency	1.5 to 120mhz (HF/VHF)
Number of sub bands	8
Jammer operation range	Approximately 700 meters
Jammer operation time	60 ± 5 minutes
Operating Temperature Range	-40° to +50° C
Type of Battery	Lithium
Jammer Shelf Life	10 years
Projectile Range	16.5 km (with full charge) 11.5 km (with reduced charge)

While weapon systems and capabilities such as sophisticated information warfare exist, the hybrid threat retains the capability to employ low-tech yet highly effective techniques such as the employment of smoke or obscurants extensively in an operational environment (as the situation permits) to make it difficult for an enemy to conduct

observation, determine the true position of hybrid threat forces, and conduct fires (including precision weapon fires) or air attacks. The presence of toxic smoke may cause the enemy to use chemical protection systems, thus lowering their effectiveness, even if the hybrid threat is using only neutral smoke. For example, during Operation Desert Storm, Iraqi forces set fire to some of their oil fields that in turn provided cover of their forces and slowed down the advancing coalition forces. In essence, the use of fire to produce obscuration (such as forest fires, burning of tires, setting fire to buildings, etc.) has the potential to slow or delay the advance or movement of a BCT.

Another technique is the flooding of areas (due to the destruction of dams, canal locks, dikes) to deny or limit the freedom of maneuver. For example, the Germans flooded selected areas of Normandy prior to D-Day to deny allied airborne forces suitable landing zones for gliders and drop zones for paratroopers. The end result was a limitation of suitable areas for allied forces to conduct logistical resupply or reinforcement using cargo aircraft and gliders. Additionally, the flooding canalized advancing allied armor and mechanized forces to road networks that either slowed their advance or set the conditions for German defensive kill zones. More information regarding the tactics that could be employed by a hybrid threat may be found in TC 7-100.2, *Opposing Force Tactics* Chapter 7, Information Warfare and Chapter 13, CBRN and Smoke.

Training

The replication of A2AD within a given training or education environment depends on many factors such as the type of simulation—live, virtual, constructive, integrated architecture (L-V-C-IA). Regardless of the type of simulation, it is important for trainers or training developers to develop scenarios or vignettes that offer the training audience complex problem sets. The trainer should always consider the OPFOR representing a hybrid threat to be uncooperative, adaptable, and creative in the conduct of a training environment. It just is not a simple matter of designating a geographical area that denies a unit the ability to conduct maneuver operations. It is critical to replicate as many variables within the stated conditions that are reasonable, feasible, and plausible to challenge leaders and their subordinates to provide solutions to overcome the effects of A2AD. This may involve the use of media injects to paint a less than favorable impression of military operations, limitations on the use of digital systems due to sunspots, denial of bandwidth by the host country, or changes to rules of engagement (ROE) for a deployed force. While some of the conditions may be beyond the capability of a BCT to effect change, they drive leaders to conduct critical thinking to rapidly adapt their military operations to the changes with a given operational environment.

The OPFOR, when representing a hybrid threat, must be a challenging, uncooperative adversary or enemy. It must capable of stressing any or all warfighting functions and mission-essential tasks of the US armed force being trained. Training for the challenges of contemporary operational environments requires an OPFOR that is "a plausible, flexible military and/or paramilitary force representing a composite of varying capabilities of actual worldwide forces, used in lieu of a specific threat force, for training and developing US forces"

AR 350-2, *Opposing Force (OPFOR) Program*

Conclusion

The overall objective or end state of A2AD operations is to limit, delay, or deny the US and its coalition partners' freedom of maneuver and/or dominance in a specified area within a given operational environment. The hybrid threat will use various methods or techniques from strategic to tactical level to create favorable conditions against a technologically superior force to achieve their overarching goals or objectives. Whether the hybrid threat's goal is to limit the freedom of maneuver and/or dominance in a given area, for example, the challenge for a US BCT is to develop sound techniques and procedures to negate the A2AD effects and remain effective through their assigned operational mission.

References

Foster, Harry. The Joint Stealth Task Force: An Operational Concept for Air-Sea Battle National Defense University Press. 1 January 2014

Headquarters, Department of the Army. TC 7-100, Hybrid Threat. TRADOC G2 Intelligence Support Activity (TRISA)-Threats. November 2010.

Headquarters, Department of the Army. TC 7-100.2, Opposing Force Tactics. TRADOC G2 Intelligence Support Activity (TRISA)-Threats. December 2011.

Headquarters, Department of the Army. Worldwide Equipment Guide 2013 Volume 1: Ground Systems. TRADOC G2 Intelligence Support Activity (TRISA)-Threats. August 2013.

Scott, Chris. "Anti-Access Area -Denial (A2AD) in Military Domains and in Cyberspace". CTO Vision.com. 12 December 2012.

Wilgenbusch, Ronald C. and Alan Heisig. "Command and Control Vulnerabilities to Communications Jamming." Joint Force Quarterly. Issue 69, 2nd Quarter2013.

Counterreconnaissance: Threat Actions for Tactical Success

by Jon H. Moilanen, TRISA-CTID (Ctr BMA) **Part 1 of 2 Parts**

For threat forces, an essential component of military action is counterreconnaissance in order to deprive the enemy of information and intelligence, and facilitate successful threat operations. Threat reconnaissance actions represent all measures in organizing, collecting, and studying information of an operational environment (OE) in areas of current and/or future operations. The companion of creating and verifying intelligence about an enemy of the threat is all measures employed to protect threat forces. Aggressive and continuous *counterreconnaissance* is a fundamental principle of maintaining the initiative in threat military decisionmaking and mission success while protecting the force.

Counterreconnaissance
A continuous combined arms action to locate, track, and destroy all enemy reconnaissance operating in a given area of responsibility.
TC 7-100.2

US Army missions for the foreseeable future will often occur in complex OEs with dynamic and uncertain circumstances, and enemies and adversaries with the ability to adapt and counter the advantages of a sophisticated land power opponent. Recognition of an adaptable threat and its demonstrated capabilities can be visualized in a number of organizational configurations for US Army training. Assuming just one type of threat to plan and train against is a shallow understanding of history, contemporary conditions, and practical expectations for the future. Whether engaged in combined arms maneuver and/or wide area security missions, winning the counterreconnaissance (CR) fight is crucial to overarching mission success.

Counterreconnaissance and the Threat

The opposing force (OPFOR) for US Army training recognizes the value of counterreconnaissance and employs a very deliberate approach to planning and conducting CR tasks. The OPFOR conducts CR at all times and during all types of operations. The OPFOR understands the role of situational awareness and understanding in operations and will dedicate significant resources to a continuous CR mission.

The *Opposing Force (OPFOR) Program* (AR 350-2) defines the opposing force concept within an OE framework and describes various uses of opposing forces in Army training, leader development, and capabilities development events. An OPFOR is a plausible, flexible military and/or paramilitary force representing a composite of varying capabilities of actual worldwide forces (doctrine, tactics, organization, and equipment) used in lieu of a specific threat force for training and developing US forces.[1] The OPFOR can represent a particular threat, hybrid threat, and/or an adversary that can morph in capabilities and influence within a relevant population.

The US Army Training Circular (TC) 7-100 series, and opposing force (OPFOR) field manuals in transition to the TC 7-100 series are the source for threats and hybrid threats for Army training, professional education, and leader development. In CR missions, the threat commander determines enemy reconnaissance assets to be destroyed in accordance within a

higher commander's guidance. Threat tactics and techniques are based on a composite of enemy and adversary actions observed and/or experienced in recent or contemporary operations.

Threat

Any combination of actors, entities, or forces that have the capability and intent to harm United States forces, United States national interests, or the homeland.

ADRP 3-0, *Unified Land Operations*

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*

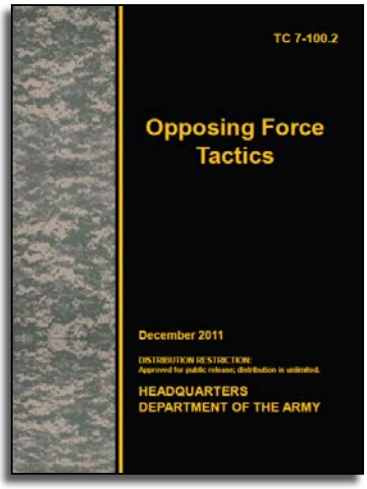
Adversary

A party acknowledged as potentially hostile to a friendly party and against which the use of force may be envisaged.

JP 3-0, *Joint Operations*

Tactical execution of threat tasks is robust and realistic to the training conditions required by the US commander or leader to effectively evaluate unit or activity readiness. Whether focused on CR or other tactical functions, the fundamental references for threat tactics in US Army training are TC 7-100.2 and additional irregular forces tactics and techniques in TC 7-100.3.

Combined Arms Capabilities



At the lower tactical echelons of regular forces—battalion and company—threat organization of combat power is typically tailored based on mission requirements. When task-organized to accomplish mission tasks and designated functions, a threat battalion or company is a combined arms organization designated a *detachment.*

Detachments based on battalion structure are typically termed battalion-size detachments (BDETs), and those organizations formed from company structure are termed company-size detachments (CDETs). In a counterreconnaissance mission, the detachment at battalion and company level use CRD as the counterreconnaissance acronym.

Some reconnaissance assets in threat force structure, such as a reconnaissance battalion of a mechanized infantry division, use the term *reconnaissance unit* for the unit rather than a detachment-term identifier. Reconnaissance units are organic to a table of organization and equipment (TOE) of the threat force structure that form the basis of a given unit.

The allocation of elements to a CRD is mission focused by functions that are expected to be conducted in the counterreconnaissance. Threat CRD command and control (C2) is an adaptive and flexible means to direct actions and functions, and embraces principles of mission, aggressive initiative, prudent risk-taking, and accurate and timely information and intelligence toward achieving mission purpose and intent. Types of CRD will vary significantly dependent on the mission and the known or expected adversary or enemy in an operational environment (OE).

Based on the echelon of threat unit involved, the term *force* identifies units at brigade level and higher organization, and the term *element* for battalion and lower echelon units. The CRD is primarily composed of constituent and dedicated units within a battalion or company task organization. *Constituent* is a C2 relationship based on the TOE of the force structure forming the basis of a given unit, assigned at the time the unit was created, or attached to it after its formation. *Dedicated* is a command relationship identical to constituent with the exception that a dedicated unit still receives logistics support from a parent headquarters of similar type.

However, supporting command and/or support relationships may be necessary to bring specialized capabilities to bear for limited periods of time. For example, when countering enemy mechanized forces, a baseline mechanized or motorized CRD task organization could typically include—

- Reconnaissance.
- Infantry.
- Armor.
- Artillery and/or mortars.
- Air defense.
- Engineers.
- Maintenance.
- Logistics.
- Medical.
- Signal.

Examples of specialty support capabilities based on mission analysis can include—

- Special purpose forces (SPF).
- Flame weapons.
- Antitank weapons.
- Guided missiles.
- Information warfare (INFOWAR) electronic warfare.
- Signals reconnaissance assets.
- Chemical, biological, radiological, and nuclear (CBRN) and smoke.
- Unmanned aerial vehicles (UAVs).
- Rotary-wing aircraft.
- Fixed-wing aircraft.
- Elements from joint, combined, or other intergovernmental activities.

Nonmilitary or paramilitary groups can be a*ffiliated* with a CRD. No command relationship exists between an affiliated organization and a detachment operating in the same area of responsibility (AOR). Cooperation between or among organizations is based on mutual temporary agreement as the norm. Affiliation to a CRD can include but is not limited to—

- Guerrilla units.
- Insurgent organizations.
- Criminal organizations.
- Active supporters, willing and/or coerced, within a relevant population.

Counterreconnaissance Task Organization

When enemy forces are known or expected to be mechanized and/or armored, the threat commander may task-organize a significant mechanized CRD capability. A typical battalion-level CRD that could be tasked by a higher tactical or operational level headquarters is at Figure 1 (next page) as a generic model. Distinguishing units that are mission-focused as counterreconnaissance from other units operating in an AOR or threat disruption zone is often problematic in that weapon systems and tactical arrays may appear very similar to other security forces or elements. This example of task organization that could represent a CRD is similar to current real-world configurations used to form a mobile combat group.[2]

Tactical information may be exchanged either directly between and/or among threat units and detachments, or may be routed through a higher headquarters. Examples include special purpose forces (SPF) reporting to a division tactical group (DTG) or brigades of an operational strategic command (OSC). Other threat units may be operating in the same AOR but have no affiliation with a CRD. In the example (above), the SPF team has coordinated affiliation with an insurgent cell and criminal organization to assist in its mission tasks and support to the CRD.

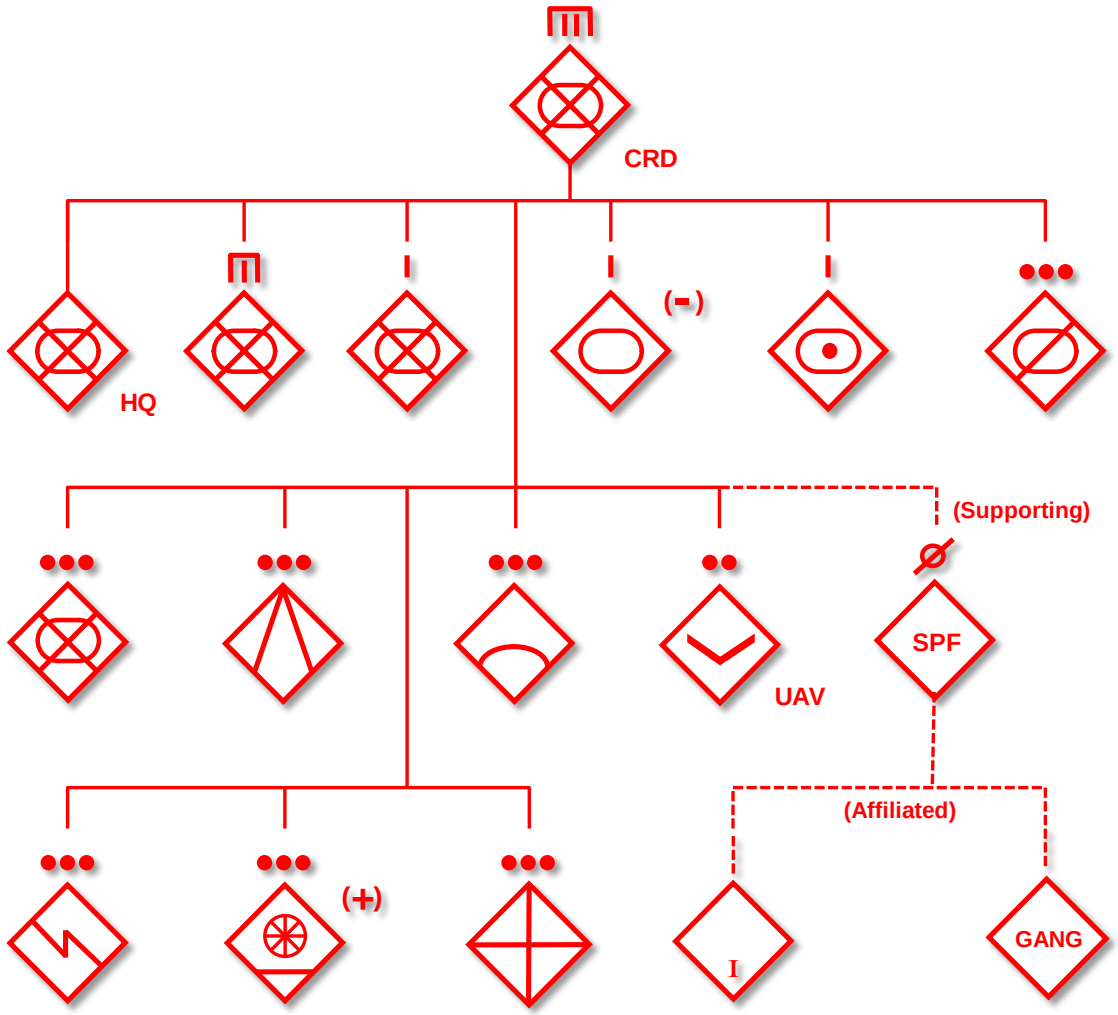


Figure 1. Battalion-level counterreconnaissance detachment task organization (example)

Figure 2 illustrates an example of selected subordinate assets in a CRD task organized from a motorized infantry company. Wheeled vehicle mobility transports infantry to its mission area in what is primarily a dismounted maneuver operation. Other assets are either wheeled or towed to support the CRD. Additional mission tasks in this instance include assessing enemy obstacle efforts and the status of mobility corridors being considered as axes of advance by threat forces. Reporting on possible chemical contamination in designated locations informs the higher headquarters on information indicating suspected use of chemical agents in rural areas of the threat disruption zone.

The SPF information warfare (INFOWAR) team is in a *supporting* relationship. This supporting team is commanded by and receives its logistics from their parent SPF headquarters, but is positioned and given mission priorities by its supported headquarters. An insurgent cell from the geographic area of counterreconnaissance is affiliated to the CRD. In this example, the SPF are shaping the perception of introducing threat forces as supporting the regional ethnic demands for autonomy from the current state governance.

The insurgent cell is affiliated with the CRD and provides current intelligence on lanes through obstacles and the location of patrol routes the insurgents have observed during the recent increase in tactical actions long the international boundary. Insurgents who have infiltrated state militia units provide information on alerts being distributed on what is known of threat reconnaissance efforts.

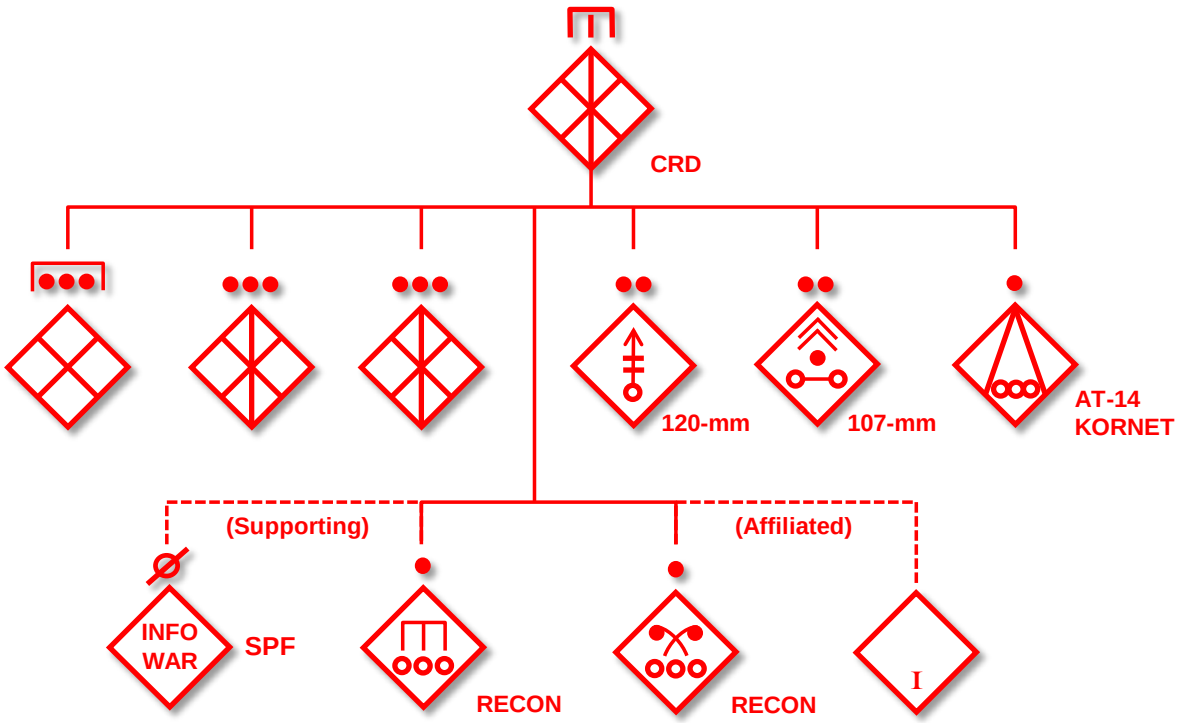


Figure 2. Company-level counterreconnaissance detachment task organization (example)

Mission Task: Counterreconnaissance

Counterreconnaissance is a mission task. A CRD is specifically designed to locate and *destroy* enemy reconnaissance and intelligence collection elements. To accomplish this task, a threat commander may have a CRD operate as a component of a larger threat security force, or operate in conjunction with security elements or force in the same AOR. Selected security tasks may be assigned to a CRD in addition to the typical offensive tasks of a CRD. Tactical application of tasks is doctrine-based, flexible, innovative, and adaptive with agility and initiative.

Threat tasks are listed in TC 7-101, *Exercise Design*, at Appendix B. Reconnaissance is an inseparable aspect of the counterreconnaissance task. When conducting counterreconnaissance, the four typical offensive tasks are:

- Ambush.
- Assault.
- Raid.
- Reconnaissance attack.

The execution of functional tactics, based on functional analysis, is an integrated way to optimize capability effects with movement and maneuver in a designated space and specified time period. Function is the underpinning to understand and effectively apply tactics and techniques.

Hybrid threats in counterreconnaissance actions can be simultaneous combinations of various types of activities by enemies and adversaries that will typically change and adapt over time. For more detailed discussions of hybrid threat (HT) operations, tactics, and organizations, see TC 7-100, *Hybrid Threat*, o and related TRADOC G2 supporting products and processes.

The diagram at Figure 3 displays the primary tasks in counterreconnaissance and lists the subtasks that comprise the sequential and at times concurrent actions within a CRD. Task 6.0 is the centerpoint for applying the reconnaissance of Task 5.0 in one or a combination of offensive actions.

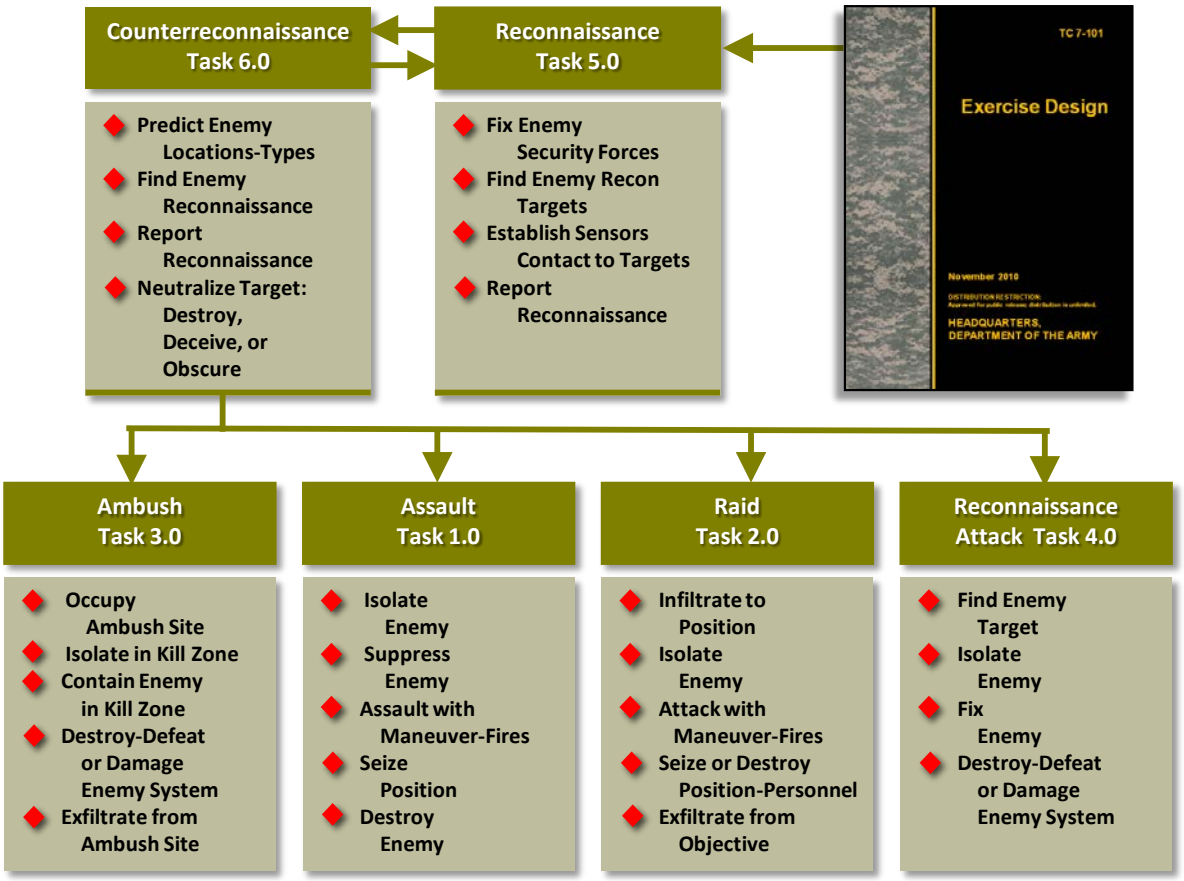


Figure 3. Offensive task actions in counterreconnaissance

Locating enemy reconnaissance elements uses current situation reports and intelligence analysis. When enemy presence is unknown or unconfirmed, analysis of an OE guides threat commander decisions and guidance on where the CRD reconnoiters and/or observes in order to find the enemy. A CRD locates, tracks, and destroys enemy reconnaissance throughout its counterreconnaissance zone (CRZ). Each CRZ is assigned as the area of responsibility to one CRD.

With confirmed presence of the enemy, mission guidance and threat commander decisions determine when and how to destroy the enemy reconnaissance elements. Typical actions involve an ambush, assault, raid, or a combination of these tasks. A reconnaissance attack is the most ambitious of the four offensive tasks and typically requires the combined arms capabilities of at least a company-level CRD.

Tactical Vignette–Counterreconnaissance

> In the November 2014 issue of the *Red Diamond*, part 2 of the "Counterreconnaissance: Threat Actions for Tactical Success" article will present a tactical vignette of threat counterreconnaissance in a complex operational environment (OE) for training US Army units at the tactical level of armed conflict.

Control measures in a counterreconnaissance mission assist in locating, tracking, and destroying enemy reconnaissance elements. Within a counterreconnaissance zone (CRZ), other measures include reference zones (RZs), predicted enemy locations (PELs), and kill zones. The tactical vignette in the November 2014 *Red Diamond* will describe and illustrate the actions and enabling support of a successful counterreconnaissance mission.

Training Implications for US Army Readiness

Threat reconnaissance and counterreconnaissance is a continuous mission. Any loss of threat reconnaissance and/or counterreconnaissance assets are reconstituted quickly to ensure the threat commander maintains timely and accurate information on an OE and adversary or enemy, and sustains situational understanding and capabilities to destroy enemy reconnaissance in order to protect threat forces or elements.

Readiness is the effective achievement of training objectives that consist of task/actions, conditions, and standards. A US Army unit commander assesses and evaluates readiness standards from the unit's mission essential task list (METL) and specified tasks for assigned or expected contingency operations. The *conditions* for training readiness include factors of a complex operational environment (OE)—and the Threat—that are realistic, relevant, and challenging to the training unit, leaders, and Soldiers.

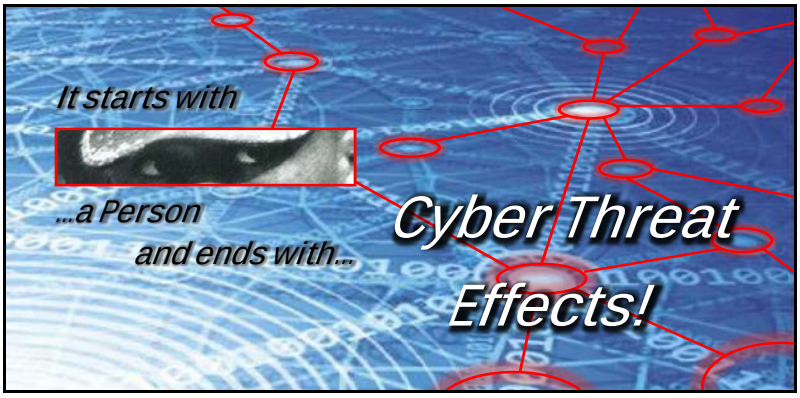
Condition
Those variables of an operational environment or situation in which a unit, system, or individual is expected to operate and may affect performance.
JP 1-02, *Department of Defense Dictionary of Military Terms*

The US Army provides several sources to describe threat opposing forces (OPFOR) for US Army and joint training. The training circular (TC) TC 7-100 series describes threat structure, tactics, and techniques with the conditions that exist for the purpose of training and achieving training objectives.

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

Notes

[1] OPFOR. AR 350-2, *Opposing Force (OPFOR) Program* (2004), p. 1.
[2] Grau, Les. Restructuring the Tactical Russian Army for Unconventional Warfare. *Red Diamond*. February 2014, pp 4-8.



CORRECTION
In the SEP14 issue of the *Red Diamond*, Figure 1 of "RPG-30 Kryuk 'Hook' Russia's Solution to Active Protective Systems (APS)" was mislabeled as an RPG-30 by the newsletter format designer. The correct identification is RPG-18 as originally listed by the author.

—What CTID Does for YOU—

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

CTID Points of Contact

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