Operational Environment Enterprise
U.S. TRADOC G2 Intelligence Support Activity

Red Diamond

Complex Operational Environment
and Threat Integration Directorate

Fort Leavenworth, KS Volume 5, Issue 3 MAR 2014

INSIDETHIS ISSUE

OEE *Red Diamond* is published monthly by TRISA at CTID. Send suggestions to CTID ATTN: *Red Diamond* Dr. Jon H. Moilanen CTID Operations, BMA

and

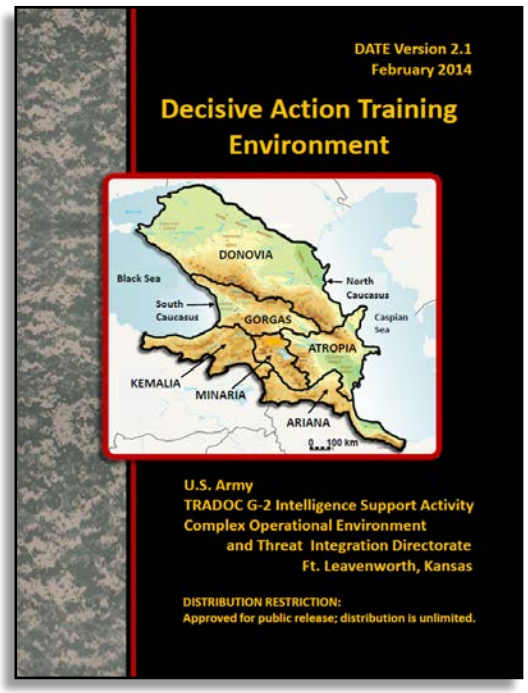
Mrs. Angela Wilkins Chief Editor, BMA

DECISIVE ACTION TRAINING ENVIRONMENT V. 2.1 2014

by Angela Wilkins, OE Assessment Team Lead (BMA Ctr)

The most recent update to the *Decisive Action Training Environment* (DATE 2.1), February 2014, is complete and available for download via the Army Training Network now. DATE is an approved TRADOC G-2 publication and is *the source* for operational environment (OE) conditions and opposing force (OPFOR) structure. It provides a complex OE with a hybrid threat which can be employed to challenge Blue METL. The OE conditions within DATE are for trainers and scenario writers to use in developing exercises.

The changes in DATE 2.1 are clearly indicated throughout the document in green text that is in bold italics, allowing trainers and scenario writers to easily view the new or changed DATE information. Changes to DATE are also described in the Strategic Setting chapter of the 2014 document, and there you will find a Threat Actor Chart. Significant items to look for in Version 2.1:



- Details about types, purposes, and general locations of underground facilities (UGFs).
- Details about nuclear capabilities and facilities.
- Information on satellite capabilities for each country has been expanded.
- The Road to War, previously part of the Strategic Setting, has become Appendix D.

(**See more DATE 2.1 a p. 15**)

RED DIAMOND TOPICS OF INTEREST

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

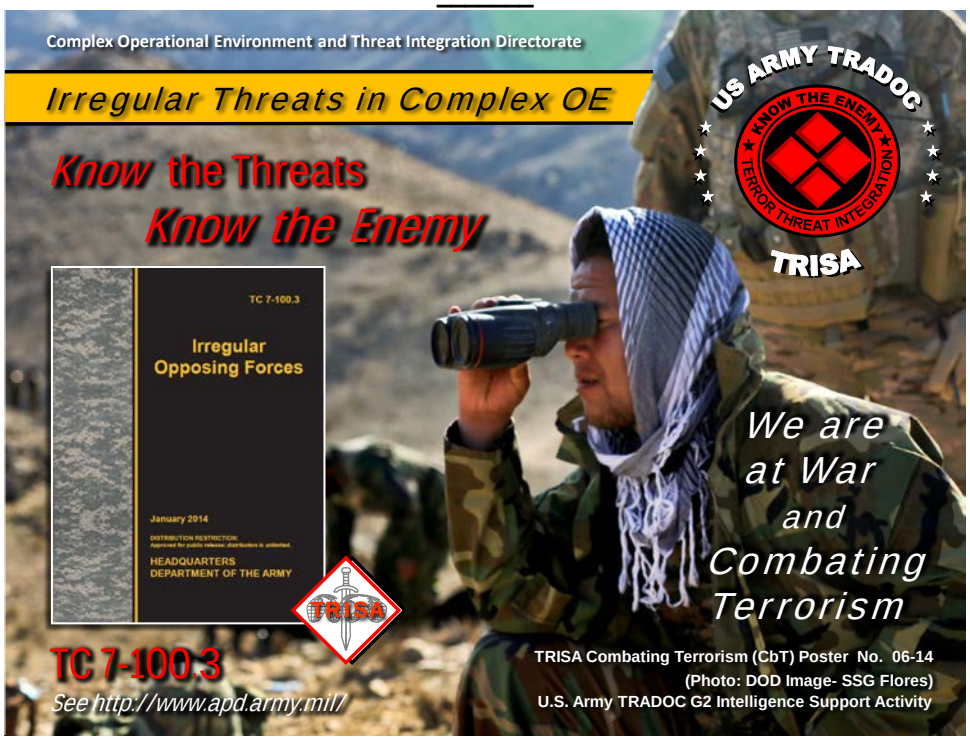
This issue of the *Red Diamond* newsletter spotlights the Army TRADOC G2 Operational Environment Enterprise (OEE). The "Director's Corner" of this issue provides more details on the expanding collaboration of OEE Army resources and capabilities that reach and share information and expertise for Army readiness.

The lead article "Exploit the Target" on cyber information warfare (INFOWAR) demonstrates the collaboration of three directorates with the TRADOC G2 OEE in the critical concerns of cyber intrusion and attacks by the threat. Describing the threat of cyber-attack include contributions from the (1) Complex Operational Environment and Threat Integration Directorate (CTID) of TRISA, (2) Training Brain Operations Center (TBOC), and (3) TRADOC G2 Training OE/OPFOR.

The second article analyzes the recent turmoil and violence in the Central African Republic (CAR). This initiates a series of articles on this region that assesses the operational environment (OE) and the power and governance conflicts of varied motivations and behavior.

Email your topic recommendations to:

Dr. Jon H. Moilanen, CTID Operations, BMA CTR
jon.h.moilanen.ctr@mail.mil
and
Mrs. 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 Operational Environment Enterprise (OEE) *Red Diamond* is a new US Army Training and Doctrine Command G2 initiative to spotlight the collaboration among the vast array of resources in TRADOC and the Army in order to enhance intelligence and training resources and share doctrinal literature. These readily available resources and capabilities focus on Soldier and Army leader readiness. This newsletter was titled formerly the TRADOC G2 Intelligence Support Activity (TRISA) *Red Diamond.* The newsletter continues to analyze complex CONDITIONS—the variables of PMESII-PT (political, military, economic, social, information, infrastructure, physical environment factors, and time)—and the tactics, techniques, and procedures (TTP) of threats operating in all US combatant commands. The newsletter also sustains observations, reports, and assessments on established and emergent capabilities and limitations of adversaries and declared enemies. The articles in this issue of the *Red Diamond* illustrate the integration of subject matter expertise in the G2 OEE. For example—

The cyber article "Exploit the Target" is a collaborative OEE effort of the Complex Operational Environment and Threat Integration Directorate (CTID) of TRISA, Training Brain Operations Center (TBOC), and TRADOC G2 Training OE/Opposing Forces (OPFOR). Analyses include continuous cyber reconnaissance and actions to identify vulnerabilities in US information systems, concepts employed by threats unrestrained by law or moral code, and ways and means that counter such threats with dedicated offensive and defensive programs. And—as with many successful operations—the requirements for awareness and understanding of alert and adaptive Soldiers and leaders are fundamental to protecting our US infrastructure, forces, and families.

The article on the ongoing strife in the Central African Republic (CAR) is indicative of persistent conflict that may confront US Army forces as we conduct decisive action as part of alliances, coalitions, and partner relationships in combatant commands. Whether offensive, defensive, or stability operations in nature, the decisive action leader must understand local or regional threats and conditions that left unaddressed will surely affect the success of US mission accomplishment. This first in a series of articles on the CAR introduces conditions and actions leading to current events. Subsequent articles will assess CAR regular military and rebel forces that continue to vie for influence in the region.

Looking ahead to future issues of the Operational Environment Enterprise *Red Diamond,* we invite your participation as a means to exchange professional ideas and doctrinal training, education, and leader development literature on threats and related operational environment (OE) topics of interest to the US Army-at-large. We look forward to your comments and articles to consider for publication in the *Red Diamond*. The publication standards are available upon request.

RED DIAMOND SURVEY

I invite you to tell us what you need to support your training, professional education, and leader development. This March 2014 user survey at the URL (below) is a simple five-minute questionnaire. This is your opportunity to focus our research and analysis resources to best serve your requirements.

https://www.surveymonkey.com/s/KV9ZKKX

I will provide our CTID assessment of survey input and way ahead in the April 2014 issue of the OEE Red Diamond.

JON

Exploit the Target:
Support and Implementation of the Cyber Attack Lifecycle

by Jerry England, John Griffiths, and Mike Saxton TRADOC G2 Operational Environment Enterprise (OEE)

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

Cyber Attack Lifecycle

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

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

Exploit Target

The Exploitation step includes many of the same functions as those activities found in the reconnaissance phase. For many tier 3 and tier 4 threats, the first four steps of the Cyber Attack Lifecycle are abbreviated and focus mainly on what can be described as smash and grab operations where stealth is of little value compared to short-term effects. However, in more sophisticated threats, the steps in the Cyber Attack Lifecycle are much more structured, as the threat emphasizes the elements of stealth, develops persistent offensive cyber resources, and matures the targeting process to maximize cyber effects. The goal of the exploitation phase is to limit the effectiveness of friendly operations by disrupting the decisionmaking process at the tactical level and having a strategic effect on the friendly will to fight through precision attacks against Mission Command Systems (MCS) and supporting ICT infrastructure.

Systemic and Operational Vulnerabilities

After cataloging the compromised portions of the target system in the reconnaissance and infiltration steps, and installing the backdoor programs in the C2 step, the threat will conduct an internal reconnaissance to locate vulnerabilities for an attack on the information resource. Vulnerabilities may be systemic or operational in nature and

are developed by the cyber threat in order to increase access, establish attack vectors, identify the most effective malicious executables, and to continue to penetrate into the targeted system. Systemic vulnerabilities are inherent to the infrastructure or network of the target system and can include the interactions of digital and or analogue system inputs and outputs to the system. Electronic avenues of approach may include a weakness in or lack of encryption, misconfiguration of system interfaces, an undiscovered hole in a software application known as a zero-day vulnerability, a sensor that is vulnerable to electronic manipulation, or any other combination of technical weaknesses in the target system. (See figure 1.)

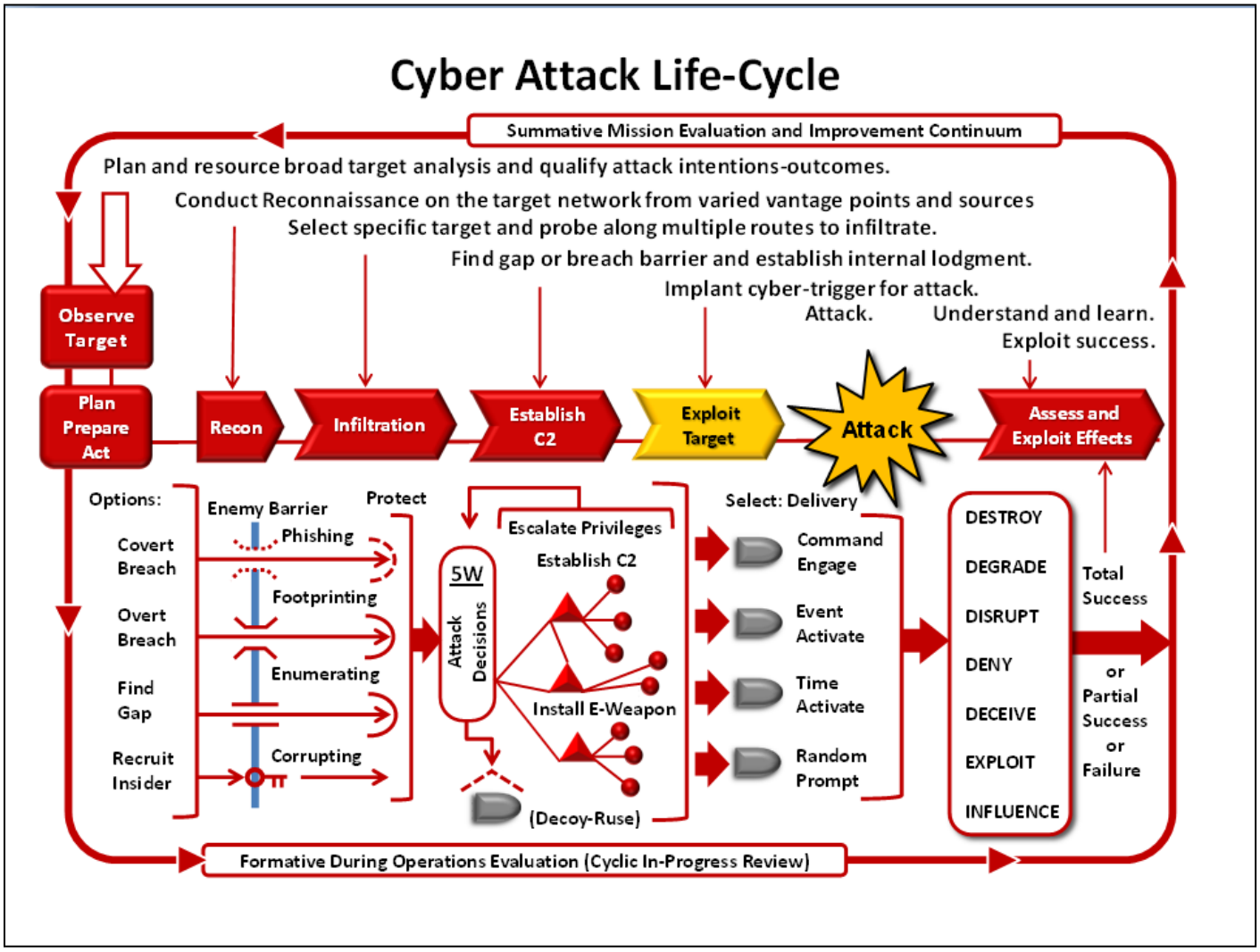


Figure 1. Cyber attack lifecycle (*Source:* TRISA-CTID, 2013)

Operational vulnerabilities include procedures and policies that dictate how the friendly forces use and/or build trust in the information resource. An example of an operational vulnerability would include a weakness in policy or governance that permits unsecured transmissions of requests for access to a secure information system such as the username and password in an open email. Another example is when third party mission support organizations are given access to military systems. Through this unique system access arrangement, the cyber threat can establish an electronic avenue of approach onto the target system by way of a seemingly unrelated activity. By stringing both systemic and operational vulnerabilities into a cyber attack campaign, the cyber threat is able to increase its capabilities.[1]

The threat will search the range of compromised hosts for data that can provide clues to identify and locate vulnerabilities and assist in vertical and horizontal movement within the information resource. Validating or footprinting is a process conducted in the reconnaissance step, but is also a part of the exploitation process. Misconfiguration of network devises and lax security represent the low hanging fruit of system vulnerabilities. Peer and near peer threats will maintain a list of known vulnerabilities and compromised users based on prior cyber reconnaissance efforts. These

vulnerabilities provide access to the targeted network as well as facilitate launching an attack at the time of the threat's choosing. Sophisticated threat organizations may discover even newer vulnerabilities if enough time is allowed for target exploitation through structured exploitation of the target. Other targets may include a database or a website that the threat harvests periodically for data or prepares with malware and logic bombs for execution at a future date. (See figure 2.)

Escalate Privileges

The threat escalates privileges inside the compromised network in order to move both vertically and horizontally to obtain access to other resources within the system. The goal of escalating privileges is to establish a secure foothold and gain administrative level access and authorization within the targeted system. Trust is established by a variety of means and may require a series of compromises to take effect. Once administrative level privileges are obtained, the threat will own the targeted system and will have the ability to manipulate or control it as it sees fit. In many cases, normal information assurance activities will discover the access points and close them to prevent future attacks, which make vigilance on the part of the targeted system of the utmost importance.

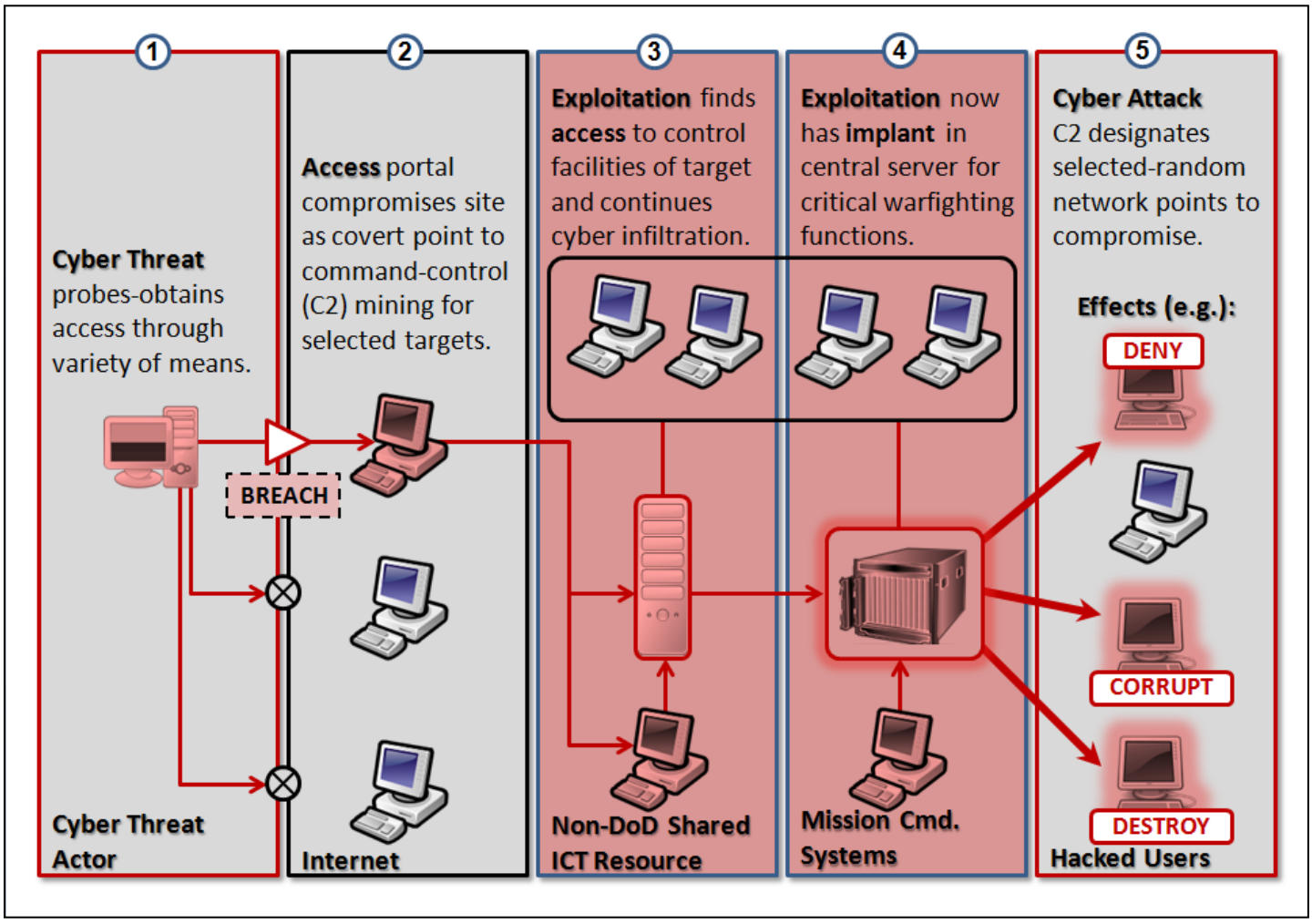


Figure 2. Movement within the target system (*Source:* TRISA-CTID, 2014)

The data targeted by attackers includes a range of information, from fueling requests, to ammunition supplies, to movement control databases. Attackers may delete these records or change them in an attempt to misdirect friendly assets.[2] Other types of data that allow the threat to penetrate deeper into friendly systems and infect other systems such as passwords and encryption data will have wide ranging effects across the entire Global Information Grid (GIG). These attacks will stress the trust relations between friendly and host nation forces and will support the threat's anti-access and area denial operations by disrupting the decisionmaking process.

Certificate authorities are organizations that issue the electronic keys needed for software and hardware to communicate over networks such as the Internet and are a key component of the trust relationship. Stolen and/or forged key signing certificates are used by the cyber threat to deceive users into connecting to ICT resources that are the targets of a cyber attack or criminal activity. If these keys are compromised without the certificate authority taking necessary action, the cyber threat can use them to issue malicious executables such as Trojans with little or no suspicion from the end user. This makes it difficult for cyber defenders to distinguish between legitimate cyber resources and those issued by the cyber threat. In 2012, DigiNotar, a Dutch certificate authority, had its certificates compromised, which caused data breaches at many Dutch government websites.[3] The DigiNotar attack was claimed by the Comodo hacker who also claimed to have attacked other certificate authorities such as Globalsign and Comodo Group. The compromised Comodo certificates could have been used to mask the distribution of malware needed to intercept the electronic communications for surveillance and criminal purposes.[4] (See figure 3.)

Install (Emplace) Electronic Weapon

The threat will begin to deploy malicious executables as soon as opportunities arise. All aspects of the friendly information systems represent a possible informational center of gravity; including logistics networks, mission command systems, RISTA systems, and possibly media and civilian targets that support friendly operations and are seen as legitimate targets. These operations are preemptive in nature and are designed to paralyze decsionmaking and render all forms of electronic communication vulnerable to attack or exploitation. They also shape the information environment for future attacks.[5]

After identifying the suitable attack method, the threat installs the executable files necessary to accomplish the desired task. Malware designed to collect enemy data for intelligence purposes is a type of electronic weapon that exploits and harvests the data on a targeted system. In this case, the attack is the exploitation step and usually constitutes a long term persistent presence on the target. These types of operations do not attempt to culminate in a final attack designed to destroy, deny, or degrade the system, since the primary mission is to gather intelligence.

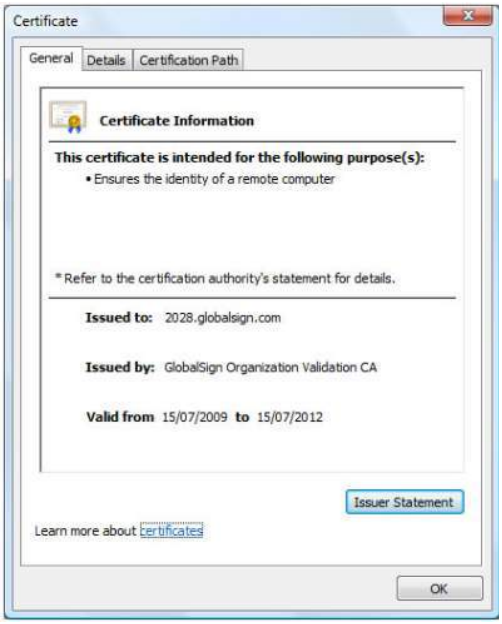


Figure 3: Digital certificate from a known certificate authority. (*Source:* globalsign.com 2014)

Other malware types will manipulate data based on manual entry, a set of pre-identified conditions, or on a set algorithm. Other types of attacks, known as logic bombs, execute code designed to disrupt or degrade key military or civilian systems and are typically executed for the purpose of denying friendly use of important information at critical times such as the beginning of an attack or a movement of a large force. Malware of this sort may be used to destroy/crash ICT assets; deny access to logistics data; or disrupt data from intelligence, surveillance, reconnaissance (ISR) assets. In the case of an attack aimed at political, economic, or infrastructure variables, the results can bring down the electric power grid, contaminate water treatment facilities, crash the stock market, or compromise the personal email of political leaders.

Much like combat engineers that will prepare a bridge or building for demolition, the threat will emplace malicious executables within an information system to ensure freedom of maneuver in cyberspace. The threat will use different trigger mechanisms such as command engaged triggers that are activated through a user interface, event activation when a certain set of conditions are met, time activated mechanisms after a certain interval, and/or randomly delivered attacks based on a programmed algorithm.

Attack Timing and Replicability

The cyber threat must consider the timing and the replication of cyber attacks as an integral part of the planning process. In order to achieve maximum effect and maintain the element of surprise, a resource should be both stealthy and persistent. The cyber threat emphasizes the need for initiative by launching a preemptive cyber attack in order to

achieve information dominance. However, in some cases a more sophisticated approach is to retain an advanced cyber asset for a situation when the operational stakes are highest – for instance, at the time of an attack.

Researchers have devised a model which can be useful in determining the best time to launch a cyber attack. The model is based on situational risk, the possibility of discovery, and the likelihood that the attack vector will be blocked sometime in the future.[6] In other words, well-known attacks which are typically easy to defend but difficult to attribute will be used early and often because the risk-to-reward ratio is low. This "spray and pray" approach would be typical of a tier 3 or tier 4 cyber threat. The use of common obfuscation tools may well confuse friendly forces as to the true identity of the attacker because the attack shares the signature of both hacktivists and cyber criminals who may hide political or tactical motives.

Another form of stealth may be achieved by developing a cyber resource that is not able to be detected by normal antivirus and/or information assurance procedures. These novel attacks can take up to 8 months before discovery and can infect a large number of machines.[7] They are typical of tier 2 and tier 3 cyber threats as they represent threats that are discovered through an advanced research and development effort. However, tier 1 and tier 2 cyber threats that have the resources to create vulnerabilities can develop persistent attacks that are not only difficult to discover but are difficult to patch because the attack is engineered into the target system. A sophisticated rootkit attack will make a targeted system all but useless once it is installed. The infection may be so deep that the target system will need to be completely rebuilt, which can take days or weeks to recover from depending on the size of the system. For this reason, it is in the best interest to retain this type cyber resource until the stakes are higher, as it would reveal the previously unknown vulnerability and cause cyber defenders to attempt to patch it immediately.

Implications for Training

- Cyber defenders must have situational awareness both inside and outside their networks in order to prevent further exploitation of internal systems.
- Encryption needs to be employed on all sensitive data nodes, both physical and virtual, in order to limit and/or control the level of data that is exploited on a target system and to prevent unauthorized usage from an unvetted fringe user or system.
- Control measures that look for the unauthorized access of sensitive systems, the download of large amounts of sensitive information, and the systematic structured exploitation of protected data (web crawlers) should be monitored vigilantly.

Cyber Threat Replication at Home Station Training

After discussion of the cyber threat above, the next section will primarily focus on the way in which the Operational Environment Enterprise (OEE) helps replicate the threat in the most realistic way possible, in order to assist in training at home station and with future Combat Training Center (CTC) rotations and/or contingencies as needed. Lastly, the final portion of this article will then concentrate on the way in which training effectiveness is assessed at both home station and at the CTCs.

To align with the future objectives of DOD and the Army, TRADOC is exercising units against a cyber threat during home station training (HST). To do this, the Training Brain Operations Center (TBOC) employs the use of real-world intelligence, trends, and incidents to drive scenario development and create an environment as close to real world as possible. As the Army continues to develop doctrine for the cyber domain, the objective will grow to integrate Defensive Cyberspace Operations (DCO) and Defensive Cyberspace Operations-Response Actions (DCO-RA) through threat portrayal to ensure that all users of Army networks can understand, identify, and mitigate a potential threat.

Method

To begin the implementation of the cyber domain into HST, the TBOC works with units to identify and exploit vulnerabilities in their systems and processes to demonstrate how various individual and collective training tasks can be affected by the cyber domain, as well as reinforce Information Assurance (IA) policies and incident response measures. Doing so has four main goals—

- Create situational awareness.
- Reduce vulnerabilities.
- Heighten network posture.
- Reduce the attack surface.

In order to integrate the cyber threat into an exercise, it is imperative to understand the capabilities of the unit, the effects specific to the threat and how they integrate into supporting the Commander's Training Objectives (CTO). Using a method developed by the Cyberspace Operations Methods, Models, and Analysis Working Group under TRADOC Analysis Center (TRAC), exercise planners are assisted through a Cyberspace Operations Assessment Taxonomy. This covers six different aspects involved in implementing cyber training and focuses on the identification of various components to be affected including warfighting function (WfF) identification, target identification, attack objective, attack method, attack effects, and mission and campaign effects.

Integration

Once the methods of integration are identified, the unit works to integrate cyber injects into the Master Scenario Event List (MSEL). Additional, important information required to set the common operating picture (COP) is provided through the road to war, historical reporting, and threat actor intelligence summaries (INTSUM). This is done to strengthen G/S 2/3/6 integration, integrate cyber as a regular part of the OE and test understanding of local IA policies to mitigate potential threats. Lastly, cyber integration allows users to experience cyber training where the annual Army IA training leaves off – bridging the gap from the test environment to real-world application.

During execution, users might experience different "effects" on their computer system. This takes the indicators, intelligence, and IA policies a step further by forcing end-users to operate in a degraded environment, reinforcing the need to understand basic concepts. Currently the focus is the non-technical users working to drive the example that all operators of DoD workstations are responsible for the overall Department of Defense Information Network (DoDIN).

Threat

After defining the threat in the road to war, historical information, intelligence reports, and MSEL injects, the cyber environment is now established. Keeping consistent with the real-world landscape, units can expect to face numerous actors: cyber-criminals, terrorist organizations, military cyber units, and hacktivists can all be integrated while having a different level of sophistication and purpose. In addition, the cyber threat might be unintentional malicious network activity caused by poor IA practices or done through potential insider threat activity.

To adequately portray the threat, the TBOC uses a Government off the Shelf (GOTS) program called Network Effects Emulation System (NE2S) to emulate a degraded environment. This software is designed to target specific user-defined systems as a means for replicating a cyber attack while leaving the rest of the network up and running, untouched. This software was successful in emulating a cyber attack against a small group such as a division Fires cell, a battalion-level network infrastructure, and up to a Unified Combatant Command (UCC) done in a "distributed" fashion with the effects being pushed to users in three different states.

Future

In the future the TBOC will continue working to integrate the cyber threat at HST through more advanced means. Additionally, TBOC will also begin integrating doctrine set forth in FM 3-38, *Cyber Electromagnetic Activity (CEMA).* This will include, but is not limited to, advanced operational cyber capabilities, request for cyber activity to directly support commander's objectives, integration of joint cyber operations and Joint Cyber Intelligence Preparation of the Battlefield (IPB), and the integration of cyber into the military decision-making process (MDMP). In doing this the TBOC will continue to work with TRISA to maintain appropriate threat characteristics, with TRADOC G2 for threat validation, and with the 1st IO World Class Cyber OPFOR (WCCO) to remain current on lessons learned from the CTCs. This collaboration will help the TBOC continue to grow a realistic medium intensity cyber threat replication capability for the home station training venue.

Assessing Effectiveness of Cyber Training Conditions

Previous discussion focused on cyber threat operational methods and how cyber training conditions are replicated. The final section addresses cyber training assessment and effectiveness at home station and the CTCs.

Home Station

At home station, commanders (along with unit training managers) will develop training objectives to set OE conditions; test the execution of IA principles/procedures; and validate tactics, techniques, and procedures (TTP) through the scenario design process. Trainers, observer controllers, or white cell members drive cyber training events through MSEL injects. For example, a network administrator might respond to a MSEL entry by physically shutting off a computer terminal to simulate loss of a terminal from a cyber attack. However, relying only on MSEL entries lacks realism. Newer initiatives, such as NE2S (mentioned earlier), create more realistic training environments by letting the training audience actually experience cyber attack effects on their computer screens and mission command platforms.

Commanders at home station can assess cyber training effectiveness by determining if their unit members are following the basic principles of "Recognize, React, & Mitigate" as captured in the 10 Jan 14, FORSCOM Cyber Home Station Training Task List. Soldiers should possess the requisite skills to recognize when a cyber attack is taking place. They should also know how to mitigate the effects of cyber attacks and understand proper reporting procedures.

Unit commanders should consider the following when assessing the effects of cyber training and condition setting:

- Cyber training should replicate the six steps of the Cyber Threat Lifecycle (Reconnaissance, Infiltration, Establish C2, Exploit Target, Deliver Attack, and Assess and Exploit Effects).
- Cyber training must build unit cyber awareness and prepare members for more robust cyber challenges at the CTCs, such as more aggressive intrusion techniques.
- Cyber opposing force (OPFOR) elements should be integrated into the OPFOR scheme of maneuver (example: taking down a C2 system via a denial of service attack as part of a ground offensive).

Combat Training Centers

At the CTCs, operations group (OPSGRP) staff design scenarios to meet the rotational unit (RTU) commander's training objectives, including cyber threats. During CTC rotations, the WCCO is employed to set robust cyber conditions. The WCCO is a team of expert Army cyber warriors that attempts to penetrate the RTU's networks and conduct operations including simulated malware emplacement, mining/exploiting critical mission data, etc.

The WCCO enables the RTU commander to gauge training effectiveness and validate TTP. The following should be considered when assessing cyber effects at the CTCs:

- The WCCO must be "competitive" (i.e. it should find an actual vulnerability in the RTU's network before introducing effects and not be granted administrative entry).
- The WCCO needs to be fully integrated within the CTC OPFOR, representing one of many options (including kinetic, EW, etc) available to the OPFOR commander and not a stand-alone entity or extension of the OPSGRP or exercise white cell.
- WCCO should be linked to the OPFOR scheme of maneuver and cyber effects introduced in concert with other options, such as an air attack, jamming, etc.

Assessment helps unit commanders judge the effectiveness of cyber training in their units and lets training managers determine if the training conditions supported achievement of unit training objectives. Finally, cyber training assessment helps support the training of Soldiers to meet the challenges of current and emerging cyber threats both now and in the future.

Endnotes

[1] Target Hackers Broke in Via HVAC Company, Krebs on Security, February 2014.

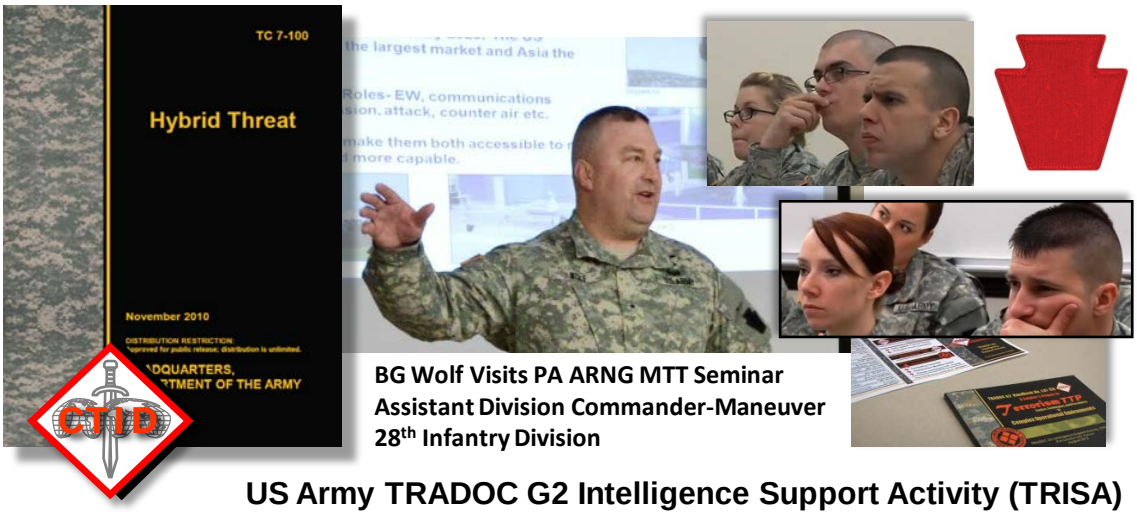
[2] Bryan Krekel, Patton Adams, George Bakos, Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage, Prepared for the US-China Economic and Security Review Commission by Northrop Grumman Corp, 7 March 2012, p 38.

[3] Peter Bright, Comodo Hacker: I hacked DigiNotar too; other CAs breached, Ars Technica, 6 September 2011.
[4] Kelly Jackson Higgins, Comodo Hacker Takes Credit For Massive DigiNotar Hack, Dark reading, 6 September 2011.
[5] Lieutenant Colonel (R) Timothy L. Thomas, China's Electronic Long-Range Reconnaissance, Military Review, November-December 2008.
[6] Regina Nuzzo, The Best Time to Wage Cyberwar, Nature News, 13 January 2014.
[7] Leyla Bige and Tudor Dumitras, Before We Knew It: An Empirical Study of Zero-Day Attacks In The Real World, 19th ACM Conference on Computer and Communications Security, 16-18 October 2012.

HYBRID THREAT AND MOBILE TRAINING TEAM OPPORTUNITIES 2014

by CTID Operations and TRADOC G2 Operational Environment Enterprise (OEE)

Hybrid Threat Train the Trainer-Mobile Training Team
21-23 March 2014 with Pennsylvania Army National Guard



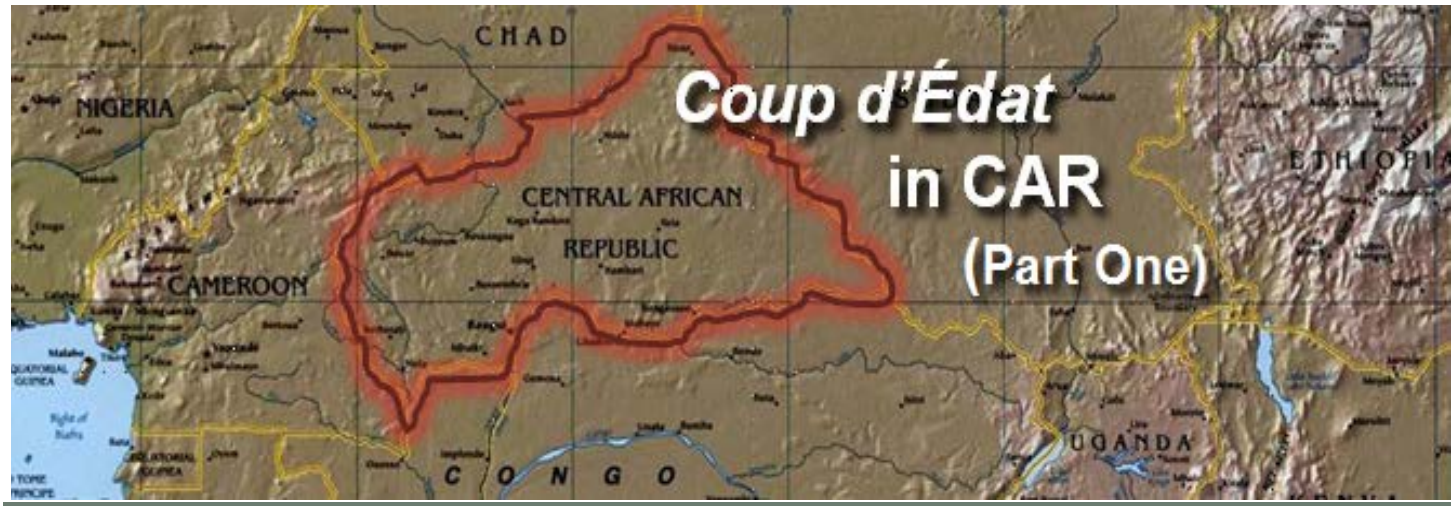
BG Wolf Visits PA ARNG MTT Seminar
Assistant Division Commander-Maneuver
28th Infantry Division

US Army TRADOC G2 Intelligence Support Activity (TRISA)
Complex Operational Environment and Threat Integration Directorate

The TRADOC G2 Operational Environment Enterprise (OEE) provided a Hybrid Threat (HT) Mobile Training Team (MTT) train the trainer seminar to Soldiers and leaders of the Pennsylvania Army National Guard (PA ARNG) 21-23MAR14 in Danville, PA. Most of the 40 ARNG member attendees were military intelligence specialties of the Military Intelligence Company (MICO), with other attendees from the brigade special troops battalion, and infantry, armor, and cavalry units of the 28th Infantry Division.

BG Wilbur Wolf, Assistant Division Commander-Maneuver (ADC-M), visited the seminar twice during the training event. He discussed the complexity of current threats and accented the significance of regular and irregular forces in future Army operations. The Complex Operational Environment and Threat Integration Directorate (CTID) of TRISA conducted the seminar with one instructor-facilitator from Fort Leavenworth, KS. This seminar follows a similar training event conducted with the PA ARNG in November 2013, and precedes another possible PA ARNG seminar in late spring 2014.

The three-day seminar was a condensed version of the five-day resident Hybrid Threat Train the Trainer (HT TTT) course that is conducted at Fort Leavenworth, KS. The next resident HT TTT at Ft Leavenworth is scheduled for 18-24 August 2014. For more information on the resident Hybrid Threat (HT) Train the Trainer seminar, contact **jennifer.v.dunn.civ@mail.mil**.



by Laura Deatrick, OE Assessment Team (CGI Federal 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 attempts to stabilize the country and keep peace. This article is the first in a series that will explore the most recent coup d'etat in CAR, which occurred on 24 March 2013 when the Séléka rebel group overran the capital.

Power and Governance

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 first man to hold power was David Dacko, who was selected to serve as president when CAR gained independence from France in 1960. Just two years later Dacko banned all opposition political parties, paving the way for him to run unopposed and win the country's first presidential election in 1964.

Dacko's first term as elected president was short-lived, however, as the very next year he was overthrown by Army commander Jean-Bédel Bokassa in a military coup d'état. Determined to maintain power, Bokassa named himself "president for life" in 1972. Four years later, Bokassa declared himself emperor and named former president Dacko as his personal advisor.

Not content with the post of advisor to the emperor, Dacko turned on Bokassa. In 1979 he re-took power in a coup backed by France, which occurred while Bokassa was out of the country. CAR remained a one-party state, and in 1981 Dacko once again ran unopposed and won the presidential election.

This term as elected president ended as quickly as the previous one – and in the same way. Only months after winning election, Dacko was deposed in a coup d'état by Army commander André Kolingba. Five years later, in 1986, Kolingba won a referendum authorizing him to remain in power for an additional six years. During that time, pressure built to the point where Kolingba had no choice but to legalize opposition political parties, which he did in 1991.

Though Kolingba lost the 1992 multi-party presidential election – the first in the country's history – the poll was annulled by CAR's supreme court due to irregularities. A new election, taken in 1993, saw the presidency passing from Kolingba to Ange-Félix Patassé in the first peaceful transfer of power since independence in 1960.

Alas, Patassé's time in high office would be no more peaceful than that of his predecessors. In 1996 he was the target of a series of military coups, none of which was successful. Former president/emperor Bokassa died during the same year. Patassé retained power in multi-party elections in 1999 with former president Kolingba, who was also on the ballot, coming in second. Not content to remain in second place, in 2001 Kolingba attempted to retake power by force. The coup attempt was suppressed and Patassé subsequently fired his Army Chief of Staff, François Bozizé, who had been implicated in the plot.

This last act eventually proved to be Patassé's undoing. Bozizé made an unsuccessful coup attempt in 2002. Undeterred, he tried again the next year while Patassé was out of the country. With the support of neighboring country Chad, this time Bozizé was successful.

Having won power by force, Bozizé kept it by peace, winning multi-party elections in 2005. That same year he had a falling-out with civil servant Michel Djotodia, prompting the latter to leave government service. Clearly displeased with the situation, Djotodia formed a rebel group in 2006 and started a rebellion while Bozizé was out of the country, which was put down with the help of France. Bozizé was re-elected in 2010 amid claims of fraud by Patassé, who was attempting to reclaim his former position. Patassé died the following year.

Figure 1. Regional and continent map in relation to the Central African Republic

Séléka and Its Components

The rebel group *Séléka CPSK-CPJP-UFDR* (commonly know by just Séléka) was created in August 2012, though its existence was not announced until December of that year. "Séléka" means "alliance" in the Sango language, and the group formed as a coalition of three existing rebel groups. Two other groups subsequently joined Séléka, though one of these left shortly thereafter. Michel Djotodia, former civil servant, became Séléka's de facto leader. The group's original goal was to force President Bozizé to comply with peace agreements that were signed with rebel groups in 2007 and 2008, though this later shifted to a desire to depose Bozizé outright. Estimates of Séléka numbers put its strength at around 4,000-5,000 as of March 2013. Rebel groups that have belonged to Séléka are predominantly Muslim and include the CPSK, FDPC, A2R/M2R, and factions of the UFDR and CPJP.

The Union of Democratic Forces for Unity (*l'Union des Forces Démocratiques pour le Rassemblement*; UFDR) was formed in 2006 by Djotodia. Led by Djotodia and Damané Zakaria, the group started a rebellion against Bozizé's government in October 2006. The UFDR captured several towns in northeastern CAR, including Birao, Ouadda, Ouanda Djallé, and Sam Ouandja, before French troops intervened in November/December of that year. The UFDR signed peace agreements with the government in April 2007 and again in June 2008 that included amnesty; disarmament, demobilization, and rehabilitation (DDR); integration into the Central African Armed Forces (*Forces Armées Centrafricaines* [FACA]) or cash

payment for demobilizing; release of political prisoners; and participation in government. A faction of the UFDR, led by Djotodia, became a founding member of Séléka due to the government's failure to keep most of these promises.

The Convention of Patriots for Justice and Peace (*la Convention des Patriotes pour la Justice et la Paix* [CPJP]) was formed in October 2008. The group was originally led by Charles Massi, who disappeared in 2010 and is presumed dead. The CPJP clashed with government forces at least twice in 2009, and in 2010 troops from neighboring Chad were deployed to help fight the rebels. The group signed a ceasefire with the CAR government in June 2011, followed by a peace agreement in August 2012. A splinter group led by Noureddine Adam became a founding party of Séléka the same month, and mounted an attack on government facilities just weeks later.

The existence of the Patriotic Convention for National Salvation (*la Convention Patriotique du Salut du Kodro* [CPSK]) was announced by Dhaffane Mohamed-Moussa, its founder, in June 2012. One of the founding parties of Séléka, little else is known about the group.

The Democratic Front of the Central African People (*le Front Démocratique du Peuple Centrafricain*; FDPC) is led by Martin Kountamaji, aka Abdoulayé Miskine, and was founded sometime before 2003. The group has been allied with the government on occasion, having fought with FACA in 2002 against rebels led by Bozizé. The FDPC signed a peace agreement with the CAR government in February 2007 that included amnesty, DDR, and participation in government. The peace was short-lived, however, as the group clashed with FACA in late 2008 and the first half of 2009. The FDPC joined Séléka in late December 2012 or early January 2013, only to withdraw within three months due to disagreements with the other coalition members. Fleeing to Cameroon, Miskine was arrested by authorities there in September 2013.

The Alliance for Rebirth and Reforging (*l'Alliance pour la Renaissance et la Refondation* [A2R]) is coordinated by Salvador Edjezekane. The group joined Séléka in late December 2012 or early January 2013, and renamed itself the Movement for Rebirth and Reforging (*Mouvement pour la Renaissance et la Refondation* [M2R]) in March 2013. Little else is known about the group.

Conclusion

Political tensions, rebel groups, and forceful regime changes are standard fare in the Central African Republic. This article focused on political events leading up to the beginning of the Séléka rebellion and the composition of the rebel group. Part Two of this series will focus on the Séléka rebel offensive of 10 December 2012 to 6 January 2013.

Sources

Aboa, Ange. "Looters, gunmen roam Central African Republic capital after coup." Yahoo! News. 26 March 2013.
Agence France-Presse. "Central Africa says repelled rebel attack." ReliefWeb. 11 December 2013.
Agence France-Presse. "4 CAR troops killed in rebel attack." News24. 13 March 2013.
Agence France-Presse. "Heavy fighting in northern CAR, many flee: military." Google News. 10 December 2013.
Associated Press. "Rebels in Central African Republic take 7th town." Town Hall. 20 December 2012.
BBC News. "CAR rebel head Djotodia names caretaker government." 31 March 2013.
BBC News. "CAR rebel head Michel Djotodia 'suspends constitution'." 25 March 2013.
BBC News. "Central African Republic profile: Leaders." 20 August 2013.
BBC News. "Central African Republic profile: Overview." 26 June 2013.
BBC News. "Central African Republic profile: Timeline." 20 August 2013.
BBC News. "Central African Republic rebels take diamond-mine town." 18 December 2012.
BBC News. "Chad deploys troops to help fight CAR rebels." 18 December 2012.
BBC News. "Q&A: Central African Republic's rebellion." 11 January 2013.
Besliu, Raluca. "Rebels in the Central African Republic approach the capital." Digital Journal. 30 December 2012.
Central African Republic Government. "Central African Republic Peace Accords of 2007 [*in French*]." 2 February 2007.
Chothia, Farouk. "Michel Djotodia - Central African Republic rebel leader." BBC News. 26 March 2013.
CIA. "World Factbook: Central African Republic." 6 December 2013.
Dembassa-Kette, Crispin. "CAR Rebels Seize Ninth Town; African Leaders Urge End to Clashes." Bloomberg News. 24 December 2012.
Encyclopedia Britannica. "Central African Republic." 5 February 2014.

Fédération internationale des ligues des droits de l'Homme [*fr: International Federation of the Leagues of Human Rights*]. "République centrafricaine : U n pays aux mains des criminels de guerre de la Séléka [*fr: Central African Republic: A country in the hands of Séléka war criminals*]." September 2013.
Fessy, Thomas. "Why CAR has descended into violence." BBC News. 12 December 2013.
Human Rights Watch. "State of Anarchy." September 2007.
IRIN. "CAR: Concern as civilians flee, government denies rebel capture of third town." 13 November 2006.
IRIN. "Central African Republic: Who's who with guns." 17 June 2009.
IRIN. "South Africa: Nation Bolsters Its Troop in the CAR." AllAfrica. 8 January 2013.
Jane's. "Séléka." 11 October 2013.
Journal L'Hirondelle . "CPSK : Dhaffane claque la porte de la CPJP et crée la « Convention patriotique du salut du Kodro » [*fr: CPSK: Dhaffane closes the door on the CPJP and creates the "Patriotic convention for National Salvation*]." 27 June 2012.
Larson, Krista. "Troops from Chad draw red line for rebels in Central African Republic." San Jose Mercury News. 2 January 2013.
Lombard, Louisa. "Meet the polygot who just took over the Central African Republic." Christian Science Monitor. 25 March 2013.
M2R. "L'A2R devient M2R : Premier Communiqué du M2R [*fr: A2R becomes M2R: First Communiqué of M2R*]." Centrafrique Presse Info. 19 March 2013.
Marima, Tendai. "CAR peace deal yet to translate into reality." La Nouvelle Centrafrique. 14 February 2013.
Marsaud, Olivia. "La France en première ligne [*fr: France is the first line*]." RFI. 6 December 2006.

DECISIVE ACTION TRAINING ENVIRONMENT V.2.1 (*Continued from p.1*)

- Expanded information on chemical, biological, radioactive, and nuclear (CBRN) munitions.
- **Threat Actor Chart:** This chart provides an up-front glimpse of the threat actors that appear throughout DATE. The name of the group and it's "type" appear (for example – insurgent, criminal, guerrilla) followed by location and type of activity and targets. (See figure 1.)

South Atropian People's Army (SAPA) Insurgent	Focuses on eight provinces in the south with cultural ties to Ariana	Primary goal is to create a separate country composed of southern Atropia and Ariana's northwestern provinces. Receives most of its training, equipment, and supplies from Ariana. SAPA and Sadvol insurgents often clash violently over ideology, limited resources, and similar recruiting pools.	Atropian government facilities and leaders

(left to right: Threat Actor and Type, OE, Activities, Targets)

Figure 1. Excerpt from threat actor chart in DATE 2.1

Over time, and as DATE is implemented across the various training venues, TRISA-CTID accepts feedback on how to improve the document to best serve trainers who work to challenge US forces so they are prepared and ready to defeat the hybrid threat.

This iteration, Version 2.1, reflects changes in response to such feedback. To access DATE 2.1, go to the ATN homepage, and under "Training for Operations," click on the "CTID Operational Environment Page."

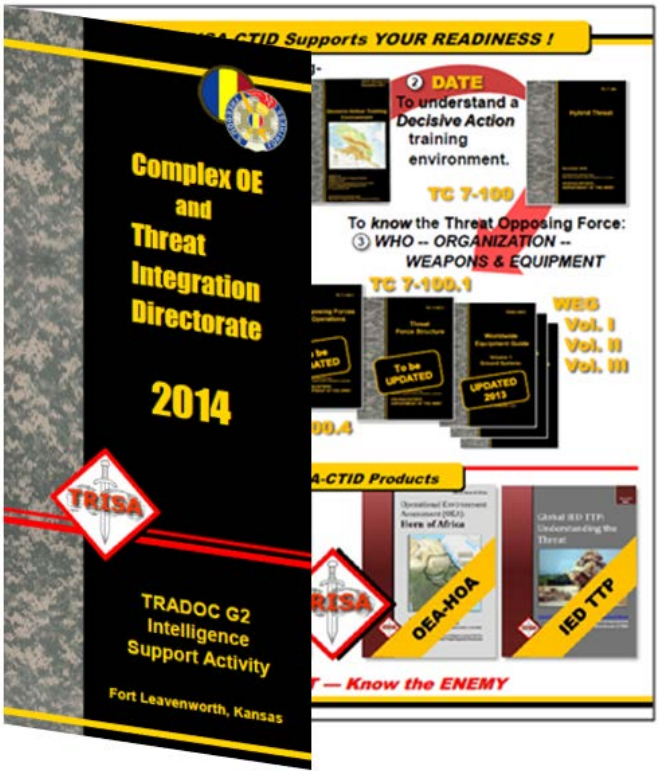
Complex Operational Environments and Threats

We must be prepared to anticipate and defeat myriad hybrid threats that incorporate regular warfare, irregular warfare, terrorism, and criminality.

General Raymond T. Odierno, Chief of Staff of the US Army

PRODUCTS SAMPLER FOR COMPLEX OPERATIONAL ENVIRONMENTS

by CTID Operations



Sampler of Products:

TC 7-100 *Hybrid Threat*
TC 7-101 *Exercise Design*
TC 7-100.2 *Opposing Force Tactics*
***Worldwide Equipment Guide* (WEG) (2013)**

TC 7-100.3 *Irregular Opposing Forces* (2014)

***DATE* v. 2.1 (2014)**
Decisive Action Training Environment

COMING spring-mid 2014!

RAFTE-North Korea
Regionally Aligned Forces Training Environment

RAFTE-Pacific
Regionally Aligned Forces Training Environment

CTID Threat Reports (TBD)

1. Go to ATN front-page.
https://atn.army.mil/

2. See "Training for Operations"
click **"CTID Operational Environment Page"**
or
3. See "DA Training Environment"
click **"OPFOR & Threat Doctrine"**

FIND DATA.

CTID Points of Contact

Director, CTID Mr Jon Cleaves DSN: 552
jon.s.cleaves.civ@mail.mil **913.684.7975**

Deputy Director, CTID Ms Penny Mellies
penny.l.mellies.civ@mail.mil **684.7920**

UK LNO Warrant Officer Matt Tucker
matthew.j.tucker28.fm@mail.mil **684-7994**

Operations -CTID Dr Jon Moilanen
jon.h.moilanen.ctr@mail.mil BMA **684.7928**

Threat Assessment Team Lead DAC 684.7960
Mr Jerry England jerry.j.england.civ@mail.mil

Threat Assessment Team Ms Steffany Trofino
steffany.a.trofino.civ@mail.mil **684.7960**

Threat Assessment Team Mrs Jennifer Dunn
jennifer.v.dunn.civ@mail.mil **684.7962**

Threat Assessment Team Mr Kris Lechowicz
kristin.d.lechowicz.civ@mail.mil **684.7922**

Worldwide Equipment Guide Mr John Cantin
john.m.cantin.ctr@mail.mil BMA **684.7952**

Train-Edu-Ldr Dev Team Lead DAC 684.7923
Mr Walt Williams walter.l.williams112.civ@mail.mil

TELD Team/RAF LNO LTC Shane Lee
shane.e.lee.mil@mail.mil **684.7907**

TELD Team/CoE LNO CPT Ari Fisher
ari.d.fisher.mil@mail.mil **684.7939**

TELD Team/JRTC LNO CGI **684.7943**

TELD Team/JMRC LNO Mr Mike Spight
michael.g.spight.ctr@mail.mil CGI **684.7974**

TELD/MCTP LNO Mr Pat Madden BMA
patrick.m.madden16.ctr@mail.mil **684.7997**

OE Assessment Tm Lead BMA **684.7929**
Mrs Angela Wilkins angela.m.wilkins7.ctr@mail.mil

OE Assessment Team Mrs Laura Deatrick
laura.m.deatrick.ctr@mail.mil CGI **684.7925**

OE Assessment Team Mr H. David Pendleton
henry.d.pendleton.ctr@mail.mil CGI **684.7946**

OE Assessment Team Mr Rick Burns
richard.b.burns4.ctr@mail.mil BMA **684.7897**

OE Assessment Team Dr Jim Bird
james.r.bird.ctr@mail.mil Overwatch **684.7919**

CTID Mission

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

What We Do for YOU

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

YOUR Easy e-Access Resource

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