



AW/IED Defeat Newsletter



“Attack the Network, Defeat the Device, Train the Force”

Attack the Network

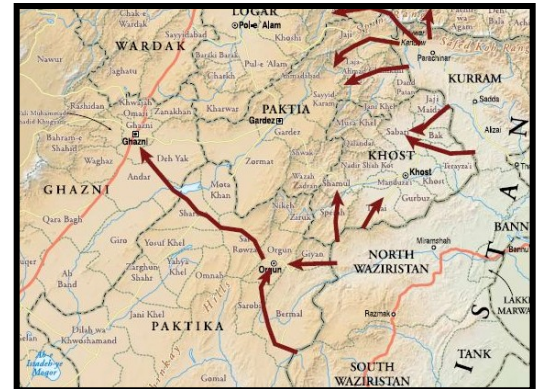
An Excerpt from: Afghanistan Report: The Haqqani Network: A Strategic Threat

This is a small excerpt from this article. Please if you would like the full forty-nine page article www.Understandingwar.org AFGHANISTAN REPORT 09: The Haqqani Network: March 2012

The Haqqani Network is the most capable and dangerous insurgent organization in Afghanistan. The network’s current leader, Sirajuddin Haqqani, effectively organizes the tribal and insurgent groups of the southern part of Pakistan’s Federally Administered Tribal Areas in ways consistent with the interests of the Pakistani government. The Haqqanis use these Pakistani bases as training areas for multiple terrorist groups, including Lashkar-e Taiba, the Islamic Movement of Uzbekistan, and Terik-e Taliban Pakistan. The Haqqani Network uses safe-havens inside Afghanistan to support insurgent and terrorist operations throughout Afghanistan.

The Haqqanis have historically operated within Afghanistan primarily in Khost, Paktia and Paktika Provinces (collectively known as Loya Paktia or Greater Paktia). Many policymakers have mischaracterized the Haqqanis, therefore, considering the group a regional insurgency limited in ambition to controlling a handful of provinces in Afghanistan. But the Haqqani Network is a strategic threat to the Afghan government and a threat to regional stability, as it hosts international terrorists with objectives in India, Central Asia, and the Arab lands. The Haqqani Network now has important logistical support bases less than fifty miles from Kabul. Since 2008, the Haqqani Network has expanded its safe-havens and operating areas into Logar and Wardak Provinces, the provinces immediately south of Kabul.

The Haqqanis and other insurgent groups have used that presence to conduct attacks in the capital as well as in those provinces. The Haqqani Network has also established itself in smaller numbers east of Kabul in Nangarhar, Kapisa, and Laghman Provinces, from which it can threaten key lines of communication between the capital and outlying provinces. Its historical home, Loya Paktia, still serves as a vital base in which the Haqqani Network maintains a sophisticated network of supply lines, facilitation nodes, and safe-havens inside of Afghanistan. That logistical network enables them to conduct operations against coalition and Afghan forces; execute assassination campaigns against key Afghan security, political, and tribal actors; and facilitate the movement of foreign fighters into and around Afghanistan. This logistical trail from Miramshah to Kabul is a key asset for the Haqqani Network, which otherwise would be confined largely to the tribal areas of Pakistan. It is also a key vulnerability, as the safe-havens close to Kabul are necessary for the Haqqanis to facilitate spectacular attacks.



The Haqqanis have long disregarded Mullah Omar’s public orders to avoid civilian casualties, mounting spectacular suicide attacks and assassinations of key security and political figures in Kabul and elsewhere. They coordinate with many other insurgent groups to conduct these attacks beyond Loya Paktia. The high-profile attacks in Kabul are an important strategic communications tool that supports the Haqqanis’ regional and international recruiting and fundraising. They also show the Afghan government and the Western public that the insurgency can launch attacks in the most protected and fortified locations in all of Afghanistan.

Source: www.Understandingwar.org Afghanistan Report: The Haqqani Network: A Strategic Threat

Special points of interest:

- Attack the Network
- Afghanistan 101
- Defeat the Device
- Train the Force
- Enemy TTP’s
- World Wide IEDs
- 52nd EOD News Blast
- Contact Information

Inside this issue:

- AtN: Haqqani Network
- MPLC
- Threat Finance Card
- PBIED-CIED Awareness Report
- Al Qaeda in Yemen
- Biometrics Case Overview

Web based resources:

JKnIFE Fusion net
<https://knife.jfcom.mil/pages/KNIFEpublic.aspx>

JIEDDO

<https://www.jieddo.dod.mil/index.aspx>

COIC Visualization Videos

<https://www.us.army.mil/suite/folder/19815283>

CALL

<https://call2.army.mil>

Engineer School House

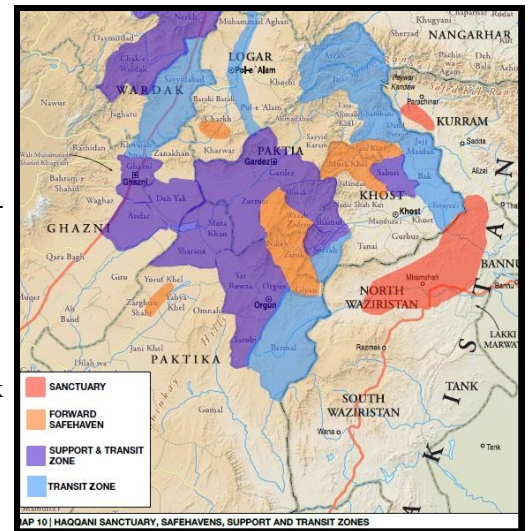
http://www.wood.army.mil/wood_cms/usaes/2390.shtml



An Excerpt from: Afghanistan Report: The Haqqani Network: A Strategic Threat *Continued*

The Haqqani Network has expanded its operational reach into the northern provinces of Baghlan, Kunduz, and Takhar through a partnership with the Islamic Movement of Uzbekistan (IMU). The Haqqanis are able to capitalize on Uzbek disenfranchisement in the north while simultaneously infiltrating the isolated Pashtun communities in that area. The Haqqanis and the IMU also use their northern bases to assassinate political and security officials linked with powerful northern figures, particularly ethnic Tajiks affiliated with the Jamiat-e Islami Party. These assassinations are meant to undermine Jamiat and the northern leadership generally, which has been a historical rival to the Pashtuns as well as to Pakistan. The Haqqani Network is the preferred insurgent group to represent the interests of the Pakistani security services going forward in Afghanistan, as the group is more effective than the much-diminished southern Taliban. The following is where Haqqani Network normally operates:

- The Haqqani Network nevertheless uses Ghazni as a transit and support zone, and has moved foreign fighters into and through Ghazni since 2008. Foreign fighters, including Punjabis, Arabs, Chechens, and Uzbeks, have been reported to be moving through the area facilitated by the Haqqani Network. The activity in Ghazni probably resulted from the Pakistani government's peace deal with Pakistani Taliban commander Baitullah Mehsud in South Waziristan in April 2008. Militants who were no longer engaged in attacks against Pakistani security forces became attractive recruits to the Haqqani Network fighting in Afghanistan. The influx of foreigners caused some tension with local Taliban fighters. Ghazni also serves as a facilitation node in the Kabul Attack Network (KAN), a confederation of insurgent groups, including the Haqqani Network, Quetta Shura Taliban, and Hizb-i Islami Gulbuddin, that work together to execute attacks in Kabul.
- The Haqqani Network, with the support and cooperation of other insurgent groups, has expanded its presence in Logar province over the past several years. Two of the most important factors that aided the insurgency's attempts to expand their presence into Logar were the corruption of state institutions and the sidelining of influential religious leaders in a province with historically high levels of religious sentiment. The Haqqanis' primary motivation for establishing a presence in Logar has been to project men and materiel into Kabul to launch attacks on Afghan, coalition, and other foreign governments operating in Afghanistan's capital city.
- The insurgency in Wardak is comprised of Quetta Shura Taliban, Hizb-i Islami Gulbuddin, and Haqqani fighters. Insurgents use Wardak to engage in a variety of activities, including attacking coalition convoys and extorting travelers on Highway One. Additionally, insurgents in Wardak transit fighters to Afghanistan's Northern provinces and facilitate attacks in the Afghan capital of Kabul, the key focus of the Kabul Attack Network.



The Haqqani Network maintains limited but effective operational reach into Afghanistan's eastern provinces of Nangarhar, Laghman, and Kapisa. Nangarhar is an important and densely populated province in Afghanistan's east. The provincial capital of Jalalabad is a large city that serves as the southeastern gateway to Pakistan via the Khyber Pass. A major highway through the province connects Kabul to the Pakistan border. Nangarhar is bordered by Laghman to the North and beyond that, Kapisa.

The Haqqani Network is well-poised to present a grave challenge to the stability of the Afghan state. Unlike the Quetta Shura Taliban in southern Afghanistan, the Haqqani Network has not been the target of a major coalition offensive. Although coalition efforts have degraded the Haqqani Network's capabilities at intervals over the past several years, the network has tremendous regenerative capacity due to its sanctuary in North Waziristan, recruiting capability in Pakistan, and support from elements of Pakistan's security establishment.



Man-Portable Line Charge (MPLC)

AW/IED-Defeat currently able to provide training on this system; for more information please contact the OPS OIC or NCOIC for further details



The MPLC provides troops conducting dismounted operations the capability to counter trip-wire-activated IEDs and mined antipersonnel obstacles emplaced in urban or other complex environments that restrict tactical movement to selected targets. The mined antipersonnel obstacles come in the form of IED emplacements activated through trip wires at various heights or pressure plates. The MPLC is designed to assist in the clearing of a narrow footpath to a target by exposing, disrupting, or neutralizing IED trigger mechanisms while minimizing collateral effects on noncombatant personnel, structures, and property. The MPLC ability to breach mined antipersonnel obstacles is a critical capability needed by U.S. maneuvering units conducting dismounted operations. Currently, U.S. maneuvering elements have limited capability to breach areas containing mined antipersonnel obstacles where the ISAF Rules of Engagement require the use of precision fires. The mined antipersonnel obstacles come in the form of IED emplacements activated through trip wires (sometimes placed in an elevated position), pressure plates, or command detonation. The Man-Portable Line Charge (MPLC) is a lightweight, man-portable, rocket-launched explosive line-charge system that allows for safe breaching through a complex mined or trip-wired environment. The MPLC provides a precise, portable mine-clearing weapon system at the small tactical unit level that provides forces the ability to conduct clearing operations in urban and complex mined or trip-wired environments with immediate precision fire, from covered or concealed positions, thus increasing mobility and survivability.

NOTE: *The MPLC is not intended to defeat or detonate the IED itself. Any path created by the MPLC must be proofed before it is considered clear.*



The series of photographs in show the detonation and the resulting footpath created by the explosive line charge.

Source: US Army Asymmetric Warfare Group (AWG)



UNCLASSIFIED//FOR OFFICIAL USE ONLY//

Threat Finance Smart Card



Afghan Threat Finance Cell (ATFC)

LNOs:

Cell (07x) xxx-xxxx
SVOIP (308) 237-xxxx

Tactical Site Exploitation Considerations

When conducting a TSE, the following items are considered important to threat finance investigations and should be seized:

- Ledger books, spreadsheets (including blank ledger books)
- Cash, credit cards, cash value cards, ATM cards
- Electronic media (computers, PDA's, CD's, discs, thumb drives, external hard drives)
- Cell phones, calling cards, SIM cards, phone charge cards
- Any paper with letterhead or numbers, Receipts of any kind
- Checkbooks or bank statements
- Business cards (look for hand written phone numbers on card)
- Catalogs or vendor manuals, any mail (envelopes)

Corruption / Bribery / Protection Money Questions

- Who meets with the Police / Gov't office / Taliban to negotiate the bribe / protection money?
- What are the names and phone numbers of individuals involved?
- What is the frequency?
- What is the name (individual, Business) sending the money?
- Are there any specific days that money is transferred?
- Where is the money coming from? (country, city, individual)
- Where is the money sent?
- Why are the funds paid (fear, collaboration, family relationship)
- How much money is paid on a weekly basis?
- How is the money transferred?



Hawala / Financier Questions

- What are the business name(s) of the hawalas?
- What is the **owners' name**? Where does he live?
- Who works in the hawala? **Manager's name**?
- Where is the hawala located? **Address? Grid?**
- What are Hawala's **telephone numbers**?
- Is it co-located with any **other businesses**?
- Does the Hawala use any banks? (get bank names and locations)
- When during the week does the Hawala make the most transactions?

• Routine high value customers? **Names / Tele#s**

a business card is an easy way to gather this information

a photo of the front of the hawala shop is also useful

UNCLASSIFIED//FOUO

Contractor Questions

If you suspect a contractor is being extorted by the Insurgents or paying excessive bribes these questions will help with an official investigation.

- Who is overseeing / funding the project? (USAID, CERP, etc.)
- Are you dealing with the primary contractor or sub-contractor? (Identify the primary contractor)
- How many projects has this contractor completed?
- How many offices does the contractor have? (get addresses, phone numbers, names, etc)
- What is the name / phone number of the manager / supervisor?
- How is the contractor paid? (should be electronic)
- What bank is used to pay the contractor?
- Who provides security for the contractor?
- How much money is the security company paid?

Last Update 16 June 2011

UNCLASSIFIED//FOR OFFICIAL USE ONLY//



EAGLE BLAST — Asymmetric Warfare-IED Defeat


101st Airborne Division (Air Assault)

UNCLASSIFIED//FOR OFFICIAL USE ONLY//

Page 5

Enemy TTP's


Volume 3, Issue 03




Person Borne IED/Suicide Borne IED (Pakol)


C-IED AWARENESS

C-IED AWARENESS REPORT







INERT FOR TRAINING USE ONLY



INERT FOR TRAINING USE ONLY




INERT FOR TRAINING USE ONLY



INERT FOR TRAINING USE ONLY

(U//FOUO) outward appearance of Pakol device does not show evidence of hidden PBIED threat
(U//FOUO) Homemade explosive hidden under the lining
(U//FOUO) Homemade explosive hidden in outer roll of Pakol



INERT FOR TRAINING USE ONLY

(U//FOUO) On 12 February 2012, a Person Borne Improvised Explosive Device/ Suicide Borne Improvised Explosive Device disguised as a Pakol was discovered in a Northern Afghanistan Regional Command Area of Operations. Upon investigation of the device, two layers of a homemade explosive embedded with steel rivets and screws were found hidden in the lining and outer roll of the Pakol. Neither a trigger for the device or blasting caps for initiating the two layers of explosives had been installed.

(U//FOUO) The Pakol is a soft round-topped men's hat, typically made of wool. The hat originated in the Chitral and Gilgat regions of what is now Northern Pakistan. It gained popularity among the Northeastern Pashtun tribes in the early twentieth century largely as a substitute for the turban. It also gained popularity amongst the Nuristanis and the Tajiks of Pansjsher and Badakhshan. It is worn by some Pashtun tribes in Kunar and Laghman. The hat has been identified as a Muslim, Pashtoon or Mujahedeen cap however, it does not have specific religious origins. It was the favored head cover for Afghan Mujahedeen from 1979-1989.

ASSESSMENT

(U//FOUO) There have been several previous events involving Person Borne IEDs/Suicide Borne IEDs disguised as turbans and head wear. Turban devices were used in assassinations and attempted assassinations of Government Islamic Republic of Afghanistan dignitaries. The most notable being the successful assassination of former Afghan President and chairman of Afghanistan's High Peace Council Burhanuddin Rabbani who was killed at his home in Kabul City on September 20, 2011. Following the last attack in 2011 it was assessed that the assassination tactic would evolve to using pakols due to the cultural and religious significance of turbans. These forms of PBIEDs and SBIEDs are assessed as devices which are easily hidden and intended to circumvent security inspections and undisciplined searches at entry control points. It is recommended that ALL hats, head coverings and turbans be inspected however, special cultural and religious sensitivity must be observed regarding search of turbans and other specific ceremonial and religious head wear. Afghan National Directorate of Security officials have warned Coalition Forces in Afghanistan that searching a turban is an insult to Afghan males as the headdress is not easily removed or replaced. CF Personnel conducting Key Leader Engagements should remain vigilant and maintain situational awareness of this threat.

(U//FOUO) ALL SECURITY FORCE PERSONNEL should...
UTILIZE ALL AVAILABLE DETECTION & FORCE PROTECTION MEASURES TO DEFEAT THIS ASSASSINATION TACTIC. ENTRY CONTROL POINTS AND PERSONAL SECURITY DETAILS MUST CONTINUE VIGILANCE AND FORCE PROTECTION MEASURES TO IDENTIFY, LOCATE, AND MITIGATE THIS PBIED/SBIED THREAT.

C-IED AWARENESS REPORT

UNCLASSIFIED//FOR OFFICIAL USE ONLY//



Four dead in south Yemen blasts, al Qaeda blamed

Two suicide bombers drove a car packed with explosives into a Yemeni army base in the southern province of al-Bayda on Saturday, killing one soldier, the Defence Ministry said, in an attack for which al Qaeda claimed responsibility.

Another soldier was killed by one of two blasts aimed at a central security forces building in the southern coastal town of Mukalla, where a March 25 suicide bombing killed at least 26 people. Authorities said they had made several arrests.

Militants linked to al Qaeda have exploited political upheaval to strengthen their foothold in Yemen, particularly in the south which is also home to rising secessionist sentiment. Yemen's south has been mired in violence since protests against former President Ali Abdullah Saleh took hold early last year, weakening already loose central government control over whole swathes of the country. Saturday's attack in al-Bayda, which targeted barracks of the Republican Guard forces, came just days after the interior ministry said it had information about an al Qaeda plot to blow up eight cars in the capital Sanaa and the port city of Aden. "The explosion was very loud and took place in Dar al-Nasr, which is a military site of the Republican Guard," said an opposition website.

"Residents of the town were frightened by the force of the blast, which was felt more than two kilometers away and damaged dozens of neighboring houses and blew their windows out."

In a text message sent to Reuters, al Qaeda claimed responsibility for the attack it said was revenge for crimes committed by the Republican Guard. There was no way to verify if the text was from the militants but they have used the method to communicate with media in the past. The group similarly claimed responsibility for assassinating the security chief in the town of Shibam on Saturday in southern Hadramout province, where a local security source said gunmen fired on the official's car, killing him instantly.

The United States, wary of al Qaeda entrenchment in Yemen, backed a plan brokered by Yemen's wealthy Gulf Arab neighbors under which Saleh handed over power to his deputy last month and secured himself immunity from prosecution.

The suicide bombing in Mukalla last month coincided with the swearing in of new President Abd-Rabbu Mansour Hadi and also targeted the Republican Guard, led by Saleh's son. Al Qaeda's Yemen-based wing claimed responsibility for that attack as well. On Friday, gunmen opened fire on a U.S. security team as it trained Yemeni soldiers in the south.



Source: <http://www.reuters.com/article/2012/03/03/us-yemen-explosion-idUSTRE8220BD20120303>



Biometrics Overview



With a large number of targets across the battle space and an enemy that can freely travel, US Forces in Afghanistan are at a disadvantage of knowing who the enemy is, and being able to accurately identify them. While other Afghans have a distinct knowledge of personalities in their area, knowing who belongs and who doesn't, US Forces must rely on technology and instinct to positively identify nefarious actors. The most effective means of providing this identification is through the use of biometric technologies. Most soldiers are aware of many of the biometric collection devices such as the BAT, HIIDE, SEEK, etc; but many soldiers are unaware of how these devices actually work into the intelligence cycle and support both kinetic and non kinetic targeting.



All tactical biometric enrollments are maintained in a stateside database that constantly searches the fingerprints against millions of biometric records. The records are the result of years of biometric collection in the battle space as well as forensic exploitation efforts at the various forensic laboratories in theater. Most frequently the biometric community will highlight biometric matches to latent fingerprints that were recovered from IEDs and other captured enemy material, however, the bulk of the matches that occur are from “known Biometric collections”. A known collection refers to a biometric enrollment of an individual that is associated with other biographic data such as name, DOB, POB etc. In other words the individual was

physically present and knew the collection occurred. An “unknown Biometric collection” refers to latent fingerprints recovered from material whereas the identity of the individual to which the fingerprint belongs was unknown to the collector. Therefore, there are three basic types of matches that occur: known to known, known to unknown, and unknown to unknown.

Once a match is made someone must review that match to ascertain its importance or as the intelligence community likes to say “provide the so what”. In order to answer the “so what” Biometric Enabled Intelligence Analysts review the circumstances of the enrollments that resulted in the match and link associated intelligence data. The results of this work will often times generate numerous intelligence reports but the primary report that is generated is referred to as a Biometric Identification Analysis Report (BIAR). These reports are then disseminated to the tactical units via S2 channels allowing the S2 at every level to gain a greater understanding of who is operating within their assigned battle space.

Most often this feedback via the BIAR process does not reach the individual soldier who is collecting the actual biometric enrollments which leaves them to ask “why am I required to do this?” To understand the effects of biometrics one must realize the flow of information from beginning to end. While the soldier typically will not see the BIAR, he or she will receive the feedback via the Biometric Watchlist.

The Biometric Watchlist is the means by which all the intelligence work discussed thus far becomes operationally relevant to the war fighter. Many soldiers are familiar with the Biometric Watchlist but have never been taught the full intelligence process that occurs in order to create it. In short, all of the individuals, for which we have a biometric record, that have been classified by the intelligence community as a threat to US interests are added to the watchlist in order to enable soldiers the ability to positively identify these individuals in the battle space.

Joel Reeder
52nd EOD Biometrics and Exploitation Specialist



Biometrics Overview



While background and process information may be nice to know, what the average soldier truly needs to understand are the Biometric Watchlist levels and how to respond to a watchlist encounter. The following is a description of the Biometric Watchlist levels and the appropriate action to take for each.

WL 1 - Detain (High threat, has a warrant or is a targeted individual)

WL 2 - Question (based on potential derogatory information. Enough evidence exists to highly suspect this individual of being involved with insurgency / terrorism related activity. In some cases the subject is considered a developing target and simply awaiting approval from higher commands to kinetically target)

WL 3 - Assess (The person is of interest based on a previous biometric enrollment or situation that garnered the attention of Intelligence professionals. WL3 is not used on tactical devices but instead is monitored at higher echelons. Any further action would be coordinated by higher with the maneuver element.)

WL 4 - Disqualify (Should not receive any DoD sponsored benefits or base access / training / employment. The subject is a previously known threat and has engaged in anti CF activity, however no current information is known that would indicate current anti CF actions. Ground forces should treat as a potential threat and have heightened awareness of the subject's activities. No direct negative action (other than disqualification) should be taken unless circumstances require.)

WL 5 - Deny (the subject is to be denied access to CF bases. The subject has previously engaged in criminal activity. In some cases the subject may have previously been deemed a threat to CF however has since then reconciled their differences with CF and has chosen to reintegrate into a peaceful society.)

WL 6 - Track (any interaction with the subject should be simply to ascertain facts of the subject's movements and purpose and is then to be annotated in the biometric record. The subject is being monitored based on previous suspicious activity or placement and access.)

For additional information and lessons learned, the below MILSUITE site provides a good starting point for biometric discussions. <https://www.milsuite.mil/book/groups/biometricsdiscussionboard>



Watchlist Process



EAGLE BLAST — Asymmetric Warfare-IED Defeat

101st Airborne Division (Air Assault)

UNCLASSIFIED//FOR OFFICIAL USE ONLY//

Page 9

AW/IED Defeat Mission Statement

Volume 3, Issue 03



Provides a comprehensive training environment to prepare military personnel for the deployment to any operational environment, focusing on asymmetric warfare. AW/IED Defeat incorporates current enemy and friendly TTPs into relevant training through the use of classroom instruction, hands-on familiarization exercises, virtual simulators, and FTX/ IED lane support; furthermore, instruction is enhanced by the integration of Mobile Training Teams (MTTs) and the experience of embedded Law Enforcement Professionals (LEPs). AW/IED Defeat also provides instruction in valuable specialized skills to include CREW II Operators Training, Robotics Familiarization, Sensitive Site Investigation Training, Biometrics Training, Search Procedures Training, MINE-HOUND Detector Training, HME Awareness Training, and guidance on the latest counter IED equipment being fielded to the military.

AW/IED Defeat Contact Information

OIC:
LTC Jason Norton
(270) 412-6498
jason.norton@us.army.mil

OPS OIC:
1LT Smith
(270) 461-0253
william.t.smith7@mail.mil

NCOIC:
SFC Jesse West
(270) 461-0253
jesse.r.west.mil@mail.mil

CI2C Lead:
Mr. Thomas Wilson
(270) 412-6497
thomas.wilson3@us.army.mil



Mr. Bill Craft (EW/CREW)
(270) 461-0276
william.e.craft.ctr@mail.mil

Mr. John Cameron (Mobility)
(270)-412-6499
john.cameron@us.army.mil

Mrs. Kristi Sandoval (AtN)
(270)412-6501
kristi.k.sandoval@us.army.mil

Mr. Chris Siget (TSE)
(270)412-6499
chris.siget@us.army.mil

Mrs. Anneliese Ebaben(ColST)
(270)412-6499
anneliese.ebaben@us.army.mil

Volume 3, Issue 04 Unclassified Newsletter will be released 30 April 2012

Newsletters will be posted on the 101st ABN DIV (AASLT) NIPR portal under Special Staff/Engineers/RCP_CIED

Additional Contact

Range 60 Red Team- (Steve Hieber)
(270)798-2638
steve.a.hieber@us.army.mil

RCP Vehicle Sign Out (Scott Galbraith)
(270)352-6654
scott.galbraith@us.army.mil

MCIT Simulator (Mr. Brett Reeves)
(910) 987-6257



RG-31 Trailer- (4)



Buffalo Trailer- (4)

Route Clearance Training Services (RCTS)

VRCT consists of 4 self-contained mobile trailers containing the following equipment:

- 4 Buffalo MPCV virtual simulators
- 2 VMMD (Husky with/without MDT) Virtual simulators
- 4 MMPV (RG-31) Virtual Simulators (Converted to RG-33L after first year)
- 1 MMPV (JERRY) Virtual Simulator
- 1 MTRS (Talon IIIB) Virtual Simulator
- 5 Instructor/Operator Station (IOS)/After Action Review Stations
- 3 On-Site Contractor Personnel
- 5 Separate 40 hour Crew Courses and 5 Separate 16 hr TTT courses

Contact SFC West for more information

UNCLASSIFIED//FOR OFFICIAL USE ONLY//