Intelligence Resource Program

UNIT INT HQ INF BN

Combat Intelligence Team CRPF

April 21
2021

BIJAPUR/CHATTISGARH

Creating Organic Multidimensional Intelligence Capability for CRPF BIJAPUR.

KESHAV CH MAZUMDAR SENT ON A MANDATE FROM CRPF DTE NEW DELHI TO BIJAPUR ON MISSION TO CREATE INTELLIGENCE UNITS.

TRAINER/INSTRUCTOR KESHAV CHANDRA MAZUMDAR ANTITERRORISM OFFICER ID CARD NO A7949976535G

PROJECT CRPF 2020
Organic Intelligence Capability

बल रक्षा करता है
जब
बल संरक्षित होता है

REPORT OF MANDATED MISSION

TO

ADG TRAINING CRPF

CRPF DTE

NEW DELHI

Bn Int Section

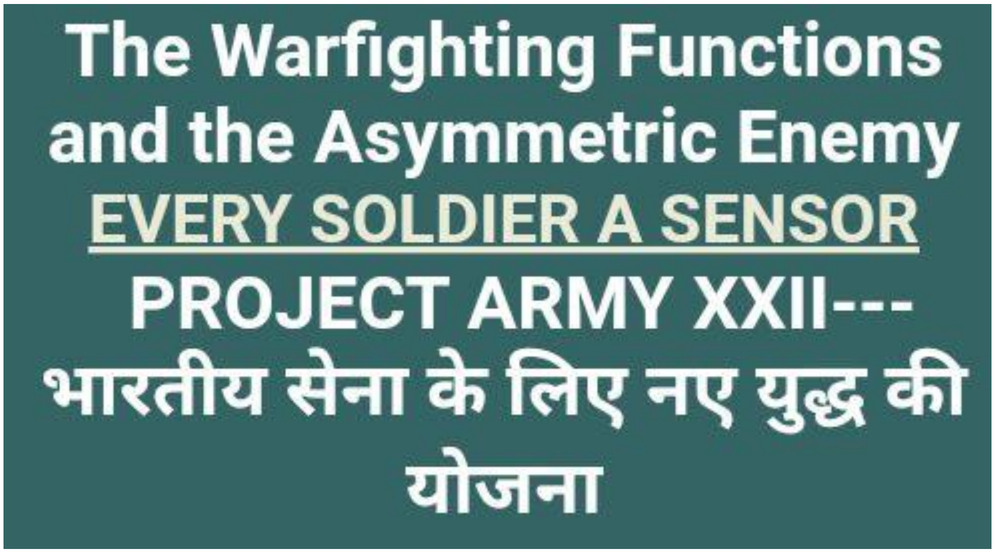
SILO

Structured Intelligence led Ops

REPORT OFMANDATED MISSION TO ADG TRAINING CRPF DTE NEW DELHI

Intelligence Redefined

The area between War and Peace is not empty..intelligence prevades everything

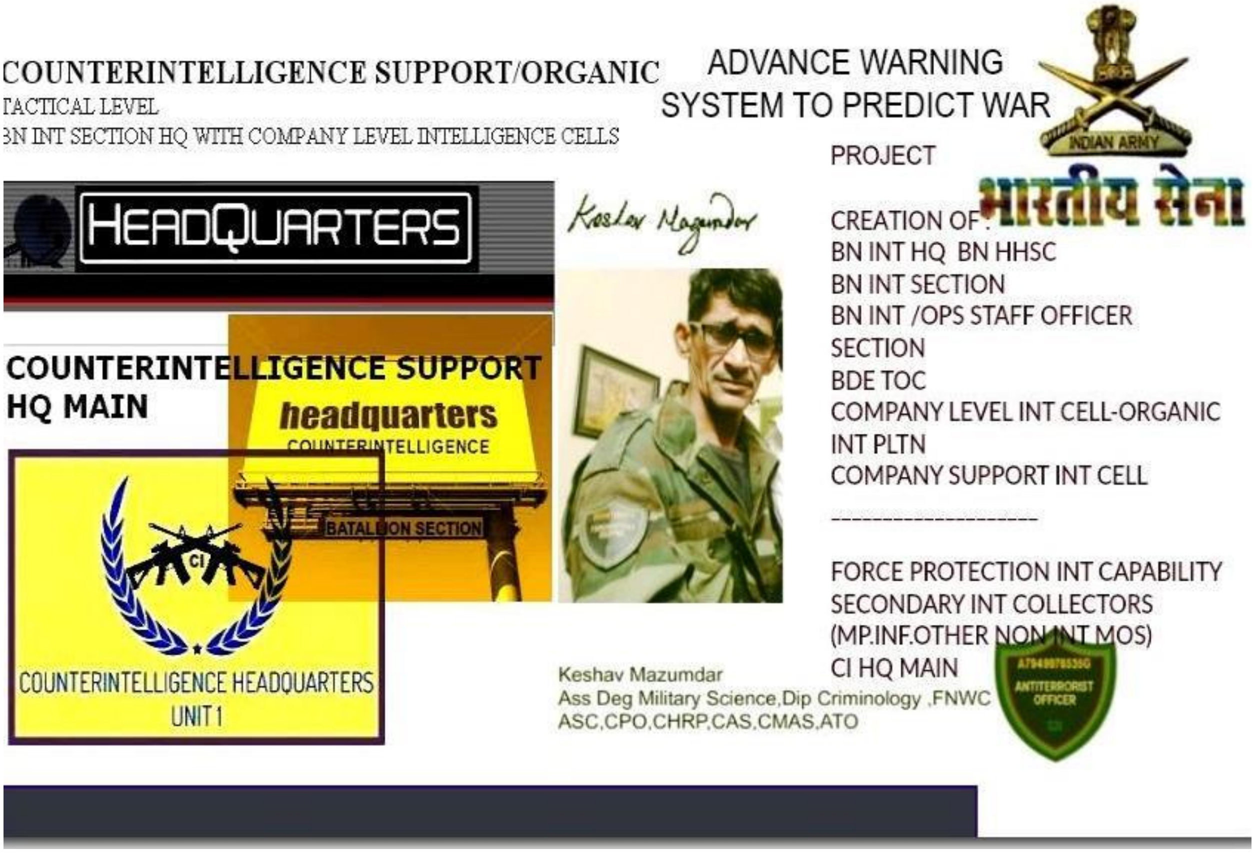


The Warfighting Functions and the Asymmetric Enemy

EVERY SOLDIER A SENSOR

PROJECT ARMY XXII---

भारतीय सेना के लिए नए युद्ध की योजना



COUNTERINTELLIGENCE SUPPORT/ORGANIC
TACTICAL LEVEL
BN INT SECTION HQ WITH COMPANY LEVEL INTELLIGENCE CELLS

ADVANCE WARNING
SYSTEM TO PREDICT WAR

PROJECT

CREATION OF :
BN INT HQ BN HHSC
BN INT SECTION
BN INT /OPS STAFF OFFICER
SECTION
BDE TOC
COMPANY LEVEL INT CELL-ORGANIC
INT PLTN
COMPANY SUPPORT INT CELL

FORCE PROTECTION INT CAPABILITY
SECONDARY INT COLLECTORS
(MP.INF.OTHER NON INT MOS)
CI HQ MAIN

COUNTERINTELLIGENCE SUPPORT
HQ MAIN

COUNTERINTELLIGENCE HEADQUARTERS
UNIT 1

Keshav Mazumdar
Ass Deg Military Science,Dip Criminology ,FNWC
ASC,CPO,CHRP,CAS,CMAS,ATO

EXECUTIVE SUMMARY:

Statement:The Battalions organic tactical int unit intelligence officer plans supplemental intelligence missions so as to adequately exploit the human terrain as infantry soldiers in a COIN environment are the closest to the local population than intelligence assets deployed by higher HQ Int Section.

Elaboration: **The Bn Commander may have access to intelligence from higher HQ assets but frequently the available intelligence lacks the necessary information to plan tactical operations , these intelligence gaps are crucial , and it is imperative the Commander takes initiative to execute supplemental intelligence missions. For this the requirement of organic int platoons is a must. The intelligence officer's duty is to precisely state intelligence requirements after assessing the local environment, threat-populace-other factors, these requirements stem from lack of certain information when planning operations/missions. It is very important that there must be someone who will help the commander to adjust the way he requests intelligence and here the intelligence officer comes into play, aided by the Bn int section. It is extremely critical that the commander has access to the necessary intelligence once it is apparent that, despite intelligence feeds from higher HQ Int assets the**

feeds lack the information necessary for mission planning. Supplemental intelligence mission should follow after a supplementary analysis. This can be achieved by integrating trained inf soldiers within teams, task organizing them with commanders prioritized int requirements clearly stated. Once a supplementary analysis is carried out after int gaps are evident, it is not difficult to plan local int missions by organic int platoons or patrol/combat R&S teams embedded with one of two inf-turned int personnel.

Operationalizing intelligence

Military operations are not all alike even if standard tactics , techniques and procedures are employed or the operation is template on a previous similar operation. The reason is intelligence requirements vary. Each operation success banks heavily on correct intelligence , the risk must be kept to a minimum with success rate high. Intelligence must be available in a format relevant to the military operation. Relevant that is.Operationalized.This is extremely important to understand. The intelligence officer and his staff should understand the military operation in detail and the ops officer of the military unit must understand the intelligence sections argument , predictions, assets limitations and capabilities. What I want to drive home here is say there is a time constraint which prohibits intelligence collection, such as a pre dawn strike or an assault in 24 hours—no time for collection activities. Here required information is not available for planning the operation. Now the intelligence officer will elaborate indicators already known or anything about the particular scenario and going on these lines he will list out key questions that still need to be answered. As he is putting forth all this to the ops officer the latter will reciprocate by making the int officer understand the mission tasking and available options , thus prompting the intelligence officer to take the cue and refine and refocus intelligence collection and analysis in the very short time available. Had there been no this int-ops dynamic , the intelligence officer would have been confused how to allocate and direct his resources/assets in the very short time available for collecting actionable intelligence. This is what is operationalizing intelligence. The primary gain is situational awareness for the commander which will aid mission planning and minimize risk. Risk and options become more apparent and tactical performance is positively ensured by allowing quick and sure responses to rapidly changing conditions in short frames of time. This sort of derived intelligence from int-ops dynamic is operational intelligence.

When commanders are concerned about time constraints, they frequently may not task their collectors and analysts for additional intelligence on the human terrain. There may result inadequacies in the analysis about COIN specific human terrain and battlefield factors due to the difficulty in acquiring required intelligence. Commanders can deploy created organic int teams or augmented combat/recce platoons to collect information as they conduct their own missions. We cannot tolerate inefficient planning for combat

missions due to intelligence gaps. That is what is missing apart from handed down intelligence products from higher HQ int section. Now that is indeed difficult for int higher HQ as personnel limited and cannot cover the entire tactical commanders requirements-boot level that is. For this purpose the tactical organic int capability must be created so that battalion commanders can get their own int platoons crafted out of inf soldiers who can exploit the human terrain , atmospherics , conduct tactical questioning , docex and CEE..all can be easily learnt without prior int knowledge..the result being addressing int gaps not apparent to higher int HQ and boot level collection ops leading to the most imp element—situational awareness of the commander.

We usually find most analysis of collections of information will be isolated from the operational environment in which the data originated(tactical level in fact), and the analysts will therefore be unable to apply the appropriate perspective to the intelligence assessment and correlate data to operational activities at tactical levels. The analysis will therefore offer little insight or contextual understanding of the way a particular piece of intelligence should be considered or whether its use may have unintended effects.

By enhancing the role of intelligence operations, unit personnel can find subtle, ambiguous or fleeting observables that indicate seemingly hidden enemy activities or behaviors. Soldiers must not only collect this information but also quickly record and report mission results, which will prompt additional analysis and result in a better understanding of the situational atmospherics.

The organic field collectors are able to immerse themselves within an area and have daily contact with numerous sources. With their analytical skills, they develop a capacity for judgment, and they may be in the best position to comprehend indicators or warnings that likely would not set off the same alarms within the larger intel apparatus. Under many circumstances, their comprehension is beyond the scope of a distant analyst from higher int HQ who is more focused on a very broad area of operations rather than SOF tactical battles or non kinetic operations on human terrain (locals), who may frequently discard what he deems as irrelevant information. In short, the local collectors can become their own camp-based intelligence community.

An enhancement to operational intelligence would be the conduct of more counterthreat and counteraction activities to collect intelligence clandestinely or to gain intelligence insights for missions. Insurgencies and guerrilla movements facilitated through illicit border-crossing activities rely on mobility, elusiveness and availability of a safe-haven. The trade and transport of drugs, arms and humans rely on the same factors. All these illicit acts require significant active and passive civilian material support, which is deeply

rooted in the human sociological framework. And mind you its these ground troops who encounter most human suspects during the illicit transfer. And these troopers can augment their daily ops by inducting an int platoon drawn from other troopers and basically trained in tactical question and mobile on the spot interrogation at forward areas to extract info of int value in very short span of time and then MP escort them to rear to CI cages. On the spot tactical questioning and interrogation works very well on fresh confused scared suspects and gives them no time to overcome the initial shock of arrest and cook alibi/stories enroute the long way as would be the case when standard TTPs dictate escorting suspects to rear for interrogation with lip service at the time of arrest.

When correctly managed, operational intelligence will be more proactive and pre-emptive and less a reactive, "off the shelf" product that has not been framed for the TACTICAL battle but for a broad AO operational int requirements and created by higher HQ.Point is higher HQ has no way to ascertain and address individual tactical commanders int gaps...this must be NOTED. They just can’t deploy int assets for every commander and very good shortage of int personnel compounds the difficulty. You tell me how many int operatives we have for NE area of operations? Minimal.

DEFICIENCIES

INDIAN ARMY/CRPF INTELLIGENCE – A REVIEW

Lack of Boot-level intelligence capability (Organic int capability – CLIC BLIP)

Lack of Common Operating Picture from Div to Coy level

Lack of aggressive/surge component in HUMINT/CI

Lack of int-enabled RSTABDA – ‘’Fighting for Information’’..rather its ‘’avoid engagement passive R&S’’

Lack of complete understanding of HUMINT term. Confusion between HUMINT and CI.CI Relegated.

Lack of TOCs at every level. Even for deep R&S ops.

Lack of organic int-capability for far flung tactical units engaged in ops—away from Bde HQ Int Section/SO.

Lack of well defined TOE for COIN units.

Lack of full understanding of center of gravity in case of COIN.

Lack of a systematic preparation of intelligence/CI products like Int Estimate ; CI Estimate; Current int brief. CI Review,Targeting report,CI Worksheet

Lack of intelligence preparation of the battlefield ‘’in its entirety’’.No Int/Ops template to find Int gaps from history in AO.

Lack of Force Protection Doctrine and the embedded condition of CI as an enabler.

Lack of functional HUMINT teams such as CEE Team , Human Exploitation Team, Human Terrain Teams.

Lack of Mobile Interrogation Teams

Lack of a complete Int architecture with full technical control , requirements-collection-asset management protocols, synchronized ops-intel,4-way (Higher/lower HQs and adjacent unit HQs)push-pull especially bottom-up push, controlled int-reach for soldiers on the ground and need-to-know at every echelon, integrated WAN/LAN for COP at every level, and many other factors not excluding professional military education for all officer ranks and training routines for enlisted soldiers , NCOs and Senior NCOS/JCOs (with openings for induction of non-int MOS Riflemen).

Lack of Asymmetric Warfare Doctrine – Int

Lack of mission-needs-capability analysis.

Lack of line soldiers indoctrination in basic tactical questioning , screening and DOCEX.

Lack of Concentric-rings methodology

Lack of CI Ops inside camps/bases in peace-time to create vulnerability assessment report. Same during military ops other than war.

Lack of ‘’insider threat’’ prevention-controls enforced by CI.

Lack of Battle-hand off –Int.Be it MOOTHW or Stability Ops.Or URI type scenario.

Intelligence is not just sourced information..corroborated and ops undertaken.Ops should not be designed around only corroborated or validated information..even if the three attributes of intelligence are met..viz specificity accuracy and timeliness.

We are the Blue Forces.Enemy is Red.Like we call on our int assets to visualise Red during the entire int collection process we must use Counterintelligence to visualise ourselves by keeping ourselves in enemy's shoes..red visualising blue.Only then can we know Enemy Intent..the primary goal of the int-counterintelligence double edged sword.

Bn Combat Soldiers as intelligence secondary collectors

कमांडरों की मिशन जिम्मेदारियां (उन सैनिकों के संबंध में जो खुफिया कार्मिक नहीं हैं, लेकिन सामरिक पूछताछ के बारे में जानकारी प्राप्त करते हैं —माध्यमिक संग्राहक)

यह मैंने विशेष रूप से कश्मीर में तैनात हमारे जवानों के नजरिए से लिखा है।

हमारे सैनिक द्वितीयक संग्राहकों के रूप में कैसे कार्य कर सकते हैं

दस्ते/अनुभाग/गश्ती/टीसीपी/रोडब्लॉक/काफिले के नेता:

1. पेट्रोल, रोडब्लॉक, चेकपॉइंट, काफिले - ये सभी दुश्मन कर्मियों (पकड़े गए), नागरिकों, नागरिक संदिग्धों / बंदियों और आपराधिक तत्वों के संपर्क में आते हैं, जिनसे सामरिक पूछताछ की जा सकती है। इसलिए मिशन शामिल कर्मियों को सामरिक पूछताछ में प्रशिक्षित करना है और इसे उक्त गतिविधियों की योजना और तैयारी / निष्पादन में एकीकृत करना है। इसके अनुसरण में गश्ती दल आदि के सभी कर्मियों द्वारा इकाई के खुफिया अधिकारी को रिपोर्ट करने के बाद डीब्रीफिंग की तैयारी करें

2. सामरिक पूछताछ के बाद निकाले गए किसी भी अवलोकन या जानकारी पर मौखिक रूप से (डीब्रीफिंग) या लिखित रिपोर्ट तैयार करें, जिसमें इतनी महत्वपूर्ण (लड़ाकू खुफिया) की किसी भी जानकारी को पहचानने में सक्षम होना शामिल है कि इसे बिना किसी देरी के तुरंत रिपोर्ट किया जाना चाहिए।

3. गश्त, काफिले आदि जैसी गतिविधियों के दौरान सभी ईपीडब्ल्यू/बंदियों और जब्त किए गए दस्तावेजों का सावधानीपूर्वक शोषण किया जाना चाहिए क्योंकि ये खुफिया जानकारी के प्रमुख स्रोत हैं।

4. उपरोक्त सभी को प्राथमिकता वाली आसूचना आवश्यकताओं का कार्य करने वाले यूनिट आसूचना अधिकारियों द्वारा पूर्वनिर्धारित किया जाना चाहिए, लेकिन यदि संबंधित स्रोत द्वारा ऐसी जानकारी दी जाती है तो इनके बाहर संग्रह को नजरअंदाज नहीं किया जाना चाहिए। वे कमांडर या HUMINT अधिकारियों के लिए सामरिक महत्व के हो सकते हैं।

पलटन नेता:

दस्ते/अनुभाग/गश्ती/सीपी/रोडब्लॉक, और काफिले के नेताओं को उच्च मुख्यालय द्वारा निर्धारित खुफिया आवश्यकताओं के आधार पर पलटन नेता द्वारा काम सौंपा जाता है।

इसे निर्देश दें और देखें कि यह पुस्तक का पालन किया जाता है कि गश्त, चौकी, काफिले आदि से लौटने वाले सभी कर्मियों को सब कुछ रिपोर्ट करें और पूरी डीब्रीफिंग के अधीन हो जाएं।

उनके सामने तत्काल सामरिक महत्व की जानकारी प्रस्तुत करने के उच्च महत्व पर प्रकाश डालें

बिना किसी देरी के। यह स्पष्ट करें कि यह अनिवार्य है। इस आशय के लिए उन्हें बटालियन के खुफिया कर्मचारियों द्वारा इस संबंध में निर्धारित प्रक्रियाओं से सभी को अवगत कराना चाहिए।

कंपनी/ट्रूप/बैटरी कमांडर:

दस्ते/अनुभाग/गश्ती/सीपी/रोडब्लॉक, और काफिले के नेताओं को उच्च मुख्यालय द्वारा निर्धारित खुफिया आवश्यकताओं के आधार पर पलटन नेता द्वारा काम सौंपा जाता है।

गश्त में शामिल कर्मियों और संग्रह के साथ काम करने वाले कर्मियों द्वारा सभी खुफिया सूचनाओं की समीक्षा की जाती है और बीएन खुफिया कर्मचारियों और बीडीई कर्मचारियों को अग्रेषित की जाती है। ऐसा करते समय उस जानकारी को हाइलाइट करें जो वर्तमान संचालन या एओ पर्यावरण से जुड़ी है।

उच्च मुख्यालय के खुफिया कर्मचारियों द्वारा निर्धारित प्रक्रियाओं के अनुसार सभी के लिए डीब्रीफ करना अनिवार्य बनाना।

सुनिश्चित करें कि हर कोई यह समझता है कि महत्वपूर्ण मूल्य की सूचना को तत्काल रिपोर्ट करना अनिवार्य है।

बटालियन स्टाफ INT अधिकारी और S3 अनुभाग:

खुफिया आवश्यकताओं पर कंपनी, अनुभाग, स्क्वाड कमांडरों को कार्य दें और स्टाफ मुख्यालय के माध्यम से उनका मार्गदर्शन करें।

इन कमांड स्तरों पर खुफिया जानकारी को नीचे धकेलें ताकि उन्हें बेहतर स्थितिगत समझ प्राप्त हो सके और यह जान सकें कि उनसे क्या अपेक्षित है। इस प्रकार वे सामरिक प्रश्नों को बेहतर ढंग से तैयार करने में सक्षम होंगे।

यह देखें कि सभी गश्ती दल आदि के बारे में जानकारी ली जाए और कोई भी छूट न जाए।

महत्वपूर्ण सामरिक महत्व की जानकारी की तत्काल रिपोर्टिंग के लिए प्रक्रियाएं स्थापित करें।

- **INTELLIGENCE UNIT SETUP**

- **An Organized Intelligence Unit**
- **The importance of a strong intelligence and counter intelligence program at all levels is now a widely accepted doctrine.**
- **It is imperative that all commanders and cadre understand the ultimate goal and the importance of a well organized intelligence program and the benefit that gathering timely intelligence has to the overall unit mission.**

Create a Basic Intelligence Team Structure With The GOALS:

- **1.To identify the enemy top-tier officials**
- **2.The enemy intent (current tactical goals and strategic goals)**
- **3.The strength, disposition, capabilities and organization structure of the enemy.**
- **4.The possible COA's**
- **5.The most likely COA and the most dangerous COA.**

Primary Intelligence Requirement "S.A.L.U.T.E."

- **Enemy's Composition, Disposition, Strength:**
- **Size,**
- **Activity,**
- **Location,**
- **Unit,**
- **Time,**
- **Equipment**

Creating Teams

- **2-3 manned teams,**

- **Each team is assigned a separate task of collection.**

Team Leaders

- **The team leader should exhort his members that given the intelligence requirement by HQ they should strive to generate further Intelligence Reports based on the information available and during collection.**
- **New information may require further probing and exploration.**

Intelligence is Both Reactive and Proactive

- **Members and team leader should be proactive.**
- **Intelligence too is both reactive and proactive.**

Reactive Intelligence

- **An indicator associated with an Intelligence Report should propel the agent to look for corroborating information.**
- **That's reactive. Sometimes we are totally unaware of the unknown.**

On Going Intelligence Gathering

- **The intelligence agent can have an informant or source network in place which constantly looks for items such as enemy movements or any change in enemy positions.**

Intelligence Gathering is Fluid

- **A troop movement can be routine which on first sight can be a normal movement or displacement but on further probing reveals an offensive intent.**

Proactive Mindset

- **The intelligence agent needs to have a proactive mindset, always curious, probing and exploratory.**

Civilian Collection Units

- **Covert or Overt civilian collection units whose members are either having access to physical addresses frequented or inhabited by the enemy or are geo-located in close proximity to the latter.**

Open Source Intelligence

- **Our teams are exhorted to resort to open intelligence.**
- **Frequently OSINT such as any news or enemy propaganda on private and government discussion boards, analyses of tv panel discussions on current situations with reference to the disturbing elements posted on the web, in dailies, or aired on**

radio or tv programs.

OSINT is A Useful Tool

- **It should be borne in mind that globally 90% useful intelligence is collected from OSINT sources and the remaining from ISR platforms.**

Organization Strength

- **Organization, Composition or Disposition, Strength**
- **The command structure and organisation of headquarters and subunits, geographical locations of unit headquarters and subunits, Strength expressed in units and weight of fire delivered by its weapon systems.**

Leadership

- **Leadership**
- **Intent**
- **Weaponry and Equipments**

Combat Effectiveness

- **Capabilities / Combat effectiveness**
- ***TTPs—historical in the concerned area of operations and area of interest.(Tactics used by the enemy unit and Miscellaneous data related to specific task, mission or operations…this will help in determining enemys most likely course of action. Unit history used to judge expected performance based on its past performance)***

Threat Ranking

- **Threat ranking-by violence or activity.**

Enemy propaganda

- **Enemy Propaganda**

Incidents of Violence

- **Recent incidents of violence irrespective of sporadic or concerted nature.**

Local Support

- **Local community and political support.**

Ideology and Political Goals

- **Other friendly groups Such as criminal gangs sympathetic to enemy causes or having same ideology or political goals.**

Logistics

- **Where and how the enemy are receiving logistical support.**
- **Are they self supported.**
- **Are they supported by the local population?**
- **Do they pillage for supplies.**

COMMAND AND CONTROL

- **We must have a command and control setup which will incorporate management, analysis and control of all-source intelligence, and technical control of the operations of the respective intelligence disciplines.**

Headquarters and Communications

- **Have a Headquarters with 2 section Headquarters under its control.**
- **Communications would come directly under Headquarters purview.**

Section One Headquarters

- **One section Headquarters has oversight over All:**
- **Source production teams,**
- **Collection management teams,**
- **Target nomination teams,**
- **Dissemination teams,**
- **Operational management teams.**

Section Two Headquarters

- **The other section Headquarters had responsibility and oversight over:**
- **The technical control element with oversight over:**
- **HUMINT**
- **Counter Intelligence**
- **SIGINT**
- **IMINT Teams.**

All Source Production Team

- **The All-source production team will have a:**

- **HUMINT platoon,**
- **CI platoon or a combination of the two—a Tactical HUMINT platoon and if assets are available an IMINT team.**

Tactical HUMINT

- **The Tactical HUMINT Platoon can have a HQ designated authority, a HUMINT Control team, three HUMINT Teams and one CI Team.**
- **The CI team may be further divided into 2 teams composed of 2 operatives each.**

Size Requirements

- **Mission requirements define size and composition which can vary from the stated composition.**

Counter Intelligence Teams

- **The CI team will conduct Counter Intelligence Investigations, assessments and C-HUMINT ops but may not engage in Counter SIGINT or Counter IMINT as it hasn't any organic capability.**

Intelligence Programs

- **Advanced Intelligence programs provide better actionable intelligence to aid Targeting Officers in the placement of attacks.**
- **The Western Worlds needing to warn civilians of coming attacks also warns those that we are attacking.**
- **Warnings of coming attacks and bombings on ISIS and ISIL clearly show the ISIS fighters evacuating along with the civilians to mix in with the population to come back after the bombings.**

At the very basic Bijapur Field Security in it's most basic form consists of:

Bn Int HQ composed of :

Ops and Int Staff manned by 2 SI and 6 Jawans including 2 Havildar Major..Beneath the Int staff section is the Int Technical Control NCO and the Ops staff section has 2 Havildar Major As Section 1 HQ commander and Section 2 HQ commander.The Bn Commanders Int Requirement Advisor is an SI who also has a berth in Staff.

The two section commanders oversee 3 platoons of 8 soldiers each .

Each of these platoons are made up this way..the table of organization:

- **R&S platoon x 2 x 8 soldiers each**
- **Force Protection Platoon x1x4 soldiers**
- **Counterintelligence Platoon x1x6 soldiers**
- **Interrogation and Exploitation Platoon x1x4 soldiers**
- **Collection and Exploitation platoonx1x10 soldiers**
- **Topography and Terrain Platoon**

INTELLIGENCE OPERATIONS

The success of Counterinsurgency operations are predicated by the availability of timely, accurate and specific intelligence about the enemy,its plans and intent and its strength,dispositions,capabilities and TOE.

HUMINT and CI are two disciplines which help in detecting enemy capabilities , intent and countering enemy intelligence collection activities.In a typical Army Intelligence structure , the intelligence assets are located at Div and Bde levels , with the Bde having a HQ company and Intelligence Bn , each Bn catering to a specific collection/counterint discipline. For example there can be an Ops Bn , a reconnaissance Bn , a tactical exploitation Bn,a forward collection Bn ,or a strategic SIGINT Bn.There is also a Div MI Bn and a theater intelligence Bde.

Military intelligence brigades coordinate, manage, and direct intelligence and surveillance; they conduct collection management, all-source intelligence analysis, production; and they disseminate information in support of national, joint, interagency, multi-national, regional combatant command, and Army service component requirements.

- ➢ **I have attempted to create platoon/company level intelligence structures intelligence support teams , forward projection force with int as enabler--all three with HUMINT and CI assets plugged in.A plug-and-**

play or modular int capability can achieve desired results in today's unconventional warfare where it is distributed , non-linear.Such teams can also play a major role in a very large operational battlespace.

Intelligence Whatever be the divisions in function or overall structure , HUMINT and CI are indispensable to thwart enemy intelligence activities , to conduct force protection in a optimum manner,to keep our forces combat-ready to deliver precision strikes and to always keep the decision advantage in our favor with the element of surprise by the enemy being put at the minimum.Both disciplines are time intensive and inter-human interactions over prolonged periods have turned the tradecraft into a very specialized skill involving human perception,behavior,psychology and other traits.Unlike other disciplines like SIGINT,IMINT,MASINT,GEOINT HUMINT and CI have in common human sources , the human element and hence is susceptible to error , deception by the enemy , fraught with risks and psychological stress including human vices predicated by money and other factors which are usually the byproduct of information-transactions (quid-pro-quo).But it is exactly these problems which prompts intelligence professionals to come up with newer tactics so as to minimize these negative factors and the resulting exploration and research in the field of HUMINT and CI leads to refined methodologies , TTPs which have been found to be effective in many cases.

ISR assets require the flexibility to detect a wide range of emerging threats. While the ability to detect conventional military threats remains important, the ability to address the asymmetric, non- conventional threat gains importance. Tracking the location and activity and predicting the intent of individual threats is a new challenge at the tactical echelon.

HUMINT COMMAND AND CONTROL

Commanders that conduct HUMINT operations take responsibility for :

- **Constituting task organizations**
- **Assigning missions**
- **Execution of the mission**
- **Mission accomplishment**
- **Designating the AO for each mission tasking.**

Commanders must ensure mission accomplishment by optimally allocating resources and logistics to support HUMINT operations,keeping in mind the constraints and time.The Commander should make adequate arrangements of training of his MI unit personnel.There should also be cross training of HUMINT operators and HUMINT applications personnel.Each Should know the others method of operation.Thus he can ensure the operational readiness of his

personnel.The Commander analyses higher headquarters intelligence requirement,requests for information from adjacent and subordinate units,tasks his organization,states the mission,tasks the HUMINT collectors,executes the mission,accomplishes it and conducts a post operation review,manages any discrepancies or gaps in intelligence(maybe again tasking his men).He is accountable to and responsible for all HUMINT activities and should see that they confirm to doctrinal guidelines.At this juncture he should fully liaise with the technical control team and OMT. He issues mission orders to subordinate unit commanders, being as detailed as possible and giving as much time as can be allowed.

Commanders must:

ϖ Must understand and know the enemy,his organization,his ISR capability,his counter-ISR capabilities,his threat platforms,the terrain over which it exercises control and how the terrain can be an enabler for his HUMINT/C-HUMINT operations.

ϖ As regarding his own HUMINT units he should understand the constraints,technical and operational,under which they function

ϖ Should ensure synchronization of operations with intelligence

ϖ Should ensure the best training of all personnel in his units

ϖ Optimum reconnaissance and surveillance in close co-ordination with higher HQ , adjacent units,subordinate units and staff is very important--he should implement this.

ϖ Should keep higher HQ informed of manpower,equipment ,logistical and operational updates,any shortcomings,requirements or any enhancements required.Advises higher HQ of capabilities and limitations of his HUMINT assets.

ϖ Should continually supervise each and every operation,create a feedback system and use the feeds to ensure high quality and technical control of both the operations and HUMINT products.

ϖ Ensures personnel are working within legal, regulatory, and policy Guidelines.

Your intelligence system has some limitations you must understand. These include-

1. Dissemination of information is highly dependent on communications systems and architecture and these are usually limited and under constraints in different fighting environments. Often requests for information from ground units are not disseminated in time. Accurate, timely and specific actionable intelligence is necessary to drive operations with that distinctive competitive edge and this is usually lacking.

2. Single-source collection is susceptible to adversary control and deception.Muliple sources need to be deployed and multidisciplinary intelligence collection platforms should be employed.
3. Counterinsurgency operations may be affected if the enemy resorts to non-usage of communications/no communications equipment (to avoid getting intercepted or DF'd)thus affecting adversely COMINT and ELINT based intelligence collection. Thus our intelligence collection effort gets degraded by the enemy.
4. Weather degradation of traffic ability and the negative effects of high winds on antenna arrays and aviation collection and jamming systems.
5. Inability of ground-based systems to operate on the move. Positioning and integration of mutually supporting ground and airborne systems is critical to continuous support.
6. Lack of sufficient organic intelligence assets to satisfy all your intelligence requirements.
Current asymmetric intelligence collection is the primary means to combat insurgency successfully by gaining a thorough situational understanding and developing first hand combat intelligence. This tactical environment needs our fighting troops to be trained in tactical intelligence collection to deal with an asymmetric enemy.
When a battalion is deployed, and usually stability and support operations are at battalion level we usually see that the battalion itself rarely executes its operation as a single unit. It devolves into sub-divisions which take up strategic areas in the overall area of operations. Detached posts/stations are set up in these strategic areas and these posts /sections create and maintain unit intelligence cells engaged in tactical intelligence collection on the enemy. Each garrison unit engages in low level source operations using standard intelligence collection methods, and getting a feel of communication routes.locational economics, topography and geography, human terrain intelligence and the political forces operating in the community together with any other criminal enterprises working hand in hand with the insurgent elements

ISR OPERATIONS

Commanders Role

1. You must clearly state your intelligence requirements, prioritized and otherwise, to your intelligence

officer. You should also tell him when you must know the information.

2. Ops must be integrated with intelligence. Hence your ops officer should work closely with your intelligence officer and every plan, course of action must be coordinated with the intelligence officer.

3. Be fully aware of all the multidisciplinary collection platforms available to you and their capabilities. You must also be aware of any collection platforms being used by adjacent units and to what extent arte they available to your unit.

You must take stock of your intelligence requirements along with these limited intelligence collection resources and pair them in an optimal manner so as to achieve maximum efficiency despite resource constraints.

4. Involve your entire staff while performing the intelligence assessment of the battlefield, the enemy, the course of actions open to both, the strength, capabilities, dispositions of the enemy. The intelligence officer should not be the one conducting these functions. Everyone should be involved with you, the Commander steering the effort in the right direction.

5. Make sure that the ops officer understands all intelligence platforms available, their capabilities, which are the ones to be configured for his needs and similarly the intelligence officer must understand the ops details, tactics etc.

6. Regarding reconnaissance, detailing personnel and allocating them the collection assets and sending them on a well defined mission after briefing them with well defined, clearly stated priority intelligence requirements, these are your job as a commander.

7. Required intelligence information may be several. In other words you may have identified several intelligence gaps. But at the same time you must be aware that the limited collection assets you have in hand may not be sufficient to answer all your intelligence requirements. Hence first prioritize your intelligence requirements. Out of all these prioritized intelligence requirements, properly listed, choose the ones that are critical to your decision making process , those that are very time sensitive. Handle these first. Be careful to see that collection efforts stay focused on the prioritized ones and do not get diffused. To this end keep a close tab on your ops officer and intelligence officer.

8. Synchronize ISR ops with higher HQ and ensure that subordinate units have sync’d their ISR plans with yours.

Keep the summary given below in mind:

MISSION ANALYSIS --◊ begins with higher headquarters order analysis to extract ISR tasks with all constraints implied.

Ist Step-◊ IPB Intelligence preparation of the battlefield.IPB products viz., enemy characteristics, event/situation development, terrain, demographic and weather characteristics, High Payoff Targets and High Value Targets (Target folders) and updated intelligence estimates.

The intelligence officer (supported by the ops officer) armed all the above information identifies t intelligence gaps in the following manner:

Those that can be answered by intelligence reach , requests for information to higher headquarters , existing running ISR operations

Those that are not yet determined and ISR operations need to be conducted.

The second type of information gaps pave the way for Information Requirements, Critical Information Requirements and Prioritized Information Requirements as inputs for the next step of ISR planning.

The intelligence officer , in addition to identifying intelligence requirements properly classified needs also to take into account threat factors , terrain effects , weather effects , civil considerations that may benefit/constrain/limit ISR assets functioning and capabilities and overall affect the ISR planning.

CRPF

FIRST INT UNIT

DESIGNED ON AMERICAN TTPS

KESHAV MAZUMDAR

TACTICAL INTELLIGENCE OPS CONTROL CENTER

K.Mazumdar
Project Army XXII
2016-2017
INDIA

EXECUTIVE SUMMARY

The WHY behind a new approach to dealing with uncertainty.

My intent is to incorporate solution for UNCERTAINTY in warfare in existing Doctrine.Uncertainty leads to Surprise , something which is the primary endeavour of any Commander in warfare.Indications and Warning surely affords a solution , but indications and warning often leads to a reactive intelligence collection..we wait until a new capability or weapons system is discovered , that capability or system is implemented by the enemy with devastating results , still we cannot counter it as it being new we do not have a defense system nor a counter-system , and by the time we develop it they have either have had sufficient time to test it practically on us and develop it further or we have had terrible losses in our armed forces , installation , C2 nodes or for that matter overall defeat.Had we incorporated adaptability , creativity , exploration , continual experimentation , critical reviews of existing tactics , techniques , procedures and SOPs in light of intelligence information about an asymmetric enemy with our counterintelligence being totally offensive to get us information on plans before the indicators surface (thats why I said reactive intelligence collection--before the indicators surface we know nothing of their plans) then we wouldn't be taken by surprise and we would have been prepared for that new developed capability or weapons system.

In present times we are dealing with asymmetric enemies more and more be it insurgency , terrorism or even conventional enemy with a solid devastating new capability or weapons system or tactics which far offsets our capabilities , weapon system or tactics granting him an asymmetric advantage.

Lets start by touching on tactics and techniques and procedures in this light of asymmetric warfare:

Tactics:

At the point of engagement.We have a repository of tactics , laid down the ages by different types of combat scenarios.In order to counter an enemys attack we resort to an arrangement of methods known as tactics.We cannot depend on one particular tactic.What we have is a menu..We simply choose which one suits the current tactical/operational environment to inflict a defeat on the enemy.We can never have a surety of which tactic to use in the case of asymmetric warfare , each application is unique.It could be that previously the tactic was used with success in one particular type of combat situation.It could very well be the asymmetric enemy has adapted itself to most of our existing tactics

and invented their own newer tactics and here we are caught badly;we have nothing in the menu to choose from.An adaptive enemy can inflict havoc if our doctrine is not flexible..Is tuned to conventional form of warfare.We should remember UNCERTAINTY leads to a lapse in the situational awareness and development of the commander , thus he does not know what to plan , and thereafter what tactics , techniques or procedures he will employ.Doctrine SHOULD focus well on a WARNING system.To envisage and implement a good warning system so as to reduce the critical factor uncertainty and hence eliminate SURPRISE , we need a solid proactive intelligence setup in place with a robust counterintelligence framework.

1.Without a good intelligence setup we cannot fathom enemy's intentions ;hence uncertainty exists.

2.We have intelligence reports about the timing , plan and even existence of an enemy attack but we interpreted so badly that uncertainty still exists as to why the attack happened.Here again intelligence failed..We did get intelligence on plan , timing and on the attack itself but could not collect sufficiently to decipher the strategic intent..Or even the intermediate intent.We defined our intelligence requirements improperly(critical in collection management , given in my book on HUMINT);in fact facing an asymmetric enemy or even the invisible terrorist it is very difficult to judger intent despite the happening of the attack.This is usually not the case in conventional warfare.Where we can make good guess about the OB , conduct an intelligence preparation of the battlefield..conduct aerial reconnaissance , exploit using counterintelligence and intercept radio signals.But in asymmetric warfare , in urban/jungle terrain;all this is very difficult or near impossible.

3.Even the existence of a new weapon by the enemy..Or tactic..creates uncertainty.Ok we have information on this new weapon.Fine.But did we study it closely?Did we log all the attacks made by this new weapon or did we focus only on its particular characteristics which just fits our current tactical requirements?If its a new tactic developed by the enemy did we explore to see how often it has been used and to what degree of success?The latter can pinpoint our vulnerabilities to this type of attack. As the potential for asymmetry increases, so does the level of uncertainty and the potential for tactical, operational, and strategic surprise.

These 3 cases demonstrate that despite good collected intelligence there will still be gaps..And in the case of the elusive asymmetric enemy these gaps can be big..And these intelligence GAPS NEED TO BE IDENTIFIED , INTELLIGENCE REQUIREMENTS CAREFULLY DEFINED IN LINE WITH THESE GAPS AND A COLLECTION PROTOCOL DEVISED.Only then we can reduce uncertainty and hence the critical element SURPRISE.There is no playbook of tactical solutions;

Techniques and procedures.

Techniques are the general, detailed methods soldiers and commanders use to perform missions and functions--in particular they are methods how we utilkise equipment and employ manpower.Procedures are standard and detailed courses of action to achieve objectives or complete an assigned tasking.Doctrine is built up on the foundation of techniques and procedures--these form the lowest rung.Techniques and procedures are built in the force , integral to the force , are set standards and give an uniformity to the overall setup of the security of an installation or information acquisition/dissemination and the security of plans , operations and other activities.If we have to project any changes we keep as baseline the SOPs..the SOPs are the ''technicals'' in war matrix.Techniques and procedures vary with organization , equipment and environment.In brief techniques and procedures set down standards of operating and are instilled by repeated training.The military saying--''Train as you fight and fight as you train'' aptly describes the importance of techniques and procedures.The adage that forces fight as they train is applicable. Armies cannot afford to make everything up as they go. Of necessity we apply existing techniques And procedures against asymmetric opponents, and with some adaptation, they work. In other cases, if there are no existing techniques and procedures, and innovative combinations of existing Techniques and procedures will not work, we develop New techniques and procedures to integrate into existing Ones to solve a unique problem. If it appears the situation that prompted the change might recur, we must tell other forces about the solution so they do not have to learn from bitter experience.

Uncertainty is critically responsible for defeat through surprise and to reduce uncertainty combat forces need to be aggresively adaptive.Combat is adaptive in nature as all military forces adapt to changing tactical , operational environment.No admixture of tactics , techniques and procedures can be used as standard prescription solutions , doing so might resulty in defeat.Here again I stress on uncertinty--be it conventional warfare or asymetric

warfare.Military drills and OPs need to be continually assessed against current scenarios.Especially so in an asymmetric type of conflict.Techniquers and procedures need to be adapted to the current environment , for this creativity , experimentation , exploration training , dissemination and critical reviews are needed.

Existing doctrine e might have the answer to the employment of a tactic by the enemy to ensure their asymmetric advantage.This means that the commander can selectively apply existing tactics to counter that advantage by recognizing some inherent weakness in the enemy.We have a certain weakness the enemy knows and who can capitalize on that.To prevent that we go by selected relative strengths and complementary means to protect that weakness.Say for example the enemy employs a hit and run technique with high mobility in hilly areas and on the plains..As being on foot they can negotiate areas/lanes/passes easily than us who are mounted on vehicles.The enemy here has a clear asymmetric advantage.But come winter the commander got intelligence that they cannot move far from their camps but we can as we are moving in self contained vehicles to counter the winter and adequately armed and protected.Now the commander has an asymmetric advantage.Hence during the winter the enemy does not venture far from their bases so the commander envisages a plan wherein we attack hard right on the enemy camps.As a result they either have to vacate and retreat to safer bases or get killed/captured.So the commander develops an asymmetric approach which the enemy cannot counter.Here we find the solution was standard tactics existing in our doctrine , only what needs to be done is to understand perfectly their weakness vs.-a visa our weaknesses and hence the corresponding asymmetric advantages and disadvantages.The commander need not develop any technology to solve the military problem.The answer is there but available only if the commander can correctly asses the enemy actions. that during winter the enemy is most vulnerable in terms of mobility. The commander MUST EXPLOIT ANY ASYMMETRICAL DISADVANTAGE. OF THE ENEMY , or in other words any asymmetrical advantage he gets his hands on.But the most important thing to note here is even if we realize our asymmetric advantage we must properly tie it to a strategy..Not just employ tactics randomly.We had the asymmetric advantage in winter in terms of mobility..The strategy that worked was to hit them right at their bases .

So on one hand doctrine might not have the answer to a new tactic and again on the other hand our commanders must possess creativity and the ability to take rapid initiative to achieve an asymmetric surprise using standard selective tactics , techniques and procedures against the backdrop of careful assessment of the enemy tactics ;or in other words the commander executes doctrine in newer ways hitherto unexplored. .

Counterinsurgency or for that matter when we write doctrine for any form of asymmetric warfare we must remember we have to adapt to ther enemys asymmetric capabilities , both potential and actual and configure our asymmetric capabilities in tune of the formers so that when they apply their new tactics they cannot counter our capabilities.True we have a huge repository of tactics by virtue of being a much superior force in terms of all military factors but these are useless if we do not incorporate flexibility and adaptability in our doctrine.This is not the conventional enemy with a predictable order of battle , table of organization and equipment and standard army doctrine. While writing doctrine we must not forget asymmetric warfare leads to second and third order effects which further requires more flexibility and adaptability.For example in a COIN environment there are more players like local village heads , centers of political influence , corrupt administration officfials of the local government , press , social groups and the local inhabitants themselves in the area of operations apart from religious institutions.Any tactical victory ..that is to say victory in first sight can have second and third order repercussions among these environmental variables and these can be negative or positive , they can be capitalized by the enemy , the enemy can extract sympathy from affected villagers or can resort to extensive propaganda highlighting the negative effects of the so called victory on local variables.Second and third order effects can give rise to further exploitation opportunities to both sides.

Characteristics Of Effective Doctrine

Effective doctrine in an era of increasing asymmetry must have the following characteristics:

Conventional warfare doctrine projects combat scenarios assuming a symmetric enemy.We retain an edge over the enemy with our superior strength defined by superior capabilities.As long as we have these capabilities we can match any symmetric enemy.What if we are facing an asymmetric enemy which doesnt stand a chance against our capabilities?What if recognizing this fact they resort to a newer capability whose configuration is so different that our conventional capabilities repository lacks an answer to that capability?We resort to an examination of our capabilities vis-a-vis to their newer capabilities and find we are short of effectiveness , say in one particular capability.We

delete it from our repository and unless we cannot design a superior capability an area of vulnerability is created , inviting the enemy to resort to an effective course of action..We must replace that void with a superior capability or we suffer defeat.It could very well be that particular enemy capability is there before our eyes but we failed to assess the efficacy of the capability in the long run.The japanese lance torpedo inflicted good casualties for quite some time on the US Navy in the second world war until one day this lack of counter-capability was realized by the americans and they designed a counter-system.Hence Doctrine must have an operational concept that includes more than high-intensity conventional warfare.

During writing doctrine we must forecast , not predict what is going to happen in the near term or in the long run.We should be able to accurately assess the enemys future intent and mind you this is not predictive intelligence , this is forecasting based on collected intelligence inputs.Prediction is different from forecasting.In forecasting we have as premise a database of information which you can say acts more or less like a statistical system on which operations are executed to infer , to forecast.In intelligence parlance we conduct intelligence analysis.Again here we should have a solid collection and asset management system with requirements management in the fore.Properly defined requirements , that is intelligence requirements predicated by intelligence gaps , can save a lot of time and effort and very less wastage of collection assets would result.Also ISR synchronization will be feasible.

In our doctrine we must pull our past successes and failures , current developments , including all available combat information-be it theoretical , historical or empirical so that the database on which forecasting is based can be well understood by our commanders and line soldiers.

In asymmetric warfare we are confronted with an enemy which is quick to adapt , moves unpredictably , has no properly discernible order of battle or movement patterns which are rather very ambiguous , which uses the physical and human terrain very effectively , which resorts to cunningness and deception , which mixes in with the local population and wears no uniform--all these factors present a highly asymmetrical enemy and hence the first and foremost thing we need to incorporate in our doctrine is exactly what are we after , the precise definition of the problem which is facilitated by an intensive study of the physical and human terrain , sending in our HUMINT collectors and agents to conduct a thorough intelligence preparation of the COIN battlespace--so very diff from conventional ones--to determine the social , cultural , demographic , political , military , logistical networks and

,physical terrain and other physical factors like safe houses , staging areas,--so that we clearly understand the problem in hand and devise a suitable remedy.We must be adaptive.Highly adaptive--discarding standard intelligence collection ops and resorting more to HUMINT , CI supported where possible by IMINT.Tactical HUMINT teams at platoon level comprised of a mix of HUMINT and CI operatives , one linguist , one psyops agent and one civil affairs /liaison operative can accompany standard R&S Patrols --tactical questioning does not require specialised intelligence training and there will be ample opportunity during recce when you come across civilians , refugees , village heads who can be exploited and valuable information extracted.Hence the bottomline while writing a doctrine is you need to be adaptive and creative like your enemy and be prepared to innovatively implement newer techniques of intelligence collection.More important is that the entire command should be involved , right from the highest level to troop level.Pushing intelligence capability right down to troop level is a MUST.Every soldier should be a sensor..even infantry men or support services personnel.These are secondary collectors , very very vital furan accurate assessment of the battlespace , for building up the situation awareness of the Commander.Only detailing intelligence detachment personnel to support units is NOT enough.THIS POINT SHOULD BE NOTED.In my books elsewhere on this site I have detailed company intelligence support teams structure , platoon level/company level organic intelligence unit , projecting intelligence capability beyond area of operations (as insurgency in the current AO can have second order effects in adjacent areas or it could well happen that the moment current ops are over in a particular AO the commander is ordered to proceed further into unexplored territory and doing so without previously allocating some intelligence resources so as to gain advance info(while ops are currently on in the previous AO) will cause a wastage of critical time as assets will have to be deployed again with reconnaisance and surveillance teams to conduct an intelligence preparation afresh--you just cant barge into unknown territory , particularly a jungle or urban environment where a highly cunning adaptive asymmetric enemy lies in wait.

Doctrine must educate the Army to the fact that military actions often have second- and Theodore Effects (the law of unintended consequences).Uncertainty and asymmetry compound these unintended consequences.The insurgent force for example may or may not have a match for one particular capability of our much superior deployed military force If it doesnt then to them we are most asymmetric and hence will be deterred from making attacks.Hence we must reinforce and capitalize on our strengths and apply them in an asymmetric fashion.Doctrine should do exactly this , focussing on our particular strengths and capabilities which may or may not find their equivalent in enemy forces and guiding us to properly apply them in an asymmetric fashion to retain the asymmetric edge over an asymmetric enemy.

Doctrine must include a system able to rapidly reassess current TTP against emerging threats,capture innovative solutions to new tactical problems,and promulgate new TTP to the field, actively and regularly collect lessons learned in the form of new and modified TTP and produce and disseminate reports that capture new TTP. We need to support this effort and improve its already superb ability

Promulgating New Doctrine

If out army is a dominant one , the enemy will resort to more and more asymmetric attacks.We should recognize this and base our Doctrine on exactly this concept.Offensive , Defensive , Stability and Support operations should evolve around the nucleus of asymmetric dimension.In asymmetric environment , its a two sided street.In fact tactical combat are the order of the day..we are fighting battles , not wars.The soldier on the ground needs to take the initiative , intelligence capability must be pushed down to him and all technological advancements should be made with the objerctive to complement his capabilities , not replace them.Conventional ISR platforms should never be solely depended upon , HUMINT should be given top priority alongwith CI and SIGINT.C2 should emphasis ground level initiative , technical control should be more refined and a must and asset , collection management predicated by sound requirements defibnition.Tactical questioning , secondary collectors , and counterintelligence plugged into modular intelligence support teams should come into existence rather than the standard Det-type support networks.Execution of military operations should be decentralized , more initiative given to lower and middle levels of command , every soldier a sensor , mission command will be successful if all these levels are involved by their commanders exercising a disciplined initiative keeping the the main commanders primary intent in perspective.

We should not only assess the current operational environment by conducting pre and post operation review on standard lines , such as intelligence preparation of the battlefield , battle damage assessments ,successess of psyops , humint and CI successess and failures , but also on the 2nd and 3rd order effects , and tertiary effects like that on contiguous area or near-distant areas where , say , insurgency is in the budding stage and developments here can influence that movement--for example the insurgents could escape to safe areas there and reinforce while at the same time assist the budding movement , or post battle effects in current AO leads to a psychological effect in the adjacent areas or other areas of interest initiated by political groups , pro-insurgent groups and the like.Doctrine should strews creativity and exploration--the latter can also be manifested by intelligence

projection cum R&S Teams , foraying into unknown and untested territory with the intent to aid the commander still busy in ops in current AO in situation awareness and development of the area of interest where orders might come anytime to move in to clear and secure , hence the commander wont have to waste time and effort in intelligence collection and resources wont be wasted .Doctrine should include all military theory of conventional battle operating systems and conduct a thorough review in light of asymmetric conditions to achieve all what has been said so far.Where do we stand right now in terms of Army Doctrine for operations against increasingly asymmetric Opponents?

Uncertainty is the lowest common denominator for Doctrine to be written for current operational theorems and recent operational experiences.Am not saying that we discard earlier doctrinal concepts or expunge them.In fact Doctrine came into existence since the earliest Wars like those during the era of Napoleon Bonaparte and during WW1.Over the centuries combat principles , phenomena have been observed , distilled , compiled and assimilated.Classical theories like battlefield operating systems have also been studied and incorporated.Wars have been won using these doctrinal concepts.But wars have been lost too--like the Japanese Lance torpedo , the sudden advent of the machine gun , tilting an asymmetric advantage in favour of the proponent force or the total lack of technology to clear minefields.A conventional enemy could also get a huge asymmetric advantage by the creation and successful deployment of a capability or weapons system , which springs as a total surprise for our military , has devastating destructive effect and where we have absolutely no defense system.This is where previous existing doctrine fails.We need to continually study and assess our past successes and failures , but most important we need to undertake a critical review of our existing operational and tactical environments , experience and leave room in our doctrine for adaption to the uncertainty arising out of asymmetric nature of current conflicts as uncertainty leads to intelligence gaps and this gaps if not attended to leads to bad situational awareness of the commander finally leading to the very tenet of victory in war by the enemy--SURPRISE.

Doctrine should be so developed to support all levels of operation,from tactical to strategic.Int assets are usually at Div/Bde levels,to place CI assets vat operational/tactical levels requires a great expansion of the CI Corps.Organization structure , training and equipment for CI Corps depends on Doctrine which is created by drawing on wartime experiences and after action reviews AAR.

Hence we must write doctrine where :

Doctrine must keep uncertainty in the fore , in focus , sharp focus and where applicable may permit usage of prescriptive type of solutions (if absolutely the combat scenario is a template mimicking a previous situation) but should not encourage only such type of solutions but should keeep uncertainty as a predicate or in other words , should be prepared to adapt to the most asymmetric type of conflict where standard routine combat templates dont exist. Everything is fluid , changing , with the element of surprise not only in the beginning of the conflict but can happen again anywhere during the course of conflict.Doctrine should enable exploration , criticism , experimentation , creativity and adaptation. Current TTPs should be creatively applied to newer battle configurations.And thee should be room to create entirely new TTPs to confront newer battle conditions.

We must recognize our asymmetric advantages , these may not be recognized as such ..may be misinterpreted as enhanced capability--the term "asymmetric advantage" is important here as if we view it from this perspective with all knowledge about nature of aymmetric opponents and warfare , we can then leverage our advantage in a proper manner , asymmetrically.Yes-asymmetrically.

Continual assessment , review and feedback with regard to e existing doctrine is critically important.We must retain successful and useful concepts and discard those which have failed to stand againmst our enemies or more important those that have been rendered useless by our enemies.

Doctrine should emphasise a new form of leadership training where leaders are tuned to asymmetric conflicts apart from education in conventional warfare.Just like a fresh intelligence graduate from the intelligence officers school who is assigned to a Det takes a long time to be an intelligence professional , thus his throughput being much low during his tenure in the unit till he has imbibed professionalism , similarly commanders who have led conventional operations find it difficult to properly handle asymmetric type combat situations where their experience fails , where they get trapped in intelligence traps wherein previous experience moulds their behaviour while taking decisions , planning , setting COAs and issuing intelligence requirements to collection agents.Not only this ,they , due to this intelligence trap ,discard others opinions with the "I AM RIGHT AS THIS IS THE ONLY WAY OUT , THE SITUATION IS MORE OR LESS SIMILAR TO THAT SO AND SO OPERATION'.Here had he been exposed to an academic programme together with real life simulation or training where asymmetric opponents are the enemy he would have had entirely different perspectives about the conflict.Hence we must not have just an education system but a professional military education system where both

conventional and asymmetric types of warfare are dealt with , for enlisted personnel , for commissioned officers and also higher echelon staff and commanders.If we don't do this we cannot do the most important thing about doctrine , promulgating it.Its not sufficient to write a doctrine after understanding the need to write it anew..its much more important to promulgate it in the field and the Armys educational system.We cannot make evey individual study the doctrine , we can have internet and other systems so that soldiers to commanders can access the doctrine but still individual study cannot be 100% nor compliance to that can be ensured--to offset this we can have educational programmes where studies are professionaly oriented , leadership courses are so configured so as to churn out professionals who have assimilated thoroughly the new doctrine.

Intelligence-Asymmetric Warfare perspective

An efficient intelligence service must conduct planning, deployment and management of collection assets and platforms, execute, control and evaluate the operations with the primary mission to retain a decision advantage over the opponent, both in peace time and during War/LIC.Two main approaches must be embodied: Criminalization Strategy and Prevent disrupt and counter the enemy's multidimensional intelligence threat. In the first approach the apprehended elements are captured and convicted as per court of law whereas in the second strategy we intend to thwart enemy actions using HUMINT/Counterintelligence. Intelligence feeds into both strategies in four modes of deployment: to make strategic assessments, including of the sources, nature and levels of threat, and the need for new resources or security measures; to feed into criminalisation operations in which individuals may ultimately be dealt with through the courts; to feed into control operations such as disruption and surveillance; to feed into control operations which deal with individuals by overt executive measures. These modes are not exclusive to terrorism, save for the final option.

HUMINT is generally considered ''passive''—assets and platforms in the form of HUMINT operatives and governmental/commercial (or official cover/unofficial cover) bases. This is an approach with a fallacy---HUMINT should be proactive, sometimes defensive and not always reactive. A patrol debrief tells us there is a sudden troop movement in named area of interest alpha and so we begin intelligence activity.Thats reactive.Had we depoloyed HUMINT agents well in advance to look beyond the forward areas by intermingling with the local population on a daily basis, eliciting information, keeping continuous contacts with the sources/informers,liasing with local police, keeping a tab on political developments and open source intelligence like publications,newspapers,media,rallies,public meetings, information gleaned from the internet about enemy govt policies, their arms purchases, their foreign policies with respect to our nation—all these will definitely give the HUMINT agent a feel of the pulse in the area of operations and if there is any ''imminent'' change in it (mind you, I didn't say any ''change'' in it like the reported deployment) he is bound to catch the new pulse. Before

deployment to an area of operations HUMINT and CI personnel should move in first to secure the ‘’human terrain’’ as well as the physical terrain from the intelligence perspective. This is what we can term –‘’intelligence and force projection capability’’ for an area of operations which is unknown to us in all terms. This is frequently the condition when the tactical commander successfully wraps up an operation in a defined AO and then is suddenly ordered to move into a new area much forward and totally unknown and occupied by enemy provocateurs and agents. Had he projected his force and available intelligence assets(after deploying his main assets for current operation and earmarking those available for projection tasking , like HUMIT,CI..) in the new AO while he was conducting his ops in the present AO , he could have been well prepared when the order came in. Here intelligence preparation of the battlefield will focus on both the local populace and the physical environment. The intent is to act as a forewarning system for the to-be deployed troops. This is also a force-protection intiative.Similarly when operations are being conducted in one Area of operations during a larger campaign commander’s pitch in all platforms of intelligence collection systems to accomplish a tactical victory. That is fine and is the standard procedure in the event of a conflict. What the commander doesn’t think is to extend his view beyond the Area of operations far away in hostile territory which is yet to see our troops in action and which is in control of the enemy. We need to project a part of our intelligence collection assets into that area/territory.

Foremost in the analysis of Intelligence tactics/strategies are the following questions: what was the quality of the intelligence; what were the processes in which the intelligence was used and did they put the intelligence to a suitable test?

Security Education and Training

The Indian forces need to be instilled with adequate security awareness and to this end programs and education/training materials and methods should be designed more appropriately/Personnel, installation and information—these three are critical assets and need to be fully secured against multidimensional threat intelligence collection efforts. Security education and training should be inducted in the force with exactly this intent. The focus should be primarily on the multidimensional threat intelligence collection efforts, the espionage threat and overall security threat factors. The soldier’s awareness should be heightened in these fields. The concept of insider-threat should also be a major area of study.Terrorism and insurgency should be dealt with Force Protection in the fore. The basic philosophy (here it is defensive in nature) is to deny unauthorized access to classified information together with personnel, physical, and information security. The design of the

training program should take into considerations unique characteristics and requirements of each unit.We should push down intelligence to the boot level--Every Soldier is A Sensor.This is the transformation in current intelligence doctrine.Even the average infantry man can gain intelligence during patrolling , cordon and search ops or during recce/surveillance by tactical questioning.

The Bijapur area of operations can be subjected to a military intelligence battle plan wherein the primary objective of enhancing the situational awareness of the commander at the concerned echelon is attained. A proper mix of intelligence collection assets is divined to obtain the necessary information in keeping with intelligence gaps and prioritized intelligence requirements as laid down by the commanders at Bde and Div levels. I would like to point out at this juncture that intelligence gaps are much more evident to company/battalion commanders than to higher headquarters. True intelligence is disseminated to lower tactical levels, intelligence that is collected from human assets, from overhead surveillance platforms and from reconnaissance and surveillance platoons but it is only the soldier on the ground who is the closest to the local populace, the terrain and sometimes the enemy that makes him aware of the need to answer certain immediate questions--answers to intelligence gaps and these gaps are not evident to higher headquarters. Say for example there is a possibility of extracting information from a local who has suspected connection with the enemy sympathizers , and here it is the line infantryman who doubts this as he is in the best position to be in close proximity to the local populace but the soldier has no previous training in immediate tactical extraction of intelligence , which i term tactical questioning and this coupled with basic surveillance-reconnaissance-document and captured equipment exploitation can be very easily taught to the infantryman thus rendering him as a secondary collector for HIS battalion int officer, an indispensable organic int asset who can contribute in his own little way to the battalion commanders immediate intelligence needs or answers to intelligence gaps. Ill clarify the term intelligence gaps more here : Aptly it is the gap between received intelligence from higher headquarters and the intelligence requirements in toto of the battalion commander. It is the existence of such unanswered intelligence gaps that contribute to most operational/tactical failures.Another way of putting forth the argument is the resolution of the concerned echelon's ''world'' or ''area of operations taken into account'',if I draw a parallel between intelligence collection system and image resolution on a computer graphic.We view the ''world' around us as representating the knowledge we have about that ''world''.For the 3 companies of Bravo Coy of 12 Bihar Regiment which has to be deployed to Assembly Area Sigma at (Geolocational coordinates) on (Date) , all three companies are at the same resolution of elevation of terrain (more granular and less

coarser) (we take terrain as an instance) whereas the Command HQ at Delhi overseeing operations in Bijapur -- this echelon will be seeing the "world' at a much higher and coarser resolution as its field of view to assess the situation is much much broader than the companies whose "concerned area of operations is very limited terrain , a geographical point.The commanders intelligence requirements at any echelon is a function of his situational awareness , he must fully understand the context in which the intelligence gap is felt.For any echelon there are 3 concerned echelons , the higher HQ which passes on the mission orders based on intelligence requirements(the level whose commanders intent is to be understood properly) , its own level (the echelon--goals,planning and courses of action,execution) and lower units or subordinate units (how they understand higher HQ commanders intent).Down these echelons granularity increases from coarser to finer.The platoons in the company are at a much finer resolution of knowledge representation of the world around them , the immediate and adjoining terrain to be explored for ambushes ,perform route recce and planning,locate and determine assets.At a much coarser level higher up than the said echelon , its a "bigger picture" for the commander and intelligence requirements at the much finer level (platoon) will not be apparent to him. Intelligence requirements being correctly assessed and more importantly correctly phrased is the prime requirement in any military decision making process prior to execution.*Granularity takes on enormous significance as shifts in command take place.*

For example as all three companies are at the same level of resolution we can state a collaboration amongst themselves , an entity-relational framework , such as one company does route planning , one looks for likely threats such as ambush points (recce)while the third focuses on available assets.

All this being said , Bijapur area of operations is amenable to tactical intelligence collection by organic intelligence platoons of the deployed infantry units. A very positive feature of tactical intelligence capability is the number of intelligence assets available in the length and breadth of the area of operations. With organic intelligence platoons in every battalion this is made possible. But this is important, very important secondary collection operations. Still intelligence collection at higher headquarters level must be more streamlined. The architecture must he altered to rein in intelligence assets from different perspectives of task organization. Plus a seamless communication protocol is required where information flow from soldier on the ground to the Bde int server or the other main cloud server and vice versa , adjacent headquarters intelligence exchange , flow between commands --tactical , operational rear headquarters (be it operational or even line tactical units and headquarters like deep entry tactical humint reconnaissance teams and corresponding forward and rear temporary headquarters setups).Communication is crucial as it ensures proper command and control of intelligence assets and more importantly conveying to them (or actuating sensors) changing intelligence requirements due to battle tempo or passive changes in enemy intentions. I have created tactical operations centers TOC's with all this in mind , staffed not by intelligence military occupational specialty personnel but by line infantrymen of the rank of Sr NCOs , JCOs and a battle Captain. Networked all these Bn TOCs with the Bde Int Server , the Cloud server (where apart from storage and

retrieval of information and push-pull with the combat soldier on the ground , it has a microprocessor based system with software to reposition and actuate sensors in accordance with incoming changes in intelligence or any other change as perceived by tactical units , intelligence personnel or other assets).

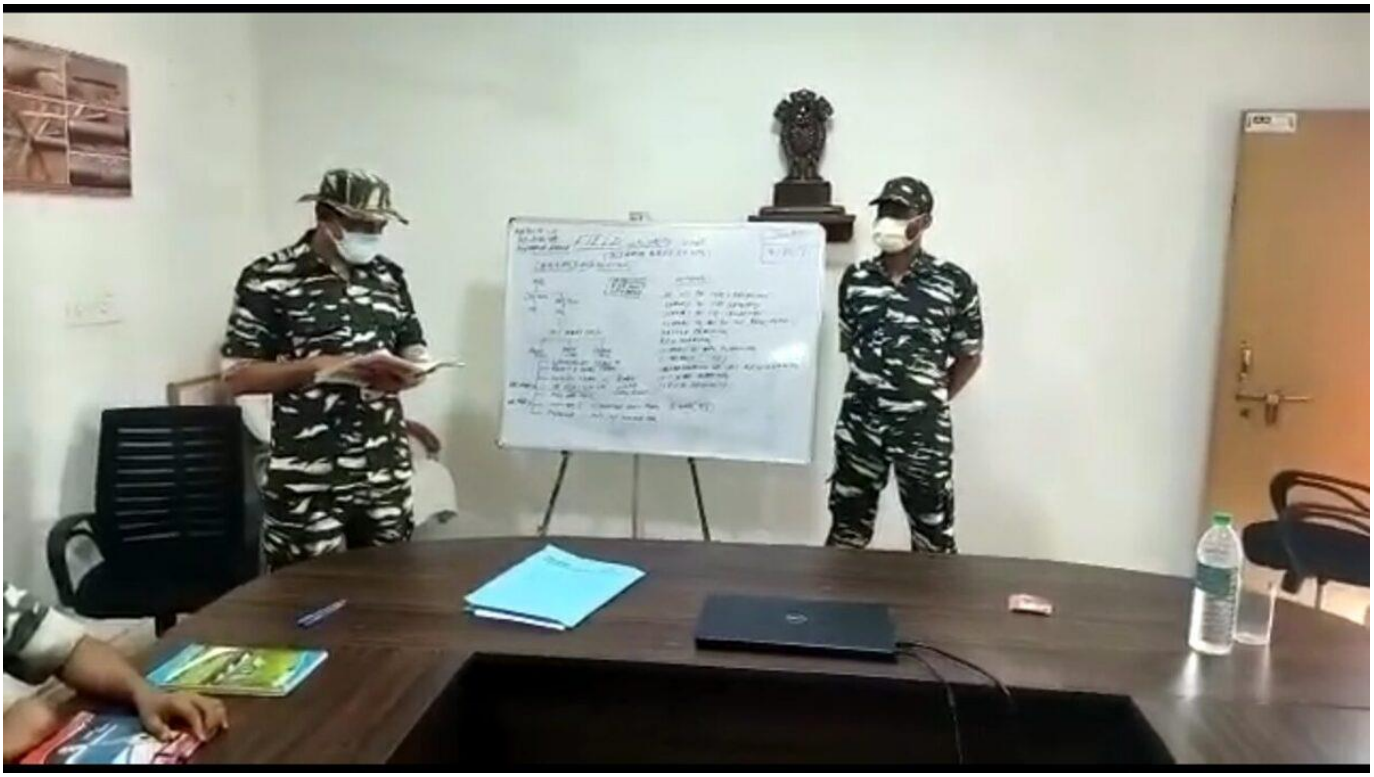
OPS

I conducted 4 Intelligence Surveillance and Reconnaissance Operations in Bijapur cityin the following areas:

NEW BUS STAND

2 LOCAL MARKETS

229,170,168,85 BATTALION ADJOINING AREA AND CONNECTING ROADS AND DIG OPS AREA.



#1 Tactical Ops Center Room

.#2 Counter Reconnaissance and Counter Surveillance Team

#3.All teams

.#4 Combat Int Platoon

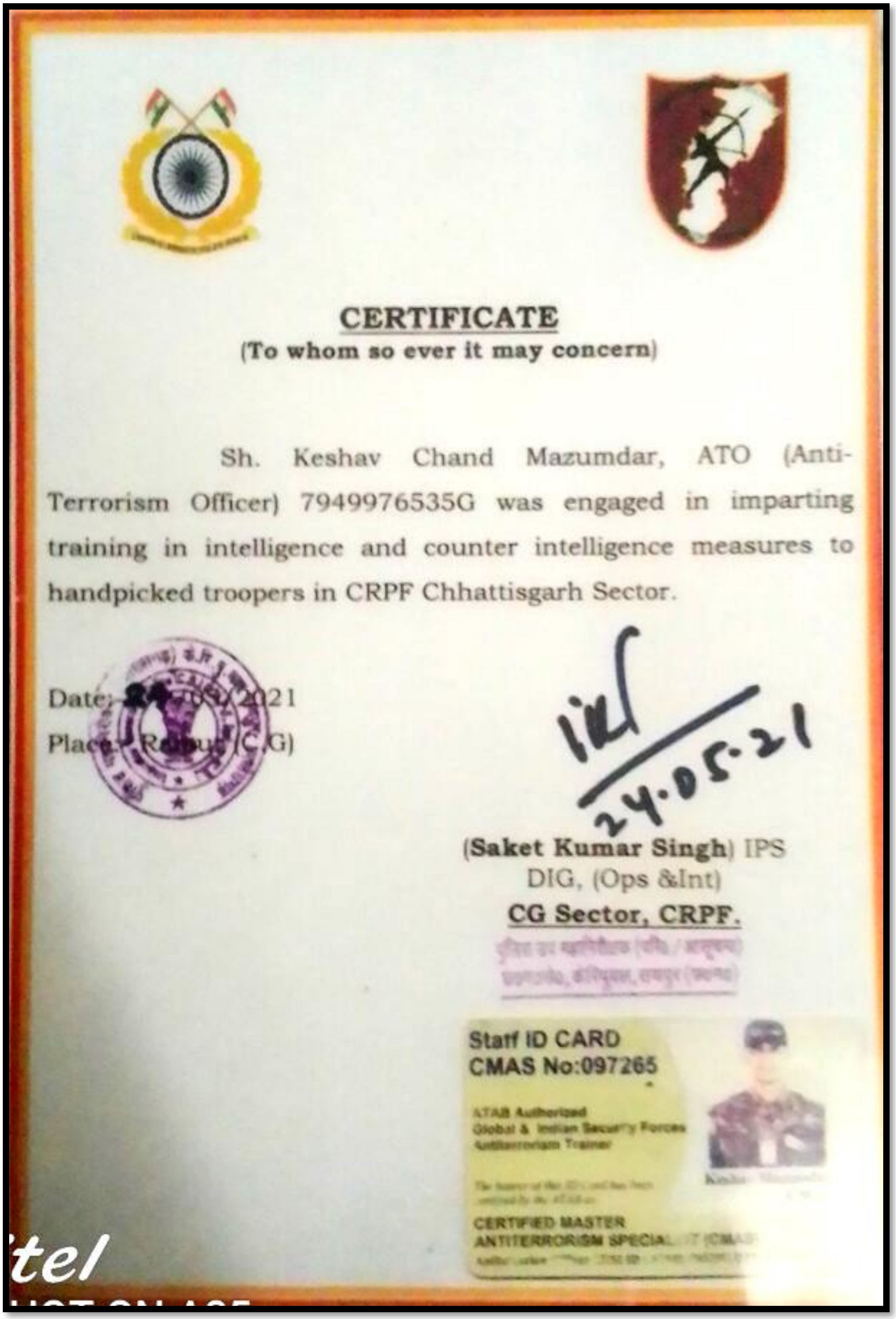
REDMI NOTE 8 PRO
AI QUAD CAMERA

#5 Reconnaissance and Surveillance Team

#6Mission Security Element

#7Tactical Ops Center Room

#8 Planning and Classes Room



CERTIFICATE

(To whom so ever it may concern)

Sh. Keshav Chand Mazumdar, ATO (Anti-Terrorism Officer) 7949976535G was engaged in imparting training in intelligence and counter intelligence measures to handpicked troopers in CRPF Chhattisgarh Sector.

Date: [illegible]/05/2021

Place:- Raipur (C.G)

24.05.21

(**Saket Kumar Singh**) IPS
DIG, (Ops &Int)
CG Sector, CRPF.

पुलिस उप महानिरीक्षक (परि. / आसूचना)
छ.ग.सेक्टर, के.रि.पु.बल, रायपुर (छ.ग.)

Staff ID CARD
CMAS No:097265

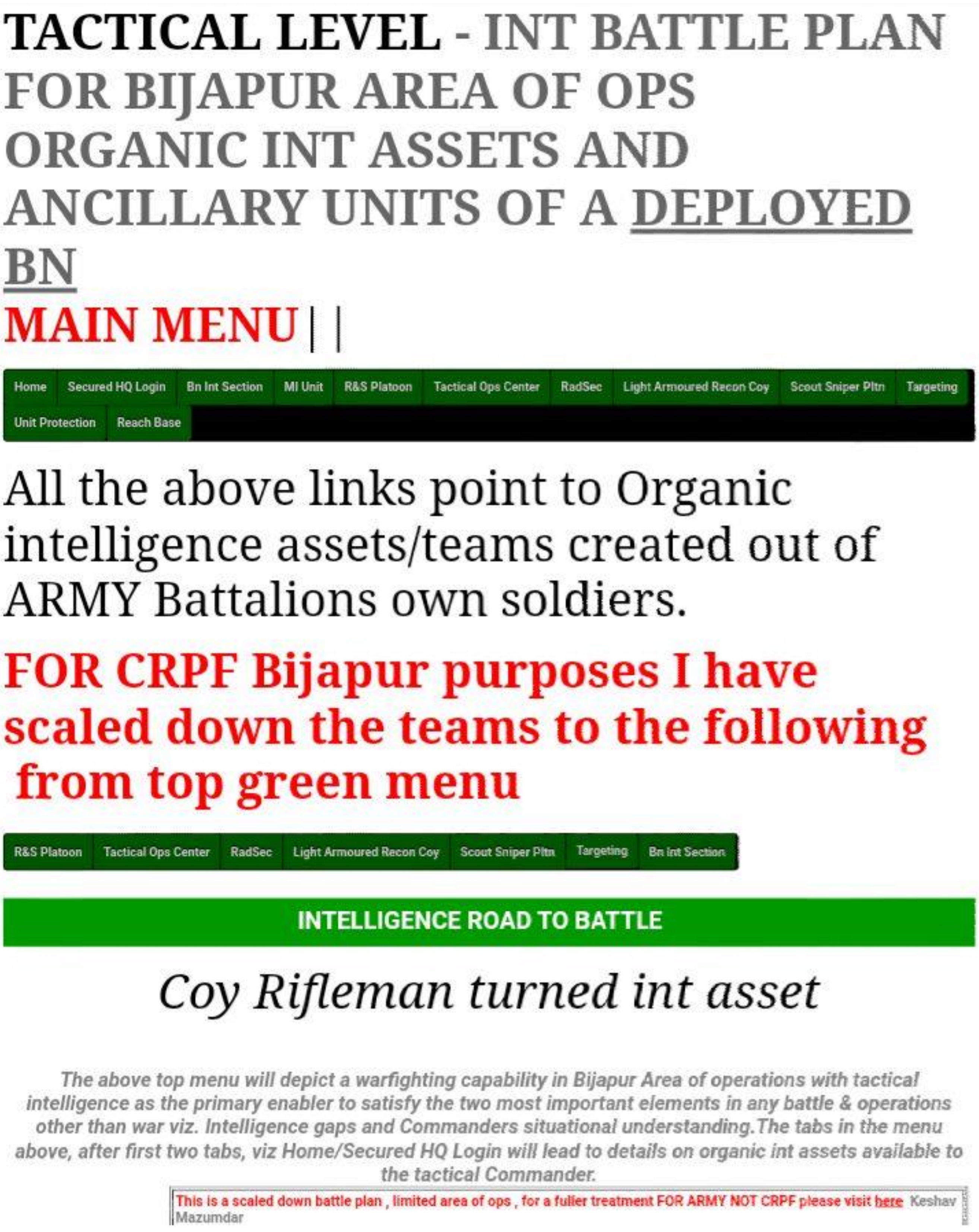
ATAB Authorized
Global & Indian Security Forces
Antiterrorism Trainer

The bearer of this ID card has been certified by the ATAB as

CERTIFIED MASTER
ANTITERRORISM SPECIALIST (CMAS)

Keshav Mazumdar

Bijapur Battle Plan



TACTICAL LEVEL - INT BATTLE PLAN FOR BIJAPUR AREA OF OPS ORGANIC INT ASSETS AND ANCILLARY UNITS OF A DEPLOYED BN

MAIN MENU | |

All the above links point to Organic intelligence assets/teams created out of ARMY Battalions own soldiers.

FOR CRPF Bijapur purposes I have scaled down the teams to the following from top green menu

INTELLIGENCE ROAD TO BATTLE

Coy Rifleman turned int asset

The above top menu will depict a warfighting capability in Bijapur Area of operations with tactical intelligence as the primary enabler to satisfy the two most important elements in any battle & operations other than war viz. Intelligence gaps and Commanders situational understanding.The tabs in the menu above, after first two tabs, viz Home/Secured HQ Login will lead to details on organic int assets available to the tactical Commander.

This is a scaled down battle plan , limited area of ops , for a fuller treatment FOR ARMY NOT CRPF please visit here Keshav Mazumdar

PROJECT ARMY XXII
CONCEPT

CONFIGURED FOR CRPF
A VISION FOR A STRONGER ARMY IN XXII CENTURY WITH INTELLIGENCE AS THE PRIMARY ENABLER TO MISSION SUCCESS FROM TACTICAL TO STRATEGIC BANDS OF THE CONFLICT SPECTRUM.

BOTTOMLINE : EVERY SOLDIER A SENSOR.TRANSLATED TO EVERY BATTALION HAVING ITS OWN ORGANIC INT UNIT.THESE ARE SECONDARY COLLECTORS TO ACT AS ENABLERS FOR COMMANDERS SITUATIONAL DEVELOPMENT AND AWARENESS.AND ADDRESS THE NEED FOR ACTIONABLE INTELLIGENCE.HIGHER HQ INT ASSETS ARE LIMITED , IN HEAVY DEMAND AND HENCE NOT ADEQUATE FOR ALL REQUIREMENTS OF FIGHTING UNITS , RESULTING IN INTELLIGENCE GAPS , CRITICAL FOR MISSION SUCCESS BUT NOT ANSWERED.ORGANIC INT PLATOONS CAN SOLVE THIS PROBLEM ADEQUATELY.

RIFLEMEN WILL BE TRAINED IN BASIC INTELLIGENCE TTPs AND A NEW FORM OF QUESTIONING-TACTICAL QUESTIONING AS OPPOSED TO INTERROGATION WHICH IS VERY INTIMIDATING AND USUALLY ACCOUNTS FOR 80% WRONG INFORMATION EXTRACTED FROM DETAINEEES SUSPECTS AND PRISONERS.

A VERY CRITICAL AREA FORCE PROTECTION CALLING FOR TOTALLY SEPERATE DOCTRINE AND TTPs WILL BE ADDRESSED.

KESHAV CHANDRA MAZUMDAR

THE APPLICATION TO THE CRPF DOMAIN IS MUCH MORE SIMPLER IN DESIGN AND ADAPTABLE TO URBAN , RURAL COIN BATTLESPACE.

ONLY FEW INTELLIGENCE COLLECTION ASSETS FROM THE MENU BELOW WILL BE CONFIGURED FOR LIMITED BATTLESPACE LIKE COIN WHERE CRPF WARFIGHTERS ARE ACTIVE.

HUMINT/CI ASSETS FOR VISION XXII

My effort is not to re-engineer existing intelligence and counterintelligence systems but to better posture and equip them for the future battlefield with support from organic intelligence sections and embedding intelligence capability in Long Range Surveilance and Special Operations Forces.

OBJECTIVES

1. **Protect our Forces**
2. **Shape the Battlspace**
3. **Gain Information Domnance**
4. **Integrated intelligence and counteintelligence structure from Strategic to Tactical levels, organized..trained and equipped to give maximum flexibility during conflict.**

CRPF MISSION COMMAND

TACTICAL STRATEGY:

1.Take over from outgoing unit and review int ops & threat/non kinetic/cultural data..battle handoff

2.Confirm what we think we know.

3.Assess locals data..threat..own vulnerability..compare with battle handoff info

4.Report changes

5.ID Int Requirement and Prioritize

6.State Cdrs Intent

7.Conduct population centric and area study and life pattern ..int pltns embedded in patrols tasked

8.Answer Int Requirements...int pltns tasked

9.ID potential targets..nominate white grey black..lists

10.Develop Target Packs

11.Confirm Targets.

///COA SELECTION//

12.Execute Kinetic+Non Kinetic Ops..integrate police EW Higher HQ G2

13.Assess success and collateral damage plus 2nd 3rd order effects

14.After Action Review

15.Change int requirements after int collected while executing ops

16.New Cdrs Intent

That's my continuos running Tactical int ops cycle for CRPF

My pilot unit will address insurgent tactics not insurgent forces.And the cdr will be taught to differentiate on knowledge domain..what he thinks he knows..what he actually knows and what he NEEDS to know.Confirm what he thinks he knows.Compare with what he actually knows.Then zero to missing info.Tempo demands simplicity.

No complex architecture. Am simply giving everything a structured form aided by Coy Int Section

---

Coy level int capability COIN Enduring Effects:

1.Deter insurgent activity through lowering their probability of success and increasing their risk of death or capture.

2.Disrupt insurgent activity by dominating their operating space and constraining their

freedom of action.

3.Detain positively identified insurgents wherever possible.

4.Develop targets by acquiring more intelligence for subsequent ops - either by us or other agencies.

AND

1. **Reassure locals that we operate in their local interests.**
2. **Relieve suffering, poverty within means, without unrealistically raising expectations or**
3. **becoming fixed.**
4. **Regain trust, consent, support or lost networks through disaffection or lack of continuity.**
5. **Reinforce our own Force Protection through local sympathy/goodwill and creation of a**
6. **non-permissive environment for the insurgent.**

To these ends i have created:

1. **Bn level organic int:**
2. **Coy level int sections.**
3. **Force Protection Dets.**
4. **Human Exploitation Teams using friendly elicitation and non aggressive tactical questioning techniques.**
5. **Target nomination teams**
6. **Document exploitation and captured equipment exploitation teams.**
7. **Int enabled combat R&S teams.**
8. **Topographical Teams.**
9. **Psyops Teams.**
10. **MI Bn**
11. **Collection and Exploitation Coy in a dedicated seperate MI Bn**
12. **Humint Coy**
13. **CI Coy**

In addition i have templated a conflict targeting spectrum tending to both SOF and conventional missions..with target feasibility..nomination..requirements management..int collection all with different int-ops integration as applicable to both ends of the spectrum.

We must clearly understand int -ops dynamic..inseperable..integrated..int residing within ops.Not int led ops but int "driven" ops.Period.

The OISO..a new staff officer function will do away with the lack of synchrony between ops and int..contribute to military decision planning by aiding in precise int requirements determination through awareness about available collection assets as against each operation tactic employed..ops being broken down into manageable sections for int collection.

He will be assisted by GSO2A-Ops and GSO2B-Int..distinct from the standard GS Ops and GS Int functions.

This is the only way int will drive ops.

The two will understand all facets of each others domains..interact in an integrated manner and together with the Requirements-Asset-Collection officer advise the OISO..who will feed info to both Ops and Int Staff.

Tactical Common operating picture is gained once ground soldiers trained in basic int establish int-reach with the two junior assistants of OISO.Cdrs planning should include live feeds from battle area of ops or simulated battle environ.That is all Sir

OISO will help in correcting identified

capability gaps and shortfalls:

(1) Improve collection planning across all echelons

(2) Improve collection assets visibility

(3) Improve collection requirements visibility

(4) Reduce unintentional redundancy of collection assets

(5) Implement a cross-echelon prioritization scheme

(6) Improve intelligence, information and data visibility

(7) Improve the dynamic ad hoc re-tasking process.

COLLECTION ASSETS [DESIGNED FOR ARMY BUT CAN BE SCALED DOWN TO FIT CRPF REQUIREMENTS.]

1. **MI Bde**
    - **Ops Bn**

        - MI Bn
    - Aerial Exploitation Bn
        - -
    - Fwd Collection Bn - CI/HUMINT
        - MI Bde 2 0
    - Fwd Collection Bn -SIGINT
        - MI Bde 3 0
    - Comm Bn
    - Electronics Bn
2. MI Bn
    - MI Coy
    - Tactical Exploitation Bn
3. Coy level MI Cell (Organic)
    - HQ Section
    - MI Unit (CI)
    - MI Unit (Interrogation & Exploitation)
    - MI Unit (Collection & Exploitation)
4. Tactical Humint Team
5. Multidimensional Recconnaissance
6. Unit IR Platoon
7. Mobile Interrogation Team
8. Int enabled SOF/R&S Teams
    - Int enabled teams.Sec Collectors.
9. Military Source Operations
    - Tactical Questioning
    - Screening
10. Architecture-Int Support
    - Int support to targeting
    - Architecture-Int Support 1
11. Cloud based ISR Integrated Blue Forces/HUMINT System

STRUCTURED INTEGRATED INTELLIGENCE ENVIRONMENT

BOTTOM UP PUSH
BOOT LEVEL DISTRIBUTED SECONDARY COLLECTORS BASE (Bn level organic int sections composed of trained riflemen)
LATERAL NETWORKING BN INT SECTION HQ WITH TOC NODES
GROUND TOCs NETWORKED WITH HIGHER HQs INT SECTION

TOC WARRIOR TERMINAL STRUCTURE:
HUMINT DESK
CI DESK
OSINT DESK
FORCE PROTECTION DESK

INTERROGATION DESK
R&S DESK
SOF INT DESK
COMBAT INT DESK

STAFF..battle captain etc.

BDE INT SERVER
TOC LAN GROUND LEVEL
GROUND LEVEL CLOUD STORAGE-INTERMEDIATE SERVER

INT OPS INTEGRATED.
CREATION OF NEW STAFF ELEMENT OISO ASSISTED BY TWO JUNIOR STAFF , ONE FROM OPS OTHER FROM INT.
PLANNING STAFF OFFICER ASSISTED BY RM AND ASSETS MANAGER
COLLECTION STAFF OFFICER (WILL OVERSEE COLLECTION
TTPs..indicators..PIRs..specific indicators etc.

Basic Training for Line Soldiers

BASIC TRAINING

This section will give you a preview of important basic training for Coy Riflemen

INT ENABLED LINE SOLDIERS -BASICS

1. MODEL UNIT
2. TACTICAL QUESTIONING
3. SECONDARY COLLECTORS
4. INT ENABLED MILITARY POLICE
5. CAPABILITY ANALYSIS
6. HUMINT EXPLOITATION TEAM
7. BATTLE STAFF NCOS
8. JCO/NCO STAFFED TACTICAL OPERATIONS CENTER
9. DOCUMENT EXPLOITATION
10. CEE
11. COLLECTION MANAGEMENT
12. REQUIREMENTS MANAGEMENT
13. REPORT WRITING

14. **COIN-TACTICAL OBSERVATION POSTS**
15. **IPB-COIN**
16. **IPB-CONVENTIONAL BATTLE**
17. **MI BN**
18. **MI BN (CI COMPANY , HUMINT COMPANY , COMBINED)**
19. **TACTICAL HUMINT**
20. **ISR SYNCHRONIZATION**
21. **INT ENABLED RSTA BDA**
22. **R&S**
23. **BDA**
24. **OBSERVATION AND SURVEILLANCE SKILLS**
25. **EXAMPLE CASE STUDY -AAR**
26. **FORCE PROTECTION AWARENESS FOR LINE SOLDIERS**
27. **OPSEC FOR LINE SOLDIERS**
28. **TRAINING 9WW2 BOOK)**
29. **ORGANIZATION TOE (WW2 BOOK)**
30. **COURSE STRUCTURE (WW2 BOOK)**
31. **BASICS OF SIGINT FOR LINE SOLDIERS**
32. **BASICS OF CI FOR LINE SOLDIERS**
33. **RSTA BASE , FOB , AOB**
34. **RSTA TEAM STRUCTURE ENABLED WITH INT ASSETS**
35. **INTELLIGENCE BCT-INTERIM**

BASIC TRAINING -1

This section will give you a preview of important basic training for Coy Riflemen

INT ENABLED LINE SOLDIERS -BASICS

Tactical Questioning (TQ)

TQ is

■Gathering information from people.

■An expedited interview in the field.

■Used to gain and exploit time-sensitive information for follow-on missions.

■Always an interview, NOT an interrogation.

Conduct TQ when

■Target is secure.

■People of interest are on the objective.

■Talking to a local national.

Prepare for success

■Prepare a TQ annex in the unit OPORD.

■Rehearse TQ (use interpreters).

■Develop standard basic questions.

■Develop a TQ plan.

■Have needed equipment accessible.

■Use site that is out of earshot of segregation area and is undisturbed.

…

Leads are statements or answers that indicate the detainee may have information on another significant subject or additional information on the question being asked.

■Hot lead: Time-sensitive information of immediate value or information that answers PIR.

■Cold lead: Information that does not meet criteria of hot lead and does not warrant a change in the current interview or current operations.

■Source lead: Information that identifies a source that has the knowledge you seek.

Initial Screening (JUMPS)

JUMPS is an acronym to guide any Soldier on the types of questions to ask in any interview. First question always is: “Is there any immediate danger to my patrol?”

■J – Job: What is your job/profession/rank/tribe (clan)/father’s name/place of birth/age?

■U – Unit: What is your unit/the name of your company? Who is your boss/supervisor?

■M – Mission: What is the mission of the unit/company you work for? Mission of next higher unit/company, current mission, anticipated future missions?

■P – Priority information requirement (PIR): Ask questions pertinent to your commander’s PIR.

■S – Stuff: Ask questions about anything that does not fit in the categories above: This is a catch-all category and a good place to tie questions to items that were found on the individual (e.g., “explain this map and these circled spots”).

Types of Questions

Direct: (Only authorized technique)

■An efficient method of asking precise questions toward a specific objective. Normally, who, what, when, where, why, and how begin the question.

■DON’T FORGET “ELSE”! (Who else, why else, where else, etc.)

Tips

■ “War game” your techniques in rehearsals.

■ Do not depend on lists or cheat sheets (you may lose eye contact and miss an indicator of deception).

■ Have a focused approach (erratic questions all over the map will confuse both you and the detainee).

■ Be specific and focused with questions (if you want to know what the person's profession is, ask "What is your profession?" not "What do you do?").

■ Ask questions that cannot be answered with yes or no.

■ If you are doing most of the talking, he is winning!

Do Not Use:

Vague:

■Questions that are not specific. These may lead to answers that are misinterpreted by the interviewer or elicit broad answers that are of no use.

Compound:

■Multiple questions contained within a single question: "When did you stage and conduct the attack?"

Negative:

■Phrasing that prompts the interviewee to make a negative response, whether true or not: "You didn't see any CF while on your recon, did you?"

Leading:

■Questions that prompt the interviewee to give the answer he believes you want.

EVERY SOLDIER A SENSOR

Every Soldier a Sensor

Your intelligence system has some limitations you must understand. These include- 1.Dissemination of information is highly dependent on communications systems and architecture and these are usually limited and under constraints in different fighting environments. Often requests for information from ground units are not disseminated in time. Accurate, timely and specific actionable intelligence is necessary to drive operations with that distinctive competitive edge and this is usually lacking.

2.Single-source collection is susceptible to adversary control and deception.Muliple sources need to be deployed and multidisciplinary intelligence collection platforms should be employed.

3.Counterinsurgency operations may be affected if the enemy resorts to non-usage of communications/no communications equipment (to avoid getting intercepted or DF'd) thus affecting adversely COMINT and ELINT based intelligence collection. Thus our intelligence collection effort gets degraded by the enemy.

4.Weather degradation of traffic ability and the negative effects of high winds on antenna arrays and aviation collection and jamming systems.

5.Inability of ground-based systems to operate on the move. Positioning and integration of mutually supporting ground and airborne systems is critical to continuous support.
6.Lack of sufficient organic intelligence assets to satisfy all your intelligence requirements.
For the Commanding Officer 12 BIHAR

PROPOSED UNIT BRIEF

December 22, 2017

All these point to the necessity of empowering the soldier on the ground with certain capabilities so as to convert him into an effective sensor. Totally depending on intelligence personnel and other intelligence collection platforms for actionable intelligence is impracticable given todays asymmetric enemy operating with newer and newer asymmetric tactics and in an environment where the human terrain that offers sanctuary plus counterintelligence and intelligence support to the enemy, line of sight problems for aerial and Sigint sources, highly distributed and non linear characteristics of the battlespace,the high workload on very limited (in strength)HUMINT/CI personnel and the prevailing demographics.
(The above points are strictly my observations and no one else).
The ‘Every Soldier is a Sensor’ (ES2) concept ensures that Soldiers are trained to actively observe for details for the commander’s critical information requirement (CCIR) while in an AO. It also ensures they can provide concise, accurate reports. Leaders will know how to collect, process, and disseminate information in their unit to generate timely intelligence. They should establish a regular feedback and assessment mechanism for improvement in implementing ES2. Every Soldier develops a special level of exposure to events occurring in the AO and can collect information by observing and interacting with the environment. Intelligence collection and development is everyone’s responsibility. Leaders and Soldiers should fight for knowledge in order to gain and maintain greater situational understanding.

RESOURCES

As Soldiers develop the special level of exposure to the events occurring in their operating environment, they should keep in mind certain potential indicators as shown in DIG OPS Page.These indicators are information on the intention or capability of a potential enemy that commanders need to make decisions. You will serve as the commander’s “eyes and ears” when–

·Performing traditional offensive or defensive missions.

·Patrolling in a stability and reconstruction or civil support operation.

·Manning a checkpoint or a roadblock.

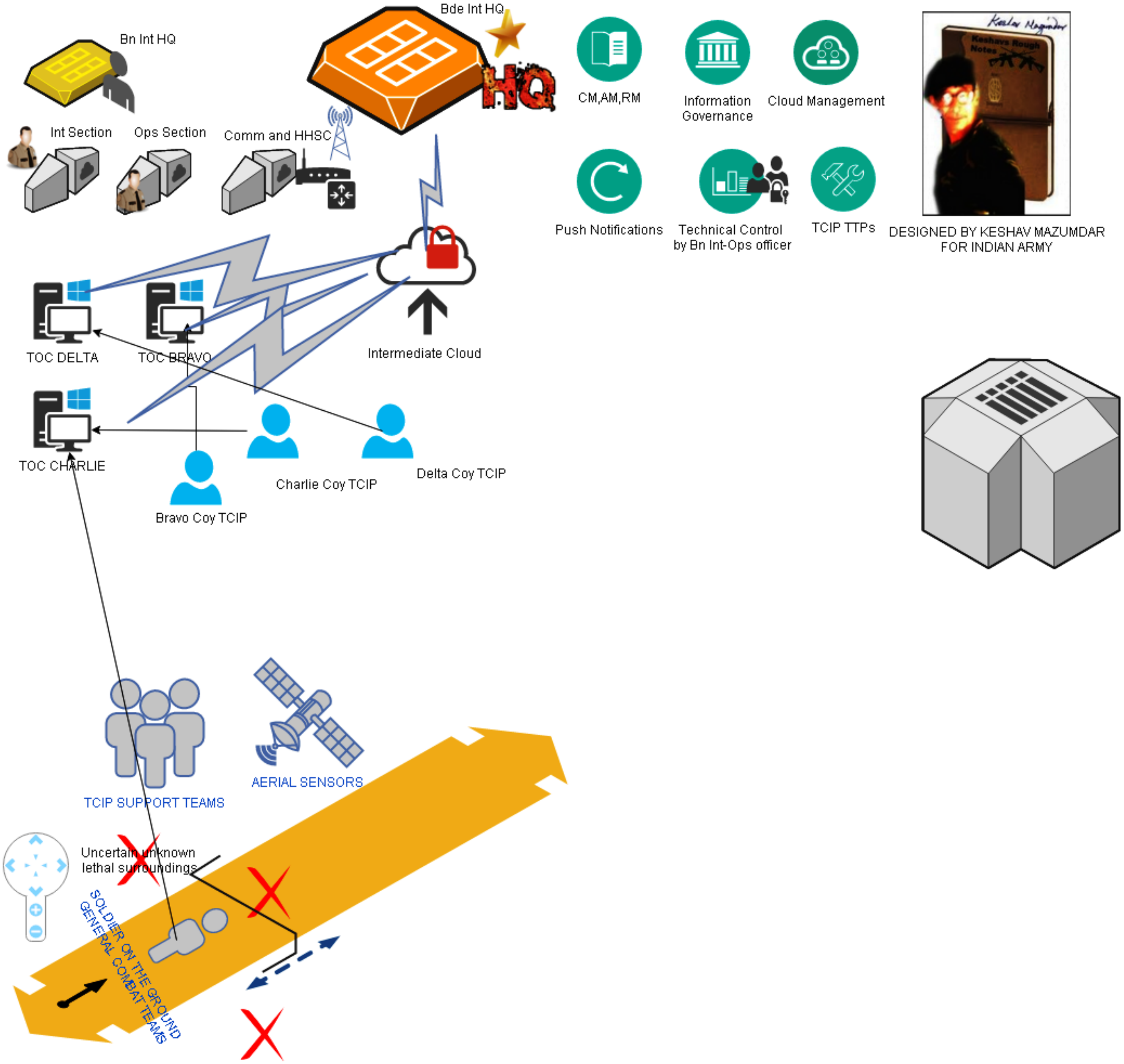
·Occupying an observation post.

·Passing through areas in convoys.

·Observing and reporting elements of the environment.

·Observing and reporting activities of the populace in the area of operations.

The design of COP Architecture


Bde Int HQ
HQ
Bn Int HQ
Int Section
Ops Section
Comm and HHSC
CM,AM,RM
Information Governance
Cloud Management
Push Notifications
Technical Control by Bn Int-Ops officer
TCIP TTPs
DESIGNED BY KESHAV MAZUMDAR FOR INDIAN ARMY
Intermediate Cloud
TOC DELTA
TOC BRAVO
TOC CHARLIE
Charlie Coy TCIP
Delta Coy TCIP
Bravo Coy TCIP
TCIP SUPPORT TEAMS
AERIAL SENSORS
Uncertain unknown lethal surroundings
SOLDIER ON THE GROUND
GENERAL COMBAT TEAMS

THE UNIT

Provide TOC for Battle Tracking in COIN and Conventional ops manned by NCOs and Senior NCOs/JCOs.Concept is to train them so that they can handle effectively the various War fighting functions.
Provide UNIT1 and UNIT2 support.
Provide CI capability to RSTA-BDA.
Provide CI support to FP.GOD.
Provide particularly int support by getting proficient in TQ,Screening,DOCEX.
To enable SECONDARY INT COLLECTION CAPABILITY-MP,Check Points Inf Soldiers,
R&S Teams, Patrols.

TABLE OF ORGANIZATION AND EQUIPMENT:
COMMAND AND CONTROL:

COMMAND:
HQ (S1 S2 S3 S4)
HQ SERVICE COMPANY
HQ-FORCE PROTECTION SECTION
HQ-PLANNING SECTION
HQ-OPS SECTION
HQ-INT SECTION

---HQ-INT SECTION---
STAFF OFFICER S2 CONTROL (FULL INTEGRATION WITH S3 OPS)
Planning Captain
ISR TASKING INTELLIGENCE OFFICER
INTRACOMPANY LNO

CONTROL:
TECHNICAL CONTROL UNIT
MISSION ORDER RECEIPT AND ANALYSIS UNIT
INT ANALYSIS UNIT
REQUIREMENTS,COLLECTION,ASSEST MANAGEMENT UNIT
HUMINT AND CI OPS MANAGEMENT SECTION
OPERATIONS MANAGEMENT TEAM OMT (HUMINT/CI)

TEAMS:
OPERATIONAL TEAMS--HUMINT TEAM , CI TEAM , TACHUMINT TEAM, TOPOGRAPHICAL COLLECTION TEAM,PSYOPS TEAM,LNO,EW TEAM, RECONNAISSANCE PLATOON(INT ENABLED),SURVEILLENCE TEAM.

SUPPORT:
PROVIDE INT SUPPORT TO:
LRS UNIT COIN
BN COMPANY
FORCE PROTECTION
AREA SECURITY
MILITARY SECURITY
AUGMENTING CHECKPOINTS
COIN
IPB

INT ENABLED RSTA TEAM REPORTS TO RSTA HQ BUT CI ELEMENT REPORTS TO HQ-INT
IN SAME AO HUMINT/CI TEAMS REPORT TO HQ-INT (BENEFIT?)

SUPPORT TO COIN
SECURING FOB.COMBAT OUTPOST

There will be a cell for analysis and control (incl technical control)of :
1.Collection TTPs , 2.HUMINT-CI Teams and 3.Collected/Open Source Intel.
This cell will also conduct mission-capability-needs analysis periodically
to ascertain optimum humint-CI mix in case of Tactical Humint teams,
whether to assign mission to exclusively HUMINT or CI team or TACHUMINT team,
whether at all to go for field intel collection or resort to open source int collection
and to determine usability,efficacy of existing teams.

This cell will be termed CONTROL UNIT
CONTROL UNIT WILL HAVE A HQ, AND TWO SECTIONS.ALL SOURCE INT SECTION(ASIS)
AND TECHNICAL CONTROL/PROCESSING SECTION(TCPS).

The two sections will have two SECTION HQ respectively.

The one under ASIS will:
look after the:
All-source production team
Collection Management Team
Target Nomination Team
and Dissemination Team.

The TCPS HQ will look after:
HUMINT AND CI TEAM(Multidisciplinary)
IMINT TEAM

SIGINT TEAM

CONTROL HQ will look after all communications and administrative matters logistics and maintenance.

UNIT SETUP DRAFT

STEPS IN IMPLEMENTING PROJECT XXII MILITARY INTELLIGENCE ARCHITECTURE

1. **INITIATION PHASE**
2. **SELECTION AND TRAINING**
3. **FORMATION OF BATTALLION INT HQ (OPS-INT, TECHNICAL CONTROL , COMM), COMPANY INT SECTION AND COMPANY LEVEL INT PLATOONS ****
4. **FORMATION OF MI BATTALLION (MI Coy, CI Coy , COLLECTION AND EXPLOITATION Coy, INTERROGATION AND EXPLOITATION Coy)****
5. **FORMATION OF MI Bde****
6. **Formation of Tactical Operation Centers TOC manned by Battle Staff NCOs and one Battle Captain.**
7. **Networking these TOCs in a single Area of Operation , horizontally with adjacent unit HQs and vertically with Higher HQs.**
8. **Connecting this network with the WAN Network of all the Bde's deployed in the wide Area of Ops which finally connects with the DIV NET , thus the objective of attaining the Common Operating Picture COP is met with Commanders at all echelons , from the DIVISION level down to the Company Commander and the Platoon Int Forward HQ sharing the same picture -- real time visualization of operations. Moreover parallel/lateral exchange of information between adjacent and far flung units is made possible. Also in COIN ops second and third order effect of kinetic/non kinetic attacks in Areas of Interest and those beyond AI can be gauged and strategies/tactics changed.**

Support:(Modular packages to plug in either Direct Support or General Support to Host UNIT; Each package can constitute 3-4 soldiers from the Battallion Int Platoons to assist other fighting units with no intelligence capability (organic))

- **Company Intelligence Support Teams**
- **Modular UNIT : Pulled from Platoons to support COIN**
- **Support to Reconnaissance and Surveillance - Fighting for Information or Passive No-Engage**
- **Mode , either with int capability**
- **Support to HUMINT**
- **Support to CI**
- **Training other Non-INT Military Occupational Speciality soldiers like from the CMP to act as**
- **Secondary Collectors.**
- **Support to Cordon and Search Operations.**

1. **<u>INITIATION PHASE</u>**
2. **<u>SELECTION AND TRAINING</u>**

TOTAL TIME - 11 MONTHS

PHASE 1.
Screening and selection of 7 riflemen. Out of which 4 enlisted soldiers , 2 Senior NCO , 1JCO.
Training in Observation skills , reconnaissance. Screening, Cordon and Search ops with basic intelligence trained non-int military occupational specialty riflemen. Asymmetric Enemy as different from Conventional Enemy (Elaborate doctrine/TTPs that much that can be assimilated)Total time allotted 2 months.
PHASE 2.
Training in tactical questioning in preferably model village. Total time allotted 2 months.
PHASE 3.
Training in CEE DOCX.Tagging.OSINT. Report Writing. 1 month.
PHASE 4.
Basic training in IPB.SALUTE FORMAT. How to manage sub-unit cells.Leadership,logistics,social networks,TOE,Historical IED/Attack profiles, Terrain analysis, Climate profiles, Political and village panchayat/police profiles,PSYOPS, Time allotted 3 months.
PHASE 5.
Debriefing unit patrols. Phase A/B/C/D Reports, Total time allotted 1 month.
PHASE 6.
Educational classes: Intelligence , HUMINT, CI,Force Protection, Collection Management, Requirements Management, Knowledge of Commanders intelligence requirements and what predicates their need-intelligence gaps.ISR.What an ISR platoon does , how it

conducts ops and what are the constraints,risks.Exam.
PHASE 7.
Communication , Dissemination. Time Allotted 1 month
PHASE 8.
Tactical Operations Centers , its networking , battle staff comprised of NCOs--their responsibilities (ops-intel-admn).How secondary collectors can alleviate pressure/workload on primary int personnel. CASE STUDY: How the Military Police function can be converted to Intelligence-led-policing function. Time Allotted 1 month.
PHASE 9.
Studying C2 relationships , how they change during conduct of battle.How to create forward bases and reporting channels between deployed teams and forawrd base and base HQ Int Staff Officer.

Every Soldier a Sensor

Your intelligence system has some limitations you must understand. These include- 1.Dissemination of information is highly dependent on communications systems and architecture and these are usually limited and under constraints in different fighting environments. Often requests for information from ground units are not disseminated in time. Accurate, timely and specific actionable intelligence is necessary to drive operations with that distinctive competitive edge and this is usually lacking.

2.Single-source collection is susceptible to adversary control and deception.Muliple sources need to be deployed and multidisciplinary intelligence collection platforms should be employed.

3.Counterinsurgency operations may be affected if the enemy resorts to non-usage of communications/no communications equipment (to avoid getting intercepted or DF’d) thus affecting adversely COMINT and ELINT based intelligence collection. Thus our intelligence collection effort gets degraded by the enemy.

4.Weather degradation of traffic ability and the negative effects of high winds on antenna arrays and aviation collection and jamming systems.

5.Inability of ground-based systems to operate on the move. Positioning and integration of mutually supporting ground and airborne systems is critical to continuous support.

6.Lack of sufficient organic intelligence assets to satisfy all your intelligence requirements.

All these point to the necessity of empowering the soldier on the ground with certain capabilities so as to convert him into an effective sensor. Totally depending on intelligence personnel and other intelligence collection platforms for actionable intelligence is impracticable given todays asymmetric enemy operating with newer and newer asymmetric tactics and in an environment where the human terrain that offers sanctuary plus counterintelligence and intelligence support to the enemy, line of sight problems for aerial and Sigint sources, highly distributed and non linear characteristics of the battlespace,the high workload on very limited (in strength)HUMINT/CI personnel and the prevailing demographics.

(The above points are strictly my observations and no one else).

The 'Every Soldier is a Sensor' (ES2) concept ensures that Soldiers are trained to actively observe for details for the commander's critical information requirement (CCIR) while in an AO. It also ensures they can provide concise, accurate reports. Leaders will know how to collect, process, and disseminate information in their unit to generate timely intelligence. They should establish a regular feedback and assessment mechanism for improvement in implementing ES2. Every Soldier develops a special level of exposure to events occurring in the AO and can collect information by observing and interacting with the environment. Intelligence collection and development is everyone's responsibility. Leaders and Soldiers should fight for knowledge in order to gain and maintain greater situational understanding.

RESOURCES

As Soldiers develop the special level of exposure to the events occurring in their operating environment, they should keep in mind certain potential indicators as shown in Figure 9-1, page 9-2. These indicators are information on the intention or capability of a potential enemy that commanders need to make decisions. You will serve as the commander's "eyes and ears" when–

- **Performing traditional offensive or defensive missions.**
- **Patrolling in a stability and reconstruction or civil support operation.**
- **Manning a checkpoint or a roadblock.**
- **Occupying an observation post.**
- **Passing through areas in convoys.**
- **Observing and reporting elements of the environment.**
- **Observing and reporting activities of the populace in the area of operations.**

Figure 1. Potential indicators.

SIGHT Look for–	SOUND Listen for–	TOUCH Feel for–	SMELL Smell for–
• Enemy personnel, vehicles, and aircraft • Sudden or unusual movement • New local inhabitants • Smoke or dust • Unusual movement of farm or wild animals • Unusual activity–or lack of activity–by local inhabitants, especially at times or places that are normally inactive or active • Vehicle or personnel tracks • Movement of local inhabitants along uncleared routes, areas, or paths • Signs that the enemy has occupied the area • Evidence of changing trends in threats • Recently cut foliage • Muzzle flashes, lights, fires, or reflections • Unusual amount (too much or too little) of trash.Signs of fresh faeces , urine.Cigarette stubs.	• Running engines or track sounds • Voices • Metallic sounds • Gunfire, by weapon type • Unusual calm or silence • Dismounted movement • Aircraft	• Warm coals and other materials in a fire • Fresh tracks • Age of food or trash	• Vehicle exhaust • Burning petroleum products • Food cooking • Aged food in trash • Human waste

OTHER CONSIDERATIONS

Armed Elements Locations of factional forces, mine fields, and potential threats. Homes and Buildings Condition of roofs, doors, windows, lights, power lines, water, sanitation, roads, bridges, crops, and livestock. Infrastructure Functioning stores, service stations, and so on. People Numbers, gender, age, residence or DPRE status, apparent health, clothing, daily activities, and leadership. Contrast Has anything changed? For example, are there new locks on buildings? Are windows boarded up or previously boarded up windows now open, indicating a change in how a building is expected to be used? Have buildings been defaced with graffiti?

Commanders get information from many sources, but you are his best source. You can in turn collect information from the following sources:

- **Enemy prisoners of war (EPWs)/detainees are an immediate source of information. Turn captured Soldiers over to your leader quickly. Also, tell him anything you learn from them.**
- **Captured enemy documents (CEDs) may contain valuable information about present or future enemy operations. Give such documents to your leader quickly.**
- **Captured enemy equipment (CEEs) eliminates an immediate threat. Give such equipment to your leader quickly.**
- **Enemy activity (the things the enemy is doing) often indicates what the enemy plans to do. Report everything you see the enemy do. Some things that may not seem important to you may be important to your commander.**

- **Tactical questioning, observation, and interaction with displaced persons, refugees, or evacuees (DPRE), during the conduct of missions, can yield important information.**
- **Local civilians, however often have the most information about the enemy, terrain, and weather in a particular area. Report any information gained from civilians. However, you cannot be sure**

which side the civilians are trying to help, so be careful when acting on information obtained

from them. If possible, try to confirm the information by some other means.

FORMS OF Questioning may be achieved by tactical or direct methods. The following paragraphs detail both methods:

UNIT SUPPORT TO HUMINT COLLECTION (Secondary Collectors)
Small units contribute to HUMINT collection through a number of different ways.
Tactical Questioning

Tactical questioning is the initial questioning for information of immediate value. When the term applies to the interaction with the local population, it is not really questioning but is more conversational in nature. The task can be designed to build rapport as much, and collect information and understand the environment. You will conduct tactical questioning based on your unit is SOPs, ROE, and the order for that mission. Your leaders must include specific guidance for tactical questioning in the operation order for appropriate missions. Information reported because of tactical questioning is passed up through your chain of command to the battalion/brigade intelligence officers, which forms a vital part of future planning and operations. Additionally, you are not allowed to attempt any interrogation approach techniques in the course of tactical questioning.

Every soldier is a Sensor—this statement is a major transformation in Intelligence Doctrine.It
should be strongly emphasized that dedicating/deploying only multidisciplinary intelligence collection assets is NOT enough.The soldier on the ground,who is in direct contact with the local environment,be it at times of small scale operations,patrolling missions,handling EPWs/detainees or captured documents – HE IS THE EYES AND EARS OF THE COMMANDER.
Hence a culture of intelligence collection , or in other words a natural tendency to probe and collect information—should be inculcated in each and every soldier,irrespective of trade or speciality.This is Tactical Questioning which is guided by the units SOP,ROE,and the order for that mission. Tactical questioning aids in proper visualization of the existing situation (Situational Understanding of the Commander) by enabling the soldier to conduct expedient enquiries in order to extract critical mission-specific information of immediate tactical value.
Soldiers can conduct TQ when they are:

1. Manning a check post/roadblock
2. Executing traditional offensive/defensive operations
3. Handling detainees/EPWs during the very initial stages of apprehending them
4. Handling captured documents
5. Occupying an OP
6. On a patrolling mission
7. In conversation with the local populace after an operation and securing the area
8. Conducting questioning as MP personnel
9. Passing through an area in a convoy
10. Involved in any operation whatsoever where they get the opportunity to observe and report on environmental factors – factors pertaining to the mission/Area of operations
(See Appendix for more)

ISR Operations

The soldier conduct Tactical Questioning which needs to be passed up the chain of command.In tactical operations the soldier conducts TQ which offer critical information which
are of immediate tactical value and may affect mission success positively by enabling the Commander and staff to plan the ongoing operation more efficiently.Careful and expedient handling of EPWs/detainees and captured documents lends good support to the overall ISR operations.

Direct Questioning–Direct questioning is an efficient method of asking precise questions according to a standard pattern. The goal is to obtain the maximum amount of intelligence information in the least amount of time. Direct questions must clearly indicate the topic being questioned as they require an effective narrative response (i.e., be brief, simple, but specific). Clearly define each subject using a logical sequence. Basic questions are used to discourage "yes" or "no" answers. Direct questioning is the only technique authorized for ES2 tactical questioning. Soldiers who are not trained and certified interrogators are forbidden to attempt to apply any interrogation approach techniques. When it is clear that the person being questioned has no further information, or does not wish to cooperate further, tactical questioning must stop.

Principles of Questioning

The HUMINT specialist must thoroughly understand the source and adopt a role which is appropriate. The
verbal and non-verbal cues which are productive should be included. Time must be spent upon
understanding the subject making sure all real life constraints are managed effectively. The constraints
include time availability, knowledge from other sources and information value from other sources.
Walton, (2003), presents 10 rules of game which covers the interrogator or proponent and the interrogator or

respondent.
1. The respondent must not unintentionally present statements or infer facts which he is trying to
conceal.
2. By allowed means, the proponent must threaten or sanction the respondent to present information.
3. Questions must be created for the proponent that are loaded, deceptive and leading.
4. It is possible for the respondent to serve his end if the answers are ambiguous, vague or misleading.
5. The respondents reply must be critically assessed to extract vital information.
6. The replies by the respondent must be consistent to make sure his commitment remains intact.
7. If inconsistencies are present in the commitment of the respondent, there should be a critical
examination and all information that is inconsistent must be removed.
8. The goal is achieved once the information required is extracted. This is specifically if the dialogue is
in favour of the proponent.
9. It would be in the respondents favour if the dialogue ends without information collection for the
proponent.
10. To achieve their own ends, the two parties could carry out arguments which are fallacious or
irrelevant.

Various AOs will have different social and regional considerations that can affect communications and the conduct of operations (i.e., social behaviors, customs, and courtesies). You must also be aware of the following safety and cultural considerations:

- **Know the threat level and force protection (FP) measures in your AO.**
- **Know local customs and courtesies.**
- **Avoid using body language that locals might find rude.**
- **Approach people in normal surroundings to avoid suspicion.**
- **Behave in a friendly and polite manner.**
- **Remove sunglasses when speaking to those people with whom you are trying to create a favorable impression.**
- **Know as much as possible about the local culture, including a few phrases in the local language.**
- **If security conditions permit, position your weapon in the least intimidating position as possible.**

COLLECTION MANAGEMENT

PROBLEM: The Intelligence Collection Management System comprises of a Collection Management

Officer and CI/HUMINT specialists and the CI/HUMINT collectors.The CMO takes charge of the collection plan and tasks his specialists with constantly keeping an eye on current intelligence requirements as well as intelligence requirements that surface as tactical situations changes rapidly during combat due to the highly fluid nature of the latter.This tracking of all intelligence requirements is extremely important as collection operations are driven by intelligence requirements—the correct IRs.Hence the CMO ensures that the collectors are properly focusing on the prioritized intelligence requirements.That also includes the passive HUMINT collectors like Civil Affairs,Military Police,Medical units,Psychological ops and Information ops.

During combat operations,tactical intelligence systems develop problems.ISR Ops during combat MUST be synchronized.But as tactical situations change during combat rapidly forcing development of more different intelligence requirements the ISR assets need to be retasked and synchronized again and that too in pace with the changing scenario and that proves to be very difficult.

Intelligence exploitation operations too suffer.During operations pulling intelligence from higher headquarters or feeding intelligence inputs as per requests from subordinate units again proves difficult.Proper dissemination to the maneuver division Commander and subordinate brigades,battalions,units suffers due to inadequate communication systems and database management/processing capability.

The commander,the staff, and the higher and lower headquarters across the depth and width of the battlefield must coordinate with the CM section while formulating plans for future operations and to support ongoing missions.Variations in enemy actions or changes in perception of the enemy’s movements give rise to new sets of intelligence requirements and the CM section should take this into account.The battlefield is an area of high fluidity and hence changes must be expected and Requirements Management must be flexible enough to incorporate these changes.

The two most critical steps in collection management is identifying and prioritizing the intelligence requirements.To this end 6 areas of interest must be considered and they are force protection,situation development,targeting,battle damage assessment BDA,indications and warning and IPB.The intelligence requirements stems from these areas and all of the competing requirements needs to be

consolidated,.Thereafter the collection plan is created and the scarce IEW resources are tasked more efficiently.

Requirements Management,Mission Management and Asset Management constitute the Collection Management process.They are treated separately but together constitute integrated operations as a whole.

The six steps in the CM process are:

¬ Develop Requirements,

¬ Develop a Collection Plan,

¬ Task/Request Collection,

¬ Disseminate,

¬ Evaluate Reporting,

¬ Update Collection Planning

The various activities inherent in these steps need to be synchronized and placed under constant review.

While devising the Collection plan,the intelligence officer in charge of designing the plan (henceforth known as Collection Manager CM) takes into account the following:

¬ Commanders Priority Intelligence Requirements

¬ Low Priority Intelligence Requirements

¬ Requests from subordinate units,

¬ Taskings from higher HQ's

¬ Intelligence requirements for targeting purposes

Now,he prioritizes these keeping in mind the Commands intelligence needs and the commanders priority intelligence needs.

When BICCE study was initially conducted with the development of possible enemy COAs , the intelligence analyst attempts to develop all indicators of these COAs.(Indicators are those details of enemy action/inaction that may suggest an enemy COA.

COLLECTION FORMAT

There are two collection plans.One designed for conventional battlefield operations whereas the other caters to a LIC environment.LIC battlefield operations tend to be dispersed.The PIR and IR's are highly diverse and collection becomes a tough task.

In the latter case the following steps are followed:

¬ List the PIRs and IRs,priotize them and enumerate them using control numbers and alphabets.This helps in prioritization.

¬ Now ascertain the indicators

¬ Determine potential indicators-prioritize those that will answer the PIR and IR.

¬ Delete all indicators that do not answer the intelligence requirements.

¬ Develop specific intelligence requirements.These are the requirements as stated by the commander,
prioritized and general,broken down into manageable specific requirements.A PIR may have several
specific intelligence requirements.

¬ Analyse these SIRs and the target characteristics keeping all the indicators in perspective.

¬ Finally prioritize the SIRs and determine the suitable collection discipline/platform/agency keeping
its capabilities,limitations,backlog of collection taskings allotted to it and whether adjacent units,lower units are also using it.

¬ Prepare the tasking list by creating a prioritized SIR list and deploy the collectors.

CM'S need a thorough knowledge of the threat,the characteristics of the AO and the general capabilities of
collection assets before they can translate the commander's PIR and IR into indicators.
This includes a detailed knowledge of the—

- **a. Threat organization, equipment, and doctrine.**
- **b. Biographical data on major personalities.**
- **c. Present and past performance of units and organizations.**
- **d. Terrain and weather constraints.**
- **e. Patterns of current operations.**
- **f. Degree of popular support.**

AGENCIES AND AGENCY
COLLECTION PRIORITY.

The collection manager decides on the agency/agencies/assets to be tasked with the collection.To this he
must judge the capabilities , availability and constraints of the assets with regard to the collection
priorities(the intelligence requirements,PIR,IR,SIRs). These include factors such
as—

- **Frequency ranges for intercept radios.**
- **Aircraft mission durations.**
- **Number of flights.**
- **Mobility.**
- **Linguistic capabilities.**
- **The assets may be organic or external**

The collection manager then compares all the agencies or assets who can answer a particular SIR and
chooses the best one depending on the 3 factors.Then he selects the next best one and so on thus creating a
prioritized assets/agencies listing. Next, he determines which agency
or asset can best answer the SIR and prioritizes them.(EX: CI Team=1,CA Team=2,HUMINT Team =3 in

answering SIR-4 which is ‘’Report strangers movement in NAI-alpha)

THE TASKING LIST
The CMO prioritizes the SIR and tasks appropriate sources to answer them. The list of taskings for each source also should be prioritized.
SIRs 1 to 10 are prioritized as follows:
1=3
2=6
3=1
4=7
5=5
6=2
7=4
8=10
9=9
10=8
Team (Support ops team)is tasked with SIR 3,5,8,10.
We see the prioritized tasking becomes: SIR3,SIR5,SIR10,SIR8
The team will report about SIR3 first,then SIR5,then SIR10 and finally SIR8.
Example:
This means the CMO must provide the SOT-A (1) with a prioritized tasking list as follows:
1 — Report time, frequency, and location of insurgent radio traffic or EW activity (SIR 28).
2 — Report the number, size, equipment, composition, route, and time of suspected insurgent patrols in the area (SIR 6).
3 — Report the location, quantity, and type of unexplained firings in the area (SIR 1)

Indicator Examples
Indicators can be broken into three categories:
• Immediate threat indicators.
• Preparatory indicators.
• Secondary indicators.
All three categories appear at strategic, operational, and tactical levels.
Immediate Threat Indicators. Imminent threat activities or a threat which is already in progress give rise
to indicators known as Immediate threat indicators.We take into consideration all factors possible like
activities,tactics,movemernts,current dispositions,propaganda,and any preparations indicating a dangerous

**course of action.The following might be good indicators:
Recovery of huge cache of arms and ammunition in close proximity to any objective
Increased troop movement towards objective
Very aggressive rhetoric by the military leadership of the enemy nation
Preparatory indicators: Before the decided course of action/s is/are undertaken there are preparations to be
made.Indicators of such preparations are termed Preparatory threat indicators.We must analyse
multidimensional threat intelligence,planning,training activities and logistics.Examples of such indicators
could be:
Diplomatic support by other countries
Increased media rhetoric
Very aggressive TV discussions
Increase in training tempo
Lightly armed reconnaissance who engage and break contact quickly
Mock
Overt/covert weapons shipments
Regional countries showing support for the enemy government's policy
UN embargos/sanctions ignored by countries who support the policies of the enemy nation
Increased media support for the enemy country**

**Secondary indicators: The local population is affected by any threat activity.The population is affected by
tactical preparatory indicators of the enemy and we can thus observe reflections in the economy,
commodities and population to infer the preparations.We might observe that:
A fear psychosis has developed among the population, most schools unattended,and locals avoiding contact
with the authorities and streets deserted before evening
Huge purchases of rations by locals, stockpiling of medicines and emergency stuff at home
Shortages reported in non-lethal material
Very less presence of their community members in festivals,places of entertainment.Cinema theaters
reporting huge losses in revenue as very low attendance.
Now the CM in collaboration with the intelligence analyst attempts to assign a set of specific information
requirements to address each of the indicators -- the overall focus being to answer each prioritized
intelligence requirement. These SIRs go into making the collection plan.The CM unit must constantly keep a
track of the progress,and any incoming information may also part a play in outstanding information
requirements or in any future information requirement tabled for tasking to the collection platforms.The CM**

section continuosly evaluates the collection/reporting processes and disseminates the required intelligence to the Commander.

SIR is a direct function of enemy Order of Battle and the gaps in intelligence.We can have a huge number of SIRs as each PIR can generate several SIRs /SORs(A division can have upto 12 PIRs for current operations and envisage an equal number or more for future operations.Note here that we have several intelligence collection platforms—HUMINT,SIGINT,IMINT,MASINT.Now the collection manager will assign different SIRs/SORs to each collection platform.Thus overall we have a huge task at hand as now the collection manager unit may have to handle hundreds of information requirements while combat operations are underway.

Each PIR may have a number of SIRs. This number would also include the intelligence requirements to support targeting, lower priority information requirements, requests for information from subordinate units, or taskings from higher headquarters.Hence proper synchronization with operations and deconfliction(particularly in case of HUMINT/CI collection processes) is a prime necessity.

Thereafter the step of preparing the collection plan is undertaken by the collection manager.The collection plan is created using the PIRs,indicators,SIRs,SORs and all the collection assets at his disposal. Regarding the available assets for collection ,factors such as accuracy,range,platform type and technical capabilities-- these are matched with the target characteristics in question and the most appropriate collection resource/s is/are allocated.Redundancy is important here and the assets need also to be integrated and if there is an admixture of assets then that has to be carefully planned.

Mission management is about how the collection task will have to be executed.A collection strategy is formed keeping in perspective collection taskings to subordinate units,support requests to higher and adjacent units and exploitation of all intelligence inputs available from other agencies at the corps,theatre and national levels. The important objective guiding the strategy formation is synchronization of collection and dissemination schedule with the PIR.

Here again it is critical that operations be synchronized with the collection plan.The taskings must be issued to the collection platforms as quickly as possible. This also involves specific intelligence exploitation

operations and systems management.

A Sample of the Process

If the commander's PIR and JR demand to know ifthe enemy will attack, focus on those enemy activities and preparations which will confirm or deny the enemy's capabilities and probable COA.

Steps:

Immediately first focus on ''immediate threat indicators''.Thus during prioritizing immediate threat indicators translated into SIRs must be given high priority.It is important to not waste time and create and deliver the SIRs quickly to the collection teams.That is don't delay in tasking out to the teams.At the same time when immediate threat indicators are being looked into go ahead with deciding on SIRs for preparatory and secondary indicators.The same SIR may have to be specified differently to different collection platforms in accordance with the nature of the latter.For example we need information about insurgent hideout.Now the SIGINT unit may be given this SIR: Report on any radio intercept in named area beta.The same requirement has to be put forth to the HUMINT team as ''Report on any frequent insurgent movement in to the named area beta'' or to the IMINT team ''Report on any camouflaged structure , cleared foliage area.foot tracks in named area of interest beta'

REPORT LEVELS

For tactical operations, there are four levels of reporting which assists the Unit intelligence section to factor in all useful tactical information gained during the small units activities in the overall planning of the mission (and also update ISR planning):

• Reporting immediately any information the soldier considers of critical tactical value.The soldier may resort to his commonsense/experience or any predetermined criteria to arrive at his judgement.•

• Normal reporting

• Information during normal debriefing sessions by the intelligence officer.

• Follow-up reporting, after debriefing by the intelligence officer is over.

All information collected by patrols, or via other contact with the local population, is reported through your chain of command to the unit Int officer (he will be an officer of the inf Bn). He is responsible for transmitting the information through intelligence channels to the supported military intelligence elements, according to unit intelligence tasks and the

OPORD for the current mission. Therefore, if everyone is involved in the collection of combat information, then everyone must be aware of the priority intelligence requirements (PIR). All Soldiers who have contact with the local population and routinely travel within the area must know the CCIR, and their responsibility to observe and report. The four levels of mission reports follow:

LEVEL 1

Information of critical tactical value is reported immediately to the unit int section, while you are still out on patrol. These reports are sent via channels prescribed in the unit SOP. The size, activity, location, uniform, time, equipment (SALUTE) format is an example of Level I reporting.

LEVEL 2

Immediately upon return to base, the patrol will conduct an after-action review (AAR) and write a patrol report. The format may be modified to more thoroughly capture mission-specific information. This report is passed along to the unit int section prior to a formal debriefing. Your leaders must report as completely and accurately as possible since this report will form the basis of the debriefing by the S-2 section.

LEVEL 3

After receiving the initial patrol report, the unit int section will debrief your patrol for further details and address PIR and CCIR not already covered in the patrol report.

LEVEL 4

Follow-up reporting is submitted as needed after the unit int section performs the debriefing.

Note: Any patrols or activities should be preceded by a prebriefing, which is a consolidated summary of the AOs historical activities.

SALUTE FORMAT (US term)

These four levels help the unit int section record and disseminate both important and subtle details of for use in all-source analysis, future planning, and passing on to higher int HQ.This information helps them analyze a broad range of information and disseminate it back to your level and higher. Report all information about the enemy to your leader quickly, accurately, and completely. Such reports should answer the questions who, what, and where after when. Use the SALUTE format when reporting. Make notes and draw sketches to help you remember details. Table 9-1 shows how to use the SALUTE format.

Table 1. SALUTE format line by line.

Line No.	**Type Info**	**Description**
1	**(S)ize/Who**	**Expressed as a quantity and echelon or size. For example, report "10 enemy Infantrymen" (not "a rifle squad").**

If multiple units are involved in the activity you are reporting, you can make multiple entries.

2	**(A)ctivity/What**	**Relate this line to the PIR being reported. Make it a concise bullet statement. Report what you saw the enemy doing, for example, "emplacing mines in the road."**
3	**(L)ocation/Where**	**This is generally a grid coordinate, and should include the 100,000-meter grid zone designator. The entry can also be an address, if appropriate, but still should include an eight-digit grid coordinate. If the reported activity involves movement, for example, advance or withdrawal, then the entry for location will include "from" and "to" entries. The route used goes under "Equipment/How."**
4	**(U)nit/Who**	**Identify who is performing the activity described in the "Activity/What" entry. Include the complete designation of a military unit, and give the name and other identifying information or features of civilians or insurgent groups.**
5	**(T)ime/When**	**For future events, give the DTG for when the activity will initiate. Report ongoing events as such. Report the time you saw the enemy activity, not the time you report it. Always report local or IST time.**
6	**(E)quipment/How**	**Clarify, complete, and expand on previous entries. Include information about equipment involved, tactics used, and any other essential elements of information (EEI) not already reported in the previous lines.**

HANDLING AND REPORTING OF THE ENEMY

The following paragraphs detail adequate protocol for handling enemy documents, EPWs, and equipment:

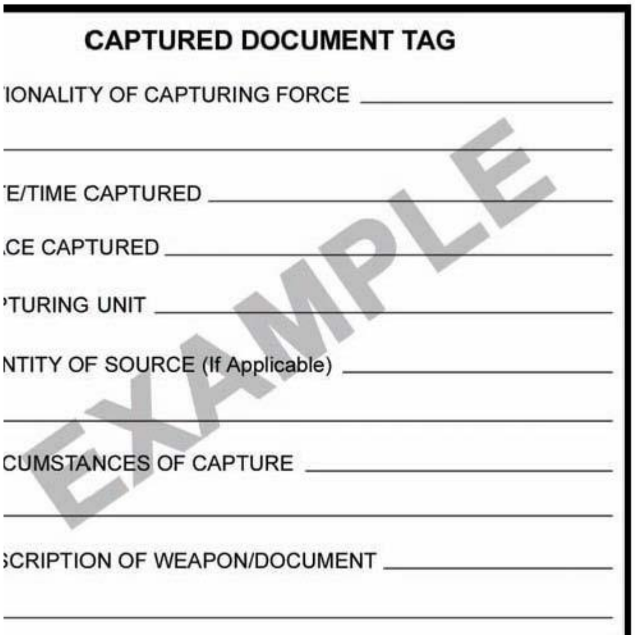
CAPTURED ENEMY DOCUMENTS

A CED is defined as any piece of recorded information obtained from the threat. CEDs are generally created by the enemy, but they can also be Indian or multinational forces documents that were once in the hands of the enemy. CEDs can provide crucial information related to answering the commander's PIR or even be exploited to put together smaller pieces of an overall situation.

Every confiscated or impounded CED must be tagged and logged before being transferred through the appropriate channels. The tag contains the specifics of the item, and the log is a simple transmittal document used to track the transfer of CEDs between elements. Your leaders are responsible for creating the initial CED log.

While the information required is formatted, any durable field-expedient material can be used as a CED tag if an official tag is unavailable. Ensure that the writing is protected from the elements by covering it with plastic or transparent tape. The importance of the tag is that it is complete and attached to the CED it represents. The following information, at a minimum, should be recorded on a CED tag. Instructions for filling out the tag follow (Figure 2):

Nationality–Detail the country of origin of the unit that captured the enemy document.
Date-Time Group–Include date and time of capture.
Place–Include a six-to eight-digit grid coordinate and describe the location where the document was captured. Identity–Define where the CED came from, its owner, and so on. Circumstances–Describe how the CED was obtained. Description–Briefly describe the CED. Enough information should be annotated for quick recognition.



CAPTURED DOCUMENT TAG

IONALITY OF CAPTURING FORCE ____________________

____

E/TIME CAPTURED ______________________________

CE CAPTURED _________________________________

TURING UNIT _________________________________

NTITY OF SOURCE (If Applicable) _______________

____

CUMSTANCES OF CAPTURE ______________________

____

SCRIPTION OF WEAPON/DOCUMENT ______________

____

TREATMENT OF EPWS AND DETAINEES

EPWs/detainees are a good source of information. They must be handled without breaking international law and without losing a chance to gain intelligence. Treat EPWs humanely. Do not harm them, either physically or mentally. The senior Soldier present is responsible for their care. If EPWs cannot be evacuated in a reasonable time, give them food, water, and first aid. Do not give them cigarettes, candy, or other comfort items. EPWs who receive favors or are mistreated are poor interrogation subjects. In handling EPWs/detainees, follow the procedure of search, segregate, silence, speed, safeguard, and tag (the 5 Ss and T). It implies the legal obligation that each Soldier has to treat an individual in custody of, or under the protection of, Indian Soldiers humanely. The 5 Ss and T are conducted as follows:

Search–This indicates a thorough search of the person for weapons and documents. You must search and record the EPWs/detainees equipment and documents separately. Record the description of weapons, special equipment, documents, identification cards, and personal affects on the capture tag.

Silence–Do not allow the EPWs/detainees to communicate with one another, either verbally or with gestures. Keep an eye open for potential troublemakers, both talkers or quiet types, and be prepared to separate them.

Segregate–Keep civilians and military separate, and then further divide them by rank, gender, nationality, ethnicity, and religion. This technique helps keep them quiet.

Safeguard–Provide security for and protect the EPWs/detainees. Get them out of immediate danger and allow them to keep their personal chemical protective gear, if they have any, and their identification cards.

Speed–Information is time sensitive. It is very important to move personnel to the rear as quickly as possible. The other thing to consider is that an EPW/detainee's resistance to questioning grows as time goes on. The initial shock of being captured or detained wears off and they begin to think of escape.

Note: Exercising speed, in this instance, is critical because the value of information erodes in a few hours. Human intelligence (HUMINT) Soldiers who are trained and who have the appropriate time and means will be waiting to screen and interrogate these individuals.

PERSONNEL AND EQUIPMENT TAGS

Use wire, string, or other durable material to attach , Enemy Prisoner of War (EPW) Capture Tag, or a field-expedient alternative, to the detainee's clothing. Tell him not to remove or alter the tag. Attach another tag to any confiscated property. On each tag, write

the following, making sure that your notes clearly link the property with the person from whom you confiscated it:

- **Date and time of capture.**
- **Location of the capture (grid coordinates).**
- **Capturing unit.**
- **Circumstances of capture (why person was detained).**
  — Who?
  — What?
  — Where?
  — Why?
  — Witnesses?

OPERATIONS SECURITY

Operations security (OPSEC) is the process your leaders follow to identify and protect essential elements of friendly information (EEFI). The Army defines EEFI as critical aspects of a friendly operation that, if known by the enemy, would subsequently compromise, lead to failure, or limits success of the operation and therefore must be protected from detection. All Soldiers execute OPSEC measures as part of FP. Effective OPSEC involves telling Soldiers exactly why OPSEC measures are important, and what they are supposed to accomplish. You must understand that the cost of failing to maintain effective OPSEC can result in the loss of lives. Understanding why you are doing something and what your actions are supposed to accomplish, allows you and your fellow Soldiers to execute tasks more effectively. However, this means that you and your fellow Soldiers must–

- **Avoid taking personal letters or pictures into combat areas.**
- **Avoid keeping diaries in combat areas.**
- **Practice camouflage principles and techniques.**
- **Practice noise and light discipline.**
- **Practice field sanitation.**
- **Use proper radiotelephone procedure.**
- **Use the challenge and password properly.**
- **Abide by the Code of Conduct (if captured).**
- **Report any Soldier or civilian who is believed to be serving with or sympathetic to the enemy.**
- **Report anyone who tries to get information about US operations.**

- **Destroy all maps or important documents if capture is imminent.**
- **Avoid discussing military operations in public areas.**
- **Discuss military operations only with those persons having a need to know the information.**
- **Remind fellow Soldiers of their OPSEC responsibilities.**

OBSERVATION TECHNIQUES

During all types of operations, you will be looking for the enemy. However, there will be times when you will be posted in an OP to watch for enemy activity. An OP is a position from which you watch an assigned sector of observation and report all activity seen or heard in your sector.

DAY OBSERVATION

In daylight, use the visual search technique to search terrain. You must visually locate and distinguish enemy activity from the surrounding terrain features by using the following scanning techniques:

Rapid Scan–This is used to detect obvious signs of enemy activity. It is usually the first method you will use. To conduct a rapid scan–

- **Search a strip of terrain about 100 meters deep, from left-to-right, pausing at short intervals.**
- **Search another 100-meter strip farther out, from right-to-left, overlapping the first strip scanned, pausing at short intervals.**
- **Continue this method until the entire sector of fire has been searched.**

Slow Scan–The slow scan search technique uses the same process as the rapid scan but much more deliberately, which means a slower, side-to-side movement and more frequent pauses .

Detailed Search–If you find no targets using either the rapid or slow scan techniques, make a careful, detailed search of the target area using M22 binoculars. The detailed search is like the slow scan, but searching smaller areas with frequent pauses and almost incremental movement. The detailed search, even more than the rapid or slow scan, depends on breaking a larger sector into smaller sectors to ensure everything is covered in detail and no possible enemy positions are overlooked . You must pay attention to the following: –Likely enemy positions and suspected vehicle/dismounted avenues of approach. –Target signatures, such as road junctions, hills, and lone buildings, located near prominent terrain features. –Areas with cover and concealment, such as tree lines and draws.

LIMITED VISIBILITY OBSERVATION

Although operating at night has definite advantages, it is also difficult. Your eyes do not work as well as during the day, yet they are crucial to your performance. You need to be aware of constraints your eyes place upon you at night, because 80 percent of your sensory input comes through them. Your ability to see crisp and clear images is significantly reduced.

Dark Adaptation

Dark adaptation is the process by which the human body increases the eye's sensitivity to low levels of light. Adaptation to darkness occurs at varying degrees and rates. During the first 30 minutes in the dark, eye sensitivity increases about 10,000 times. Dark adaptation is affected by exposure to bright light such as matches, flashlights, flares, or vehicle headlights. Full recovery from these exposures can take up to 45 minutes. Your color perception decreases at night. You may be able to distinguish light and dark colors depending on the intensity of reflected light. At night, bright warm colors such as reds and oranges are hard to see and will appear dark. In fact, reds are nearly invisible at night. Unless a dark color is bordered by two lighter colors, it is invisible. On the other hand, greens and blues will appear brighter, although you may not be able to determine their color. Since visual sharpness at night is one-seventh of what it is during the day, you can see only large, bulky objects, so you must recognize objects by their general shape or outline. Knowing the design of structures common in the AO will help you determine shape or silhouette. Darkness also reduces depth perception.

Normal Blind Spots–The normal blind spot is always present, day and night. It is caused by the lack of light receptors where the optic nerve inserts into the back of the eye. The normal blind spot occurs when you use just one eye. When you close the other eye, objects about 12 to 15 degrees away from where you are looking will disappear. When you uncover your eye, the objects will reappear.

Night Blind Spots–When you stare at an object at night, under starlight or lower levels of illumination, it can disappear or fade away. This is a result of the night blind spot. It affects both eyes at the same time and occurs when using the central vision of both eyes. Consequently, larger and larger objects are missed as the distances increase. In order to avoid the night blind spots, look to all sides of objects you are trying to find or follow. Do not stare. This is the only way to maximize your night vision.

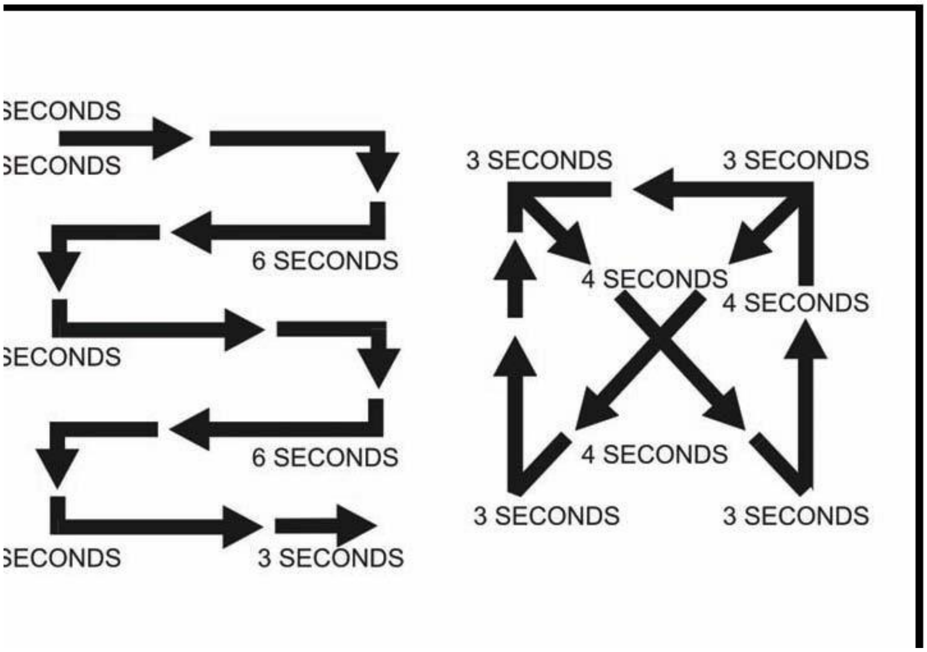
Night Observation Techniques

The following paragraphs detail night observation techniques:

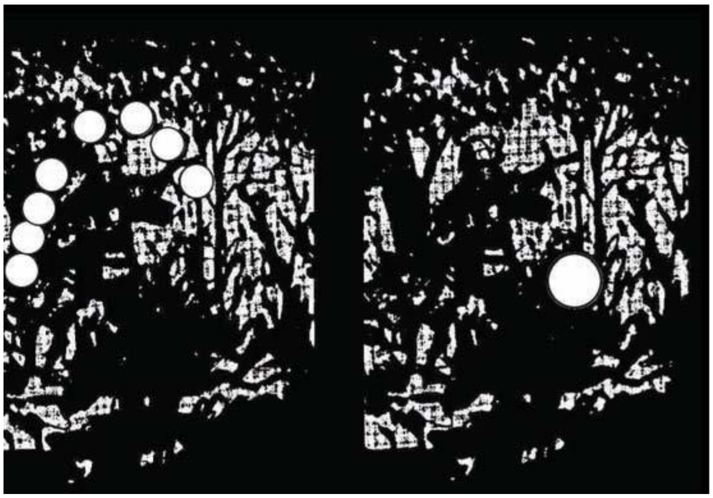
Dark Adaptation Technique–First, let your eyes become adjusted to the darkness. Do so by staying either in a dark area for about 30 minutes, or in a red-light area for about 20 minutes followed by about 10 minutes in a dark area. The red-light method may save time by allowing you to get orders, check equipment, or do some other job before moving into darkness.

Night Vision Scans–Dark adaptation is only the first step toward making the greatest use of night vision. Scanning enables you to overcome many of the physiological limitations of your eyes (Figure 9-5). It can also reduce confusing visual illusions or your eyes playing tricks on you. This technique involves looking from right to left or left to right using a slow, regular scanning movement. At night, it is essential to avoid looking directly at a faintly visible object when trying to confirm its presence.

irm its presence.



Off-Center Vision–The technique of viewing an object using central vision is ineffective at night. Again, this is due to the night blind spot that exists during low illumination . You must learn to use off-center vision. This technique requires viewing an object by looking 10 degrees above, below, or to either side of it rather than directly at it. Additionally, diamond viewing is very similar in that you move your eyes just slightly, a few degrees, in a diamond pattern around the object you wish to see. However, the image of an object bleaches out and becomes a solid tone when viewed longer than 2 or 3 seconds. You do not have to move your head to use your peripheral vision. By shifting your eyes from one off-center point to another, you can continue to pick-up the object in your peripheral field of vision.



LIMITED VISIBILITY DEVICES

The three devices used to increase lethality at night include night vision devices (NVDs), thermal weapon sights, and aiming lasers. Each provides different views of the infrared (IR) spectrum, which is simple energy. The electromagnetic spectrum is simply energy (light). Before you can fully operate these devices, you must know how they work in the IR range, and you must know the electromagnetic (light) spectrum. You should also know the advantages and disadvantages of each piece of equipment. This is the only way to know when to employ which.

ANALYSIS

IPB, all-source, and single-source analysis are conducted to understand enemy order of battle.Analysis aids the commander to get a complete picture (situational understanding0 which
gives him a decision advantage over the enemy.HUMINT elements study and analyse operational taskings carefully to tailor the intelligence requirements(prioritized) to available
collection assets.Analysis is a continuous process.As information is analysed they are fed into
other collection platforms and
fused with intelligence from other sources ,interpreted and translated into intelligence products.The analysed information is also fed back to the HUMINT collectors to refocus collection efforts.Raw information,open source and finished intelligence are analysed by the
analysis team.Analysis occurs at the tactical,operational and strategic levels.

TRAITS OF A HUMINT COLLECTOR

HUMINT collection is a fine-tuned science and a delicate work of art. Although many HUMINT collection skills may be taught,

---

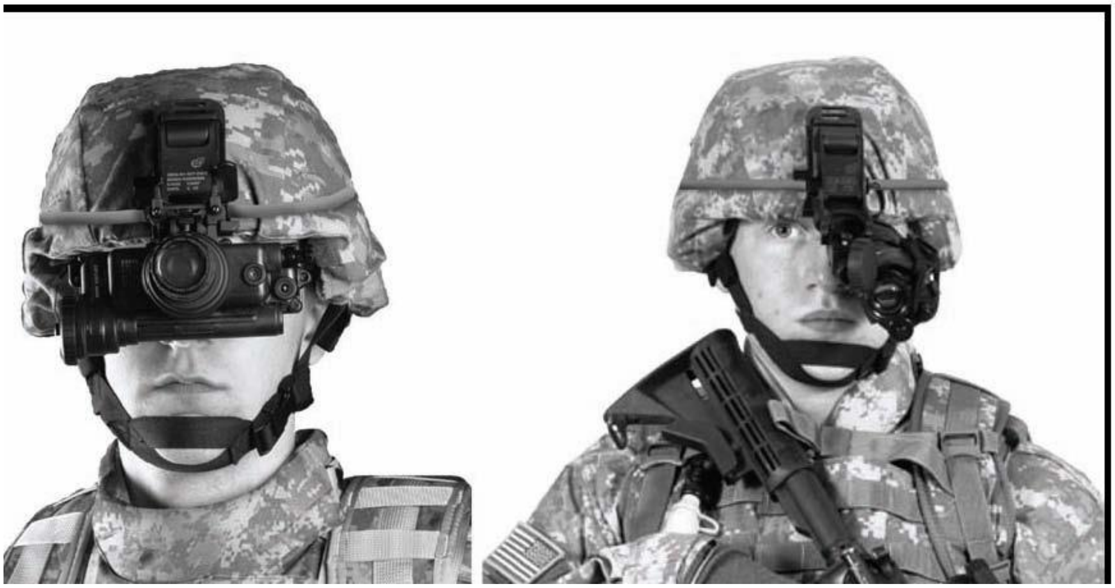
NOTE: THIS PART I HAVE INCLUDED HERE FOR INFORMATION ONLY.HOW THE DEVICES ARE BEING USED BY AMERICAN ARMY TO RENDER LINE SOLDIERS GOOD SENSORS USING OBSERVATION SKILLS ENHANCED BY USING THESE DEVICES

Image-Intensification Devices–An image intensifier captures ambient light, and then amplifies it thousands of times electronically, allowing you to see the battlefield through night vision goggles (NVGs). Ambient light comes from the stars, moon, or sky glow from distant man-made sources such as cities. Humans can only see part of this spectrum of light with the naked eye. Just beyond red visible light is infrared (IR) light, which is broken down into three ranges–near, middle, and far infrared. Leaders can conduct combat missions with no active illumination sources, just image intensifiers. However, the main advantages of image intensifiers as NVDs are their small sizes, light weights, and low power

requirements. Image intensifiers increase vision into the IR range. They rely on ambient light and energy in the near IR range. This energy emits from natural and artificial sources such as moonlight, starlight, and city lights. Image intensifiers include the following :

— AN/PVS-7A/B/C/D.

— AN/PVS-14.



Thermal Imaging Devices

The second type of device that uses IR light is the thermal imaging device . This type of device detects electromagnetic radiation (heat) from humans and man-made objects, and translates that heat into an electronic image. Thermal imagers operate the same regardless of the level of ambient light. Thermal weapon sights (TWSs) operate in the middle to far IR ranges. These sights detect IR light emitted from friction, from combustion, or from any objects that are radiating natural thermal energy. Since the TWS and other thermal devices operate within the middle/far IR range, they cannot be used with image intensifiers. Thermal devices can be mounted on a weapon or handheld. The TWS works well day or night. It has excellent target acquisition capabilities, even through fog, haze, and conventional battlefield smoke.

- **AN/PAS-13(V1) light weapon thermal sight (LWTS).**
  –M16- and M4-series rifles and carbines
  –M136 (AT4) light antiarmor weapon
- **AN/PAS-13(V2) medium weapon thermal sight (MWTS)**
  –M249 machine gun
  –M240B series medium machine gun

- **AN/PAS-13(V3) heavy weapon thermal sight (HWTS)**
  –M24 Sniper rifle
  –M107 Sniper rifle
  –M2 (50 Cal.) HB machine gun
  –MK 19 machine gun

Aiming Lasers

Aiming lasers–both the AN/PAQ-4-series and the AN/PEQ-2A –also operate in the electromagnetic spectrum, specifically in the near IR range. [These lasers] are seen through image-intensification devices. The aiming lasers cannot be used in conjunction with the TWS, because the latter operates in the middle to far IR spectrum.

[illegible]

PROPER ADJUSTMENTS TO THE IMAGE INTENSIFIERS

You must make the proper adjustments to the image intensifiers in order to get the best possible picture. The aiming lasers cannot be seen with the unaided eye; they can only be seen with image intensification devices. You must know how these devices work to maximize the quality of what is being viewed by making the proper adjustments to these devices.

Scanning

The NVDs have a 40-degree field of view (FOV) leaving the average shooter to miss easy targets of opportunity, more commonly the 50-meter left or right target. You must train to aggressively scan your sector of fire for targets. Target detection at night is only as good as you practice. Regular blinking during scanning, which must be reinforced during training, relieves some of the eyestrain from trying to spot far targets. After you have mastered the art of scanning, you will find that targets are easier to detect by acknowledging the flicker or movement of a target.

Walking

Once a target has been located, you must be aware of the placement of the aiming laser. Laser awareness is necessary. If you activate your laser and it is pointing over the target into the sky, you will waste valuable time trying to locate exactly where your laser is pointing. Also, it increases your chances of being detected and fired upon by the enemy. When engaging a target, aim the laser at the ground just in front of the target, walk the aiming laser along the ground and up the target until you are center mass, and then engage the target. Walking your laser to the target is a quick and operationally secure means of engaging the enemy with your aiming laser.

IR Discipline

Once a target has been located and engaged with the aiming laser, the laser must be deactivated. On the range, IR discipline means actively scanning with the laser off. Once a

target is located, walk the laser to the target and engage. After the target has been engaged, the laser goes off.

RANGE ESTIMATION

You must often estimate ranges. You must accurately determine distance and prepare topographical sketches or range cards. Your estimates will be easier to make and more accurate if you know various range-estimation techniques.

FACTORS

Three factors affect range estimates:

Nature of the Object

Outline…………………………. An object of regular outline, such as a house, appears closer than one of irregular outline, such as a clump of trees.

Contrast……………………….. A target that contrasts with its background appears to be closer than it actually is.

Exposure ……………………… A partly exposed target appears more distant than it actually is.

Nature of Terrain

Contoured terrain ………….. Looking across contoured terrain makes an object seem farther.

Smooth terrain………………. Looking across smooth terrain, such as sand, water, or snow, makes a distant object seem nearer.

Downhill………………………..Looking downhill at an object makes it seem farther.

Uphill …………………………..Looking uphill at an object makes it seem nearer.

Light Conditions

Sun behind observer ……… A front-lit object seems nearer.

Sun behind object………….. A back-lit object seems farther away.

ESTIMATION METHODS

Methods of range estimation include–

- **The 100-meter unit-of-measure method.**
- **The appearance-of-objects method.**
- **The flash-and-sound method.**
- **The mil-relation method.**
- **A combination of these.**

100-Meter-Unit-of-Measure Method

Picture a distance of 100 meters on the ground. For ranges up to 500 meters, count the number of 100-meter lengths between the two points you want to measure. Beyond 500 meters, pick a point halfway to the target, count the number of 100-meter lengths to the halfway point, and then double that number to get the range to the target. The accuracy of the 100-meter method depends on how much ground is visible. This is most true at long ranges. If a target is at a range of 500 meters or more, and you can only see part of the ground between yourself and the target, it is hard to use this method with accuracy. If you know the apparent size and detail of troops and equipment at known ranges, then you can compare those characteristics to similar objects at unknown ranges. When the characteristics match, the range does also.

Appearance-of-Object Method

To use the appearance-of-objects method, you must be familiar with characteristic details of objects as they appear at various ranges. As you must be able to see those details to make the method work, anything that limits visibility (such as weather, smoke, or darkness) will limit the effectiveness of this method. If you know the apparent size and detail of troops and equipment at known ranges, then you can compare those characteristics to similar objects at unknown ranges. When the characteristics match, the range does also. Table 2 shows what is visible on the human body at specific ranges.

Table 2. Appearance of a body using appearance-of-objects method.

RANGE (in meters)	WHAT YOU SEE
200	Clear in all detail such as equipment, skin color
300	Clear body outline, face color good, remaining detail blurred
400	Body outline clear, other details blurred
500	Body tapered, head indistinct from body

600	**Body a wedge shape, with no head apparent**
700	**Solid wedge shape (body outline)**

Flash-and-Sound Method

This method is best at night. Sound travels through air at 1,100 feet (300 meters) per second. That makes it possible to estimate distance if you can both see and hear a sound-producing action. When you see the flash or smoke of a weapon, or the dust it raises, immediately start counting. Stop counting when you hear the sound associated with the action. The number at which you stop should be multiplied by three. This gives you the approximate distance to the weapon in hundreds of meters. If you stop at one, the distance is about 300 meters. If you stop at three, the distance is about 900 meters. When you must count higher than nine, start over with one each time you hit nine. Counting higher numbers throws the timing off.

Combination of Methods

Battlefield conditions are not always ideal for estimating ranges. If the terrain limits the use of the 100-meter unit-of-measure method, and poor visibility limits the use of the appearance-of-objects method, you may have to use a combination of methods. For example, if you cannot see all of the terrain out to the target, you can still estimate distance from the apparent size and detail of the target itself. A haze may obscure the target details, but you may still be able to judge its size or use the 100-meter method. By using either one or both of the methods, you should arrive at a figure close to the true range.

Mission Responsibilities of commanders (with regard to soldiers who are not intelligence personnel, but come across information on tactical questioning—secondary collectors)

I have written this particularly from the perspective of our soldiers deployed in Kashmir.
Keshav
How our soldiers can act as secondary collectors

Squad/Section/Patrol/TCP/Roadblock/Convoy Leader:

1. **Patrols, roadblocks, checkpoints, convoys—all these come into contact with enemy personnel (captured), civilians, civil suspects/detainees and criminal elements who can be subjected to tactical questioning. Hence the mission is to train the involved personnel in tactical questioning and integrate it in the planning and**

preparation/execution of the said activities. Pursuant to this prepare for debriefing after all personnel of patrols etc report to the unit intelligence officer

2. **Prepare reports , verbally (debriefing) or written on any observations or information extracted after tactical questioning including being able to recognize any information of so much importance(combat intelligence) that it must be reported immediately without delay.**
3. **During such activities like patrolling, convoy etc all EPW/Detainee and seized documents must be subjected to exploitation carefully as these are prime sources of intelligence.**
4. **All the above should be predicated by the Unit intelligence officers tasking of prioritized intelligence requirements but collection outside these should not be ignored if such information is delivered by the source concerned. They might be of tactical value to the Commander or HUMINT officers.**

Platoon Leader:

Squad/section/patrol/ CP/roadblocks, and convoy leaders are tasked by the platoon leader based on intelligence requirements as laid down by higher headquarters.

Instruct and see to it that it is followed to the book that all personnel returning from patrolling, manning checkpoints, convoys etc report everything and get subjected to full debriefing.

Highlight before them the high importance of submitting information of immediate tactical value without ANY delay. Make it very clear this is mandatory. To this effect he should apprise everyone of the procedures laid down by the battalion intelligence staff in this regard.

Company/Troop/Battery Commander:

Squad/section/patrol/ CP/roadblocks, and convoy leaders are tasked by the platoon leader based on intelligence requirements as laid down by higher headquarters.

All intelligence inputs by the personnel involved in patrolling and tasked with collection are reviewed and forwarded to the Bn intelligence staff and Bde staff. While doing this highlight that information that is linked to the current operations or the AO environment.

Make it mandatory for everyone to be debriefed in keeping with the procedures laid down

by higher headquarters intelligence staff.

Ensure that everyone understands that it is mandatory to report information IMMEDIATELY of critical value.

Battalion STAFF INT OFFICER and S3 Sections:

Task the company, section, squad commanders on intelligence requirements and guide them through the Staff headquarters.

Push down intelligence information to these command levels so as to enable them to get a better situational understanding and know what is expected of them. Thus they will be able to frame tactical questions better.

See to it that all patrols etc are debriefed and no one is left out.

Establish procedures for immediate reporting of information of critical tactical value.

SPECIAL NOTE:

ADVISORY BDE (A special note for Commanders)

We have 5 geographical combatant Command HQs handling day to day administrative duties (theater command?) and in case of sudden major operational task would require major reinforcements. Yes Corps HQ can be deployed to run the operation but it remains to be seen to what proximity to the potential warzone are they located. The 5 Command HQs are located far from these war zones and emergency deployment is impracticable. We must conduct a thorough study to calculate the optimum combatant command requirement considering all operational plans if the need arises for simultaneous multiple fights. Administratively focussed theater armies (the 5 Command HQs) cannot fulfill the purpose so why not amalgamate the CHQ and the Corps HQ into operations focused Corps organization? All can be termed Corps? India is a place with diverse culture , language and relationships.We must build up on these regional knowledge and relationships if we have to effectively combat the enemy , particularly in North East and elsewhere and mind you the Command HQ Staff are in no position to develop this situational awareness/cultural understanding CU (Leading to the all important Situation Development SD for mission success) by being located inside major cities far away from action-zones. What is needed the newly formed Corps HQs can be deployed permanently forward in their assigned

theater of operations so much better regional knowledge and relationships can be built up , facilitating , say COIN operations. But it has been to date a terribly difficult task to build up such regional knowledge and relationships. For example a Coy may get deployed to an insurgent affected area in a NE State for some period and then get phased out with another unit replacing it. Already we do not use intelligence products in a systemized fashion (military intelligence is not just "military intelligence" ..its a war fighting function and like all the other 5 war fighting functions it has an execution and management profile , cutting through all possible enemy patterns (courses of actions) and to facilitate this its process , institutional and product representations all go into creating specific product packages , intelligence products , aptly named and categorized , like the current int summary , the intelligence estimate , threat assessment ,vulnerability assessment , counterintelligence review of the camp/installation , counterintelligence estimate , force protection review , intelligence preparation of the battlefield,pre-RSTA IPB Report(lack of this is exactly what is responsible for deaths of our deep recce troops beyond LOC..Same applies for SOF troops too operating deep into enemy area),local human terrain reports which include everything from insurgent sympathizers to supporters to enemy agents etc..some of these are invaluable during battle-handoff as the new unit takes over provided the outgoing Bn/Coy has its own organic int staff officer who turns over the estimates to the incoming units SO thus enabling him to take security measures , foremost force protection--URI could have been avoided) and hence now the incoming unit is new to the area without any regional knowledge and no relationships to build upon save trained in combat. Extrapolating this , summation of all deployed components of the Corps HQ the picture is the same ..we are fighting the enemy without full situational understanding including the local human terrain factor. Hence not only getting primed for combat but also regional knowledge (geography,demographics,other atmospherics like cultures , language , customs , political system , religion factors etc) and relationships are extremely important when taking cognizance of the entire area of operations..so instead of creating small disparate advisory ad hoc teams out of combat units it is far better and practicable to have dedicated units with language skills and regional knowledge. Or else the conventional troops will have to do the job with little or no training at all. Why not create an Advisory Brigade or a Security Assistance Brigade or an Advisory Corps? Echeloned under the newly Corps HQ in the particular geographic command area? Further we can set up an Advisory School. Now say the Brigade has 200 personnel. These personnel can rotate amongst the various Companies/.units ..Impart training and stay in that commands geographical area their entire career and intermittently attend refresher and other courses to keep abreast of current knowledge in the Advisory School. Again and again they would return to the same units to impart knowledge and training. In the long run the Army Command will have the pulse of the region and the deployed units too , and the factor of uncertainty and surprise by the enemy will be reduced significantly giving our forces a heightened SD and that competitive combat edge for effective and accurate kinetic/non kinetic targeting and

overall mission success. To build up and retain talent and institutional memory of COIN ops we require this organizational and cultural change. Mind you , how many individual platoons really have combat experience in COIN operations? Apart from routine parade and combat training and deployment to peace areas thought the country? It is not important to assess how the current COIN ops are being handled; it's important to note how quickly experiences in COIN operations are fading."Experiences''..Soldiers trained in COIN operations in real time ..not soldiers who are graduating out of COIN schools and only a very small fraction getting deployed , that COIN combat patch..and then being routinely phased out to a peace area unit..The experience going to a waste. In any given platoon or Coy its roughly 15-20% who have actual COIN experience—look 5 years further? Maybe dwindled down to 5%.?? I leave an open question here. I am not an army personnel but whatever I have voiced here I think it holds water. Another thing..my concept of organic int units can also alleviate the problem to some degree because the training regimen I have designed for them includes human terrain collection and IPB…by normal riflemen , not int operatives and with basic training , not involved intelligence education/training.

A DEDICATED BRIGADE

Military Intelligence Brigade

Military intelligence brigades coordinate, manage, and direct intelligence and surveillance; they conduct collection management, all-source intelligence analysis, production; and they disseminate information in support of national, joint, interagency, multi-national, regional combatant command, and Army service component requirements.

Each BRIGADE: ---4-5 SUBORDINATE MI BNS.

Brigade designated combat team has striker team with HUMINT and CI capability in addition to R&S assets.

Brigade headquarters

Ops Bn,

Aerial exploitation/reconnaissance Bn

Fwd collection Bn(CI/HUMINT) ,

Fwd collection Bn (SIGINT),

Comm. Bn.

And electronics Bn,

We need to push down intelligence capability to boot level.

We start by creating a MI Company

Military Intelligence (Ml) Battalion

The MI Bn provides a focused approach for Bde Int staff as it is a fully contained organization with specialized companies, the CI Company, the C&E Company and the I&E company. All these companies provide a better situational understanding of the Bde Commander by providing support to HUMINT, (Tactical HUMINT teams), conducting intelligence preparation of the battlefield, interrogation and document/equipment exploitation operations, support to targeting and battle damage assessment/restrike options, developing threat disposition estimate. The Companies further have MI enabled platoons which on account of being near the ground can collect and provide timely threat intelligence data. Each platoon may be specialized in its own way; one can be a tactical HUMINT platoon , HUMINT platoon, one an ISR analysis platoon all being controlled by the Company headquarters element which also interfaces with the Company

commander and staff and laterally with the other specialty MI companies under the MI Bn.Fusing of intelligence data from the platoons and lateral companies with those that are pushed down from higher HQ on requisition gives a far better threat assessment. Ultimately combat intelligence, target information and otrher satisfied priority intelligence requirements are at the hands of the Commander for necessary action.

The MI company in support provides-

Communications intercept, direction finding (DF), and ECM.

CI.

Interrogation.

Ground surveillance.

Personnel to staff the Intelligence Section, These soldiers conduct-

-Collection Management.

-All-source analysis and reporting.

-Dissemination.

-Technical control and tasking.

-Multidiscipline force protection and OPSEC support.

The TEB Unit provides

1.CI

2.interrogation of prisoners

3.ground-based SIGINT and EW support

4.and LRS support to corps operations

CLIC (This part is relevant to your UNIT in Bijapur)

Under the command and supervision of the Inf Bn STAFF INT OFFICER Int officer intelligence platoons can be created. From among the Bn soldiers according to capability, availability and performance should be selected.

There wil be two echelons in each platoon.

(SECTION A supports Bn HQ.The Bn Int HQ Section will be composed of one Int officer,one intelligence specialist of the rank of JCO, and 3 enlisted soldiers. The Int officer can serve both as staff officer for the Bn Command and also as Commander of the operating forces in the Company. He is responsible for analyzing intelligence and planning deployment and tactical employment of ISR assets. The intelligence specialist can be a ground recon specialist whose duties involve observe and report on enemy activity and other information of military importance in close operations.

(Close operations are operations that are within the commander's area of operation (AO) in his battle space . Most operations that are projected in close areas are usually against hostile forces in immediate contact and are often the decisive actions. It requires speed and mobility to rapidly concentrate overwhelming combat power at the critical time and place and exploit success. Dominated by fire support, the combined elements of the ground and air elements conduct maneuver warfare to enhance the effects of their fires and their ability to maneuver. As they maneuver to gain positions of advantage over the enemy, combined arms forces deliver fires to disrupt the enemy's ability to interfere with that maneuver.)

SECTION B is the CLIC.Colocated with the Company. (One intelligence analyst and five enlisted infantrymen.)

Each company of the Bn should select and train at least 6 personnel.

The formation of this platoon will facilitate initial and sustainment training by ensuring consistency throughout the battalion and eliminating additional training requirements for the companies. It will also ensure standardization in processes and reporting formats, and

further promote lateral communication among the CLICs. Armed with the BLIP the Commander now has his own organic intelligence unit which will provide him additional support apart from the intelligence feeds as a result of his request for information from higher ups.Moreover and more important the BLIPs of all the companies in the Bnb conduct lateral communication , exchanging combat intelligence and other information, thus keeping abreast of latest developments and enemy tactics which the other company is confronting and the tactics, techniques and procedures employed by the company with an element of success. With the passage of time the initial training given to say the enlisted soldiers or the intelligence specialist helps in sustainment training ,the training a byproduct of the operations the soldier is involved with without resorting to tutored training. Soon the BLIP transforms itself into a robust intelligence unit of the Bn,

Company Level Intelligence Cells

Coming to the CLIC level we have an organic capability to acquire combat intelligence directly at the ground level. Actionable intelligence is needed desperately by our fighting forces but the time delay from sensor to shooter(sensors on receipt of request for information collect the data

matching given coordinates, pass it on to the intelligence section for interpretation who in turn sends it to his higher up for evaluation and dissemination to the ground unit; in case of map/imagery obtained by aerial surveillance the time delay is much more) is often so much that despite accurate target nomination the operation slips out of hand. With the CLIC at his disposal the commander now can obtain, analyze and act on readily available combat intelligence without having to wait for intelligence feeds.C2, intelligence and operations are hereby synchronized and integration achieved successfully. That too at the lowest level. The CLIC is supervised by the company commander. The two sections of CLIC , collection and analysis and production are looked after by the officer in charge , usually a JCO and there will be two soldiers , one from each section to function as intelligence watch and are assigned to the company combat ops center.

Functions/responsibilities:

CLIC O-I-C: Reports to Company Comander,assists the watch officer in operations situation development (common tactical ops picture),managing and supervising CLIC ops,interacting with adjacent units , lower units and higher echelons and utilizing the intelligence flow.

If required, the CLICs now have the capacity to surge intelligence trained soldiers to support operations such as cordon and searches and raids.

After an area of operations is identified inhabited by an asymmetric enemy in a complex terrain with weak transportation and logistical infrastructure. We need to deploy an interim combat team complete with HUMINT/, CI/. SIGINT assets which will act as an early combat team, mounted infantry organization with the capability to rapidly assess the environment, physical terrain, community, cultural and political and conduct an intelligence preparation of the battlefield by assessing the enemy's strength, capabilities, disposition, TOE thus enabling the striking force to project itself before deployment. The primary intent here is to develop a situational understanding of an unknown area inhabited by an enemy against the backdrop of distributed, asymmetric, nonlinear simultaneous operations. Here the problem is to determine the OB of an enemy that doesn't have a conventional standing force nor is easily identifiable. We don't see any typical military structure, units, rear and forward areas or logistical networks characteristic of conventional enemy forces. It is a big question how to deploy ISR assets for collecting intelligence or conducting reconnaissance or for that matter determining the center of gravity of the enemy.

LRS units provide reliable HUMINT against second echelon and follow-on forces and deep targets. LRS units conduct stationary surveillance and very limited reconnaissance. They deploy deep into the enemy area to observe and report enemy dispositions, movement and activities, and battlefield conditions. They arc not equipped or trained to conduct direct-action missions.

EXTRA NOTES:

PROJECTING COMBAT POWER WITH ORGANIC ISR CAPABILITY

Reason for creation of interim tea

Without sending in the interim combat team to gain a situational understanding it is totally impracticable to deploy the striking forces. What we need is a interim combat force with reconnaissance, surveillance and target nomination capabilities—all these facilitated by an organic MI company with organic intelligence assets.

The recce platoon, in addition to reconnaissance and surveillance should also engage in HUMINT activities for thorough situational understanding. The situation in asymmetric warfare is different. Here the recce platoon can conduct HUMINT operations. The

reconnaissance platoon should be equipped with CI capability. This heightens its HUMNINT collection ability.

The HUMINT teams (4 teams) are in effect Tactical HUMINT Teams each with 3 HUMINTcollectors and one CI agent. Once deployed, the teams report their information to an operational management team (OMT), which collates intelligence data gathered by the tactical teams. The information is then passed on to the brigade INT section for further analysis and integration into the brigade's collection plan.

C2:

The reconnaissance platoon HQ and the HUMINT platoon HQ both should contain one CI NCO.The reconnaissance squads each should have one CI soldier. Thus at the lowest tactical level organic CI capability with the deployment of maximum possible CI soldiers is hereby achieved thus increasing significantly the reconnaissance troops HUMINT collection capability. We can optimally have in the recce patrol 3 six-man squads, each having a CI soldier.

HUMINT OR MI BN IDEA

INTERIM COMBAT TEAM WITH ORGANIC INT AND R&S CAPABILITY – TO PROJECT FORWARD OF AO

Operations Battalion

Collection Management Section

Production Section ASPD & OB Teams

BDA & TGT Team

CI Team

Single Source Teams.

MASINT Team

SIGINT Team

HUMINT Team

IMINT Team

Corps Military Intelligence Support Element

Intelligence Support Elements

FUNCTIONS AT BN/PLATOON LEVEL(CLIC)

HUMINT Collection Operations

Combating terrorism support

Rear operations support

Information operations support

Civil disturbance support

Local operational data collection

Debriefing and interrogation

HUMINT threat assessment

Reconnaissance HUMINT Missions

Elicit information from the local populace.

Interrogate EPWs and Detainees.

Debrief Allies and U.S. personnel.

Document exploitation.

Vulnerability assessments.

Source screening operations.

Spotting/assessing for Tactical HUMINT Teams.
Civil -mil ops
OPSEC Support

MY DESIGN OF DEDICATED INT COMPANIES/BN

COMPANY LEVEL MILITARY INTELLIGENCE CELL:

Organization
The MI cell (C& E), shown at Figure 2, is organized into a headquarters section, an MI unit (CI), an MI unit (interrogation and exploitation), and an MI unit (collection and

exploitation). Headquarters section provides C2, administrative services, and logistic support for units of the company.

Roles and Functions

The Collection and Exploitation section provides interrogation and CI support. Functions , include:

- ❖**Setting up interrogation centers and executing interrogation operations of enemy prisoners of war.**
- ❖**Determine enemy multidisciplinary intelligence threat, analyze it and recommend countermeasures, both on the passive defensive side as well as offensive methods.**
- ❖**Conduct exploitation of turned enemy agents. Conduct polygraph techniques and technical operations.**
- ❖**Conduct DOCEX**
- ❖**Conduct debriefing of high level military/political figures,refugees,patrols,military personnel who are released by enemy from capture or who have escaped from captivity, detained civilians and other people who have information of interest.**
- ❖**Conduct Counterintelligence Force Protection Source Operations (CFSO).**

MILITARY INTELLIGENCE UNIT (CI)

Mission

"The mission of the MI Unit (CI) is to conduct CI operations and multidiscipline counterintelligence (MDCI) threat analysis in support of the Commanders intelligence requirements''.

Organization

The MI Unit (CI) will be composed of a section HQ, an Ops section, and CI platoon.

Roles and Functions

- ❖**Provides C-HUMINT support**
- ❖**Conducts Vulnerability assessment**
- ❖**Supports OPSEC**
- ❖**Supports targeting , nominates HVT**
- ❖**Conducts CI investigations**
- ❖**Conducts Counterintelligence FP Source Operations**
- ❖**Conducts counterespionage,countersubversion and counter sabotage operations.**
- ❖**Liaises with other intelligence agencies**

❖Conducts offensive operations during wartime Areas of interest:

- **❖Known or suspected acts of treason,sedition,espionage by Army personnel**

- **❖Known or suspected association with elements of threat intelligence**
- **❖Terrorism, assassination incidents**
- **❖Defections and unexplained absence of Army personnel**
- **❖People impersonating as military intelligence personnel.**

MI UNIT (INTERROGATION AND EXPLOITATION I&E) Mission

"The mission of the MI Unit (Interrogation and Exploitation) is to conduct interrogation of enemy prisoners of war EPW,debriefing of persons having information of intelligence value and exploitation of captured doicuments,media and hardware."

Organization

The MI Unit (Interrogation and Exploitation) consists of a HQ section, an Ops section, communications section and I&E platoon.

Roles and Functions

□➢Setting up interrogation facilities during wartime

➢Interrogation of EPWs.Establishment of a joint or combined interrogation facility and conduct interrogations of EPWs. Conduct debriefings of high level political and military personnel, civilian internees, refugees, displaced persons, and other non- US personnel.

➢Conduct debriefing of high level military/political figures,refugees,patrols,military personnel who are released by enemy from capture or who have escaped from captivity, detained civilians and other people who have information of interest.

➢Conducts DOCEX,and translation of captured documents. Translate and exploit documents acquired, found, or captured in the theater AO.

➢Debrief US and Allied personnel having escaped after being captured or having evaded capture.

MI UNIT (COLLECTION AND EXPLOITATION C&E)

The above two units, viz MI (CI) and MI(I&E) are combined into one UNIT , collection and exploitation MI(C&E) and hence executes all the functions which are inherent in the 2 units. This is a modular unit, can hence plug as a detachment support into any Battalion/Company which requires CI/HUMINT support but does not require a full intelligence battalion /Company expertise. It can also be situation may not allow the

deployment of full intelligence assets –in such a case the MI(C&E) can be scaled and tailored to suit the requirements of the Battalion. This unit can pull operatives from both the MI (CI) and MI (I&E) to create CI and I&E platoons to conduct tactical HUMINT (CI/HUMINT) missions with the available CI, collection, and exploitation and interrogation expertise.

Mission

"The collection and exploitation unit collects intelligence information through the acquisition, training, briefing and debriefing of HUMINT assets in support of Army requirements and provides CI support within the area of operations, conducts interrogations of prisoners of war and other personnel of intelligence interest; translates and exploits selected foreign documents/ media; and exploits foreign materiel of intelligence interest."

Organization

The MI Unit (Collection and Exploitation) consists of a section headquarters, CI operations section, interrogation operations section, and counterintelligence and I & E platoons.

BN HQ CO INT SEC (RELEVANT TO BIJAPUR UNIT)

We can have an integral organic intelligence capability at the Battalion level:

The Bn Intelligence section will consist of the Bn intelligence officer, a JCO , 2 havildars and 6 infantry soldiers. The Bn Intelligence section will interface between the companies and the Bde.The companies pass on intelligence information for processing to the Bn Intelligence section who in turn passes them on to the Bde and also as per ground requirements from the companies and Bn staff .The Bn intelligence section will develop sources and contacts from among the local population and liaise with the civil police and intelligence agencies. The question of deconfliction arises at this stage as the line companies and platoons have their sources , contacts and liaisons as well as the civil agencies. It is the responsibility of the Bn intelligence section to deconflict its sources with all these sources, contacts and liaisons. The Bn intelligence section will use its HUMINT and other capabilities to detect weapons/explosives caches, collect incriminating evidentiary information for prosecution by the civil agencies and increase the overall situational understanding of the Bn and Bde commanders and staff. Delineation of sources between the Bn , the line companies , the platoons and the HUMINT units is very important by

clearly defining the responsibilities of each with respect to the sources. We can have contacts like community leaders of influence , local politicians and councilors , surface and witting contacts as well as those contacts who are very useful , can supply information of rich intelligence value but need protection which will be the responsibility of the HUMINT units. The overt contacts like the community leaders etc can be the responsibility of the Bn intelligence section while the surface contacts and liaison can be given to the line units and platoons. The same line units and platoons can forward to HUMINT units any source of HUMINT interest which they come across community operations , patrolling or tactical operations

APPLICATION:

Support to Division:

The focus of intelligence and counterintelligence should shift from purely strategic to the support of strategic through tactical operations.

Thus far detachments/units working to collect intelligence functioned under one chain of command , a rather autonomous function , what is needed now the individual operator or special agent operates as a part of a much larger team than his own unit.Adjacent and far flung companies should be interconnected w.r.t ''intelligence-awareness'' and hence lateral communication between all the organic int sections and CI agents.Shifting from pure strategic to support of strategic through tactical operations requires modifications in doctrine , requires organic int capability in combat units.

Every Battalion has its own organic int section.This int section will also have 2 CI agents.The int section will be authorized to communicate with the Regiment G2 Int and laterally with other Battalion int sections.The G2Int office will have two commissioned officers of the rank of Captain and Lieutenant.Apart from executing secondary collection activities of the int requirements of the Battalion Cdr , a Battalion Detachment Cell composed of selected personnel from among the int sections will provide int support to the Division separately.As the personnel staffing the BDC are from among local battalion int cells they are close to the ground situation in the overall Area of Ops of the Division and as they come from far and seperated sub-AOs , the composed team will have personnel of varying rich experience from their own AO and as a result the admixture will be better able to prioritize and execute intelligence tasks and be in a much better position (due to enhanced situational awareness) to feed adequate and accurate intelligence to the DIV G2.This is lateral intelligence operations (Battalion wise) and upward vertical intelligence operations(push to DIV G2).The Battalion int section CI agents will form the Counterintelligence Control Line spanned across the full area of operations along the forward/near-border perimiter.Details in next section.This combitorial arrangement will act as a double sheathed sword , and mind you the number of collectors per unit AO (due to every Battalion having its own int cell) is increased considerably with much greater exploitation of the physical and human terrain.

This horizontal and vertical arrangement has following objectives:

1.Localized intelligence collection activities , each Coy level int cell focussing on the area of operations under its purview.

2.Inter-Battalion intelligence exchange thus apprising every commander of the overall situation thus leading to enhanced situation awareness and development.
3.Seperate CI activities in the same vein as above.
4.More intensive coverage w.r.t human terrain exploitation and physical terrain profiling.
5.Organic intelligence support(with local knowledge and expertise) in form of Battalion Detachment Cell supporting Div G2 Int planning and execution , rather than external detachments from Int Corps HQ.
6.Establishing the Counterintelligence Control Line to check infiltration , exfiltration and other ops.

Counterintelligence Control Line:

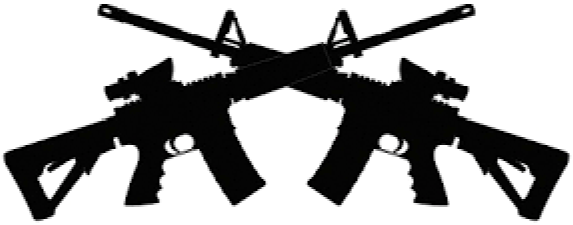
Composed of CI agents belonging to Battalion int section , this control line will be running across the length of the Div or Army sector with check points established at road junctions , bridges , cafes,hotels,villages near the border or a bit more inside.The objective is to prevent infiltration by screening individuals for travel reasons/authorization documents,identify suspected enemy agents and terrorists,and terrorists or enemy soldiers/agents in civilian clothing.Secondly prevent outward movement of terrorists sympathizers , would be terrorists and escape of terrorists .The underlying concept is increased security consciousness and counterintelligence effort.Identification documents and stories will be closely scrutinized by CI personnel in conjunction with troops and MP soldiers manning checkpoints and roadblocks.As for other points such as hotels , villages , cafes , mosques , CI personnel in strength of two can keep a watch and if need be detain and question suspects.The Counterintelligence Control Line is a very important line of defense against the launchpads of terrorists operating from POK.CI agents , Military Police and Combat elements can collaborate to render the Counterintelligence Control Line effective.The points of control inside civil areas can be manned by CI agents in civil attire , trained in observation and tactical questioning (not interrogation) skills.These are all 24 hour security posts with small interrogation centers established near border areas , where questioning of all suspicious elements will take place..Communication between the control nodes will make it possible for not too distant units to know about developments which might affect their area.Communication between CCL nodes and Army areas will help further in deterring infiltration and apprehend/identify/liquidate those who have infiltrated or going outward.

MY DESIGN FOR COP

(Can be skipped for now.Its slated to come up after a year of the creation of organic int unit.)

NON-LINEAR DISTRIBUTED BATTLESPACE

ASYMMETRIC/HYBRID ENEMY



BATALLION LEVEL INTELLIGENCE CAPABILITY (PUSHING INT CAPABILITY TO BOOT LEVEL)

INTRODUCING CENTRALISED INTELLIGENCE AND COMBAT OPERATIONS CONTROL THROUGH TOCs

BATTLE STAFF NCOs

&

INT/OPS NETWORKING THROUGH THE CREATION OF THE DIV INTELLIGENCE NET FOR NORTH EAST (EASTERN COMMAND)

ANNEXE-1

TACTICAL LEVEL INTELLIGENCE CAPABILITY

BN INT SEC STAFF

J2Int---He is the main staff officer handling all security procedures ensuring strict compliance.To this effect he takes into account:

Mission precise definition

Mission breakdown into subcomponents & Analysis

Wargaming

Planning

Operation execution

(He will coordinate with JSO(Ops) throughout so as to integrate intelligence and operations.Intelligence drives ops;and vice versa--this he should always bear in mind.In fact the S1 and S2 should be colocated in the same operations center.)

(The Division must maintain an intranet capability wherein all intelligence and operations data,historical , current and projected are maintained in the database.For example,all sensors,humint-sigint-elint-comint-techint-masint deployed in the Brigade area of the Division should be able to channel the information collected to the specific tactical operations center Desk NCO.Each Brigade will have seperate TOCs installed for each/group of (as the case may be depending on manpower availability to staff TOCs)company/companies of every batallion.The humint team will send reports to the HUMINT Desk NCO.Similarly with the other intelligence collection disciplines/sensors.Now after analysis by the analysis element in the TOC the intelligence information is passed on to the LAN server.Say we have as the TOTAL NORTH EAST battlespace comprising of the disturbed States.Every State is broken down territory/area wise into specific area of ops.Each area of ops is subjected to intelligence collection by the Bn Intelligence organic units,wherein the information as said above is passed on to speciic intelligence sensor based TOC.or it could be one TOC may cater to all sensor types with each Desk NCO allocated to each sensor information receipt channel.Each subset area of operations within the boundaries of each State has as its intelligence and ops database input nodes at the TOCs of the Brigade (each Bn)/Bn group.A group of such TOC nodes are conected to one LAN node.In this manner an entire network of LAN nodes are dispersed in each State.The complete LAN is connected with the total AO WAN system..Now the total battlespace which comprises of all the affected NE States has as its information repository domain the WAN Servers.Each WAN NODE will cater to each State intelligence ops as well as all tactical combat ops(linked to all the TOCs of the State AO.).. This entire system in its totality should be viewed as concentric circles.The outermost ring is the deployed sensors (or as I aim to achieve , organic company level-platoon level intelligence sections--that is boot level sensors);The next ring will be the individual TOCs and the DESK NCOs receipt/dissemination terminals.The inner ring will be the LAN chain of all the States; each LAN being comprised of all the sub-LANs of that

State to which feeds come from all the State TOCs.All feeds from this inner LAN ring will be into the next inner ring - the WAN Network Main Server.In this manner we have overcome the probs of decentralized command and control of intelligence and tactical operations in a nonliner distributed wide battlespace (it is not possible for every tactical unit to push upwards all intelligence and combat operation to higher headquarters in a very wide (State) area of operations , there is an inundation of information at Bde level intelligence section--it cannot manage easily even with intelligence detachments sporead out without the installation of Bn-level TACTICAL OPS CENTERS (and Company level organic intelligence cells created out of a team of non-int occupational speciality personnel--like the infantry soldiers,MP,patrols-- trained in basic tactical questioning,elicitation,observation and surveillance skills.The TOCs bring in an element of control and ease of information push to much lower levels than higher HQs for the tactical units deployed.In each sub-sector of each AO within each sub-region of each State the tactical units find it easy to push information to the locally installed TOC.The group of TOCs in the State can exchange information laterally among themselves and get a clear picture of all activities and trends.This helps to give the Bde Commander a clear common operating picture COP--which means the exact ground situation without being inundated with unnecessary or conflicting or excessive intelligence information.(In my CFET web portal I have detailed the battle-staff functions of each TOC wherein cases like deconfliction , technical control of int/counterint TTPs,updating and management of source network and source registries,requirement,collection assets management and collection management,administrative control,ops management,dissemination--all being handled by NCOs and a JCO with one battle Captain).This TOC network through the Overall LAN system of each State can effectively push/pull information from the main WAN Network.Thus we find that an effective command and control of the entire NE intelligence and tactical combat operations is ensured due to the availability of intelligence and combat information at the boot level (Company level int capability and lower) ,TOC level , State level (LAN System) and the entire Battlespace (NE) Level THROUGH THE MAIN WAN NETWORK(Each Bde Level).All Bde's will have their own network system on similar grounds in their AO with the main linkages to the DIV MAIN INT/OPS DATABASE SERVER.This is what I will call the Div Ops and Intelligence Net (the main WAN System).

During deployment for combat the Bn intelligence section int officer can enter this Div NET AND CAN ACCESS THE division ops and intelligence activities if necessary.He can thus maintain a current intelligence situation report/map within the Bn TOC reflecting the current enemy situation.At every level trends,pattern recognition , analytical (link diagramming,forecasting trends,association mapping,time series analysis,PERT/CPM applied to operations etc)software can be used to manipulate and research information on the servers.Such information may be pushed down on request to operational/tactical levels.

(To be elaborated more in subsequent pages....,with detailed intelligence requirements,asset management and collection management , Company int cells for each specific adversary

function/activity/ops,insertion of collected information to each soldier terminal , push to sector TOC , push to sector LAN , uploaded to MAIN WAN SERVER..trend recognition , analysis and pattern recognition software installation on server to work on all information contained in servers , and querying syntax specifically designed from boot level to seniormost oficers --with the ''need to know'' clearance)

CP/TOC
BATTLE STAFF NCO-INTELLIGENCE WARFIGHTING FUNCTION

Roles and Functions of Battle Staff

Noncommissioned Officers in the Intelligence Warfighting Domain

Battle staff noncommissioned officers (NCOs) focus on assisting their respective

staff officers and senior NCOs. The entire staff contributes to making and executing timely decisions. Commanders and staffs continually look for opportunities to streamline cumbersome or time-consuming procedures. The following paragraphs, organized by warfighting function (WFF), suggest activities and functions common to all members of a particular staff section. Principal staff officers along with their senior NCOs determine

what specific functions are performed within their sections based upon the skill sets of available personnel.

Commanders and Staff concentrate on achieving a streamlined picture of the ensuing battle , in fact at any moment of time the Staff and the Commander should be able to grasp the immediate current situation as simply as possible without the presentation getting inundated with information overflow.This common operating picture viewed explicitly and concretely enables the Commander to take swift decisions in an otherwise fast evolving uncertain battle environment.It is not possible for the Staff to accomplish this by themselves and the standard office personnel who assist them (in the Tactical Ops Center)..what is required that the battle staff from among the JCOs,Senior NCO and NCOs assist the Staff Officers in the respective warfighting functions , viz: intelligence and CI;maneuver;sustainment;command,control,communication and computers C4;plans;fires;protection;engineer and provost marshall functions.The main objective is to acquire the best situational understanding about the common operating picture within the tactical operations center/command post. .

The TOC/CP has two primary functions:

. • To track Soldiers and equipment during the battle to assist the leader in

the command and control of the unit.

• To serve as a data center that processes enemy and friendly information

Intelligence (Intel) Function

Intelligence readiness,tasks,synchronization,counterintelligence,other intelligence support and support to force protection , coin , and other security programs—these war fighting functional domains if properly executed, supervised and controlled ,help the Commander to a great extent in visualizing the battlefield from the correct perspective and shape the battle in his favor by deciding promptly on course of actions. It is here where the most must be extracted from the Battle Staff NCOs who are assisting the Battle Staff Officers.

Intel readiness:

• Throughout the AO the Battle staff NCOs should coordinate with horizontally dispersed units and intel staff and lower and upper echelon staff,establishing and maintaining the proper relationships/procedures.

• There should be a proper command intelligence training plan and the Battle staff NCOs should see to it that threat force considerations,intelligence,counterintelligence and force

protection are properly integrated in this training plan.This will ensure good intelligence readiness.

- **Prepare the command intel-training plan and integrate intel, counterintelligence,**

and enemy/threat considerations into other training plans.

Intel tasks:

- **Recommend priority intelligence requirements (PIR).**

- **Execute and manage the intelligence preparation of the battlefield in line with changing intelligence requirements due to the rapid tempo of battle,co-ordinate with the IPB efforts of the rest of the staff and other unit staff.**

Create situation reports,intelligence estimates,update enemy/threat/terrain/weather factors so that the commanders situational perspective is heightened thus leading to a clear common operating picture COP.

Provide support to indications and warning with respect to operations.

Provide support to Force Protection

Provide intelligence support to battle damage assessment.

Provide support to targeting:Develop targets,Create and manage target grey,white and black lists,target folders,target reduction,target acquisition and tracking of HPTs.

Information operations is the mainstay in any battle and to this end the Battle staff NCOs should provide intelligence support by providing intelligence feeds during IO planning and while intelligence planning to consider IO factors.

Other intel support:

- **Provide intel updates, other products, and additional support to ISR integration, the concept of operations, and mission accomplishment.**

- **Advise the commander so that all collection, production, and dissemination adhere to special security, legal, and regulatory restrictions.**

- **Facilitate the military-intelligence-unique deconfliction of collection among assigned, attached, and supporting intelligence-collection assets and other collection assets in the area of operations (AO).**

• Prepare the intel annex to plans and orders and the intel estimate.

• Coordinate technical control and technical support for military intel assets and units.

• Debrief friendly personnel.

• Identify linguist requirements pertaining to intel support.

• Determine all foreign languages and dialects proficiencies needed for mission accomplishment.

• Coordinate security investigations of local-hire linguists.

Counterintelligence:

1. **See to it that the counterintelligence activities are conducted properly, in line with standard TTPs (technical control) and coordinate all such activities keeping deconfliction in perspective.**
2. **Keep a tab on all contingency funding and source-rewards programs.**
3. **Identify threat multidimensional collection capabilities and activities which are geared against the unit.**
4. **Match these intelligence collection capabilities against the unit's security and intelligence capabilities , activities and plans. These include operational security,countersurveillance,signals security , military security, deception planning, force protection,PSYOP,area security operations. Here it is very important to conduct a mission-needs-capability analysis to properly utilize counterintelligence assets without wasting them or utilizing assets which cannot put up with enemy capability or unable to satisfy the Commanders intelligence requirements.**

Support to security programs:

1. **Conduct a counterintelligence review of the unit installation-physical security**
2. **Evaluate security programs of the command. Supervise these programs as they relate to Command , personnel , information.**
3. **Support to OPSEC**
4. **Support to deception practices as applied to units plans , intent and actions.**
5. **Ascertain unit vulnerabilities and advise accordingly**
6. **Ensure biometrics systems are in place and functioning properly.**

TACTICAL OPS CENTER/CP BATTLE STAFF INTEL NCO

The Commander needs to see , shape , shield , strike and move within the Battlefield most efficiently while retaining that competitive edge over the enemy.Battlefield conditions are extremely fluid and the current type of prevailing Battlespace--distributed and non-linear-- compounds intelligence collection highly.

I would like to view the Battlespace not as a whole , operationally or strategically but rather as a tactical-nodal-network..numerous tactical battles being fought at various points distributed throughout the battlefield..in fact so numerous that its a very very hard task for limited intelligence collection assets to cover the entire battlefield with the result (what has been happening till now) intelligence/information feeds up the channel to higher HQs are only from the major battles , the routine tactical battles going ignored.Unlike our american counterpart , the boot level indian soldier is not equipped with hand-held data entry system which can also access pertinent intelligence required by him from the central intelligence database at rear-HQ/Higher HQs.Hence if in any tactical combat operation the soldiers gain valuable intelligence , say after exploitation of captured enemy personnel or documents they cant ''push'' it above.Again the limited information flow upwards by intelligence collection assets is ''limited'' as only major battles and some tactical engagements are covered.With the result that the higher HQs does not get a complete situational understanding and also limited responses in the form of targeting instructions or need for further intelligence is pushed down to the operational and Bn levels..with most of the urgent actionable intelligence required by the soldier on the ground being unobtainable. We need to make the average soldier on the ground int-savvy.It is not difficult , as he needent be trained in all intelligence functions but rather be acquainted with tactical questioning,screening and document exploitation plus surveillance/reconnaissance skills. Regarding the last two he need only understand how R&S is conducted , and all the factors that go into it--predeployment,insertion and the two activities itself(collection)--he needent be proificient in R&S,the intelligence asset (the CI man[or one member of the R&S team trained in TQ,DOCEX] with the R&S team) can look for intelligence/CI information while the R&S team does its own bit.

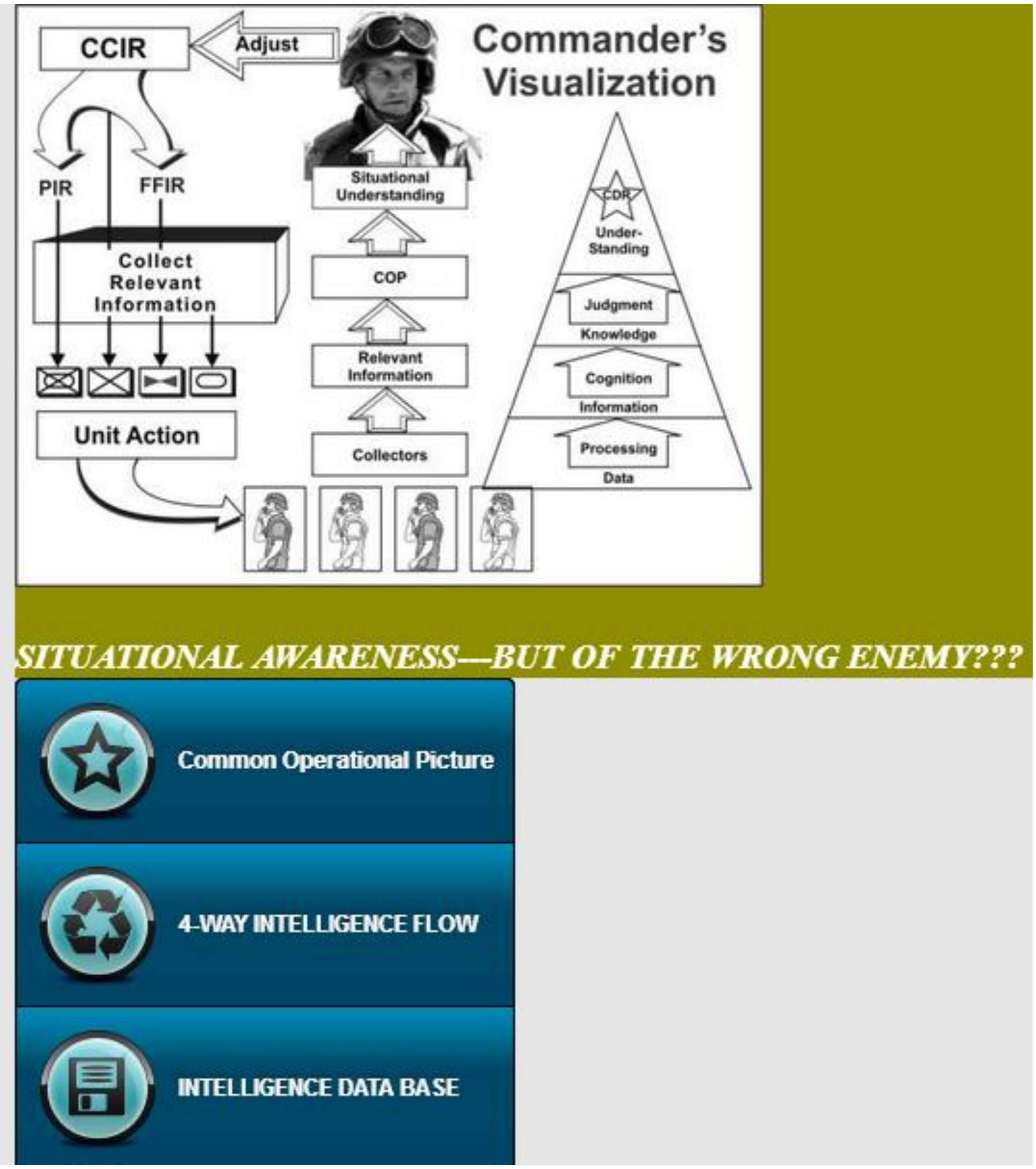
Battle Staff man the TOC/CP;besides the officers/JCOs there are the Senior NCOs and NCOs.These people can be trained to assist in intelligence duties; if the TOC/CP suffers casualties and if we have a pool of int-savvy soldiers which can be drawn from the combat troops,well the TOC/CP is again operational. The next section will elaborate Battle Staff (NCOs and Senior NCOs) functions w.r.t the intelligence warfighting function.

The CP officers role is to configure operations in such a manner so that he can ''see'' the battle space in the most simple, direct manner , without any ambiguity or inundating information and maintain a wide view of operations. Military decision making and planning processes occur at all levels of Command and similarly at the CP/TOC too. Battle staff officers should be able to analyze higher headquarters mission orders , adjacent headquarters feeds/requirements and lower units requirements and ''pushed-up'' intelligence feeds – ensuring seamless operations. They should be able to assess the tactical situation , the enemy's intent and the long and short term friendly courses of actions. They use MDMP to properly steer TOC/CP operations in conformation with the Commanders intent and priority intelligence requirements and develop estimates and plans within the various war fighting functional areas. These are sort of ''managerial roles'' which can only be accomplished successfully with a trained battle staff NCOs and Sr NCOs in the CP/TOC team. . The TOC/CP battle staff officers should not routinely post the Operations map, work digital command and control (C2) systems, or answer Telephones. These roles should be fulfilled by battle staff NCOs.These Battle staff NCOs must have access to all war plans at the CP/TOC ,must understand fully what are the critical and priority intelligence requirements of the Commander as laid down before the Battle staff officers , must be able to receive and analyze intelligence feeds from the ongoing tactical operations in the AO overseen by the CP/TOC,maintain and understand ops schedules , execution matrices and overall common operating picture. He is the frontline information manager. The battle staff NCO and battle captain must work together and understand each Other's roles and responsibilities.

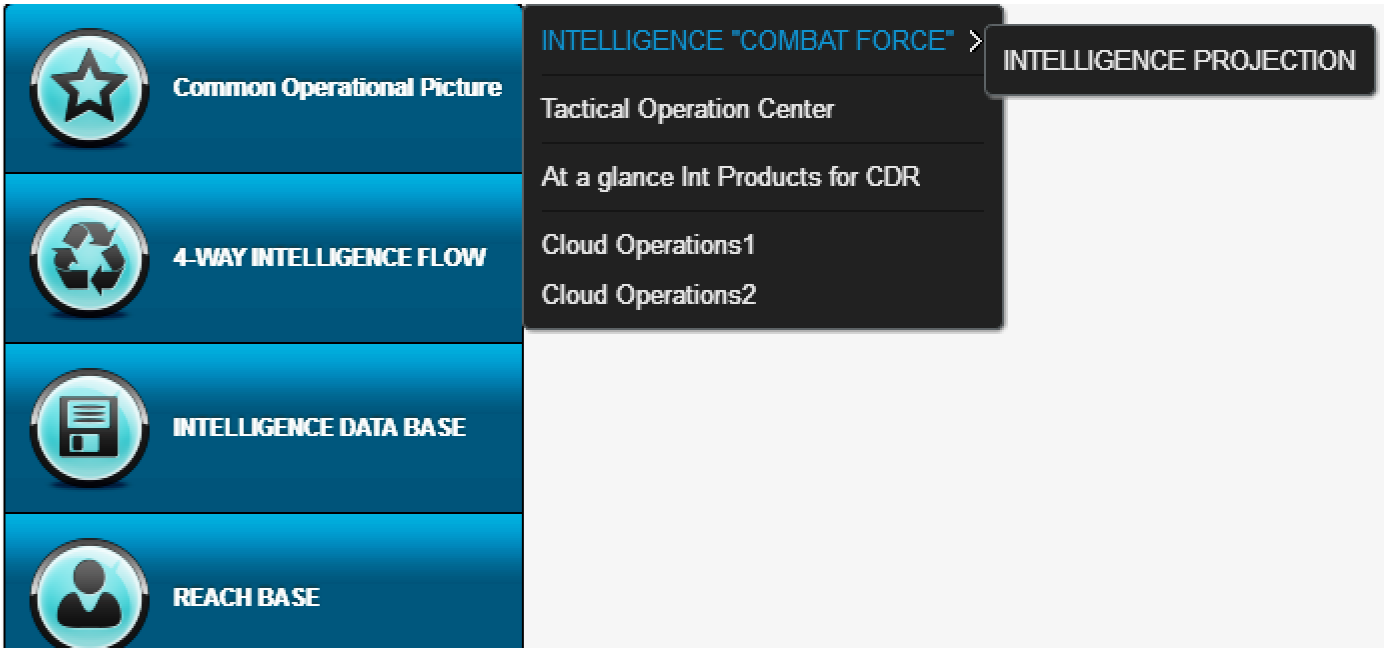
Commanders and Staff concentrate on achieving a streamlined picture of the ensuing battle , in fact at any moment of time the

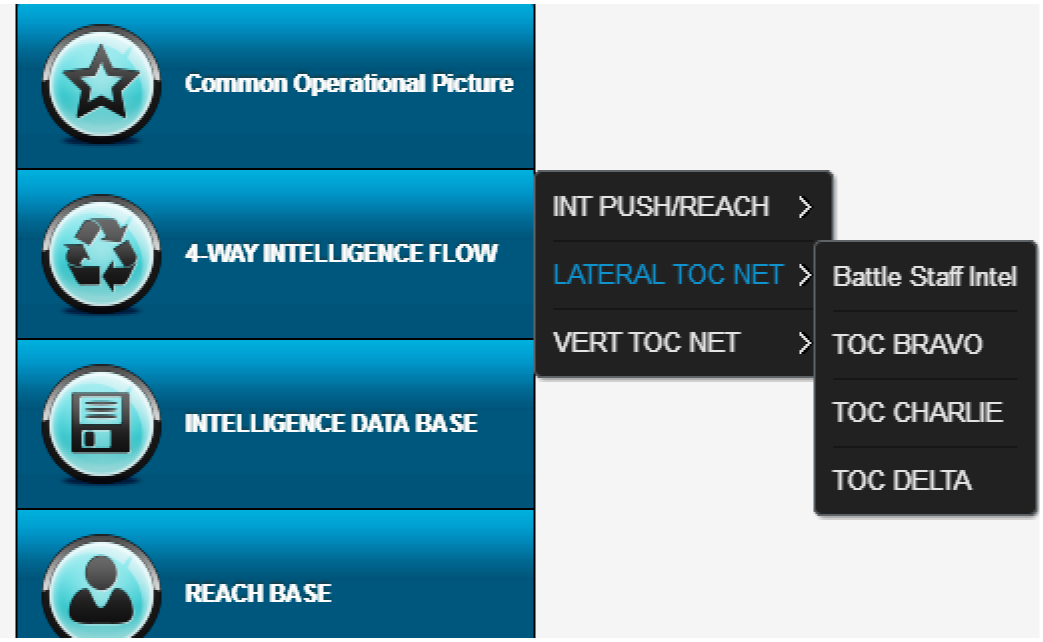
Staff and the Commander should be able to grasp the immediate current situation as simply as possible without the presentation getting inundated with information overflow.This common operating picture viewed explicitly and concretely enables the Commander to take swift decisions in an otherwise fast evolving uncertain battle environment.It is not possible for the Staff to accomplish this by themselves and the standard office personnel who assist them (in the Tactical Ops Center)..what is required that the battle staff from among the JCOs,Senior NCO and NCOs assist the Staff Officers in the respective warfighting functions , viz: intelligence and CI;maneuver;sustainment;command,control,communication and computers C4;plans;fires;protection;engineer and provost marshall functions.The main objective is to acquire the best situational understanding about the common operating picture within the tactical operations center/command post. . The TOC/CP has two primary functions: • To track Soldiers and equipment during the battle to assist the leader in the command and control of the unit. • To serve as a data center that processes enemy and friendly information. The role of the battle staff is a critical component to achieve mission success in a counterinsurgency environment. Battle staff noncommissioned officers (NCOs) perform a multitude of vitally important roles and functions in the tactical operations centers and command posts. They are the principal managers of battle tracking, which supports the timely analysis and processing of plans and orders, and they continually adapt these plans and orders to counter the threat.

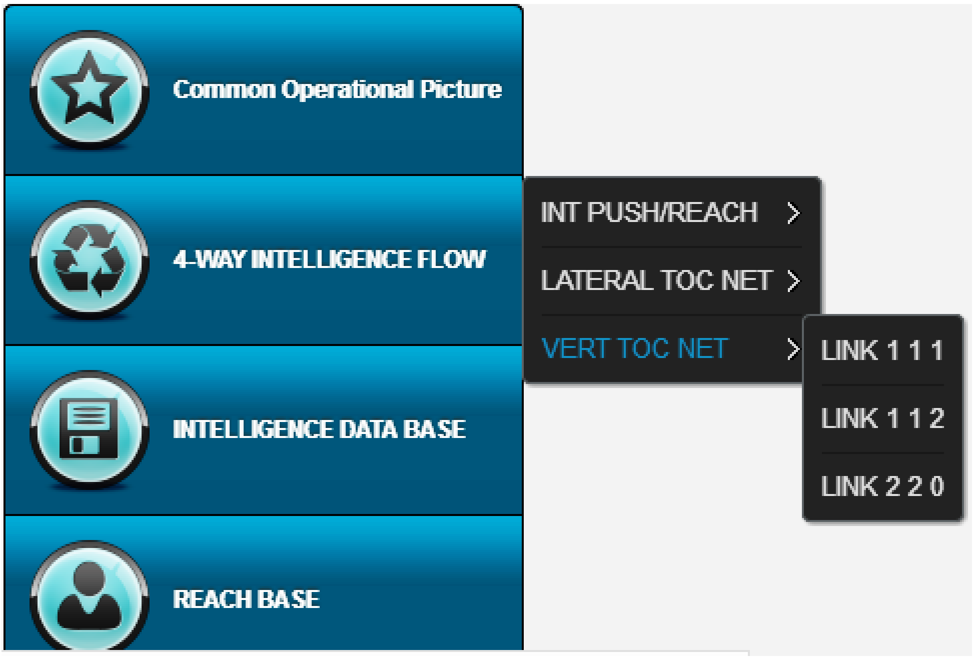
TACTICAL OPERATIONS CENTER
HUMINT/CI

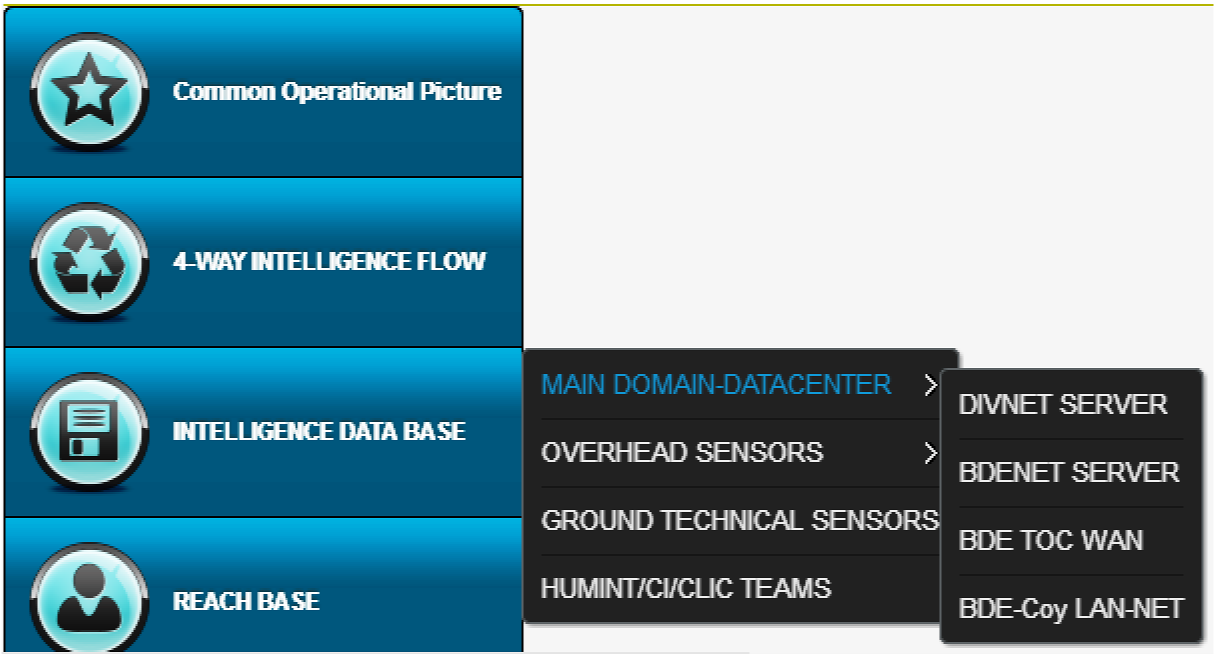


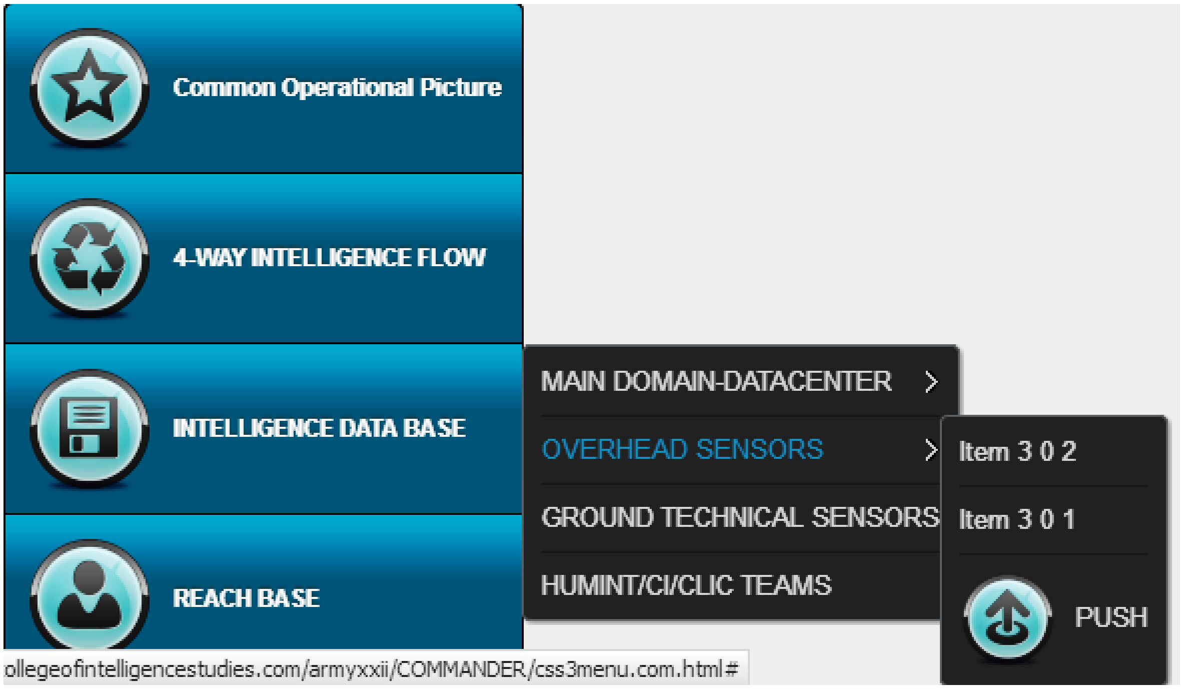
SITUATIONAL AWARENESS—BUT OF THE WRONG ENEMY???

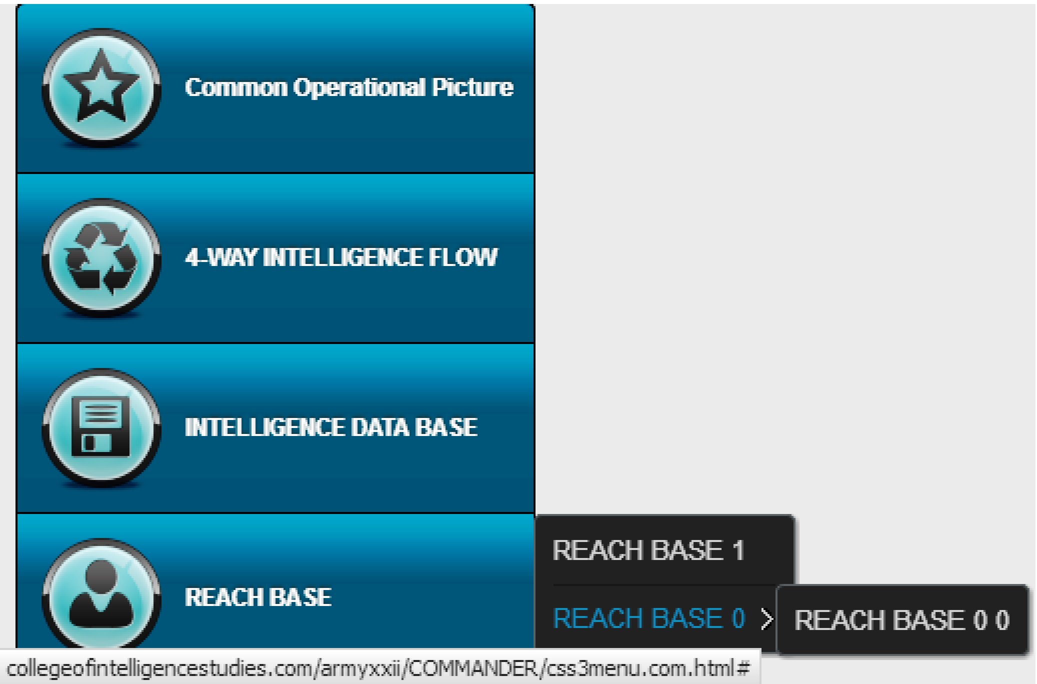

Common Operational Picture
4-WAY INTELLIGENCE FLOW
INTELLIGENCE DATA BASE
REACH BASE
INTELLIGENCE "COMBAT FORCE"
Tactical Operation Center
At a glance Int Products for CDR
Cloud Operations1
Cloud Operations2
INTELLIGENCE PROJECTION


Common Operational Picture
4-WAY INTELLIGENCE FLOW
INTELLIGENCE DATA BASE
REACH BASE
INT PUSH/REACH
LATERAL TOC NET
VERT TOC NET
Battle Staff Intel
TOC BRAVO
TOC CHARLIE
TOC DELTA


Common Operational Picture
4-WAY INTELLIGENCE FLOW
INTELLIGENCE DATA BASE
REACH BASE
INT PUSH/REACH
LATERAL TOC NET
VERT TOC NET
LINK 1 1 1
LINK 1 1 2
LINK 2 2 0


Common Operational Picture
4-WAY INTELLIGENCE FLOW
INTELLIGENCE DATA BASE
REACH BASE
MAIN DOMAIN-DATACENTER
OVERHEAD SENSORS
GROUND TECHNICAL SENSORS
HUMINT/CI/CLIC TEAMS
DIVNET SERVER
BDENET SERVER
BDE TOC WAN
BDE-Coy LAN-NET


Common Operational Picture
4-WAY INTELLIGENCE FLOW
INTELLIGENCE DATA BASE
REACH BASE
MAIN DOMAIN-DATACENTER
OVERHEAD SENSORS
GROUND TECHNICAL SENSORS
HUMINT/CI/CLIC TEAMS
Item 3 0 2
Item 3 0 1
PUSH
ollegeofintelligencestudies.com/armyxxii/COMMANDER/css3menu.com.html#


Common Operational Picture
4-WAY INTELLIGENCE FLOW
INTELLIGENCE DATA BASE
REACH BASE
REACH BASE 1
REACH BASE 0
REACH BASE 0 0
collegeofintelligencestudies.com/armyxxii/COMMANDER/css3menu.com.html#

TACTICAL OPERATIONS CENTER BRAVO

Leave A Message

Live Help Offline

powered by:
Crafty Syntax

TACTICAL OPERATIONS CENTER CHARLIE

Leave A Message

Live Help Offline

powered by:
Crafty Syntax

TACTICAL OPERATIONS CENTER DELTA

BELOW IS THE SCHEMATIC DIAGRAMMING OF THE "AT A GLANCE" PICTURE OF THE INTELLIGENCE SITUATION AT DIV , Bde & Bn levels ; The Intelligence Preparation of the Battlefield Report; Threat/Vulnerability Assessments;the Force Protection Intel and FPCON Reports , the Intelligence Products brief ; the insurgent IED/Attack profiles ; the Deconfliction Reports and After Action Reviews. (Soon I will fill in example-case-study data)

COP MAIN

COMMON REPRESENTATION - ALL ECHELONS

COP	CDR PIRs	RM&CM BRIEF	IPB	TOC NET ▽	FP INTEL
REDTEAMING-ANALYSIS ▽					

INT PRODUCTS

INTSUM	INT ESTIMATE	SITREP	CI ESTIMATE	OSINTREP	PSYOPSREP

PROFILES

IED PROFILES	ATTACK PROFILES

DECONFLICREP
AFTER ACTION REVIEW

<<For meaning of above terms please go here >>

TERMS USED IN THE PAGE:

COP
Common Operational Picture

CDR
Commander

CDR PIRS
Commanders Prioritized Intelligence Requirements
or
Priority Intelligence Requirements

RM
Requirements Management

CM BRIEF
Collection Management Brief

IPB
Intelligence Preparation of the Battlefield (This gives rise a a number of intelligence products , mainly intelligence estimate , threat estimate)

TOC NET
TOC1/TOC2/TOC3/TOC4
Tactical Ops Center NET.Each TOC caters to intelligence/information inputs from several Coy Int Platoons , all these TOCs networked digitally/radio-telephony to form the TOC NET.Heightens considerably the situational awareness of the Cdr's and situational development of ther Bde Cdr.

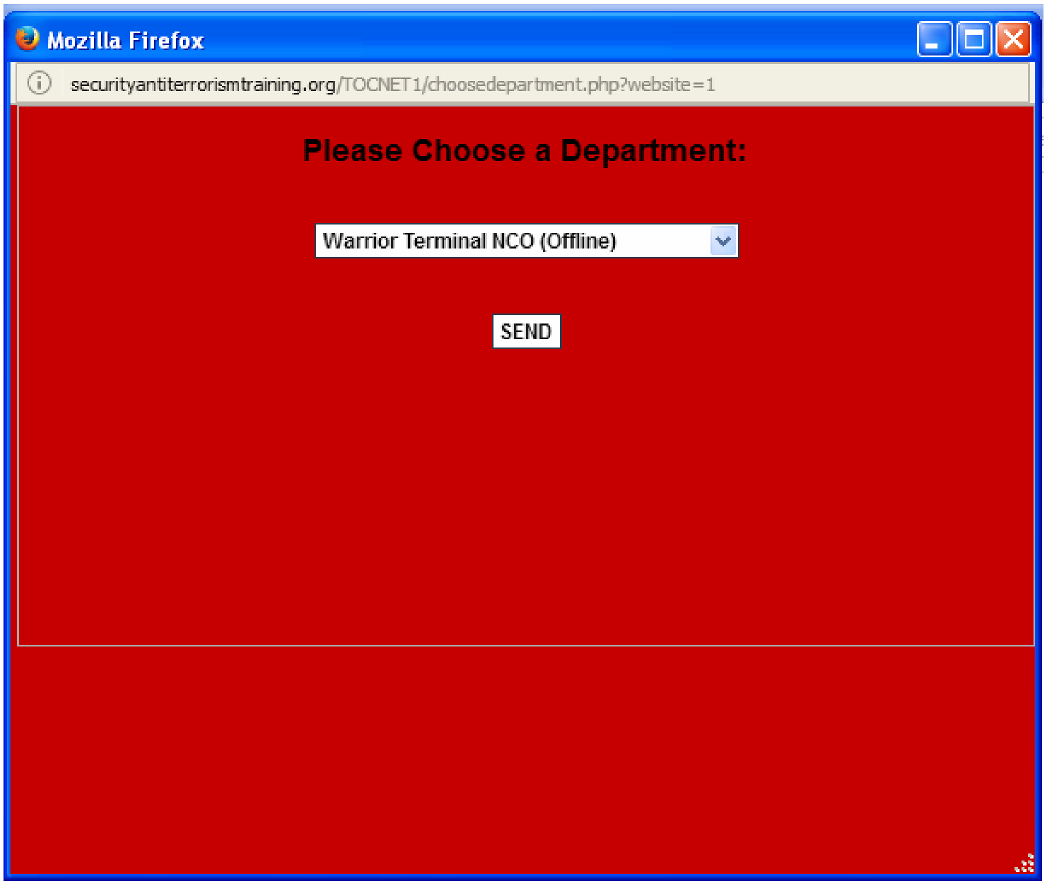
FP INTEL
Force Protection Intelligence.As different from Combat intelligence or any other mission-specific intelligence.

RED TEAMING ANALYSIS:
1.FP INTEL
2.FPCON - Force Protection Conditions (Warning Levels)
3.Vul Assessment - Vulnerability Assessment
4.Threat Assessment - TA
5.Intcaplysis - Intelligence Systems can be subjected to analysis by mission , capability , and Cdr Need.
6.R&S Brief - Reconnaissance & Surveillance Brief

INT PRODUCTS:
1.INTSUM - Intelligence Summary
2.INT ESTIMATE - Intelligence Estimate
3.SITREP - Situation Report
4.CI ESTIMATE - Counterintelligence Estimate
5.OSINTREP - Opensource Intelligence Report
6.PSYOPSREP - Psychological Ops Report

PROFILES:
1.IED PROFILES Improvised Explosive Devices Profile (frequency of blasts , common locations , which areas are never subjected to attacks , community profiling of those areas , types of IED , methods of delivery etc all plotted/calculated against other factors over a fixed time duration usually past 3 years)
2.ATTACK PROFILES - Same as above but now focussing specifically on attacks.

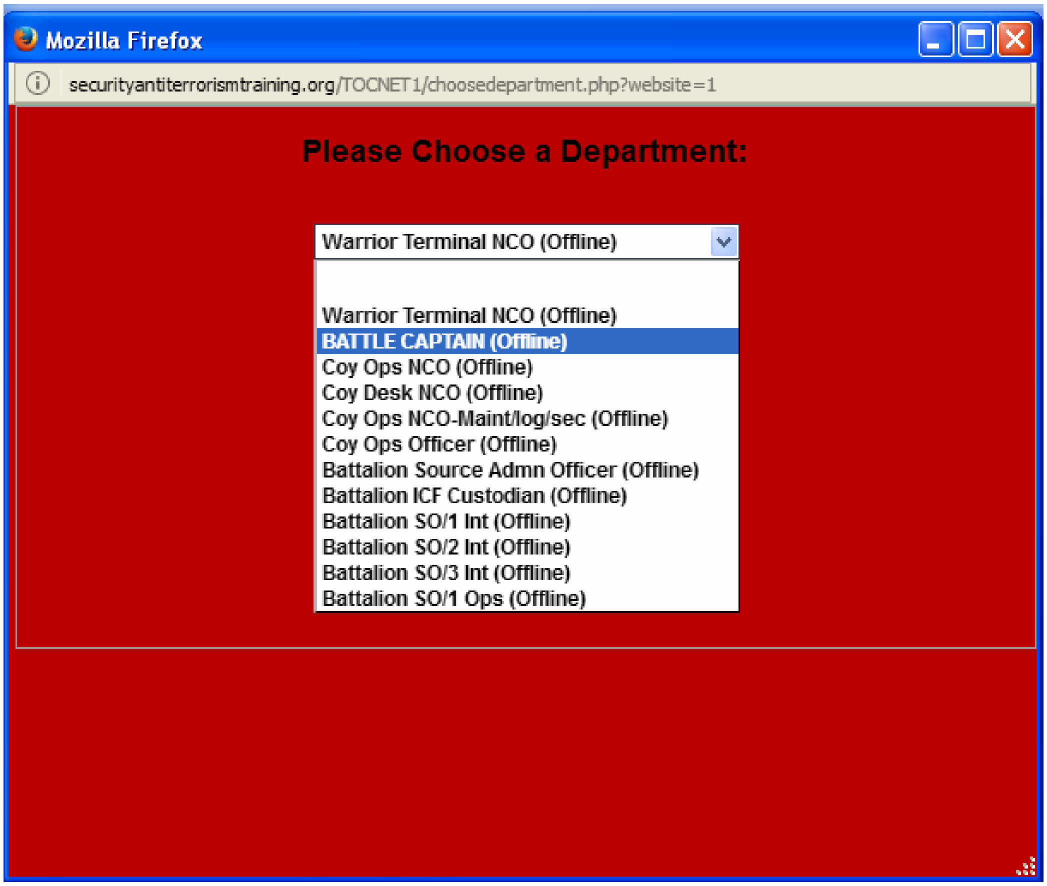
DECONFLICREP - Int Asset Deconfliction Reports (Deconflicting HUMINT and CI teams or R&S teams , Source Management by deconfliction)
AFTER ACTION REVIEW - After Action Review.



Mozilla Firefox
securityantiterrorismtraining.org/TOCNET1/choosedepartment.php?website=1

Please Choose a Department:

Warrior Terminal NCO (Offline)


Mozilla Firefox
securityantiterrorismtraining.org/TOCNET1/choosedepartment.php?website=1

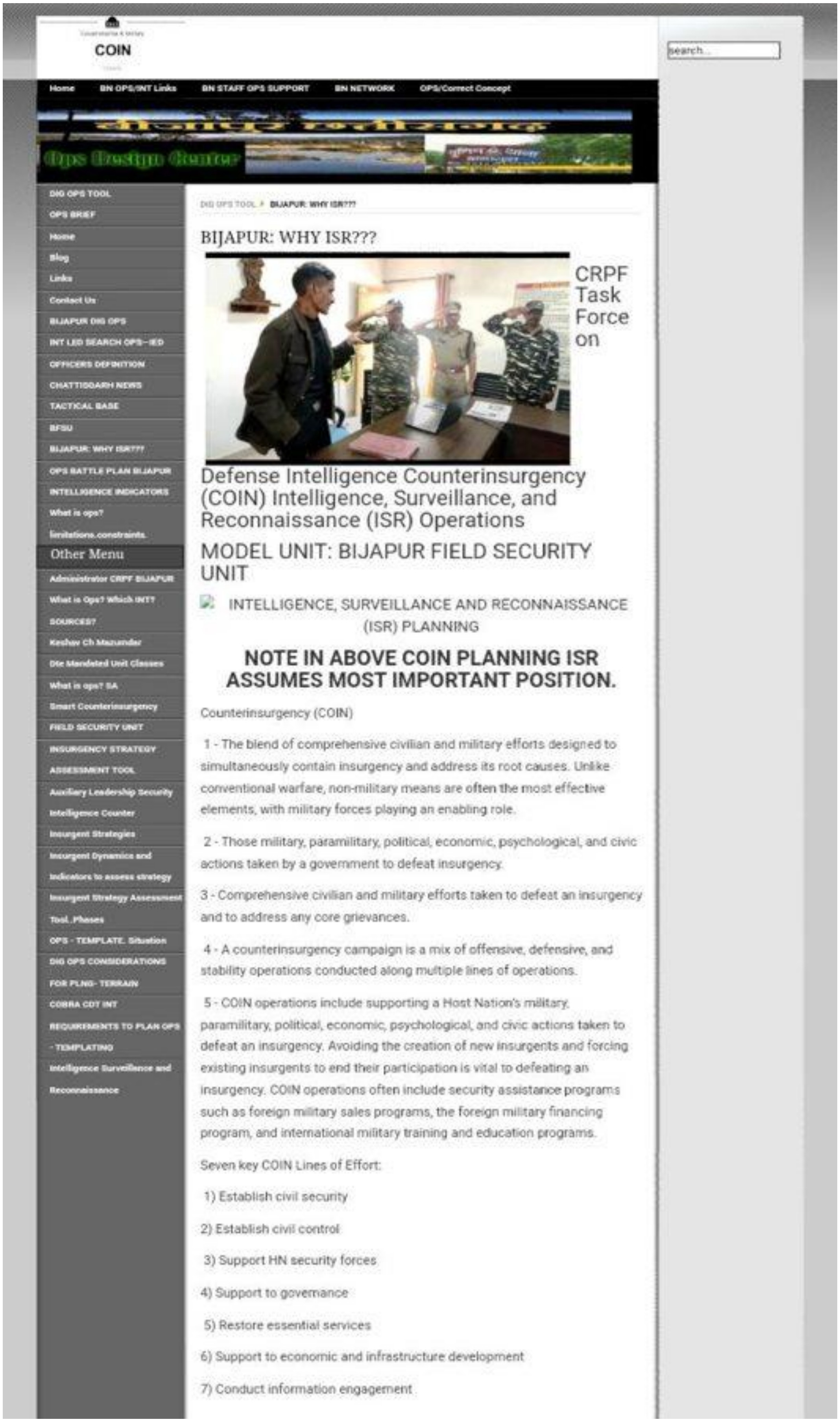
Please Choose a Department:

Warrior Terminal NCO (Offline)

- Warrior Terminal NCO (Offline)
- BATTLE CAPTAIN (Offline)
- Coy Ops NCO (Offline)
- Coy Desk NCO (Offline)
- Coy Ops NCO-Maint/log/sec (Offline)
- Coy Ops Officer (Offline)
- Battalion Source Admn Officer (Offline)
- Battalion ICF Custodian (Offline)
- Battalion SO/1 Int (Offline)
- Battalion SO/2 Int (Offline)
- Battalion SO/3 Int (Offline)
- Battalion SO/1 Ops (Offline)

Please use Cntrl+click on links below to get complete picture.

Ops Planning Bijapur



BIJAPUR: WHY ISR???

CRPF Task Force on

Defense Intelligence Counterinsurgency (COIN) Intelligence, Surveillance, and Reconnaissance (ISR) Operations

MODEL UNIT: BIJAPUR FIELD SECURITY UNIT

INTELLIGENCE, SURVEILLANCE AND RECONNAISSANCE (ISR) PLANNING

NOTE IN ABOVE COIN PLANNING ISR ASSUMES MOST IMPORTANT POSITION.

Counterinsurgency (COIN)

1 - The blend of comprehensive civilian and military efforts designed to simultaneously contain insurgency and address its root causes. Unlike conventional warfare, non-military means are often the most effective elements, with military forces playing an enabling role.

2 - Those military, paramilitary, political, economic, psychological, and civic actions taken by a government to defeat insurgency.

3 - Comprehensive civilian and military efforts taken to defeat an insurgency and to address any core grievances.

4 - A counterinsurgency campaign is a mix of offensive, defensive, and stability operations conducted along multiple lines of operations.

5 - COIN operations include supporting a Host Nation's military, paramilitary, political, economic, psychological, and civic actions taken to defeat an insurgency. Avoiding the creation of new insurgents and forcing existing insurgents to end their participation is vital to defeating an insurgency. COIN operations often include security assistance programs such as foreign military sales programs, the foreign military financing program, and international military training and education programs.

Seven key COIN Lines of Effort:

1) Establish civil security

2) Establish civil control

3) Support HN security forces

4) Support to governance

5) Restore essential services

6) Support to economic and infrastructure development

7) Conduct information engagement

Go here

GENERAL

4-1. The successful conduct of counterinsurgency operations relies on the willing support and cooperation of the populations directly involved. Greater priority and awareness is needed to understand the motivations of the parties involved in the conflict and the population as a whole. The understanding of the background and development of the conflict into which Indian Forces are intervening is of particular significance. This requires a detailed understanding of the cultural environment and the human terrain in which the Indian Forces will be operating and thereby places a heavy reliance on the use of HUMINT.

4-2. The commander requires intelligence about the enemy and the AO prior to engaging in operations. Intelligence assists commanders in visualizing their battlespace, knowing the enemy, organizing their forces, and controlling operations to achieve the desired tactical objectives or end state. Intelligence supports force protection by alerting the commander to emerging threats and assisting in security operations. Intelligence to support counterinsurgency operations focuses on three areas:

- **Factors motivating the insurgency.**
- **Appeal the insurgency holds for insurgents.**
- **Organization, leadership, and key functionaries of the insurgency.**

4-3. "Open-source intelligence" refers to the practice of drawing information from the news media and processing it into intelligence. It is an increasingly common practice among world intelligence organizations. The six categories of media and news sources providing opensource intelligence are--

- **Newspapers.**
- **Periodicals.**
- **Military and other professional journals.**
- **Internet web logs (commonly called "blogs."**
- **Visual media (primarily television).**
- **Radio.**

4-4. Units engaged in counterinsurgency operations may face multiple threats. The commander must understand how enemies organize, equip, train, employ, and control their forces. Intelligence provides an understanding of the enemy, which assists in planning, preparing, and executing operations. Commanders must also understand their operational environment and its effects on both their own and enemy operations. The commander receives mission-oriented intelligence on enemy forces and the AO from the G-2/S-2. The G-2/S-2 depends upon the intelligence, surveillance, and reconnaissance (ISR) effort to collect and provide information on the enemy and AO.

4-5. One of the most significant contributions that intelligence can accomplish is to accurately predict future enemy events. Although a difficult task, predictive intelligence enables the commander and staff to anticipate key enemy events or actions and develop corresponding plans or counteractions. The most important purpose of intelligence is to enable decision making. Commanders receive the intelligence, understand it (because it is tailored to the commander's requirements), and act on it. Through this doctrinal concept, intelligence drives operations. 4-6. The AO during counterinsurgency operations includes three primary components: physical terrain and weather, society (socio-cultural, often referred to as the human terrain), and infrastructure. These components provide a structure for intelligence personnel to focus and organize to provide support to counterinsurgency operations. These entities are interdependent, not separate. These components enable the commanders to gain an in-depth understanding of their AO during counterinsurgency operations and provide a focus for the intelligence analyst.

INTELLIGENCE PREPARATION OF THE BATTLEFIELD PLANNING CONSIDERATIONS

4-7. IPB includes information about terrain and weather and civil considerations as well as the enemy. (The six factors of METT-TC--mission, enemy, terrain and weather, troops and support available, time available, and civil considerations--make up the major subject categories into which relevant information is grouped for military operations. Relevant information is all information of importance to the commander and staff in the exercise of command and control In counterinsurgency operations, civil considerations are prominent in IPB analysis.

TERRAIN AND WEATHER

4-8. Expect terrain in counterinsurgency operations to be complex. Unit AOs may consist of various types of terrain, ranging from jungles, mountains, and deserts to rural or urbanized areas. In conventional operations, the primary factor is the natural landscape. In counterinsurgency operations, man-made factors may be the primary terrain factors that a unit must consider. Some of these factors that ought to be considered are the density of construction and population within the AO, the street patterns within urban areas, and compartmentalization of areas within the AO (such as areas separated by waterways or highways) and functional zones for example, the functions different areas serve within the AO, such as residential, commercial, and government areas).

4-9. In addition to weather effects on friendly operations, counterinsurgency operations require the consideration of how weather effects the local population. For example, an ongoing drought within the unit's AO may mean that more outside aid is required. An insurgency movement may take advantage of the population's potential dissatisfaction to recruit support and may even be able to make food or other desirable aid available, thus making the insurgents look like the only competent/legitimate authorities in the region. If the government does not provide necessary aid, the population could view those they believe to be in charge in an increasingly hostile manner for failing to help prevent a disaster.

CIVIL CONSIDERATIONS

4-10. Civil considerations comprise the manmade infrastructure, civilian institutions, and attitudes and activities of the civilian leaders, populations, and organizations within an area of operations influence the conduct of military operations. They include the population of an area and information about it. Factors of interest include the gender and mix of the populace; the cultural, religious, and socio-economic beliefs and thinking; and the beliefs, attitudes, and actions of groups and individuals.

Population and Culture

4-11. The center of gravity in counterinsurgency operations is the population. Therefore, understanding the local society and gaining its support is critical to success in. For Indian Forces to operate effectively among a local population and gain and maintain their support, it is important to develop a thorough understanding of the society and its culture, to include its history, tribal/family/social structure, values, religions, customs, and needs.

4-12. The history of a people can often help explain why the population behaves the way it does. The roots of an insurgency may become clear through that knowledge. A given AO may have several different regions, each with different sets of customs. Indian Forces can anticipate local reaction to friendly courses of action as well as avoid losing indigenous support for the mission through understanding and supporting those local customs. That support, however, must be consistent with Indian laws and the law of war.

4-13. Understanding and working within the social fabric of a local area is initially the most influential factor in the conduct of counterinsurgency operations. Unfortunately, this is often the factor most neglected by Indian Forces. The density of civilians and the constant interaction required between them and Indian Forces greatly increases the importance of social considerations. The fastest way to damage the credibility of Indian Forces and the legitimacy of our involvement with the local national government is to ignore or violate the social mores or precepts of a particular population.

4-14. The interaction of different cultures demands greater recognition during counterinsurgency operations than in other environments. This greater need for understanding comes from the increased need for interaction with the civilian populace. Every culture has a set of norms and values, and these could involve such diverse areas as protocol and social skills, attitudes toward women, manners, food, sleep patterns, casual and close relationships, and cleanliness. Understanding these differences is only the start of preparation for counterinsurgency operations.

4-15. Religious beliefs and practices are among the most important, yet least understood, aspects of culture. The role religion plays in both culture and individual value systems varies greatly from place to place. While it is never possible to disentangle religion completely from politics, mores, and the other aspects of culture, religion plays an especially powerful and dominant role in some societies. Many conflicts have a strong

religious dimension, not only in the origin of the dispute but also in the way the fight is conducted. Some religiously motivated antagonists will operate with a significantly different view of what constitutes just conduct in war than the western consensus that created the law of land warfare and the Geneva Conventions.

4-16. When assessing events, intelligence professionals consider the norms of the local culture or society. Failure to recognize, respect, understand, and incorporate an understanding of the cultural and religious aspects of the society in which Indian Forces are interacting could rapidly lead to an erosion of the legitimacy of the mission. For example, while bribery is not an accepted norm in our society, it may be a totally acceptable practice in another society. If intelligence professionals assess an incident of this nature using our own societal norms and values as a reference, it is probable the significance of the event will be misinterpreted.

Leaders and Institutions

4-17. military planners should conduct interagency coordination to identify key government officials early in the operation. policy officials determine which key leaders are supportive of the military and which are not. These key personnel can provide valuable information needed for successful completion of the operations, to include local infrastructure, a common picture of cultural norms, suspected enemy strengths, and probable means of support and locations for enemy forces. In counterinsurgency missions, Indian Forces are often supporting a state. As such it is critical to understand the potential audience.

4-18. Many governments are rife with nepotism and trading favors, are indifferent to local conditions, and support no security presence at the village level. The power of officials may be based on family and personal connections, clan loyalty, and age, and only after that on education, training, and competence. Corruption may be pervasive and institutionalized as a practical way to manage excess demand for local services.

4-19. A local government's breakdown from a previous level of effectiveness will quickly exacerbate problems of public health and mobility. Attempts to get the local-level bureaucracy to function along govt lines may produce further breakdown, passive indifference, or resentment. Any unintentional or intentional threat to the privileges of ranking local officials or tribal leaders or to members of their families will be stubbornly resisted. Avoiding such threats and assessing the importance of particular officials requires knowledge of family ties.

4-20. military planners must realize that the local populace will behave in their perceived self-interest. They will be keenly aware of five sets of interests at work: those of the Indian Forces, the insurgent/hostile elements, the local opportunists, the legitimate government, and the general population. All five elements assess these interests constantly in order to ascertain their own stakes, risks, and advantages.

Refugees and Ethnic Groups

4-21. Another significant cultural challenge is the presence of refugees within a unit's AO. Rural immigrants displaced by conflict, combined with city residents, can create a significant problem. Noncombatants and refugees without hostile intent can disrupt local missions. Additionally, there may be insurgent troops, criminal gangs, vigilantes, paramilitary factions, and factions within those factions hiding in the waves of the displaced.

4-22. The enemy knows it is nearly impossible for Indian Forces to accurately identify friend from foe from disinterested. Local combat situations can change with bewildering speed, as the supposed innocent becomes an active aggressor within close quarters and an indefensible position. 4-23. One goal of insurgent forces will be to place stress on the US and local national government soldiers in order to break down discipline and operational integrity. The constant pressure of differentiating friend from foe taxed and sometimes undermined ROE from Belfast to Lebanon, and in some cases, entire missions.

Social Structure and Customs

4-24. Defining the structure of the social hierarchy is often key to understanding the population. Identifying those local personnel in positions of authority is important. These local officials, tribal leaders or village elders are often the critical nodes of the society and influence the actions of the population at large. In many societies nominal titles do not equal power influence does. Many "leaders" are figureheads, and the true authority lies elsewhere.

4-26. Identifying and understanding trends and patterns of activity provide important information for intelligence analysts and mission planners. Every local area has discrete and discernible patterns of daily activity. The time of heaviest activity along a line of communication is one case in point. Trade and business transactions, market sales, religious practices, governmental functions, and criminal activity are other examples of daily behavior than can be analyzed for consistencies. Disruptions or irregularities in these patterns serve as a warning that something is amiss in the area.

4-27. It is important to remember that while certain general patterns do exist, most regional areas are normally composed of a multitude of different peoples, each with its own standards of conduct. Treating the local population as a homogenous entity can lead to false assumptions, cultural misunderstandings, and a poor operational picture. Individuals act independently and in their own best interest, and this will not always coincide with friendly courses of action. Do not ignore the presence or actions of the different population components within an AO when developing assessments.

Infrastructure

4-28. Understanding the infrastructure and the interrelationships of various elements within a unit's AO and the relationship with neighboring AOs is critical in counterinsurgency operations. Infrastructure has physical, social, economic, and political elements.

Physical

4-29. Intelligence staffs identify critical physical infrastructure components (transportation and communications systems, water treatment and waste disposal facilities) and the effects they have on the local, regional, and national populations. Insurgents will use and exploit existing infrastructure. A common method insurgents use to display the weakness of the current local national government is to disrupt or destroy critical components of infrastructure, such as power stations and waterworks, that affect large portions of the local population. They may also create additional infrastructure where gaps in government-provided services exist in order gain the good will of the local population. If successful, this demonstrates the government's inability to protect critical infrastructure components and their inability to provide basic services such as security for the population.

Social, Economic, and Political

4-30. The social infrastructure includes communication, religious, and education centers; and the roles of tribes, families, casts, and clans. Economic infrastructure includes banks, stock markets, and the monetary control system. Political infrastructure includes political parties, party headquarters and offices, government offices, and state institutions.

INTELLIGENCE PREPARATION OF THE BATTLEFIELD ASSESSMENT

4-31. During the military decision making process, intelligence personnel provide commanders with a battlefield assessment based upon a systematic approach known as IPB. IPB consists of four steps:

- **Define the battlefield environment.**
- **Describe the battlefield's effects.**
- **Evaluate the threat.**
- **Determine threat courses of action.**

DEFINE THE BATTLEFIELD ENVIRONMENT

4-32. In defining a counterinsurgency environment, intelligence professionals do the following:

- **Consider the nature and strategy of the insurgency.**
- **Are there internal factors, external factor, or both that form a basis for the insurgency?**
- **Is there an identifiable pattern of insurgent activities?**
- **Does the insurgent organization function primarily within the established political system or in open competition with it?**
- **Determine international and national support to the insurgents. Include sources of moral, physical, and financial support.**
- **Consider the neighboring countries, boundaries and frontiers, and coastal waterways.**
- **Consider third-country support for the insurgency.**
- **Analyze the population, government, military, demographics, and threat.**
- **Who are the vulnerable elements in the population?**

- **Are they subject to insurgent exploitation?**
- **Evaluate political structure, economy, foreign policy and relations, and policies on military use.**
- **Consider if military presence, or potential presence, by itself could be a catalyst for insurgent activity.**

DESCRIBE THE BATTLEFIELD'S EFFECTS (TERRAIN AND HUMAN)

4-33. In defining the battlefield's effects in a counterinsurgency environment, intelligence professionals do the following:

- **Determine points of entry, infiltration and exfiltration routes, C2 structures for operations, and agricultural areas.**
- **Evaluate weather's effects on the mobility of insurgents and their logistic efforts, for example, the availability of food supply due to weather extremes.**
- **Consider migration and settlement patterns to identify which areas are progovernment or proinsurgent. Identify the locations of groups that create territorial boundaries the insurgents may try to make autonomous to gain political advantage.**
- **Determine how political and religious affiliation and practices influence the people's attitudes towards both enemy and friendly operations.**
- **Examine efforts to create or increase unrest and dissension among the population. Are the insurgents conducting IO against existing or proposed policies and programs?**
- **Evaluate how economics and money affect the insurgents' ability to conduct offensive operations. They will influence the populace's active support for or against the insurgency.**

EVALUATE THE THREAT

4-34. In evaluating the threat in a counterinsurgency environment, intelligence professionals do the following:

- **Identify which insurgent groups are present, thought to be present, or have access to your AO.**
- **Is the insurgency linked to a racial, religious, ethnic, or regional base?**
- **Does the insurgent organization function through predominately legal means or clandestine operations?**
- **What and who constitute the organizational elements of the movement?**
- **Identify leaders, trainers, recruiters, staff members, and logistics personnel.**
- **Is the leadership clearly defined or do competing actions exist?**
- **Is the insurgency affiliated with any political, labor, student, or social organization?**
- **What is the philosophy of the leadership?**
- **Develop doctrinal templates based on observed operating procedures.**
- **Assess and analyze the number of functional specialties within the insurgency. For example, the number of trainers for a specific weapon might indicate the type of tactics, level of readiness, and the number of personnel trained.**
- **Determine the types of weapons that the insurgents have at their disposal. Sophisticated weaponry may be an indicator of external support as well as the insurgents' capability to attack important and possibly well-defended targets.**

- Consider the insurgent organization.
- Does it have a high degree of command and control?
- What is the level of planning and training within the organization?
- Analyze movement patterns. Movements may coincide with operational or logistic activities.

DETERMINE ENEMY COURSES OF ACTION

4-35. Enemy courses of action might include the following:

- Attacks and raids on police stations, security forces, military installations, or other government and security-related facilities.
- Attacks on public utility installations (power, water, telephone) or other forms of economic sabotage (pipelines, transmission towers, ports, marketplaces).
- Kidnapping, murder, or intimidation of public officials (and their families or family members) supporting Indian forces.
- Propaganda directed against the populace or local economic leaders (such as shopkeepers and business owners).
- Ambushes of friendly convoys; kidnapping of drivers and insurgent demands.
- Attacks on the population.

4-36. Evaluate the most vulnerable locations and facilities that can quickly affect the greatest number of the populace--such as power plants; transmission lines; road, rail and water networks; and local open-air markets--to determine the most likely locations for potential insurgent attacks, sabotage, raids, and roadblocks--most likely insurgent course of action.

4-37. Use trend and pattern analysis to template, predict, and prioritize insurgent activity to include

- Movement around potential objectives, such as infiltration or exfiltration routes.
- Assembly points, rally points, and staging areas.
- Surveillance positions.
- Centers of proinsurgent populations. Include an evaluation of individual villages and large political divisions, such as states and provinces.
- Areas of antigovernment influence and residences of insurgent leadership or key sympathizers.
- Location of known and suspected base camps.
- Location of known and suspected training camps.
- Logistic routes and transshipment hubs.
- Cache sites, water sources, agricultural areas, and fuel storage and production areas.
- Locations of communications equipment. Include commercial establishments and government installations where such equipment may be purchased or stolen.
- Potential ambush sites.

THE THREAT

4-38. Insurgents require the support of the local population. That support can be either active or passive. In order to succeed, they must increase the support of the local population in their favor. To defeat the insurgency, Indian Forces assist the local authorities in separating the insurgents from the population and ultimately in gaining the population's active support. If a substantial portion of the population does not actively oppose the insurgency, the insurgents may determine to attack soft targets and purposely inflict civilian casualties to both intimidate the local populace and undermine the legitimacy of local authorities.

4-39. Rarely are only two sides involved in modern conflicts. More often, one ethnonational group opposes other groups with conflicting interests. This poses a significantly more complex set of enemy or potential adversaries--entities that leaders must understand. Insurgents try to create conditions to defeat US and HN forces and to slow the support for friendly forces. Increasingly, insurgent groups have no regard for the law of war. They have used human shields, targeted innocent civilians, and occupied religious and health facilities as sanctuaries. These actions and techniques offset Army advantages and make it more difficult to locate and defeat the enemy. Army reaction to these tactics can also have tremendous propaganda appeal.

4-40. Insurgents develop organizational structures that are functional for their particular operational environment. Because insurgents usually operate in a hostile environment, security is a primary consideration. Therefore, insurgent organizations may be organized both conventionally and unconventionally.

4-41. An unconventional or cellular structure protects members of the organization and allows for better security. Individual elements or cells can operate relatively isolated from other elements or cells, thereby creating increased security. In the event of defection or capture, no one member can identify more than a few others. Some elements within the organization may have multifunction cells that combine several skills into one operational entity, while others create cells of specialists that come together for an operation on an ad hoc basis.

4-42. Due to its unconventional nature, the insurgent threat is difficult to determine and identify. When determining and identifying the insurgent threat, consider the following:

- **Threat staging area. A threat staging area is a geographic area from which insurgent organizations and elements coordinate operations, logistics, finance, and recruiting, as well as stage and plan missions. These areas can be thought of as either the operational or strategic areas in which the group conducts the majority of its "behind-the-scenes" activity, as well as defining the area in which the group has the largest sympathetic base to support its goals.**
- **Threat area of operations. Threat AOs are those areas in which an insurgent organization conducts operations against its enemy.**
- **Threat objectives. These are long- and short-term insurgent goals that may include but are not limited to --**

- **Attracting publicity to the group's cause.**
- **Demonstrating the group's power.**
- **Demonstrating government and Army weakness.**
- **Exacting revenge.**
- **Obtaining logistic support.**
- **Causing a government or Indian Forces to overreact.**

THREAT ANALYSIS

4-44. In counterinsurgency operations, threat analysis is a continual process of compiling and examining all available information concerning potential insurgent activities that target elements of the population, local security forces, and facilities or bases. A comprehensive threat analysis reviews the factors of an insurgent's existence, capability, intentions, history, and targeting, as well as the security environment within which friendly forces operate. Threat analysis is an essential step in identifying the probability of insurgent attacks and results in a threat assessment.

4-45. When conducting an insurgency, the threat will normally conform to the five lowintensity imperatives (political dominance, unity of effort, adaptability, legitimacy, and perseverance). Under the conditions of insurgency, the analyst places more emphasis on --

- **Developing population status overlays showing potential hostile areas.**
- **Developing an understanding of how each insurgent organization operates and is organized.**
- **Determining primary operating or staging areas.**
- **Determining mobility corridors and escape routes.**
- **Determining the most likely targets.**
- **Determining where the threat's logistic facilities are located and how their support organizations operate.**
- **Determining the level of popular support (active and passive).**
- **Determining the recruiting techniques and methods of each insurgent organization.**
- **Locating neutrals and those actively opposing these organizations. Using pattern analysis and other tools to establish links between each insurgent organization and other organizations.**
- **Determining the underlying social, political, ideological, and economic issues that caused the insurgency and that are continuing to cause the members of the organization as well as elements of the population to support it.**

4-46. As discussed earlier, evaluation of the threat in counterinsurgency operations begins early and covers a wide range of factors in building an accurate threat organizational diagram. In addition to the factors discussed, consider the following:

- **Group collection and intelligence capabilities.**
- **Does the actual desired end state differ from that which is publicly advocated? If so, how does that impact operations?**

- **Do the insurgents desire a different social or political organization than that which exists under current conditions; if so, what are the differences? How will they conduct operations to achieve that goal?**

4-47. Motivation (ideological, religious, monetary). Depending on the echelon, there may be an opportunity to use PSYOP against the group or its support network.

INSURGENT MEANS AND METHODS OF COMMAND AND CONTROL

4-48. While identifying the specific structure, leadership, and membership of insurgent organizations is important, it may also be extremely difficult to obtain this information. In the absence of specific information, identifying generalities about the insurgent groups will be of value to the intelligence analyst.

Leader Capabilities

4-49. An insurgent organization capable of exercising C2 over long distances has greater flexibility and reach than an organization that can only operate within the limitations of the leader's interpersonal capabilities.

International and National Support

4-50. Insurgents may receive support from the following sources:

- **Moral. A significant leadership or cultural figure may make pronouncements in support of an organization, activity, or action. This may have the effect of influencing international policy or increasing the success of recruitment efforts.**
- **Physical. Physical support includes safe passage, safe houses, documentation, weapons, and training at sites inside the country.**
- **Financial. Charities, banks, informal transfer of currency by traveler or courier.**
- **Transportation.**
- **Religious, political, and ethnic affiliations. Commonalities and differences are significant in terms of estimating potential support or opposition an insurgent organization may receive in a given area. However, in some cultures, such as the Muslim culture, the philosophy that "the enemy of my enemy is my friend" may cause strange and unprecedented relationships to form.**

RECRUITING METHODS, LOCATIONS, AND TARGET AUDIENCE

4-51. An insurgent organization that recruits from an idealistic and naïve upper and middle class will differ significantly from one that recruits from prisons. Some insurgent organizations recruit university students, either to join the movement as operatives and support personnel, or to prepare for future leadership roles. Insurgents recruit lower-level personnel with little or no education because they are more susceptible to insurgent propaganda, although many insurgents come from an upper-middle class background. The impact of target audiences bears directly upon the willingness of the insurgent recruit to fully commit to the cause and to sacrifice self if deemed necessary.

CIVIL CONSIDERATIONS

4-52. A thorough analysis of the population within the AO is critical to the execution of successful counterinsurgency operations. Consider the impact the local populace may have on the threat and friendly forces, as well as their location in the AO and area of interest. When analyzing the population, the following are areas to consider:

- **Identify active and passive supporters and why they are supporting.**
- **Determine what segment of the general population supports or assists the threat and how.**
- **Determine the extent to which the population will support or impede friendly operations.**
- **Identify and depict those segments of the population that are friendly or unfriendly toward counterinsurgent forces.**
- **Identify and depict those segments of the population that are pro-government or anti-government.**
- **Identify terrorist and/or criminal elements and their relationship to the insurgents and the general population.**
- **Determine the availability of weapons to the general population.**

4-53. Insurgents move among the local population the way conventional forces move over terrain. The military aspects of terrain may be used to analyze how insurgents might use this "human terrain" to accomplish their objectives.

Observation and Fields of Fire

4-54. Individuals or groups in the population can be co-opted by one side or another to perform a surveillance or reconnaissance function, performing as moving outposts to gather information.

4-55. Local residents have intimate knowledge of the local area. Their observations can provide information and insights about what might otherwise remain a mystery. For instance, residents often know about shortcuts through town. They might also be able to observe and report on a demonstration or meeting that occurs in their area.

4-56. Unarmed combatants might provide targeting intelligence to armed combatants engaged in a confrontation. This was readily apparent in Mogadishu, where unarmed combatants with the ability to observe friendly force activities without the threat of being engaged instructed hidden threat forces on where to fire.

4-57. Deception and adversarial propaganda threats may hinder a clear view of the threat's tactics or intentions.

4-58. Fields of fire can be extremely limited by the presence of noncombatants in a combat zone because restrictive ROE may prohibit firing into a crowd.

4-59. Figuratively, the population or regions within a local area can be identified as nonlethal targets for IO.

Avenues of Approach

4-60. Populations present during operations physically restrict movement and maneuver by limiting or changing the width of avenues of approach.

4-61. People may assist movement if a group can be used as human barriers between one combatant group and another. Refugee flows, for example, can provide a concealed avenue of approach for members of an enemy force.

4-62. A certain individual can provide an avenue of approach to a specific target audience when acting as a "mouthpiece" for an IO mission.

Key Terrain

4-63. The population in counterinsurgency operations is key terrain. This is based on the idea that public opinion and their support or lack thereof can change the course or the aims of a mission. Determining which population or portions of it are key to a mission should not be limited to broad-brush characterizations of large populations, however. 4-64. Captured combatants or a well-informed noncombatant can provide valuable information about the enemy. These individuals can be key terrain in terms of the information they can provide

4-65. A group of people that Indian Forces are deployed to protect might be considered key terrain because loss of that group's respect could jeopardize the entire operation.

4-66. Congregated people can be considered key terrain. Whether moving or stationary, a large gathering might be a ripe target for attack, closer observation, or attempts at manipulation.

Obstacles

4-67. One of the largest obstacles to friendly operations is the portion of the population that actively supports the insurgent.

4-68. People conducting their daily activities will often "get in the way" of any type of operation. For instance, curiosity-driven crowds in Haiti often affected patrols by inadvertently forcing units into the middle of the street and pushing them into a single file. No harm was inflicted, but the unit was made move vulnerable to sniper and grenade attacks.

Cover and Concealment

4-70. Civilian populations provide ubiquitous concealment for nonuniformed forces. Threat forces operating in any part of a local urban area can instantly blend into any type of crowd or activity.

4-71. Threat forces often find cover by operating within a neutral group. For instance, al Qaeda operatives and fighters are able to often move freely among and mix with the

rural populace living near Afghanistan-Pakistan border. However, these same people have difficulty remaining nondescript and moving freely among urban populations due to regional differences in their accent, mode of dress, hair and beard styles, and skin pigment. Reportedly, insurgents attempted to move in the company of women and children (acting as family members) and mixed among the populace exiting and entering Fallujah during operations there in spring 2004.

TYPES OF INTELLIGENCE SUPPORT

HUMAN INTELLIGENCE

4-72. Human intelligence is the collection by a trained HUMINT collector of foreign information from people and multimedia to identify elements, intentions, composition, strength, dispositions, tactics, equipment, personnel, and capabilities. It uses human sources and a variety of collection methods, both passively and actively, to gather information to satisfy the commander's intelligence requirements and cross-cue other intelligence disciplines (FM 2-0).

4-73. During counterinsurgency operations, the most important information and intelligence will come from the population and those in direct contact with them--HUMINT. The quantity and quality of this information and intelligence will depend on the credibility of the Indian Forces, the continuous security they provide the local population, and their ability to interact with the local population (communicate and establish relationships with members of the local population). Every member of the Indian force, whether on or off duty, is an informal HUMINT collector and must be aware of the overall intelligence requirements and how their interactions and observations may assist in the intelligence collection plan. This awareness can and should be developed by regular briefings and debriefings.

4-74. Trained HUMINT collectors obtain information from people and multimedia to identify elements, intentions, composition, strength, dispositions, tactics, equipment, personnel, and capabilities within and affecting the local area. HUMINT can assist to establish and more accurately understand the sociocultural characteristics of the local area.

4-75. HUMINT sources can provide early warning of deep-rooted problems awaiting Indian Forces during counterinsurgency operations. HUMINT collectors can conduct debriefings, screenings, liaison, HUMINT contact operations, document exploitation, interrogations, and tactical questioning in support of the commander's intelligence requirements.

4-76. Information provided by HUMINT can greatly assist the intelligence staff in deducing critical patterns, trends, and networks within the local area. HUMINT collection team personnel provide these types of capabilities in support of tactical forces. The G-2 coordinates these capabilities between the tactical, operational, and strategic levels, and can provide their units with access to pertinent national level HUMINT.

4-77. Intelligence planning staffs must be aware that battlespace cannot generally be defined in geographical terms for purposes of intelligence collection. This is especially important when determining the allocation of HUMINT assets. Concentrations of humans on the battlefield do not necessarily denote a need to concentrate HUMINT assets in those locations. Threat actions outside a unit's AO may be a source of significant events inside a unit's AO. Additionally, information from sources in one AO may impact operations in a distant AO. Creating arbitrary intelligence boundaries can result in a lack of timely fusion of all critical elements of information that may be available.

IMAGERY INTELLIGENCE

4-78. Imagery intelligence is intelligence derived from the exploitation of imagery collected by visual photography, infrared, lasers, multispectral sensors, and radar. These sensors produce images of objects optically, electronically, or digitally on film, electronic display devices, or other media.

4-79. IMINT has some severe limitations during counterinsurgency operations. Imaging systems cannot distinguish between insurgents masquerading as civilians and the general population. Additionally, imaging systems cannot see through buildings in built-up areas, so low-flying aerial imagery collection platforms often have restricted fields of vision. Likewise they cannot see threats that may be located inside buildings. Additionally, aerial platforms that do not have standoff capabilities may be at risk of being destroyed by local enemy air defense fire

4-80. There are several key advantages that imagery can provide to the commander. UAV imagery may be one of the fastest, least risky methods by which to conduct reconnaissance of specific areas and to update and verify current maps of that area, showing clear routes, obstacles such as damaged and destroyed buildings, and intact and destroyed bridges. The topographical team can use this imagery to create updated mapping products for planning and operational uses.

4-82. Providing patrols with a digital camera or video camera can greatly assist in the debriefing process and allow the intelligence staff personnel to make their own judgments about items of interest that the patrol reports. Videotaping of events, such as a demonstration, can allow analysts who were not on the scene to identify key elements, leaders, and potential indicators to help preclude future incidents. Gun-camera images from aircraft that can provide a stand-off reconnaissance platform may give valuable insight into enemy TTPs. Thermal sights on a vehicle patrolling an urban street late at night may note the hot engine of a vehicle on the side of the road, possibly indicating suspicious activity.

4-84. The National Geospatial Agency can provide a wide range of imagery products for use prior to and during operations in the urban environment. These products are usually easier to obtain prior to deployment and are often critical to the initial planning stages of an operation.

SIGNALS INTELLIGENCE

4-85. Signals intelligence is a category of intelligence comprising either individually or in combination all communications intelligence, electronic intelligence, and foreign instrumentation signals intelligence, however transmitted; intelligence is derived from communications, electronics, and foreign instrumentation signals. SIGINT has three subcategories:

- **Communications intelligence. The intelligence derived from foreign communications by other than the intended recipients**
- **Electronic intelligence. Technical and geolocation intelligence derived from foreign non-communications electromagnetic radiations emanating from other than nuclear detonations or radioactive sources**
- **Foreign instrumentation signals intelligence. Technical information and intelligence derived from the intercept of foreign electromagnetic emissions associated with the testing and operational deployment of non-US aerospace, surface, and subsurface systems. Foreign instrumentation signals intelligence is a subcategory of signals intelligence. Foreign instrumentation signals include but are not limited to telemetry, beaconry, electronic interrogators, and video data links**

4-86. SIGINT is of value whenever there is any form of electronic emission, whether from communications (such as hand-held or citizen's band radios and mobile phones), combat net radio transmissions, or for other purposes such as the radio control of explosive devices or use of radar for surface-to-air missile guidance. The easy availability of high-tech communications and monitoring equipment now allows most nations to have a relatively sophisticated SIGINT capability.

4-87. Insurgent groups may use unencrypted, low-power, communications systems to conduct local operations. Ground-based SIGINT collection assets must be properly positioned in advance to be certain that they can obtain the best possible intelligence from these sources.

4-88. Collection of unencrypted threat signals can provide key indicators for threat courses of action. Patterns in the amount of known enemy encrypted signals provide indications of specific threat courses of action. Because of signal bounce within urban areas, direction-finding capabilities for all SIGINT collection systems are significantly impaired. During counterinsurgency operations, it may be possible for the local authorities to monitor local telephone lines and provide relevant information they collect to Indian Forces. Likewise, it may be possible for Indian Forces to tip off local national authorities as to what telephone numbers may yield valuable intelligence.

COUNTERINTELLIGENCE

4-91. CI is focused on countering adversary intelligence collection activities against Indian Forces. During counterinsurgency operations, CI personnel primarily investigate adversary intelligence collection threats and provide force protection assistance. In conjunction with HUMINT collections, CI agents conduct screening operations to identify personnel that may be of CI interest or have CI leads. CI screening is also conducted during the process of hiring HN citizens (such as linguists). CI investigations

and operations may cross-cue the other intelligence disciplines and may in term be cross-cued by the other disciplines. CI personnel work in conjunction with military police, engineers, and medical service personnel to create threat vulnerability assessments that provide commanders and leaders with a comprehensive force protection assessment.

4-92. CI personnel provide analysis of the adversary's HUMINT, IMINT, SIGINT, and MASINT capabilities in support of intelligence collection, terrorism, and sabotage in order to develop countermeasures against them. CI analytical products are important tools in course of action development in the military decision making process.

4-93. CI technical services that may be available and of use during counterinsurgency operations include surveillance, computer network operations (assisting in protecting Army information and information systems while exploiting and/or attacking adversary information and information systems), technical surveillance countermeasures (identifying technical collection activities being carried out by adversary intelligence entities), IO, and counter-signals intelligence. As with scouts and reconnaissance patrols, CI teams are most effective when linguist support is provided.

ISR PLANNING IN COUNTERINSURGENCY OPERATIONS

4-94. ISR tasks are the actions of the intelligence collection effort. ISR tasks consist of three categories:

- **Intelligence.**
- **Surveillance.**
- **Reconnaissance.**

4-95. Developing the counterinsurgency operational ISR plan is different from developing the plan supporting conventional operations. Due to the unconventional nature of the counterinsurgency environment, the ISR effort will be significantly more complex in combining and integrating HUMINT collectors and surveillance assets with the capabilities and tasks of limited ISR-assigned assets as well as integrating with interagency resources. Techniques must be modified for every operation to accomplish ISR requirements--each operation is unique. Additionally, local, national, and multinational ISR assets must be integrated into the overall ISR plan at both the local, district, and regional levels.

4-96. The key to successful ISR efforts is the integration of all ISR-capable units, local and HN government and interagency organizations throughout the entire operations process (plan, prepare, execute, and assess). The coordinated actions of the entire staff to develop the threat and environment portion of the common operational picture are key to providing successful ISR support to the commander.

PART 1

TERRORISM

To counter terrorism, the authority must fully understand terrorism. Additionally, he must know the countermeasures that decrease the possibility of a fruitful terrorist assault against establishments, units, and work force.

This part talks about terrorism and endeavors by the administrator to stop the risk of terrorism. It additionally displays measures and precautionary measures that ought to be implemented over the operational continuum. The target should be to prevent a terrorist attack before it happens. This objective can be attained by rendering conditions unfavorable to the terrorist. The success is measured by not having a death toll, or destruction of military gear, material , infrastructure through a demonstration of terrorism.

1-1. DEFINITION

The DOD characterizes terrorism as "the unlawful utilization - or risk - of power or brutality against individuals or property to force or threaten governments or social orders, frequently to accomplish political, religious, or ideological destinations." A terrorist's mode of warfare does’nt complies with principles or laws of fighting. His techniques incorporate prisoner taking, capturing, damage, death, illegal conflagration, deceptions, bombings, assaults, seizures, utilization of NBC weapons, et cetera. Casualties are most often noncombatants, typical persons and places, and political/military figures. Regularly the casualties have no part in either bringing about or adjusting a terrorist's grievance.

1-2. NATURE OF TERRORISM

The utilization of terrorism is not restricted to the early phases of a confrontation. It can and most likely will happen in any level of contention from peace through general war. Terrorist strategies are portrayed as slippery, astonishing, and brief savage activities.

1-3. Regular STRATEGIES AND TACTICS

The regular attack system of the terrorist is to submit demonstrations of savagery. These demonstrations draw the consideration of the individuals, the legislature, and the world to his reason. The media has pivotal influence in this system by giving terrorists worldwide acknowledgment. The peril is that this sort of consideration has a tendency to actuate demonstrations of viciousness by other terrorist groups.

a. Inflicting casualties , sometimes enmasse is the terrorists objective. The objective, or point of convergence, all the more frequently incorporates the overall population, government, military installation/troops or a business area.

b. Some basic strategies terrorists employ incorporate the following:

(1) Bombing. The strategy basic to most terrorist attacks is bombing. Of all terrorist occurrences recorded amid the 1980s, 67 percent came about because of the terrorist bomb. The bomb is a prominent weapon, in light of the fact that its constituent materials are easily available , simple to make, has variable uses, and is hard to recognize and execute follow-up after the incident as terrorists are very adaptive and use newer and newer combinations of chemicals/explosives. The increment in shelling action and the refinement of gadgets utilized brought about the NATO EOD Standardization Committee to order all terrorist bombs to be labeled as improvised explosive devices (IEDs). The term IED is currently utilized by numerous law enforcement offices and also military counter terror and ant terror units. Some IED sub classifications include:

(a) Delivery implies techniques for getting the bomb to the objective.

Vehicle bombs- - booby-caught vehicles, joined gadgets, and auto bombs (autos loaded with explosives).

Laid charges- - bombs set by hand.

‘’Projectile’’ bombs- - bombs tossed by hand or launched by a mortar gadget.

Postal bombs.

Bike bombs.

(b) Activation . Three approaches to actuate an IED.

Initiation - by radio, electric leads, force wire/mechanical strikers.

Activation by the subject/target- - excursion wire, weight gadget, light touchy gadget, electric.

Time delay- - clock, blazing breaker, concoction delay, environmental weight.

(c) Usage. Two general arrangements.

Strategic extemporized hazardous gadgets (IED)- - typically viewed similar to those utilized against a person. These incorporate nail bombs, claymore gadgets, and secret bombs. In fact, any IED can be delegated as a strategic IED.

Key IEDs- - thought to be those utilized unpredictably to increase global concern/fear - for instance, in swarmed strip malls, on airplane, et cetera. They are those bombs intended to strike at society, the legislature, and the present framework.

(d) Hoaxes. Whatever the sort of IED, the terrorist regularly utilizes an opportunity to raise fear. His acknowledgment and to show he is not kidding. When he has once set up a typical mode of attack successfully , he can keep on using psychological techniques like hoax calls so as to upset, however not wreck, the administration and public by well-made and well placed scam bombs. The utilization of tricks with live IEDs can keep security strengths possessed, disturb counterterrorist operations and induce a sense of carelessness by invoking the notion that the next call (which could very well turn out to be a terrorist attack and not a deception) is just another hoax call. Another primary objective of such calls/deception methods is to waste counterterror resources and test the counterterror mechanisms readiness and loopholes.

(2) Arson. Although not a prominent strategy among terrorists, pyromania can pulverize and upset such areas of interest as open utilities, political home office, and, all the more normally, monetary/mechanical targets (shops, industrial facilities, inns). The most well known strategy for beginning an attack is with time-delay flammable gadgets, frequently conveyed in a cigarette bundle or tape holder. These gadgets are anything but difficult to disguise and hard to recognize. Like IEDs flammable gadgets are shoddy and simple to make.

(3) Hijacking. Hijacking and skyjacking were basic amid the 1960s, 1970s, and mid 1980s. Commandeering of vehicles conveying staple sustenance's was a favored strategy of the Supemaros and suited their style of outfitted purposeful publicity. The seizing would be followed by the free dispersion of the vehicle's freight to the poor and destitute alongside terrorist purposeful publicity that publicized the terrorists' reason. In any proceeding with terrorist movement, for example, in Spain or Northern Ireland, the seizing of a vehicle will probably be connected with a future outrage. Case in point, a captured fuel truck may later be used as a 50,000-pound benzine bomb set up with explosives. Likewise, seized "honest to goodness" vehicles give the terrorist a simple intends to pick up passage to a shut military post.

(4) Ambush. Well-arranged ambushes at times are very successful. Ambushes include diversionary tactics and an early warning system of incoming security forces .Insurgent HUMINT elements from within the local sympathetic portion of the population and agents from the ranks of insurgents themselves constitute this EWS. Appropriately practiced, they are executed with accuracy. The terrorist has time on his side and puts in weeks or months TO get ready for an operation and sitting tight for the right opportune moment. The terrorist can pick his own time and spot of operation and, if his expected victim/victims frequently traverse the same route, the terrorist can then carry out sufficient rehearsals and dry runs before the act.

(5) Kidnapping. Not all ambushes are geared towards kinetic killing .The intent to ambush so as to take valuable prisoners who can pave the way for a good ransom is also an option the terrorist seeks. A survey found that 8% of ambushes had this objective as a priority over killing. The victim is kept captive in a secure hideout and the terrorist relays his financial or other demands (release of prominent terrorists , political figures sympathetic to the terrorists cause , a safe passage out of the AO/Country , weaponry etc)via a chain of intermediaries , most often it is not possible to trace the terrorist or hideout due to strict compartmentalization in the intermediary circle. If the intended objective of kidnapping for ransom fails and the security forces close in on the terrorist then the situation degenerates into a case of hostage taking , with both the terrorist and security forces being forced to adopt different tactics than that thought earlier for ransom specific terrorist act.

(6) Hostage taking. The contrast between prisoner taking and taking hostage is negligible. The prisoner taker brazenly affronts the government security machinery and the govt itself and the element of violence to be inflicted on the prisoner coupled with the high desperado nature of the terrorist keeps the security forces and negotiators on the edge during the first quarter of the hostage taking cycle. The terrorist looks for the best payoffs from this transaction and will go to any length including killing his hostages sequentially to achieve his target and also to instill fear so much so that it acts as a deterrent against counter terror operations. The terrorist plays a mind game and his intent is to build up the tension rapidly and seize the opportunity fast before the tempo fizzles out , even after killing the hostages as he is well aware continued negotiations are a ploy on the part of the administration to buy time , test his defenses and set him up. Prisoner taking is another and well known terrorist strategy. By its temperament, prisoner taking pulls in the media; the way that live prisoners are included builds the dramatization of the occasion. The prisoner is in fact a resource means who can aid in getting good concessions for the terrorist , politically or with the intent to cause widespread publicity for the terrorists cause. . In this way, terrorists can apply weight to drive concessions that generally cannot be made. Through

prisoner taking, terrorists can get huge concessions at insignificant expense, in spite of the fact that dangers are included.

(7) Assassination. Assassination is an age old terrorist strategy . Targets are well nominated in advance , their daily routines studied in depth and the timer and place for execution of the act is rehearsed in keeping with the targets movement patterns and other characteristics. The killing is usually attributed to the terrorists group within 24 hours of the act. Targets are regularly unsurprising, and terrorist gatherings claim them after the occasion. Targets include government authorities, corporate administrators, police, military personnel, and security authorities. The targets are carefully chosen so as to impact the morale of the administration and the security forces very adversely and hamper any imminent counter terror operation by removing a lead actor .The elimination of a high profile personality automatically generates widespread publicity by the media and publicity is in fact the primary objective of the terrorist in most of his kinetic attacks.

(8) Other tactics. Whatever strategies terrorists use, they are easy to apply, creates socio-political dynamic ripples, the attack being essentially of the asymmetry type with an hit-and-run arrangement , taking care not to engage the security forces for any duration more than the most minimum required , surprise and speed of the attack are primary factors and all this , as per the terrorists unwritten doctrine , depends a great deal on rehearsals (dry runs) and this is the time that despite the entire operation from being conceived and put to reality , the terrorist surfaces and is vulnerable to security forces HUMINT/CI scanning. Other conceivable strategies incorporate the utilization of chemicals, provocation, surprise kinetic , seizures of chemicals , armaments , even nuclear materials etc.

1-4. Global NETWORK

Terrorist assembles today don't work alone and uninformed of each other. A worldwide system exists that gives extraordinary advantages to the individuals who have paid their "participation expense." It is not proposed that some universal base camp arrangements terrorist acts over the globe. Notwithstanding, it is demonstrated that a sort of universal terrorists' bolster system does exist. The advantages picked up from such a system appear to be unlimited: arms, ammo, cash, knowledge, explosives, safe houses. Most imperative is

the experience and help given in preparing and bolster offices. Alongside the resultant prepared labor, the system develops.

1-5. Classifications OF TERRORIST GROUPS

A terrorist bunch's decision of targets and strategies is likewise an element of the bunch's administration alliance. They are sorted by government connection. This helps security organizers predict terrorist targets, and his modern insight and weaponry. Terrorist gatherings are partitioned into three classes:

a. Nonstate bolstered - a terrorist gather that works self-sufficiently, getting no backing from any legislature.

b. State upheld - a terrorist bunch that works alone however gets support from one or more governments.

c. State coordinated - a terrorist amass that works as an operators of an administration, getting significant knowledge, logistic, and operational backing.

1-6. TERRORIST OBJECTIVES

The prompt target of any terrorist assault ordinarily consents to one or more classifications. The objectives may be either prompt or long range. Terrorists exhibit gathering force, interest reprisal, get logistic bolster, and reason a legislature to go overboard. They are perceived by pressure, intimidation, and incitement. In the meantime, terrorists addition support for themselves or an uprising.

a. Prompt Goals.

(1) Obtain around the world, national, or nearby acknowledgment for their reason.

(2) Force government response, overcompensation, and restraint prompting quick open dispute.

(3) Harass, debilitate, or humiliate government, military, or other security strengths.

(4) Obtain cash or gear.

(5) Show an administration's failure to secure its nationals.

(6) Disrupt or devastate essential method for portability or interchanges.

(7) Demonstrate force or risk validity.

(8) Prevent or deferral choices or enactment.

(9) Cause strikes or work log jams.

(10) Discourage approaching remote speculations or outside government help programs.

(11) Free detainees.

(12) Seek retribution.

b. Long-Range Goals.

(1) Cause emotional changes in government, for example, upset, common war, or war between countries.

(2) Disrupt and dishonor a built up base in backing of an uprising.

(3) Influence nearby, national, or global approach choice making.

(4) Gain political acknowledgment as the lawful body speaking to an ethnic or national gathering.

1-7. TERRORIST TARGETS

Anybody or anything can be an objective or casualty of a terrorist demonstration. Then again, to the terrorist, the military speaks to a wellspring of arms and material and additionally a political or national body. This places the military at incredible danger. The rundown underneath contains some conceivable military focuses of terrorists; it gives a few regions of concern. Targets may change as security is expanded.

Touchy night vision and correspondence things.

Arms.

Ammo.

Order and control offices.

Explosives.

Military officer preparing offices.

Regions pander to individual needs (mess corridors, sleeping enclosure, post trade, supermarket, rec centers, religious exercises, bars, group focuses).

Hydroelectric plants, dams, gas pipelines, atomic office locales.

Correspondence lines/offices, PC offices.

Compound stockpiling locales.

Hardware distribution centers.

Transportation focuses, parking garages, airplane terminals, railheads, transport stops, rail lines, shipyards.

Individuals from military power and their wards.

Key pioneers of the military.

Post workplaces and mail trucks.

PART II

ANTITERRORISM AND COUNTERTERRORISM

Fighting terrorism comprises of two noteworthy classifications. The authority must build up an arrangement that incorporates the parts of antiterrorism and counterterrorism. The arrangement ought to decrease the powerlessness of establishments, units, and faculty amid peacetime, predeployment, organization, and redeployment. It ought to likewise incorporate measures for avoiding, preventing, and reacting to terrorism.

3-8. ANTITERRORISM

Establishments, units, and people utilize antiterrorism measures to diminish the possibility of succumbing to a terrorist demonstration. These measures are viewed as both dynamic and detached, intended to keep a terrorist occurrence. They must include every individual from the military group - military, regular citizen, and relatives. The foundation for this system incorporates gathering and dispersing opportune danger data, directing data mindfulness projects, and actualizing sound guarded measures. Three sorts of efforts to establish safety to consider are physical security, OPSEC, and individual security.

a. Physical Security. Physical efforts to establish safety ensure data, material, and persons, and also counteract criminal acts. In spite of the fact that terrorist exercises are criminal acts, a few distinctions must be considered when giving physical security against terrorists. Terrorists are liable to be more sorted out, better prepared and taught, and more profoundly energetic than different culprits. They are intensely outfitted and refined in their capacity to crush physical efforts to establish safety. To give physical security against terrorists, pioneers must consider the terrorist whose objective may incorporate his own self-annihilation. This is not quite the same as security against different lawbreakers or a traditional adversary. A few activities can help figure out what physical efforts to establish safety are required.

(1) Review wrongdoing counteractive action studies/assessments. These reviews consider the whole establishment and in addition the impact on the encompassing non military personnel area.

(2) Provide photographs of known terrorists to key faculty. These photographs can be acquired through nearby regular citizen and military powers. The photographs can likewise be conspicuously shown in like manner territories so that all work force have admittance to them.

(3) Review physical security overviews/examinations. This review prescribes activity as an aftereffect of on location investigation of boundaries, watchman strengths, interchanges, transportation, possibility bolster, defensive lighting, interruption lighting, interruption recognition framework, and other physical efforts to establish safety. These activities shield establishments from misfortune, burglary, pulverization, damage, or trade off.

(4) Review status of work requests; build up the need of work taking into account risk appraisal.

(5) Determine if the establishment is shut or open. It is shut if ground and water access is restricted by an edge wall, controlled passage focuses, or other physical obstructions. If not, the officer must remunerate by assigning confined zones, giving section control, and keeping up emergency course of actions to secure or close all or some piece of the establishment.

(6) Consider physical security perspectives.

Defensive deterrents and hindrances.

Electro-optical and night vision hardware.

Bomb dangers.

Shut circuit TV.

Interchanges.

Passage control.

Interruption discovery frameworks.

Lighting.

Bolt and key control.

Bundle and mail control.

Faculty dependability.

Area of confined zones.

Review of water and nourishment.

Review of key work force vehicles.

The physical security arrangement must be adjusted in its introduction, with equivalent accentuation on forestalling criminal goes about and in addition terrorist acts. The leader must upgrade his arrangement persistently taking into account risk appraisal.

b. Operational Security. Protecting data is the foundation of the OPSEC program. The OPSEC project facilitates everything activities needed to keep an adversary or terrorist from finding out about arrangements and operations. Methods of trickiness, physical security, SIGSEC, and data security are interrelated and happen in the meantime. All arranging must incorporate measures to keep the potential terrorist from acquiring data that could help in a terrorist episode. Four ranges of data that terrorists can adventure are as per the following:

(1) Human insight. HUMINT includes utilizing individuals to accumulate data about military capacities and goals to incorporate establishment regular exercises. HUMINT sources can incorporate apparently insignificant bar or eatery discussions concerning operations, or the arrival of telephone numbers and locations of key staff. This risk can be countered by holding fast to physical security and data security rehearses, and by utilizing countersurveillance and counterintelligence exercises.

(2) Signal insight. SIGINT concerns all types of correspondences and sign discharge hardware. Terrorists will be unable to trade off refined hardware, however they can influence routine regular correspondences exercises. For instance, police or flame division frequencies are not changed when radios are stolen, or phones in delicate zones are not checked for bothering gadgets. This risk is countered by building up correspondences security and data security.

(3) Photo insight. Terrorists use PHOTOINT to pick up data through scope from airplane, high landscape components, vehicles, et cetera. PHOTOINT can be countered through counterintelligence and countersurveillance programs.

(4) Operational examples. Operational examples of military associations give data to a terrorist. To counter this danger, pioneers must wipe out examples when conceivable. Else, they ought to utilize double dealing measures to cover the set up example.

c. Personal Security. No individual is insusceptible to the danger of terrorism. Delegates of the US Government are conceivable focuses of terrorist exercises. Terrorists might preselect workplaces, assembling plants, or other establishment resources as focuses for bombarding, damage, shows, snatchings, and homicides. Who possesses these structures

may be of little concern to the terrorists. Measures that may be valuable in stopping such acts are as per the following:

(1) Control access to touchy territories and charge workplaces, both day and night.

(a) Prevent direct access to touchy territories well on the way to be focuses of terrorism. Try not to find summon workplaces on the ground floor.

(b) Equip doorways to delicate zones and summon workplaces with an alert.

(c) Have an entrance program; escort guests.

(d) Ensure direct-security power work force weigh charge zones in their twilight visit.

(e) Lock all restrooms on floors where summon workplaces are situated (and in addition others in a multistory office building) to prevent community.

(f) Lock ways to janitorial and other support storage rooms at all times.

(g) Lock ways to phone and electrical hardware rooms. Offer access to upkeep and phone work force just when they have such need.

(2) Select an inside safe space for utilization if terrorists assault; don't distinguish it as a protected room.

(3) Maintain crisis supplies, for example, emergency treatment hardware, bomb covers, candles, apportions, water, lamps, et cetera. Illuminate key staff as to where supplies are kept, and the area of crisis exits and departure courses.

(4) Restrict the individual history information on key work force since this data could be utilized by terrorists to choose casualties or to recognize their homes and families.

(5) Recommend key faculty stopping regions not be recognized by name yet rather by number.

(6) Limit data on travel motivation and arrangements of order or key staff to just need-to-know work force.

(7) Increase the impact of charge and key work force defensive measures by empowering them- -

(a) To keep up a position of safety.

(b) To be taught to perceive the indications of reconnaissance by outsiders.

(c) To utilize basic, compelling, verbal code signs to ready family or hierarchical individuals to a physical danger.

(d) To change courses to and from work.

(e) To go to cautious and shifty driving school.

(f) To review vehicles before moving.

(g) To utilize defensive vests.

(h) To maintain a strategic distance from likely terrorist focused on territories.

(i) To drive with windows shut and entryways bolted.

(j) To know key expressions in the local dialect.

(k) To precisely screen all local help.

(l) To know terrorist systems and techniques for operation.

(m) To perform guide surveillance to maintain a strategic distance from suspected terrorist focuses when venturing out to new destinations (eateries, lodgings, shopping, etc).

3-9. TERRORIST THREAT CONDITIONS

The accompanying terrorist risk conditions depict dynamic levels of terrorist danger to US military offices and staff. As Joint Chiefs of Staff-affirmed phrasing, these terms, definitions, and efforts to establish safety actualize an institutionalized terrorist ready framework all through the DOD. MACOMs and subordinate summons are not approved to change the fundamental framework; on the other hand, supplements to the framework may be distributed. The determination of suitable reactions to terrorist dangers remains the obligation of the administrator having purview or control over undermined offices or work force.

a. Danger Condition Alpha(Low).

(1) Definition. A general danger of conceivable terrorist action against establishments and work force, of unusual nature and degree, when circumstances don't legitimize full usage of

measures contained in a higher risk condition. Chosen measures from higher risk conditions may be actualized as required.

(2) Measures To Be Taken.

(an) At normal interims, remind all work force, including wards, to be suspicious and curious about outsiders, especially those conveying bags or different holders; to be ready for unidentified vehicles on or close US establishments; and to be ready for surrendered bundles or bags, or for any unordinary movement.

(b) Keep the obligation officer or other named staff accessible to clear structures and ranges, and to close territories where a blast or assault has happened. Keep key faculty accessible as needs be to actualize security arranges.

(c) Secure structures, rooms, and capacity territories not in normal utilization.

(d) Increase security spot checks of vehicles and persons entering establishments and nonclassified territories under the ward of the US summon and organization.

(e) Limit access focuses for vehicles and work force.

(f) As an impediment, apply one of the accompanying measures from danger condition Bravo separately and haphazardly:

Secure and routinely examine all structures, rooms, and capacity regions not in normal utilization.

Toward the starting and the end of every workday, and at other consistent and continuous interims, assess the inside and outside of structures in normal utilization for suspicious movement or bundles.

Check all conveyances to establishment exercises and encourage wards to check every single home deliverie.

To the extent assets permit, expand reconnaissance of local facilities (schools, wreckage heaps, clubs, and other vulnerable objectives) to enhance prevention and safeguard, and to fabricate certainty among the staff and wards.

(g) Review all arrangements, orders, staff subtle elements, and logistic prerequisites identified with the presentation of the higher risk condition.

(h) Review and execute efforts to establish safety for high-chance staff.

b. Risk Condition Bravo (Medium).

(1) Definition. An expanded and more unsurprising risk of terrorist action despite the fact that no specific danger has been distinguished.

(2) Measures to be Taken.

(a) Remind all faculty to be mindful and curious about suspicious persons, vehicles, and exercises. Caution staff of any type of assault to be utilized by terrorists.

(b) Keep all faculty accessible as needs be who are included in actualizing antiterrorist emergency arrangements.

(c) Check gets ready for actualizing measures contained in the following danger condition.

(d) Where conceivable, move autos and different articles no less than 25 meters from structures, especially those structures of a touchy or prestigious nature. Consider the utilization of unified stopping.

(e) Secure and consistently review all structures, rooms, and capacity regions not in general utilization.

(f) Make consistent and successive assessments of the inside and outside of structures for suspicious bundles.

(g) Thoroughly look at all mail for letter or package bombs.

(h) Check all conveyances to establishment exercises and encourage wards to check every home deliverie.

(i) As far as assets permit, expand observation of local facilities (schools, wreckage heaps, clubs, and other vulnerable objectives) to enhance discouragement and resistance, and to manufacture certainty among the staff and wards.

(j) Keep the staff and wards educated of the general circumstance to stop bits of gossip and avoid pointless caution.

(k) At an early stage, educate individuals from neighborhood security boards of any move being made and why.

(l) Upon section of guests to the unit, physically assess them and a rate of their bags, bundles, and different compartments.

(m) Wherever conceivable, work irregular watches to check vehicles, individuals, and structures.

(n) Protect off course military work force and military transport as per arranged arrangements. Remind drivers to bolt stopped vehicles and to organization a positive arrangement of checking before they enter and drive an auto.

(o) Implement extra efforts to establish safety for high-hazard work force.

(p) Brief staff who may enlarge the watchman power on mandates and regulations concerning the utilization of lethal power.

(q) Conduct an arbitrary pursuit of vehicles entering the establishment.

c. Danger Condition Charlie (High).

(1) Definition. A terrorist occurrence has happened or knowledge has been gotten demonstrating that some type of terrorist activity is inevitable.

(2) Measures to be Taken.

(a) Continue all danger condition Bravo activities or present those not effectively actualized.

(b) Keep all staff on obligation who are in charge of actualizing antiterrorist arranges.

(c) Limit access focuses to total least.

(d) Strictly uphold control of passage and pursuit all vehicles.

(e) Enforce brought together stopping of vehicles far from delicate structures.

(f) Issue weapons to monitors. (Neighborhood requests ought to incorporate particular guidelines on issue of ammo.)

(g) Increase watching of the establishment.

(h) Protect all assigned powerless focuses and give extraordinary consideration regarding helpless focuses outside military foundations.

(i) Erect hindrances and impediments to control activity stream.

d. Danger Condition Delta (Imminent).

(1) Definition. Terrorist assault has happened in the prompt region or insight has been gotten that terrorist activity against a particular area is likely. Ordinarily, this danger condition is announced as a restricted cautioning.

(2) Measures To Be Taken.

(a) Continue or present measures recorded for danger conditions Bravo and Charlie.

(b) Augment monitors, as required.

(c) Identify all vehicles as of now on the establishment inside operational or mission bolster ranges.

(d) Search all vehicles entering the complex or establishment and additionally vehicle substance.

(e) Control all entrance and actualize constructive distinguishing proof of all work force.

(f) Search all bags, attachés, and bundles brought into the complex or on the establishment.

(g) Enforce measures to control access to all regions under the locale of the US charge or office concerned.

(h) Check regularly the outside of structures and of stopping ranges.

(i) Minimize every single authoritative voyage and visits.

(j) Consult neighborhood powers about shutting open (and military) streets and offices that may make locales more defenseless against terrorist assault.

e. Risk Assessment Guidelines. The taking after general rules accommodate uniform usage of security ready conditions. Appraisal components are characterized as- -

(1) Existence. Applies when a terrorist gathering is available in a zone of concern. The gathering need not have represented a risk to US or DOD intrigues previously.

(2) Capability. Applies when a terrorist gathering can actualize an operation against US intrigues in territories of concern. This incorporates assets, for example, knowledge, versatility, work force, and hardware (explosives, arms, and ammo).

(3) History. Applies when a bunch's history of terrorist acts and conduct mirrors a hostile to US stand or incorporates past assaults against US intrigues.

(4) Trends. Applies if the gathering has, over the previous year, showed terrorist action that has all the earmarks of being proceeding with or expanding. Action require not have been vicious; terrorist assaults against US or DOD intrigues may be just undermining explanations.

(5) Targeting. Applies if there are known plans or affirmed expectations of a terrorist gathering to target US or DOD intrigues. Focusing on can be either particular or nonspecific. In the event that focusing on is not against US or DOD intrigues, this variable ought not be considered.

A blend of positive responses to any or the majority of the above evaluation components will deliver a danger level of either low, medium, high, or unavoidable. These rules apply just to the evaluation of terrorist danger against US or DOD intrigues.

f. Danger Condition Reporting Procedures. Department of the Army obliges MACOMs that claim establishments to actualize a reporting framework inside of their individual orders. This framework will give DA and senior Army pioneers current data on the antiterrorist pose with the goal that assets are devoted where they are generally required. (See applicableregulations for reporting methodology.)

3-10. COUNTERTERRORISM

Counterterrorism incorporates the full scope of hostile measures to avert, deflect, and react to terrorism. This is the last stage in fighting terrorism. It is receptive and accepts the broad arrangement, arranging, and reaction measures set up in terrorism neutralization

arranges. The kind of strengths and charge and control relations utilized as a part of counterterrorism operations rely on upon the area, sort of occurrence, and level of power needed. Power determination criteria are represented by legitimate and political limitations. Some military operations executed by US drives because of terrorist acts may be done by customary strengths, However, ordinarily these powers give backing to an uncommonly composed, prepared, and prepared counterterrorism unit. In executing counterterrorism activities, pioneers ought to guarantee authoritative arranging addresses the accompanying errands:

a. Intelligence. A very much arranged, sorted out, all-source insight project is crucial with a specific end goal to distinguish the risk and to give auspicious danger knowledge. (See Chapter 6.) This incorporates assessing terrorist capacities, strategies, and technique.

b. Prisoner Negotiations. Due to jurisdictional contemplations, prisoner transactions are ordinarily the obligation of another US government office or the host country.

c. Prisoner Rescue. Specially sorted out, prepared, and prepared work force and units are kept up to save and ensure prisoners.

d. Attack of Terrorist Positions. An goal of national arrangement is to stop the terrorist through the risk of countering. At the point when this gets to be fundamental, US military staff regularly direct the operation. This mission could be doled out to either uncommon operations powers, traditional powers, or both. In the event that SOFs are utilized, the US military officer must at present arrangement to build up an internal security border of MP units. He likewise sets up an external security edge of officers and a unique response component to react to other segregated episodes inside of the AOR.

Segment III.

Battling TERRORISM IN LIC

Commandants must make a move to counter terrorists. Amid peacetime, they must create and utilize antiterrorist arranges. The measures to stop, counteract, and react to risk are in view of the terrorist danger conditions. The arrangement must relate to and be incorporated in the security arrangement. This incorporates physical security, OPSEC, and individual security. As the unit conveys for COIN operations, PKOs, or PCOs, the shots of a terrorist demonstration increments. Taking into account the danger, officers must monitor unit work force and hardware.

3-11. Sending IN CONTINGENCIES

An administrator with an arrangement mission must diminish the helplessness of his unit to terrorist assault. These precautionary measures must be incorporated amid predeployment, sending, and redeployment.

a. Predeployment. The administrator must build up his unit's security to confound the terrorist's choice making. As he arranges his idea of the operation, he surveys the risk. From this, the operational arrangements, gear, and unique aptitudes can be picked that build danger to the terrorists.

(1) The idea ought to -

(an) Include security against terrorism in all requests, arranges, and preparing.

(b) Include security in the leader's direction.

(c) Deter or make hazard for the terrorist through security programs.

(2) The arranging procedure must incorporate -

(a) Mission investigation.

By what means can the mission be influenced by a terrorist assault?

What are the security parts of both indicated and inferred assignments?

Keep on looking into unit shortcomings all through predeployment, arrangement, and redeployment.

(b) Threat evaluation.

Distinguish terrorist gatherings working in the arrangement region.

Add to a rundown of PIR: strategies for operation, assault strategy, and preattack sign.

Distinguish wellsprings of data on terrorist gatherings; know how to get to them rapidly and routinely.

Routinely incorporate danger evaluation in insight gauges.

(c) Combat administration bolster contemplations.

Obtainment of uncommon security gear

Security of capacity and dissemination regions.

Upkeep of uncommon gear.

Security of upkeep unit if separate from fundamental body.

Security amid development (in light of risk).

Security in arranging ranges.

Contact with security offices that bolster the move or with controlling ranges that move (host nation).

(d) Combat bolster contemplations.

Designing need of work in light of the mission and terrorist risk.

Unique specialist hardware for leading countermine and EOD; defensive snag emplacement; developing barricades; basic site, resource, and troop security.

Unique specialist hardware.

Specialist preparing to move units on visual identification/acknowledgment of mines/booby traps.

MP check/examine/enhance unit physical security.

MP contact with nearby police/security faculty.

MP help with security arranging and preparing.

Host country security strengths helped by MP screen non military personnel and host country representatives.

No procuring of non military personnel representatives, if conceivable.

In the event that utilized, uncommon security methodology for screening and observing regular citizens.

In numerous nations, a charge for data is normal. Coordinate with the State Department for an intends to pay for data.

(e) Operational contemplations.

Unit arranges. Incorporate security in every arrangement, SOP, OPORD, and development request.

Security arranges. Get ready, audit, and redesign unit security arranges (physical security, wrongdoing anticipation, et cetera), and singular security arrangements (watchman orders).

Security programs. Create particular security projects, for example, risk mindfulness and OPSEC.

Extraordinary groups. Because of the terrorist risk, consider an alternate errand association (pursuit groups, unique response groups, defensive administration groups).

Extraordinary aptitudes. To counter the terrorist risk, add exceptional abilities to units (investigators, etymologists, FAOs, EOD work force, open issues, SOF contact, CA officer). Some may need to run with cutting edge parties.

Summon and bolster connections. These may contrast from the normal (State Department, host country, nation group, SOF groups). Resolution order and bolster connections between the development gathering of the JTF and the detachment and different offices before arrangement.

(f) Specialized aptitudes preparing. Institutional preparing for specific abilities (teacher capability, equivocal driving, uncommon response groups, risk mindfulness, look systems, prisoner transaction, barricades, sentry obligations, joint police activity with host nation).

(g) Transit to arrangement range.

Consider general security of the unit all through the whole development: crisis activity methods, option courses or preoccupations, and natural security groups with every development component.

Actualize on the way arranging and preparing.

Instantly upgrade insight/danger appraisal before landing.

b. Deployment. Deployment is the second phase of the mission. As units move and build up operation bases, administrators should not make lucrative targets.

(1) Advanced gathering contemplations.

(a) Composition. More staff are required for security and contact with host country security organizations, in light of the fact that a methods for included insight terrorism is needed.

(b) Deployment. The essential security thought for the propelled party is whether it ought to be standard or low profile (uniform or regular clothes, military or non military personnel transport).

(c) Validation. The propelled party must approve the mission and PIR. Obliged errands incorporate figuring out whether the terrorist risk evaluation tracks with genuine danger and if the risk from in nation influences the achievement of the mission; and, finding the mission, on the off chance that it is the same as the commander's.

(d) Rules of engagement. The propelled party must affirm arranged principles of engagement. It must figure out whether they are the same as those amid the predeployment stage. Issues must be determined before the primary body arrives.

(2) OPSEC measures in sending.

(an) Avoid setting aside a few minutes and spot of entry; generally, build security.

(b) Avoid setting examples of conduct/operation.

(c) Set up secure interchanges with principle body and propelled gathering.

(3) Pass strategy. On augmented operations, the spirit of officers must be considered. A pass arrangement may be set up in the mission region. Be that as it may, officers must stay under the radar. Administrators ought to do the accompanying:

(a) Provide troop data briefings on the danger.

(b) Establish pass approaches utilizing the amigo framework.

(c) Establish untouchable zones.

(4) Force security. In setting up working bases and in everyday operations, leaders must consider the security of his powers. This is a noteworthy concern when the guidelines of engagement are prohibitive. A few contemplations are as per the following:

(a) Coordinate with security compels that ensure strengths (MP, host country powers, coordinating staff).

(b) Avoid giving lucrative targets (troop fixations, engine pools, expansive static logistic establishments).

(c) Transit inside of arrangement zone.

(d) Continue danger appraisal along courses for every development.

(e) Include security in all development orders.

(f) Provide security at flight and landing focuses.

(g) Employ security strengths amid travel.

(h) Establish contact and direction with all security offices along course.

(5) Security improvement. Leaders ought to utilize TOE and specific gear to give security in light of danger evaluation.

(an) Assign the executive marshal or a military cop the obligation regarding physical security.

(b) Ensure all faculty know the administering regulations (gatekeeper requests, tenets of engagement, nearby limitations).

(c) Stay mindful of preparing and the troop data program.

(d) Include power/base insurance when organizing unit positions (great guard/obstruction arrangement, scattering of high-esteem targets far from access streets, edge wall).

(e) Maintain a position of safety (limit passes).

(f) Restrict access of unassigned faculty to the unit's area. Limit the quantity of vehicles inside of edges and continue stopping far from structures. Perform stringent distinguishing proof checks.

(h) Constantly depict a picture of polished skill and status.

(i) Continue to reassess the earth.

c. Redeployment. During the redeployment stage, get ready for a terrorist assault is as key as amid alternate stages. Truth be told, units have a tendency to unwind after an operation.

Redeployment relies on upon the mission, the reputation, and the worldwide response. It might be the most defenseless stage for aterrorist assault.

(1) The development party must keep a security alarm and mindfulness stance until the greater part of the unit has returned. The development gathering ought to create PIR for come back to home station.

(2) Stay-behind work force are most open to terrorist assault subsequent to the outfitted vicinity is less. They must keep a security pose that mirrors the shot of a more noteworthy danger. Activities incorporate keeping up contact with security strengths, adding to efforts to establish safety, and keeping tight controls on work force.

(3) The accompanying ought to be considered for opposite organization:

(a) The security of the port of passage and lines of interchanges for the arrival excursion.

(b) If the mission has changed the circumstance at home. A disagreeable political choice may open the unit to a risk upon its arrival to the US.

(c) To receive the efforts to establish safety utilized amid travel to, and development inside of, the sending region. Coordinate response capacity with security organizations along the course.

(4) A facilitated PAO approach ought to be produced to fuse the accompanying:

(a) Control of data discharged to the media guarantees exactness and culmination.

(b) Troops ought to be advised as to arrival of data to outside offices. Just open undertakings staff have discharge power.

(5) Debriefing ought to be directed. The anxiety increment in fighters amid serious arrangement operations must be permitted to die down. This serves to alter once more into a peacetime domain. These debriefings include:

(a) Briefing fighters to change their introduction from LIC obligation back to peacetime.

(b) Updating fighters in regards to new strategies, occurrences, or dangers that created following the sending operation.

(c) Inspecting fighters for maps, keepsakes, arms, and weapons.

(6) A careful after-activity report ought to be arranged. It gives two imperative administrations to units that direct future operations. It gives future leaders an advantage from lessons learned. Likewise, it serves as an asset for approving terrorism balance methodology for future operations.

3-12. Need INTELLIGENCE REQUIREMENTS AND LOCAL TERRORISM INDICATORS

Fighting terrorism, more than some other type of fighting, obliges information of the adversary's objectives and capacities. Knowledge officers, supporting a conveying unit, should constantly consider the terrorist's worries when creating EEIs and a rundown of neighborhood terrorism markers.

a. Need Intelligence Requirements. The taking after terrorist concerns can help the knowledge officer in creating PIR:

Association, size, and piece of gathering.

Inspiration, long-extend objectives, and short-go objectives.

Religious, political, ethnic association, or a blend of these.

Worldwide and national bolster (moral, physical, budgetary).

Selecting systems, areas, and targets (understudies).

Characters of gathering pioneers, go getter, and visionaries.

Bunch knowledge capacities.

Wellsprings of supply/backing.

Imperative dates (religious occasions, affliction commemorations).

Arranging skill.

Level of control.

Favored strategies and operations.

Eagerness to murder.

Eagerness for benevolence((pronounced or illustrated).

Bunch abilities (killing, destructions, masquerade, fashioned reports, modern damage, plane/pontoon operations, burrowing, submerged electronic reconnaissance, harms/contaminants).

Gear and weapons available and needed.

Transportation close by and needed.

Therapeutic backing accessible.

Opportunity of access to media and ability in utilizing it.

b. Neighborhood Terrorism Indicators. Some conditions that may show politically persuaded brutality in specific areas are as per the following:

(1) Dissent for political, social, or ethnic reasons. Charges brought against nearby government.

(2) Formation of radical gatherings, branches of national subversive gatherings, or mystery social orders.

(3) Antigovernment, against US unsettling; distinguishing proof of government or US as the foundation of the issues.

(4) New representatives for the individuals' reasons rising; away coordinators arriving.

(5) Meetings, arouses, and exhibits being sorted out; grievances taking political suggestions; incendiary addresses and charges made; incitement of powers to intercede, or go overboard; police or military ruthlessness charged.

(6) Appearance of rebellious notices, handouts, underground squeeze; taking individuals' worry into political stadium; politicization of social reasons.

(7) Use of referred to identities as draws for energizes, particularly those that have been related to radical reasons.

(8) Demonstrations, common insubordination, or challenge walks with reasons eclipsed by political talking points.

(9) Increased selecting, by known front gatherings and radical associations; support looked for among specialists.

(10) Increased activism in political circles at schools and colleges.

(11) Speeches and correspondences expressing viciousness as the main method for arrangement.

(12) Identification of remote impact or help.

(13) Threats against open works, utilities, or transportation; dangers of brutality against unmistakable identities.

(14) Agitation in evacuee, minority, or outside groups; polarization; furnishing portions of society.

(15) Reports of stolen guns and explosives; assaults on ordnances, and donning merchandise stores.

(16) Violence against property, plundering, annihilation, and torching; for the most part amid exhibitions, walks, or crowd activities.

(17) Violence against persons, homicides, endeavored killings, beatings, dangers, snatchings, or open focusing of individuals.

(18) Increased buys of elite weapons; appearance of programmed weapons, mostly of outside production.

(19) Discovery of weapons, ammo stores, and explosives; sign of terrorist preparing; expanded terrorist reconnaissance.

(20) Open assaults on police, military, and different powers.

(21) Reports of stolen distinguishing proof cards, participation cards, etc.

3-13. OPERATIONS SECURITY MEASURES

Leaders can execute certain measures to abstain from stereotyping and to deny knowledge data to the adversary.

a. Leaders ought to hold fast to the accompanying OPSEC measures:

(1) Use EEFI to control the OPSEC program. Create EEFI- - those things/exercises of arranging that terrorists can utilize.

(2) Present irregular activity in unit working techniques (change watch calendars, courses, check focuses, sentry, or gatekeeper positions.

(3) Avoid any set example for authorities, gatherings, dinner calendars, resupply action, religious administrations, or sentry or gatekeeper reliefs.

(4) Employ defensive obstructions (edge and interior).

(5) Check recognizable proof of all work force entering and leaving the border or establishment.

(6) Employ added security to limited zones (interchanges posts, correspondence focuses, engine parks, high-thickness troop ranges).

(7) Control appropriation of schedules of VIPs/high-hazard faculty.

(8) Establish descent focuses and stopping regions far from structures. On the off chance that conceivable, these ought not be seen from outside the base.

b. The accompanying are cases of insight pointers that may help a terrorist in social occasion knowledge on a unit. This is a specimen posting and ought not be translated as complete.

(1) Operation Indicators.

(a) Troops confined to the post before a move or operation.

(b) Increased watching/air surveillance.

(c) No watching by any means.

(d) Increased development between areas brought on by assignment associations before an operation.

(e) Special demands to expand apportions, transport, and ammo.

(2) HUMINT Indicators.

(a) Newspaper or other media scope.

(b) Farewells and a minute ago visits by VIPs or senior officers.

(c) Church benefits the night prior to an operation.

(d) Bulletin notification expressing that authorized rest is obliged; dispensary hours are changed.

(e) Public signs declaring changes in strategies (limiting non military personnel travel/access).

(f) Photography created by nearby builders indicating in-camp scenes and arrangements.

(3) Communication Indicators.

(a) Change in call signs and frequencies before an operation.

(b) Movement of assistant correspondence hardware (new aerials) to another territory.

DEFENSIVE CONSIDERATIONS IN COIN

PROTECTION

Protection is the maintaining the effectiveness and survivability of military installations, camps, personnel, equipment, information/communication systems and other facilities located within the area of operations in any COIN mission. In case of COIN the protection concept is different than that of a conventional force protection scenario in that the element of the protection of the local populace/communities inhabiting the AO is also taken into account. Now if this element is granted due protection, is secured from the insurgents psychological ops and transactional overtures(seeking safe houses, staging areas in the local area, taking psuedonames or as family members to deceive the forces against a false or ideologically goaded sense of protection for the community members or any other assumed social benefit not accorded by the government) then in turn the security forces gain allies who will feed intelligence about the enemy and information pertaining to military security thus enhancing the security of
the tactical units and installations itself.

TECHNIQUE CONSIDERATIONS DURING COUNTERINSURGENCIES

Insurgents resort to lethal and nonlethal attacks against groups of soldiers, unit commanders and civilians. Lethal attacks include killing and IED whereas non-lethal attacks are kidnapping and ransom, subversion or psychological/intimidation/threats. To thwart such attacks and deter the enemy the following basic site-protection operations may be included as foundation steps in the overall unit protection program.

Observation Post: An OP is inadequately capable of protecting any vital asset of the unit using combat power but it can observe any enemy visual action and alert combat support immediately. It should be capable of defending itself and must have a communications backup/night vision devices and long range binoculars.

Stationary posts and static bases: Each post/base must take into consideration following factors before being assembled:

- Critical asset dimensions
- Threat severity
- Nearest reserve troops in terms of the time to inform them and the distance.

Keeping these into consideration a detachment/s occupies the post/base, full time and equipped with night vision devices and surveillance equipment. Its a very good idea to include mobile surveillance teams to keep an eye in the area in close proximity of the base perimeter.

Patrols:

a) Foot patrols: Both critical and low priority assets may be covered by foot patrols but usually low priority assets are allocated for protection. Foot patrols are susceptible to ambush and hence patrol timings must be random. This also helps in maintaining the element of surprise. Patrols must be well armed to defend themselves and have the necessary communication facility toi call for support if the need arises. The support team should be locally positioned and not far away.

b) Vehicle patrols: All the above apply equally to vehicle patrols.

c) Aerial patrols: Inaccessible areas can be kept under routine patrolling surveillance. Here they supplement foot and vehicle patrols in that they offer an extension in the coverage area. It can so happen that critical assets are positioned long distances away in terrain unsuitable for foot/vehicular patrolling.

RANDOM ANTITERRORISM MEASURES

It is very likely that the enemy keeps our forces and installation under surveillance. Their priority is to discern the overall security plan. Hence to throw them off track we must introduce a random element whenever possible. This also helps us to spring a surprise on the enemy. The main criterion here is to alter the security posture from time to time thus defeating the enemy's surveillance attempts. The enemy through surveillance attempts to know our possible actions,intent,order of battle,dispositions,etc.True surveillance is not strictly an intelligence activity on the part of the enemy but it is an enabler of intelligence. Hence we should tackle enemy surveillance on a equal footing with our intelligence and counterintelligence efforts.

Just like we use deception in counterintelligence based defensive and offensive activities.

Similarly we must use randomness to thwart enemy surveillance efforts.

- **Vehicular barriers to route traffic around base.**
- **Random security patrols**
- **Floodlights should operate at random times.**
- **Guard duty shifts must be practiced at random times.**
- **Changing access time for entry points.**
- **Access procedures/passwords must be changed at random.**
- **Searching personnel must be randomized—the method that is.**
- **Maintaining random observation of surrounding areas utilizing unmanned systems if available/remote systems.**

Armor Protection

We can increase the quantum of protection considerably by vehicle and personnel armor. But it must be kept in mind armor weight reduces the mobility of both the vehicle and soldier—in the case of the latter his maneuverability and endurance gets affected adversely..In addition heavy armor wears engine parts of the vehicles. But it is true that insurgent attacks become very much ineffective on armor shielded vehicles and personnel.

Hardening

Hardening is intended to defeat or negate /deter an attack.

Hardening makes it very difficult for insurgents to carry out attacks.

Study the terrain carefully and see to it that natural obstacles can be emplaced to deter the movements of the insurgents. Naturally available materials can be used to protect personnel, equipment and facilities. Physical protection can be effected using sandbags, walls, shields, concrete barriers. Proper selection should be made in keeping with nature of attacks: Blast, indirect/direct fires, heat, and radiation. Electronic warfare demands

a different set of materials/systems.

COUNTERINSURGENCY BASES

COIN forces must have a base from which to operate and also project. Bases are secure areas from which the COIN objective is to isolate the insurgents from the support facilities and protect the local populace/communities. The base must be carefully selected, reinforced and rendered fully defendable. Command relationships should be clearly defined. Bases can be of 3 types:

Forward operating bases, Combat outposts, and Patrol bases. The nature of the mission and size of the unit (Company etc) determines the size and location of the base.

FORWARD OPERATING BASES

Sometimes the nature of operations, the terrain, the size of the AO as well as the size of the units necessitate a separate forward placed operating base for the Battalion which itself commands controls, communicates and supports deployed units. It provides intelligence support, sustainment, replenishment and personnel support as well as functions also as staging area. Each area of operation may have one forward base. A forward operating base acts as a secure location for the planners and command staff so as to plan operations, provides security to the local populace and acts as a deterrent for the insurgents nearby by hampering their mobility and subjecting them to an increased threat. We can have both Brigade FOBs and Battalion Fobs. In
the case of Bde FOBs they act as rear areas for Bn Companies which are forwardly deployed. FOBs should maintain either secured road/water or air sustainment capability.

COMBAT OUTPOSTS

Observation posts are reinforced with fire power and combat teams and hence take the shape of a combat outpost. They are positioned at strategic points inside insurgent-0dominated areas , are company or platoon sized, possess the ability to conduct combat operations on a limited scale and are in contact with base headquarters as well as horizontally with other combat outposts , in effect networking both horizontally and vertically so as to:
Cut of insurgent logistical lines
Provide security to the local populace in the immediate neighborhood of the COP
Maintain direct contact with the local populace and hence keep an eye on the activities / strangers
These are not possible from remote bases operating from outside insurgent dominated areas. The negative factors in this type of arrangement are increased risk to the soldiers and limited area of operations , nevertheless proper networking among the combat outposts helps greatly in keeping a grip on the insurgency and the kill ratio as well as protecting the populace. It is very important to plan the position of the outpost, the emplacement, complete with secure logistical lines, communication systems and reinforcement capability. Each COP is assigned a sector of the AO.
Outposts may be employed—

- **To secure key lines of communication or infrastructure.**

- To secure and co-opt the local populace.
- To gather intelligence.
- To assist the government in restoring essential services.
- To force insurgents to operate elsewhere.

Priorities of Work

Certain factors need to be considered while establishing combat outposts.

- **The selected area must be free of noncombatants , civilians and the like.**
- **To hinder the enemy's movement , obstacles to his entry to streets , underground passages,marked areas in rough/jungle terrain should be emplaced.**
- **Carefully choose positions to set up weapons to cover likely avenues of approach.**
- **Clearing fields of fire**
- **Cover and camnouflage.**
- **Obstacles/barriers may be integrated with weapons so as to be auto-triggered.**
- **There should be easy access between positions and the routes must not hinder speed.**

PATROL BASES

Patrol bases are secured areas which serve as long period halting points for patrols. They may be permanent or temporary.

1. Sometimes it is important for patrols to remain hidden or halt all operations as information is received that they are liable to be detected.

2. Again detailed study of an area requires long periods of reconnaissance so they need a place to hide,and then later launch recce ops.

3. After long periods of recce operations,the troops get exhausted and hence retire to a patrol base for food,sleep or rest,weapons/equipment maintenance

4. After detailed reconnaissance the patrol commander needs to sit down with his senior NCOs and devise future course of action

5. In cases when the patrol is in enemy area after infiltrating the area,in small groups , they set up temporary patrol bases where they can later meet and regroup and make further plans.

6. Finally a patrol base is a good launching pad for consecutive or concurrent operations such as

7. raids,reconnaissance,surveillance and ambush.

TERRAIN

Key terrain factors to consider include the following:

- **The terrains may add to defense by virtue of its natural characteristics.Hence conduct a thorough study of the terrain.To enhance its natural defensive characteristics more utilize artificial obstacles/barriers.**
- **The patrol bases must have all access routes to it , by road or waterways , under control.The same applies for all lines of supply and communication and civilian access.**

The best technique for base defense is the perimeter defense.

UNIT PROTECTION:

We will define unit not be size or specific function but by any military group capable of offensive, defensive or stability operations.

Unit protection is the process through which combatant and noncombatant personnel, physical assets and information are protected from adversarial threats including adversarial multidisciplinary intelligence threats.Multi layered, active/passive, lethal/non-lethal offensive and defensive measures are adopted for this purpose. Protection is composed of a variety of active and passive measures (for example, weapons, pre-emption, and warning) in the air, land, sea, and space domains. The goal of unit protection is preventing attacks on the three unit resources , manpower, physical assets and information so that the capability of the

unit to maintain its fighting potential without any degradation by the enemy is constantly maintained.

The Army must:

¬ Detect the threat

¬ Assess the threat capability to degrade the units combat capabilities

¬ Decide on protective measures , whether offensive or defensive

¬ Act to implement these protective measures

¬ Recover in very less time from any damage inflicted by the adversary so that technical countermeasures and tactical procedures may be employed so as to bring back the unit to full

operational status in the least time possible.

In order for unit protection to be 100% effective we need to ensure that the following are taken into prioritized consideration by the unit commander:

• Persistent surveillance

• Actionable intelligence

• Precise target recognition

• Interrogation

• Commanders situational awareness

• Accurate identification of unit security related intelligence gaps

In addition unit Command and Control must be properly defined as C2 aids the Commander to take proper decisions in the light of what needs to be done exactly to protect the unit and ensure that this is carried out efficiently.

Protection: Protection is a function which should be given a holistic treatment.Protection should not separately focus on weapons deployment , pre-emption and warning.All three must be integrated.No one is a separate entity.Protection must be proactive.In fact unit protection should never always be pasisive but must also include active measures.Intellighence , counterintelligence and an admixture of military and cross government capabilities should be employed to the full.Installation/camp protection should look beyond the

perimeters.Just employing passive measures(check posts,access control,perimeter security , guard functions , lighting) and OPSEC isn’t sufficient.Surveillance teams , counterintelligence operatives should foray outside into adjoining areas , even areas of

interest located far from the unit , and the communities in these areas so as to gain information/intelligence and counter enemy reconnaissance/HUMINT/subversive /sabotage/terrorist activities.Counterintelligence should be employed to screen contract workers and suppliers.A counterintelligence review should be conducted periodically on unit personnel.Red teaming should be taken up by the commander and his staff to ascertain unit vulnerabilities and critical areas.

Add to Detect , Assess and Decide the functions Act and Recover and we have the foundation for a complete protection system on which toi base our decisions regarding collection of intelligence , fortifying and strengthening/hardening our bases,decide on the optimum courses of actionsd , employ forces optimally to act on these decisions and in case of an attack which could not be prevented , recover in the shortest possible time without the base collapsing totally during/after the attack using redundancy measures/backups and thorough protection of critical assets.We should also remember protection has yet another dimension.The enemy might know the porotective measures we have employed using intelligence and might attempt to block /prevent/deter our post-attack or pre-emptive actions , hence protection must take these into account also.

Protection means ''time-critical tacrtical operatiuons'' ..not just tactical operations.Protection should be a 360 degrees hemispherical capabilkity , meaning protection from land , air and sea based attacks.

For protection intelligence is critical as everything needs to be known about the enemy , envirobnment and self.The last factor is determined by counterintelligence vreviews , technical experts and red teaming.DAD abilities must be thoroughlky integrated to handle attacks fro m land , air,information , electronic,CBRNE,and intelligence domains of the enemy.This integrated approach heightens the commanders situational awareness consuiiderably , thus acting as a forc e and decision-superiority enbabler thus leading to optimum effective course odf acrtion/s by the Commander with a decisive finish.

Thus it is clear from the above that protection must be proactive , intelligence-led and an integrated approach.

Objectives of unit protection are:

Install a warning system

Intelligence preparation of all areas adjoining the base ,camp , the route along which the troops movement takes place –in fact it must be made mandatory for units intelligence section to keep an updated file on the intelligence preparation of the entire area surrounding the base/troop movement route whether or not there is a perception of threat.IPB should include , among other things:

- **Protection must be proactive , lethal and nonlethal both.**
- **Intelligence is the primary tool in protection**
- **Increase active/passive protection measures**
- **Rapid seizure of initiatives**
- **Rapid transition to decisive operations**
- **Rapid decision making capacity as tactical operations in unit protection are ''time-critical''.Damage to our forces in combat on the battlefdield or in case of an assymetrical combat , in hilly/urban/jungle terrain but away from base is different than that of an attack**

on an unsuspecting troop movement or installation/base itself where an attack means catching us off guard , unprepared and things move so fast due to the element of surprise our forces do not have enough time to recover , regroup and counterattack in time to thwart the enemy.The enemy may have critical assets in mind when they attack the installation/camp/base.Thus tactical operations are ''time-critical''.Hence to successfully thwart an attack ,should our defences fail …we must be prepared to execute time critical axctions without falling prey to the shock due to the surprise element.This is more so say in the case of an attack on an unsuspecting convoy or troop column.

- **Reducing vulnerability to minimum**
- **Identifying critical assets , protecting them priority of all unit protection systems**
- **Understanding that most operations will be in a non-linear unconventional operational environment and hence all intelligence , counterintelligence , surveillance , reconnaissance , target determination and nomination, combat oiperations,passive and active protection measures , red teaming , and recovery options should be seen from this perspective.**
- **Should understand that a complete 360 degree hemispherical protection system must be installed which must be a thoroughly integrated intelligence and operations function keeping the factors**

DAD

in perspective and the factors which come next , viz..Act , Finish and Recover

The following types of threats should be expected in any future conflict-

- **Attacks –air based/heliborne—on logistical systems.**
- **Critical assets will be targeted with precision munitions. Staging areas , critical choke points may be targeted using missiles with medium-range to ballistic capabilities.**
- **Random attacks so as to be unpredictable, IED attacks, terrorist and insurgent attacks and special forces attacks may be conducted with twin objectives or any of them...viz...Effect destruction/undermine our fighting capability and to force the commander to waste resources, ammunition, and unneceesarily divert forces to protect facilities and personnel which in fact are not threatened.**

We must remember we are now facing a fourth generation enemy , who will attempt to put in use every means including confusion and deception to overcome the asymmetry/mismatch by increasing uncertainty and making us more susceptible to the element of surprise.The enemy will resort to continuous , random,and non-decisive engagements.The enemy will randomly and continuously threaten and interdict lines of operations and communications.They will use camouflage and deception to to reduce weapon engagement rangers and degrade our forces advantages in ''stand-off'' engagements.There are two objectives herein—

first to confuse us so much that we cannot execute the targeting process correctly , target

determnination.identification.nomination becomes very difficult against an elusive enemy employing random attack methods , and secondly frequent loss of contact with this elusive enemy has more negative consequences than that which would have occurred with a conventional more predictable echeloned enemy.

HUMINT and CI are two disciplines which help in detecting enemy capabilities, intent and countering enemy intelligence collection activities. In a typical Army Intelligence structure, the intelligence assets are located at Div and Bde levels , with the Bde having a HQ company and Intelligence Bn , each Bn catering to a specific collection/counterint discipline. For example there can be a Ops Bn , a reconnaissance Bn , a tactical exploitation Bn,a forward collection Bn ,or a strategic SIGINT Bn.There is also a Div MI Bn and a theater intelligence Bde.

Military intelligence brigades coordinate, manage, and direct intelligence and surveillance; they conduct collection management, all-source intelligence analysis, production; and they disseminate information in support of national, joint, interagency, multi-national, regional combatant command, and Army service component requirements.

HUMINT and CI are indispensable to thwart enemy intelligence activities, to conduct force protection in a optimum manner, to keep our forces combat-ready to deliver precision strikes and to always keep the decision advantage in our favor with the element of surprise by the enemy being put at the minimum. Both disciplines are time intensive and inter-human interactions over prolonged periods have turned the tradecraft into a very specialized skill involving human perception, behavior, psychology and other traits. Unlike other disciplines like SIGINT,IMINT,MASINT,GEOINT HUMINT and CI have in common human sources , the human element and hence is susceptible to error , deception by the enemy , fraught with risks and psychological stress including human vices predicated by money and other factors which are usually the byproduct of information-transactions (quid-pro-quo).But it is exactly these problems which prompts intelligence professionals to come up with newer tactics so as to minimize these negative factors and the resulting exploration and research in the field of HUMINT and CI leads to refined methodologies , TTPs which have been found to be effective in many cases.

Unit protection must integrate the protective attributes of different Army Corps. The capabilities in brief of the Corps are as follows:

1. The Air Defense artillery provides protection by acting as a warning system , intercepting threats directed from air in the form of missiles and aerial attacks (heliborne..etc) and also provide locational grid information for otrher supporting forces to target.
2. Military Police provides security by executing proactive intelligence led policing.

3. **Engineer Corps protect our force by contributing to its mobility and countermobility thus heightening its survivability.provides the capabilities of survivability, mobility, and countermobility to the force.**
4. **Military intelligence provides security to our force by adequate synchronized utilization/deployment of ISR assets and counterintelligence capability**
5. **Signals protects our command and control nodes directing/controlling communiucation,computers,and intelligence operations. Siugnals intelligence directly supports**
6. **HUMINT operations to validate information,increase the situational understanding of the Commander.**
7. **Field Artillery provides security to the force by contributing to the direct/indirect firepower,predicting impact points.**
8. **Ordnance Corp contributes to recovery by deploying its ordnance disposal systems.**
9. **Unit Protection Functions**

It's very true that conventional military threats exist and are given priority in intelligence activities but the existence and threat capabilities of asymmetric , nonconventional threats cannot be undermined. Add to these new emerging threats of this category. At the tactical level it is very important to address this type of threat by determining its identity, leadership, capabilities, tracking its location and gauging its intent.

We need to detect the enemy's entire range of hostile activity including intelligence collection and counterintelligence activities,use this information to assess its capabilities,intent to arrive at the common operation picture COP which brings to light the relationship between the terrain,enemy,mission,troops,time and the civil environment thus enabling the commander to enter the enemy's decision cycle,gauge its intent,deliver warning to force s in the area and develop suitable courses of action.After the asses step is over the commander moves on to the decide function wherein an action is decided upon or any existing action is altered or monitiored.Therafter the act function takes over where the course of action decided upon is implemented by tasking the tactical fighting unit to deliver kinetic.nonkinetic attack on nominated targets or passive protection measures..all with the intent to protect the force.Protecting the force should not entirely be passive in nature,the soldiers need to go out and attack nominated targets so as to deter attacks or fail plans to attack our installations.

CI/HUMINT Functions:

Recommending countermeasures after assessment of threat capabilities, operations, expected courses of actions, most likely COA and most dangerous COA.

Threat intent

Identify Threat leadership. Key commanders. Key lieutenants and area commanders

Identify threat C2 nodes

Identify threat logistic routes

Identify threat social reach, network, and contacts
Identify threat affiliates in other criminal networks, enterprises
Identify threat sympathizers in own area of control
Identify political/administrative figures that support threat ideology
Threat attack /defense operations location parameters
Gauge potential attack/defense methods of threat.
Recommend C2 setup to thwart threat attack.
Estimate with reasonable accuracy the expected time of attack.
Possible locations of Threat listening post/observation posts
Determine possible escape routes of threat forces after an attack or defense scenario
Possible enemy IED techniques, infiltration routes, emplacement
Gauge IED detonation methods/means
Gauge IED timings
Possible routes for IED ex-filtration
Staging areas
Safe houses
Weapons and ammunitions storage locations
Production facilities for IED and other ammunitions/explosives.
Find out what supplementary operations threat may resort to
Recommending countermeasures to threat IED
Recommending countermeasures to threat ISR/EW
Determining threat indirect fire parameters, key indirect fire

WARNING

(a) Warning. Once actionable intelligence is obtained warning or predictions is disseminated in a timely,unambiguous,specific and accurate manner.Warning is an acknowledgement of the existence ofd a threat and subsequent dissemination.

(b) Warning is of two types:

•Defensive warn

•Enemy warn

In defensive warn after receiving actionable intelligence about the adversary's possible attack the installations security is beefed up by incorporating protective measures. The warning may be digital/aural/physical or virtual.

In enemy warn the enemy is communicated the fact through non-lethal measures such as interrogation or challenging an enemy unit/capability that in case of persistent or continued enemy action our course of action/s can take on an increasingly lethal nature with the intent to prevent the enemy from taking further hostile actions and also inflict heavy damages. Thus enemy warn is a method to deter the enemy from carrying out its intent if it hasn't done so yet or to stop the enemy in its tracks...

It is very important that warning should be unambiguous, accurate and timely/specific,. In addition to this it should be actionable. Warning can be graduated; meaning the level of warning may assume increasing proportions in keeping with the feedback about the enemy

which may indicate that it has ceased its operations/.activities temporarily but is conducting discreet
operations/increased intelligence activity masked in the cloak of acceptance of our warning and
cessation of open hostilities.

WARNING SYSTEM:
The warning system must have the following features:
1. It should allow for redundancies in our act capability systems.
2. It should allow for passive proactive means so as to protect our installations, its critical assets,
command and control nodes, thus overall reducing the vulnerability of the installation/.protected area.
3. It should provide a system of integrating fires to handle threats and precluding enemy attack on our
installation , its C2 and critical assets.
4. Provide warning of threat intelligence activities.
5. Provide warning of existing threat C2 nodes
6. Provide warning of threat capabilities, disposition, strength, order of battle
7. Provide warning of threat logistic routes.
8. Provide warning of threat sympathizers.,
9. Provide warning of threats possible attack COAs
10. Provide warning of the defense capability of the threat
11. Provide warning of threats peculiar /preferred TTPs/modus operandi
12. Provide warning of threats history
13. Provide warning of threat movements
14. Provide warning of threat leadership
15. Provide warning of threat detachments, cells dispersed in and out of the area of operations.
16. Provide warning of Threat attack /defense operations location parameters.
17. Provide warning of potential attack/defense methods of threat.
18. Provide warning of the expected time of attack.
19. Provide warning of possible locations of Threat listening post/observation posts
20. Provide warning of possible escape routes of threat forces after an attack or defense scenario
21. Provide warning of possible enemy IED techniques, infiltration routes, emplacement
22. Provide warning of IED detonation methods/means
23. Provide warning of IED timings
24. Provide warning of possible routes for IED ex-filtration
25. Provide warning of Staging areas
26. Provide warning of Safe houses
27. Provide warning of weapons and ammunitions storage locations
28. Provide warning g of the Production facilities for IED and other ammunitions/explosives.
29. Provide warning of supplementary operations threat may resort to
30. Provide warning of threat indirect fire parameters, key indirect fire

Active measures will provide at stand-off distances, the capabilities to-

• We designate a stand-off area outside the installation/protected area and take active measures to deny unidentified vehicular or personnel movement in that area

• Just like we have a C2 system with respect to any mission, similarly we need to have a C2 mission with respect to active or passive defensive measures and these need to be integrated with the C2 itself. Such active/passive measures can be remotely controlled lethal/non-lethal measures.

• As for passive measure steps should be taken to deny unidentified/suspect personnel/vehicles movement inside a restricted area/protected area .Areas within buildings,facilities,structures,airfields,ammunition depot,etc can be effectively protected by employing unmanned remotely controlled nonlethal systems at standoff distances. Measures should be taken with priority to deter personnel and vehicles from entering a protected military installation again using remotely activated lethal/nonlethal systems. Physical barriers, both active and passive can be employed for this purpose.

• There can be instances of enemy fire directed at critical assets of the installation and hence we need to include modular protection packages, automatic or soldier response teams built up specifically for this purpose. The protection system should be integrated again with the C2 system. It is very important to point out here that all the passive/active measures success depends on a great deal on intelligence/counterintelligence/liaison apart from the remotely/manned protection system deployment. For example we need intelligence to apprehend any infiltrations in our camp in the form of security or non security civilian contractors. Or we can effectively liaise with the civil police/intelligence agencies to build up a mapping of probable anti-installation criminal forces operating in the area who could attempt to launch sporadic fires or explosive attacks, such attacks being in keeping with the criminal group's affiliation with the enemy. Counterintelligence can help in visualizing our vulnerable areas within the installation and then proceed to identify the critical nodes which if damaged can stop the installation operations altogether. This vulnerability assessment coupled with the threat assessment and supported by sound OPSEC practices can give adequate unit protection.

Future Modular Force leaders must be trained to aggressively manage information and instill trust in the output of decision support tools that automated systems provide. Other major implications include adoption of a lifetime of education paradigm and the creation of knowledge centers configured to support professional leader education. Leader development questions include, but are not limited to-

(1) How do we develop leaders ready to deal with the complexity of the contemporary operating environment, threats, and interagency implications?

(2) How can we develop more adaptive leaders, versatile in UP operations?

(3) How do we provide collaborative, distributed training problem solving and decision aids that empower battle command to support commanders, as well as staffs to advising commanders during planning, preparation, rehearsal, and execution of UP exercises and operations?

(4) How are leaders enabled to know the terrain and weather and appreciate their tactical implications for tactical concealment, employment of weapons, mobility, and seeking positions of advantage?

(5) How are leaders empowered to understand the operational environment as well as, or better than, the threat in order to execute UP detect, assess, and decide functions?

(6) How will units enable leaders to know the enemy, friendly unit locations, and their capabilities?

(7) How will units adapt to emerging UP situations more quickly than an adversary?

Note: UP is not force protection, although the application of protection capabilities will positively affect force protection. By integrating the protection capabilities outlined in this CCP, a commander, and consequently, the force will be offered superior protection abilities.

ISR assets require the flexibility to detect a wide range of emerging threats. While the ability to detect conventional military threats remains important, the ability to address the asymmetric, non-conventional threat gains importance. Tracking the location and activity and predicting the intent of individual threats is a new challenge at the tactical echelon. The following are future enhanced capabilities to address the future environment and will aid in the execution of the UP detect function.

Intelligence Indicators

Enemy Activity Indicators--Indigenous Population

<u>General Activities</u>

Identification of agitators, insurgents, militias or criminal organizations, their supporters, and sympathizers who suddenly appear, in, or move out of, an area.

Emergence of new leaders among the population.

New faces in a rural community.

Unusual gatherings among the population.

Disruption of normal social patterns.

Mass urban rural migration or vice versa.

Massing of combatants of competing power groups.

Influx of opposition resident and expatriate leaders into the AO.

Reports of opposition or disaffected indigenous population receiving military training in foreign countries.

Increase of visitors (for example, tourists, technicians, businessmen, religious leaders, officials) from groups or countries hostile to the United States or opposed to the current intervention.

Close connections between diplomatic personnel of hostile countries and local opposition groups.

Communications between opposition groups and external supporters.

Increase of disaffected youth gatherings.

Establishment of organizations of unexplained origin and with unclear or nebulous aims.

Establishment of a new organization to replace an existing organizational structure with identical aims.

Appearance of many new members in existing organizations such as labor unions.

Infiltration of student organizations by known agitators.

Appearance of new organizations stressing grievances or interests of repressed or minority groups.

Reports of large donations to new or revamped organizations.

Reports of payment to locals for engaging in subversive or hostile activities.

Reports of formation of opposition paramilitary or militia organizations.

Reports of lists of targets for planned opposition attacks.

Appearance of "professional" agitators in gatherings or demonstrations that result in violence.

Evidence of paid and armed demonstrators' participation in riots.

Significant increase in thefts, armed robberies, and violent crime in rural areas; increase in bank robberies in urban areas.

Opposition-Directed Activities

Refusal of population to pay or unusual difficulty to collect rent, taxes, or loan payments.

Trends of demonstrated hostility toward government forces or mission force.

Unexplained population disappearance from or avoidance of certain areas.

Unexplained disappearance or dislocation of young people.

Reported incidents of attempted recruitment to join new movements or underground organizations.

Criminals and disaffected youth who appear to be acting with and for the opposition.

Reports of extortion and other coercion by opposition elements to obtain financial support from the population.

Use of fear tactics to coerce, control, or influence the local population.

Reports of government or mission force facilities and personnel surveillance.

Activities Directed Against the Government/Mission Force

Failure of police and informer nets to report accurate information, which may indicate sources are actively supporting opposition elements or are intimidated.

Decreasing success of government law enforcement or military infiltration of opposition or disaffected organizations.

Assassination or disappearance of government sources.

Reports of attempts to bribe or blackmail government officials, law enforcement employees, or mission personnel.

Reports of attempts to obtain classified information from government officials, government offices, or mission personnel.

Classified information leaked to the media.

Sudden affluence of certain government and law enforcement personnel.

Recurring failure of government or mission force raids on suspected opposition organizations or illegal activities apparently due to forewarning.

Increased hostile or illegal activity against the government, its law enforcement and military organizations, foreigners, minority groups, or competing political, ethnic, linguistic, or religious groups.

Demonstrations against government forces, minority groups, or foreigners designed to instigate violent confrontations with government or mission forces.

Increased antigovernment or mission force rhetoric in local media.

Occurrence of strikes in critical areas intended to cast doubt on the government's ability to maintain order and provide for the people.

Unexplained loss, destruction, or forgery of government identification cards and passports.

Recurring unexplained disruption of public utilities.

Reports of terrorist acts or extortion attempts against local government leaders and businessmen.

Murder of kidnapping of government, military, and law enforcement officials or mission force personnel.

Closing of schools.

<u>Propaganda Indicators</u>

General Propaganda Activities

Dissident propaganda from unidentified sources.

Increase in the number of entertainers with a political message

Increase of political themes in religious services.

Increase in appeals directed at intensifying general ethnic or religious unrest in countries where ethnic or religious competition exists.

Increase of agitation on issues for which there is no identified movement or organization.

Renewed activity by dissident or opposition organizations thought to be defunct or dormant.

Circulation of petitions advocating opposition or dissident demands.

Appearance of opposition slogans and pronouncements by word-of-mouth, graffiti, posters, leaflets, and other methods.

Propaganda linking local ethnic groups with those in neighboring countries or regions.

Clandestine radio broadcasts intended to appeal to those with special grievances or to underprivileged ethnic groups.

Use of bullhorns, truck-mounted loudspeakers, and other public address equipment in "spontaneous" demonstrations.

Presence of nonmedia photographers among demonstrators.

Rallies to honor "martyred" opposition personnel. Mass demonstrations honoring local dissident heroes or dates significant to the opposition.

Nationwide strikes called to demonstrate the strength of the opposition movements.

Propaganda Activities Directed Against the Established Government

Attempts to discredit or ridicule national or public officials.

Attempts to discredit the judicial and law enforcement system.

Characterization of government leaders as puppets and tools of intervention forces.

Agitation against government projects and plans.

Radio propaganda from foreign countries that is aimed at the target country's population and accuses the target country's government of failure to meet the people's needs.

Propaganda Activities Directed Against the Mission Force and Military and Law Enforcement

Spreading accusations that the military and police are corrupt and out of touch with the people.

Spreading accusations that mission force personnel will introduce customs or attitudes that are in opposition to local cultural or religious beliefs.

Character assassinations of mission, military, and law enforcement officials.

Demands to remove strong anti-opposition or anticrime military and law enforcement leaders from office.

Calls for the population to cease cooperating with the mission force and/or HN military and law enforcement.

Deliberate incidents to provoke mission, military, or police reprisals during demonstrations or strikes.

Widespread hostile media coverage of even minor criminal violations or incidents involving mission force personnel.

Accusations of brutality or ineffectiveness or claims that mission or government forces initiated violence following confrontations.

Publication of photographs portraying repressive and violent acts by mission force or government forces.

Refusal of businessmen and shop owners to conduct business with mission force personnel.

Propaganda Activities Directed Against the Education System

Appearance of questionable doctrine and teachings in the educational system.

Creation of ethnic, tribal, religious, or other interest group schools outside the government educational system, which propagate opposition themes and teachings.

Charges that the educational system is only training youth to do the government's bidding.

Student unrest manifested by new organizations, proclamations, demonstrations, and strikes against authority.

Commodities Indicators

Food-Related Activities

Diversion of crops or meat from markets.

Unexplained shortages of food supplies when there are no reports of natural causes.

Increased reports of pilfering of foodstuffs.

Sudden increase in food prices, possibly indicating an opposition-levied tax.

Unwillingness of farmers to transport food to population centers, indicating a fear of traveling highways.

Spot shortages of foodstuffs in regions or neighborhoods associated with a minority group or weaker competing interest groups, while food supplies are generally plentiful in other areas. Conversely, sudden local shortages of foodstuffs in rural areas may indicate the existence of an armed opposition group operating in that region.

Sudden increase of meat in markets, possibly indicating slaughtered livestock because of a lack of fodder to sustain them.

Appearance of emergency relief supplies for sale in black markets, possibly indicating diversion from starving populations.

Appearance of relief supplies for sale in normal markets in a country or region recently suffering from large-scale hunger, which may indicate the severity of the food crisis, is diminishing.

Arms and Ammunition-Related Activities

Increased loss or theft of weapons from police and military forces.

Discovery of arms, ammunition, and explosives being clandestinely manufactured, transported, or cached.

Attacks on patrols resulting in the loss of weapons and ammunition.

Increased purchase of surplus military goods.

Sudden increase in prices for arms and ammunition to the open market.

Reports of large arms shipments destined for neighboring countries, but not intended for that government.

Reports of known arms traffickers establishing contacts with opposition elements.

Increase in armed robberies.

Reports of thefts or sudden shortages of chemicals that could be used in the clandestine manufacture of explosives.

Reports of large open-market purchases of explosive-related chemicals without an identifiable industrial user.

Appearance of manufactured or smuggled arms from noncontiguous foreign countries.

Clothing-Related Activities

Unusual, systematic purchase or theft of clothing materials that could be used for the manufacture of uniforms or footwear.

Unusual scarcity of clothing or material used in the manufacture of clothing or footwear.

Distribution of clothing to underprivileged or minority classes by organizations of recent or suspect origin.

Discovery of caches of uniforms and footwear or the materials that could be used to manufacture uniforms and footwear.

Increase of males in the streets wearing military style clothing or distinctive markings.

Medicine-Related Activities

Large-scale purchasing or theft of drugs and medicines or the herbs used to manufacture local remedies.

Scarcity of drugs and medical supplies on the open or black markets.

Diversion of medical aid donations.

Discovery of caches of medical supplies.

Communications-Related Activities

Increase in the purchase and use of radios.

Discovery of caches of communications equipment.

Unusual increase in amateur radio or cellular telephone communications traffic.

Environment-Related Indicators

Rural Activities

Evidence of increased foot traffic in the area.

Increased travel within and into remote or isolated areas.

Unexplained trails and cold campsites.

Establishment of new, unexplained agricultural areas, or recently cleared fields.

Unusual smoke, possibly indicating the presence of a campsite or a form of communication.

Concentration of dead foliage in an area, possibly indicating use of camouflage.

Presence of foot traps, spikes, booby traps, or improved mines along routes and trails.

Urban Activities

Apartments, houses, or buildings being rented, but not lived in as homes.

Slogans written on walls, bridges, and streets.

Defacement of government or mission force information signs.

Sabotage of electrical power network; pollution of urban areas' water supply.

Terrorist acts against physical targets, such as bridges, dams, airfields, or buildings.

Change of residence of suspected agitators or opposition leaders.

Discovery of message dead-drops.

Increased smuggling of currency, gold, gems, narcotics, medical supplies, and arms into urban centers.

Appearance of abnormal amounts of counterfeit currency.

Increase in bank robberies.

Work stoppages or slowdowns in essential industries.

Marked decline in product quality in essential industries.

Marked increase in equipment failures in essential industries.

Unexplained explosions in essential utilities and industries.
Establishment of roadblocks or barricades around neighborhoods associated with opposition elements.
Attempts to disrupt public transport through sabotage.
Malicious damage of industrial products or factory machinery.

SECURITY DURING MOVEMENTS

This section addresses convoy operations in a counterinsurgency environment. Convoys are planned and organized to control and protect vehicle movements. They are used for the tactical movement (personnel, supplies, and equipment) of combat forces and logistic units. Movements made during a counterinsurgency operation face a variety of potential threats, including local individuals, IEDs, and insurgents. Leaders continually assess the insurgents' tactics and implement measures to counter them. Soldiers conducting movement security operations remain vigilant at all times

CONVOY OPERATIONS

Key to the success of convoy operations is ensuring all personnel and equipment are properly prepared. All Soldiers in the convoy must have a task and purpose, and know what to do on contact during execution of convoy operations.. An important leader check is to review all actions, including their timing, to avoid setting patterns. Enemies use such patterns to predict friendly actions and plan attacks. Integrate this review throughout all operations, including after-action reviews.

CONVOY PLANNING CONSIDERATIONS

Consider the following when planning and preparing for convoys:

- **En route recovery.**
- **Ambulance/medical coverage. (Most ambulances have radio communications, to include casualty evacuation procedures.)**
- **Disperse combat lifesavers throughout convoy.**
- **Designate responsibilities such as aid and litter teams.**
- **Prepare a rest plan for drivers.**
- **Use window screens to deflect grenades.**
- **Implement security measures to prevent pilferage from the convoy.**
- **Arrange for escorts--military policy, infantry, or other.**
- **Disperse key personnel throughout the convoy. Cross-load equipment.**
- **Identify and verify convoy signals.**
- **Identify en route reference points and available fire support.**

- **Coordinate for air cover (rotary-wing security, close air support, mobile interdiction and radio frequencies and call signs).**
- **Prepare an air guard plan.**
- **Prepare a deception plan.**
- **Submit a closure report at destination and upon return.**
- **Perform a reconnaissance of the route if possible (air reconnaissance is the preferred method).**
- **Determine threat capabilities and potential courses of action (to include a mine overlay from higher, regional or local headquarters, if available).**
- **Civilian considerations along the route.**
- **Establish phase lines/checkpoints along the route to monitor progress of the convoy.**
- **Determine choke points along the route--bridges, open-air markets, over-, and underpasses?**
- **Know whether vegetation grows next to and away from the road and thereby provides concealment.**
- **Determine insurgent convoy attack patterns. Base this assessment on S-2 input and pattern analysis.**
- **Vary supply convoy SP times (by no more than 1 hour sooner or later) to keep insurgents off balance.**
- **Describe and verify the vehicle abandonment plan. Include how long to wait before stripping and leaving a disabled vehicle or trailer. Prepare a transfer-loading plan for the cargo.**
- **Establish the condition criteria to abandon a vehicle. Establish when to destroy it, burn it, or leave it.**
- **Arrange seats in the back of trucks to allow Soldiers riding to face out.**
- **Increased convoy speeds (such as 50 miles per hour) limit movement up and down the convoy line.**
- **When the roads are only one or two lanes wide, civilian traffic will impede any adjacent movement.**

MISSION BRIEFING

Execute a mission briefing two hours before the SP time. Include--

- **Tactical brief--enemy and friendly situation update from J-2.**
- **Convoy execution matrix (all drivers get strip maps).**
- **Safety brief--use risk management and risk reduction (mitigating measures).**
- **Vehicle dispersion and distance intervals during operations and specific battle drills.**

BATTLE DRILLS

Battle drills associated with convoy operations may include--

- **React to civil disturbance (not blocking the route).**
- **React to potential opposing force (blocking the route).**
- **Air attack. Artillery/indirect fire.**
- **Sniper fire.**

- **Ambush.**
- **Mines, booby traps, and IEDs.**
- **Mechanical breakdowns.**
- **Procedures for towing and being towed. React to traffic jams--partially and fully blocked roads.**
- **React to debris on the road--garbage, dead animals, other objects/trash that can be used to conceal IEDs.**

REHEARSALS

Rehearsals include--

- **Battle drills. Describe expectations for everyone. Describe who does what in each situation.**
- **Routes. Paint routes and terrain features on a large piece of canvas to allow drivers to "walk" the route prior to departure.**
- **Casualty evacuation. Establish what happens to casualties. Ensure aid and litter teams are designated and know what to do. Ensure security teams are designated, assigned cardinal directions, and rehearsed.**
- **Communications. Includes audio, visual, and radio. Ensure all know the back-up plan if primary communication fails. Can cellular phones be used effectively in an emergency? Ensure redundant means of communication are available and all know how to use them.**
- **Primary and secondary frequencies. Ensure all know the call signs and frequencies for close air and fire support.**
- **Security forces. Ensure roles and responsibilities are understood and rehearsed.**
- **Response/reaction forces. Ensure leaders know the location of response/reaction forces. Ensure all know the call signs and frequencies for them.**

CONVOY ORGANIZATION

Leaders must know how to position vehicles within the elements. Regardless of size, all columns, serials, and march units have four parts: scout, head, main body, and trail. Each of these parts has a specific function.

Scout

Two scout vehicles proceed three to five minutes in front of the main body. The scout's task is to ascertain road conditions and identify obstacles that may pose a threat to the convoy. When scout vehicles are employed, leaders plan to react quickly to an attack on those vehicles. However, conditions may not allow for the use of scout vehicles. If so, consider earlier convoys acting as scouts. Consider requesting the deployment and use of UAVs to reconnoiter the route.

Head

The head is the first vehicle of each column, serial, and march unit. Each head vehicle has its own pacesetter. The pacesetter rides in this vehicle and sets the pace needed to meet the scheduled itinerary along the route. The leader at the head ensures that the

column follows the proper route. He may also be required to report arrival at certain checkpoints/phase lines along the route. The head vehicle also looks for possible IEDs. When passing bridges, gunners first observe the approach and then the opposite side of the bridge. With the head vehicle performing these duties, the convoy commander has the flexibility to travel the column to enforce march discipline when the convoy speed is low. Use a heavy, well-protected vehicle as the head vehicle if mines or IEDs are expected.

Main Body

The main body follows the head vehicle and consists of the majority of vehicles moving with the convoy. The main body may be divided into serials and march units for ease of control. Vehicles in the main body are armed with crew-served weapons.

Trail

The trail is the last element of each march column, serial, and march unit. The trail leader is responsible for recovery, maintenance, and medical support. The recovery vehicle, maintenance vehicles, and medical support vehicles/teams are located in the trail. The trail leader assists the convoy commander in maintaining march discipline. He or she may also be required to report clear time at checkpoints or phase lines along the route. In convoys consisting of multiple march units and serials, the convoy commander may direct minimum support in the trail of each serial or march unit and a larger trail party at the rear of the column.

The convoy commander provides trail security and communications in case the trail party is left behind to make repairs or recovery. An additional technique is to establish a heavily armed and fast security detachment trailing the convoy by no more than five minutes. This time interval enables the security detachment to react and maneuver to an insurgent's flank to counterattack in the event the convoy is fixed or otherwise unable to maneuver against attackers.

SECURITY TECHNIQUES

The enemy may place IEDs at intersections where vehicles tend to slow down and bunch up. Ensure proper spacing at all times between vehicles, especially at intersections and turns.

When making turns, move the vehicle as far away from the curb as possible due to most IEDs being located on the inside turn.

Soldiers must maintain 360-degree security at all times.

Leaders must adapt quickly to the insurgents changing tactics to counter threats.

Note: Convoys must maintain 360-degree security and visibility of the surrounding areas. Attacks may occur after convoys pass a given location. Therefore, gunners must ensure rear security is maintained.

VEHICLE HARDENING PROCEDURES

When threat conditions warrant, commanders harden vehicles before convoy operations.

Adding sandbags, armor plating, ballistic glass, and other protective devices reduces the vulnerability of a hardened vehicle to the effects of explosives and small arms fire. The primary purpose of hardening is to protect the vehicle's occupants from injury, although it may make certain vehicle components and cargo less vulnerable.

Consider the following factors in determining the method and extent of vehicle hardening when a threat to friendly forces exists:

- **Flexibility. Harden vehicles to provide the degree of protection required while maintaining maximum flexibility in its use. Harden the cargo beds of vehicles with sandbags to protect troops.**
- **Weight. All vehicle hardening adds weight to the vehicle. This requires commanders to reduce the amount of cargo carried.**
- **Availability. Consider the availability of suitable materials and the time needed to complete the project.**
- **Types of Roads. Roads traveled may determine the amount of hardening protection needed. For example, hardtop roads generally present fewer hazards from mines than dirt roads.**
- **Maintenance.**
- **Vehicle hardening normally increases the amount of vehicle maintenance needed. If an excessive amount of weight is added, it may impact on the vehicle's mobility and operational capabilities.**
- **Kevlar blankets are effective and minimize extra weight. Unfortunately, the excess weight destroys the tires and the drive train quickly. Operating with hardened vehicles requires leaders to emphasize preventive maintenance checks and services.**

VEHICLE WEAPON IMPROVEMENTS

Strengthening the vehicle weapons platforms is an additional countermeasure against insurgent attacks. When convoys come under attack, the key to defeating and destroying the attackers is well-aimed, overwhelming fire. By adding to an already existing weapons mix/platform for a particular vehicle, Soldiers have the capacity to exponentially enhance their own force protection while destroying attackers. Where the situation allows, military police and other forces may be able to establish a security corridor along a supply route. This requires extensive patrolling along the route to identify potential ambush and IED sites. It has an additional requirement to search structures along the route and confiscate any weapons found. Active patrolling is a visible presence that becomes a deterrent to enemy action. In Operation Iraqi Freedom this technique was

found to provide a measure of security for convoys that was not obtained simply by arming the vehicles.

PULWAMA COMMISSION OF ENQUIRY DONE BY MYSELF

I am independently on my own initiative providing this report for your information and use. Policies and memorandums of understanding should be updated to adequately address Force Protection Detachment (FPD) requirement , creation of a seperate Force Protection Doctrine and a new intelligence discipline , namely Force Protection Intelligence and there is a need for a standardized and consistent training program. In addition, the current validation and prioritization process should be strengthened to continually monitor FPDs once they have been established.

Objective

Am conducting an assessment of the Force Protection capability and the associated intelligence component in the background of the recent Pulwama suicide bomber attack on security forces in transit. Am particularly reviewing in transit force protection. While listing the findings of the commission attention areas dealt with were existing Sops, intelligence inputs, security measures employed, the authority-direction-control of the CRPF Command with respect to the outbound movement and security, present and missing training requirements. Data for the commissions enquiry is essentially open source but I was careful in collection of open source information, extracting information only from

credible websites with a history of providing accurate, unbiased and government-worded statements. An extensive web search was conducted while collecting all information.

Background

I have studied past cases of terrorist attacks in J&K and elsewhere and took time to compare and draw parallels with such incidents in different parts of the Globe.I studied in detail intelligence practices of terrorists/insurgents from open source and the existing Force Protection and Intelligence doctrines of several nations militaries.I took into cognizance the rate of failures and successes in tactical operations preceding and after instance of attacks on our forces , be it on military bases or in-transit.I compiled data on how the local populace behaved in response to such attacks and the rising number of stone pelting and the speeches delivered by Hurriyat leaders /politicians in the aftermath of attacks.I gathered as much information as possible from open source Pak based terrorist indices of behavior as apparent from hate speeches and veiled/direct threats.One such incident was the declaration to use suicide bombers.I categorized collected intelligence from open source into intelligence , counterintelligence and force protection intelligence by applying context and greater world knowledge (knowledge repository) to the various attacks.

THE FINDINGS

Finding1:HQs from unit to command components must lay down policies and procedures so as to enable the creation of dedicated Force Protection units and to this effect it is imperative that newer policies/procedures be appended to current intelligence/counterintelligence doctrine to accommodate a new intelligence discipline namely Force Protection intelligence. ***Recommendation: The Army Intelligence Directorate should pass orders for the training and setup process for Force Protection units , properly staffed and commanded by thoroughly trained officers and personnel.They can be drawn from MI Staff Officers and lower echelon billets and imparted training.This further extrapolates to the fact that tactics , techniques and procedures of Force Protection intelligence must be established and training imparted in the same vein.***

Finding 2: A study of past attacks such as URI , Pathankot , Sukna among others highlights the fact that terrorists are adapting to defensive tactics , techniques and procedures and are resorting to and devising different attack courses of action , leveraging asymmetric advantage by changing place and weapon delivery platform as well as selective targeting. The enemy is resorting to HUMINT/CI practices utilizing local inhabitants. ***Recommendation*****:** ***The Army HQs should admit the fact that its not only asymmetric warfare but a mix of asymmetric and hybrid domains. It should be clearly emphasized at command echelons that tactical battle decision planning should take into account of all possible delivery means of assault phase of the enemy , even those not yet thought of but happening in other parts of the Globe. It should be clearly understood that the terrorist will want to use the most current means of attack so as to catch our forces off guard , our forces being tuned to specific types of attack scenarios due to historical inertia , that is attacks from the same spectrum being conducted over the years. Recommendation: We must maintain a written Force***

Protection Doctrine where will be included all past attacks , lessons learned , frequency of such attacks , tactics used , tactic-damage dynamic , newer tactics and techniques adopted among other things. Such a Doctrine will provoke/prompt newer ideas/concepts about attack regimen during tactical plannings.The Doctrine should take into account all terrorist/insurgent intelligence/CI activity and liaison with the police will be very fruitful in compiling these data. Recommendation: It is highly recommended to make all unit and command officers aware of the risk-displacement/risk-aversion technique during target selection by terrorists as this is what our officers are blind to when they harden a possible target, forcing the terrorists to look elsewhere, such as convoys instead of fortified bases. Once the terrorists decide on the target he automatically starts intelligence collection to fit his battle strategy. The police are in a better position to detect/deny such activities as the terrorist resource pool is the local inhabitant's base. Hence it is highly recommended that Army Intelligence (I should say Army Intelligence and Force Protection intelligence officers) closely liaise with local police and intelligence agencies. This is where the CI component of both AI and FP units come into play apart from Humint agents .All these will reduce the vulnerability of forces-in-transit to sporadic but planned attacks by terrorists.

Finding 3: It has been observed that attacks on bases/camps have shifted to convoys.The underlying threat translates from challenging the imperviousness of fortified military installations to personnel killings in numbers.If we further extend this line of thinking then it wont be surprising if attacks are conducted on embarking or disembarking troops at railway stations or for that matter troops-in-train-transit.All these may sound a bit far fetched right now given present circumstances of localized terrorist attacks but as I said earlier asymmetric war is characterized by the primary element of surprise. ***Recommendation: Apart from in-transit troops protection protocol inter-state-transit troops need also be given adequate preventive protection.The focus should be on detect/deny and prempt such terrorist attacks.For that intelligence , counterintelligence and Force Protection intelligence must be integrated with movement planning and security.It is important that current procedures of Force Protection are reassessed , modified and implemented in keeping with this Commissions findings.***

FINDING SUMMARY

1. **I found that the Army does not have a dedicated Force Protection Unit which could have extended counterintelligence, intelligence, security and police specific security to in transit troops. I find that there are no template Force Protection security measures such as a force protection cell specifically providing support to outgoing forces in transit as opposed to static forces in bases/camps. I find there is no dedicated separate Regimental Security Office which will have tasking authority over separate Force Protection units/detachments and effect operational synchronization (I find no separate Force Protection cells/units/detachments as said earlier).I found that liaison activities of the Army with the local police did not explore the possibility of being transformed as a Force Multiplier for the Police with respect to security of the army personnel. I find that the various stakeholders in the area of Force Protection did not actively and directly relate or participate with any dedicated Force Protection Unit , rather it was standard operating procedures , military security and intelligence led not intelligence driven involvement , with a**

broad rigid Force Protection programme and not Force Protection at a resolution at ground level , tactical and much finer than the coarse resolution level at higher echelons of the CRPF.

2. **I found that there could have been a total lack of validation and prioritization process in order to monitor Force Protection variables and whether the existing SOPs answered every question arising due to different ground scenarios , keeping earlier attacks in perspectives and historical data of adaptation of terrorists to newer force TTPs and movement security thus resorting to newer terrorist attack delivery platforms.I find that existing SOPs are rigid without any major initiative to incorporate changes in light of emerging trends after the attacks in URI , Sukna , and elsewhere.**
3. **I found that current Force Protection practices were not adequately addressed so as to be continually updated.Newer policies to this effect were not framed.I find that mission-specific Force Protection needs are only highlighted and hence only those policy guidelines are adhered to that fill in mission requirements.A 360 degrees policy adherence is not the case and hence obsolete or Force Protection practices that do not provide necessary guidance come into play.**
4. **I find that a standardized and consistent training program did not exist that addresses the training needs and this absence is primarily due to the fact that we don't have dedicated Force Protection units/cells/detachments , existence of which would have made possible separate education and training Doctrine.I find that the lack of Force Protection specific training regimen is one of the primary causes behind the disaster.**
5. **I find it is not acknowledged that SOPs have a life cycle and that adaptations , modifications and overhaul is very necessary in light of current adaptive trends in enemy tactics , techniques and procedures.**

General Note

Mission essential tasks of any unit Commander should include adequate Force Protection listed as a priority requirement.The organic intelligence capability , if created , can enhance the commanders situational awareness so he can develop security programs accordingly.We find in the Pulwama terrorist attack incident there are reports of advance warning , warning that emanated from Signals.There was a reported , verified incident in Pakistan of the terrorist group airing a video threatening an attack. Images and speech accessed by India Today show Jaish-e-Mohammed commander Moulana Rouf Asghar, younger brother of JeM chief Masood Azhar, addressing a rally in Karachi nine days ahead of the Pulwama terror attack, where he gave indications of suicide attacks being planned by the Pakistan-based terror outfit in India and Kashmir. In his speech, Asghar also mentioned Ghazi Rashid, who is being considered as the brains behind the dastardly suicide bombing in Awantipora, Pulwama which claimed the lives of 44 CRPF jawaans. The intelligence input, sent on behalf of the Inspector General of Police, Kashmir, asked all security agencies to "sanitize areas properly before occupying your place or deployment as there are inputs that IEDs could be used".Headlined "extremely urgent", the letter

accessed by IANS, was marked to the Deputy Inspector General of Central Reserve Police Force, South Srinagar; DIG CRPF, North Srinagar; DIG CRPF North Kashmir, Baramulla; DIG CRPF South Kashmir, Awantipora; DIG CRPF South Kashmir, Anantnag; DIG Sashastra Seema Bal, South Headquarters (Special Operations) Kashmir and all Senior Superintendent of Police of Kashmir zone.The information was also shared with Inspector General, CRPF, Kashmir operations sector, IG CRPF, Srinagar sector, IG Border Security Force Headquarter Kashmir, all range Deputy Inspector Generals of Police of Kashmir zone, Brigadier General Staff (operations) at the Srinagar-based 15 Corps, the DIG Indo-Tibetan Border Police (ITBP), the Air Force, , the Commandant Central Industrial Security Force (CISF) and SSP, Armed Police, Control Room Srinagar.The letter also mentioned that it should be for "all concerned".

Keeping all the above in perspective it is strongly felt that had our forces had their own organic intelligence units and a separate Force Protection Detachment assigned to the unit then such cases of external intelligence inputs from Govt/Military agencies and Open Source would not have gone ignored and could have been analysed , interpreted and disseminated more effectively , the disaster could have been averted.The point to note here is that organic intelligence units and a Force Protection detachment in Direct Support mode are more tuned to the overall protection of the unit than higher HQs as they are much closer to the ground , and the intelligence requirements is judged from a finer resolution rather than at a coarser level as seen by higher HQ.

(To Be Continued)..
(To be continued , detailed findings , policy and recommendations)

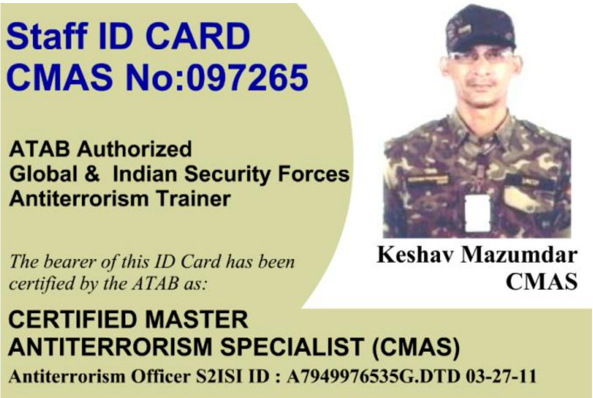
The next and final edit of the draft will dwell on the policy and procedures to enable FP dets and why the requirement of FP specific intelligence,humint CI taskorganized with various Force Protection conditions.Am color coding area sectors in keeping with threat intensity index,orange being high alert.This FP conditions will be time variable and influenced by threat perceptions and live display.A change from a lighter color to say orange will impact security forces action in a more aggressive way.Intelligence collection and human exploitation in the community will increase.There are more but we need this color coded force protection conditions live display system.

P.S.Soldiers are dying.situation chaotic and uncertain in kashmir.too many deployment but targeting based on search ops,cordon and not full int supported.paramil forces in the fray and their command cannot synchronise properly with int,officers not int savvy.admixture of army and paramilitary,concept of ops not defined clearly.this admixture is not task organized.mission specific task organized teams with int support coupled with cordon and search ops is required and aided by human exploitation teams as we are dealing with a hybrid case,terrorists,local sympathizers and those who are actively supporting terrorists.Time for CI elements under cover to conduct ops in community areas.int ops need to be preceded by thorough int/CI planning.

Example-Security application: Terrorist activity prone areas have the local populace as their center of gravity.I'll label areas most sensitive and with history of frequent attacks

orange.cordoning these areas away from the yellow labelled ones where we have large scale demonstrations and overt terrorism support.finally the grey areas where peace prevails and low public activity.setting up checkpoints roadblocks and troops chain in order to seperate these zones and then conducting search ops will be fruitful as escape routes and entry blocked.ops can be configured as per colour code.orange demands active mil ops,yellow human exploitation,detention and interrogation and intimidation while grey psychological ops.this way the battlespace can be shaped and forces optimally committed with proper usage of resources and tactical combat support such as other int disciplines , MP,Signals.

KESHAV MAZUMDAR CRC CMAS CAS FNWC ASC CPO ATO



Staff ID CARD
CMAS No:097265

ATAB Authorized
Global & Indian Security Forces
Antiterrorism Trainer

The bearer of this ID Card has been certified by the ATAB as:

Keshav Mazumdar
CMAS

CERTIFIED MASTER
ANTITERRORISM SPECIALIST (CMAS)
Antiterrorism Officer S2ISI ID : A7949976535G.DTD 03-27-11

QUESTION BANK

My team at Bijapur was given questions from here and performed satisfactorily

Q1. According to author Sun Tzu how can we elicit “foreknowledge”?

a. From spirits
b. Analogy with past events
c. From calculations.
d. Obtained from men who know the enemy situation.

Q2. ATAB stands for?

a. Anti Terrorism Accreditation Board
b. Anti Terrorism Attack Board.
c. Anti Terrorism Accreditation Battalion.
d. None is correct.

Q6. Military planning is dependent on

a. Clearly defined
b. Achievable
c. Measurable objectives
d. All are correct.

Q7. Intelligence should provide an understanding of the adversary’s

a. probable intentions
b. objectives
c. strengths
d. weaknesses
e. All are correct

Q8. Intelligence is essential for

a. plan,
b. Conduct,
c. Assess operations
d. All are correct

Q9. Intelligence should assess.

a. Whether operations are creating positive effects.
b. whether operations are creating negative effects
c. A & B correct
d. None is correct.

Q10. Humint Functions :

a. Provide intelligence support to Problem Framing.

b. Provide intelligence support to Course of Action Development.

c. Provide intelligence support to Course of Action War gaming.

d. All are correct

Q11. Intelligence estimate is based on all

a. available intelligence

b. considers everything of operational significance

c. A&B is correct

d. C is correct.

Q12. Thus the aim of the commander is to study the intents and devise appropriate course/s of actions taking into account factors are:

a. Including order of battle,

b. intelligence preparation of the battlefield,

c. enemy capabilities.

d. All are correct

Q13. What is required to understand the battle?

a. Proper War Planning and Analysis
b. Proper Mission Planning and Analysis.
c. Proper Battle Planning and Analysis
d. Proper game Planning and Analysis

Q14. What are the priorities of Defending?

a. our installation
b. our troops
c. our information
d. All are correct.

Q15. What is the Diminish means?

a. To know all solders of the enemy
b. To know all facilitators of the enemy.
c. To know all factories of the enemy.
d. To know all fighters of the enemy.

Q16. How do you Denying enemy?

a. Prevent the enemy a push-back safe area or safe haven.
b. Prevent the enemy to pull-back safe area or safe haven.
c. The enemy a pull-back danger area.
d. The enemy a pull-back no flies zone area or safe haven.

Q17. What are the 3 mission objectives?

a. Defend
b. Diminish.
c. Deny
d. All are correct.

Q18. What is the final object of a Mission?

a. Defend
b. Diminish.
c. Deny
d. Defeat.

Q19. Without intelligence solders are:

a. It's like the tiger without its nails.

b. It's like the tiger without its

teeth.

c. It's like the Lion without its

teeth.

e. None is correct.

Q20. Intelligence is the foundation of

a. Military opportunities.
b. Military persons.
c. Military activities
d. Military operations

Q21. IPB stands for?

a. Intelligence operation of the battle space.
b. Intelligence preparation of the battle space.
c. Intelligence preparation of the battle field.
d. Preparation of the battle space.

Q22. IPB supports.

a. Situation development
b. Targeting.
c. Force protection
d. All are correct.

Q23. COA stands for courses of action.

a. False
b. True

Q24. BDA stands for?

a. Battle Damage Assignment.
b. Battle improve Assessment.
c. Battle Damage Assessment.
d. None is correct.

Q25. The success of offensive operations at all levels is predicated by sound intelligence

a. About the enemy order of battle,
b. Environmental factors including but not limited to the political and human terrain dimensions.
c. A& B is correct
d. None is correct.

Q26. Threat and vulnerability assessments are paramount for successful offensive operations.

a. True
b. False.

Q27. During a conflict army commanders use a mix of operations, sequentially or simultaneously.

a. To achieve victory.
b. To achieve military
c. To defeat enemy
d. None is correct.

Q28. The success of the operations is determined by accurate, timely intelligence input.
a. To the operations planners and commanders at mid levels.

b. To the operations planners and commanders at lower levels.
c. To the operations planners and commanders at all levels.
d. To the operations planners and commanders at top levels.

Q29. Which type of operation is conducted in peacetime?

a. Defensive operations..
b. Offensive operations.
c. Suitable operations.
d. Stability operations.

Q30. How many criteria meet Intelligence requirements?

a. Two Criteria.
b. Three criteria
c. Five Criteria
d. Four Criteria.

Q31. What are the criteria that meet Intelligence requirements?

a. Accuracy
b. Feasibility
c. Timeliness
d. Specificity
e. All are correct.

Q32. If intelligence comes in late then ?
a. It is of no use
b. It is of sharp use
c. It is of proper use
d. It is of critical use

Q33. Which criteria is a very important factor for Intelligence?

a. Accuracy
b. Feasibility
c. Timeliness
d. Specificity

Q34. Our intelligence requirement is specific.

a. False

b. True

Q35. How many approaches in targeting,

a. Two
b. Three
c. One
d. Four.

Q36. Which are approaches in targeting?

a. Productive and destructive.
b. Production and destructive.
c. Productive and destruction.
d. Production and destruction.

Q37. All military planning, intelligence preparation of the battlefield and pre and post combat assessments must be focused on the.

a. Environment
b. Enemy.
c. Emergency
d. A&B correct.

Q38. During vetting by the Targeting Officer it is very important that the target meet set down selection criteria and after engagement.

a. True
b. False.

Q39. At the end of the targeting process the Commander approves the Target list and it is sent over to the

a. Various commanding units for execution of the approved targets.
b. Various subordinate units for execution of the approved targets.
c. One subordinate unit for execution of the approved targets.
d. No subordinate unit for execution of the approved targets.

Q40. The targeting process is a very

a. Involved process.
b. Solved process.
c. Involved manner.
d. Involved system.

Q41. The Targeting officer assumes a very easy position in the process.

a. True
b. False.

Q42. Conduct intelligence functions and operations which support targeting by identifying

a. Target systems,
b. Critical nodes
c. High-value/high pay off
d. All are correct.

Q43. How many points are important for Targets and providing intelligence most effectively?

a. 16
b. 10
c. 15
d. 12.

Q44. The kill equation goes like this.1 kill=10 new insurgents.

a. True
b. False.

Q45. Combat patrol which is resourced and designed as a last resort.

a. To kill
b. To capture an HVT
c. A&B is correct
d. None is correct.

Q46. What are the Primary Intelligence Tasks?

a. Conduct intelligence preparation of battlefield/AO
b. Situation development

c. Force protection
d. All are correct.

Q47. Plan, prepare, execute, and assess the mission is

a. Solders focus
b. Everybody's focus
c. Nobodies focus
d. Commanders focus.

Q48. Conduct ISR by Synchronizing ISR, Integrating ISR, Tactical Reconnaissance Ops, Surveillance

a. True
b. False

Q49. Decide on the COA out of all the possible COAs arrayed against expected enemy COAs is

a. Subordinates Decisions
b. Commander's Decisions.
c. Commando's Decisions.
d. Everybody's Decisions.

Q50. Tactical intelligence is required to answer intelligence requirements at the tactical level in response to.

a. Enemy TTPs.
b. Commando's TTPs
c. People's TTPs
d. Everyone TTPs

Q51. To analyst's information may trigger further surveillance using which system?

a. Audio to track the bomb storage and factories.
b. Audio & Video to track the bomb storage and factories.
c. HUMINT to track the bomb storage and factories.
d. Video to track the bomb storage and factories.

Q52. If the tactical analyst is at ground level he can directly access the IED without wasting time

a. True
b. False

Q53. Surveillance platforms are used to detonate the IED.

a. Remotely.
b. Directly
c. Manually
d. Other systems.

Q54. This is Combat Information and can be shared with commanders before further analysis.

a. If immediate action is required.
b. If there is any other urgent need.
c. A& b is correct
d. C is correct.

Q55. How many Operating Systems are required for battlefield?

a. Six
b. Five
c. Four
d. Seven

Q56. BOS is stands for?

a. Battlefield operating system.
b. Battlefield operation system.
c. Battlefield optimum system.
d. Battle fire operating system.

Q57. Intelligence Operations follow how many phases?

a. Follow a six-phase.
b. Follow a four-phase.
c. Follow a five-phase.
d. Follow an eight-phase.

Q58. Which phases intelligence process known as the intelligence cycle?

a. Plan and Direct the collection effort.
b. Collecting the information.
c. Processing the collected information
d. All are correct.

Q59. Commander’s intent-→operations process and intelligence process→relevant information which includes intelligence→facilitates situational understanding (commander again as end user)

a. True
b. False

Q60. CCIRs stands for?

a. Commander’s Critical Information Requirements
b. Critical Commander’s Information Requirements
c. Commander’s Critical Information Reassessments
d. Common Critical Information Requirements

Q61. PIRs stands for priority information requirements.

a. True
b. False.

Q62. FFIRs stands for friendly fire information requirements.

a. True
b. False.

Q63. Which one is correct?

a. Planning is a static process.
b. Planning is not a static process.
c. Planning is not a running process.
d. Planning is not a strategically process.

Q64. The main goal of collection is to acquire data about the enemy’s?

a. environment,
b. resources
c. activities
d. All are correct

Q65. Intelligence here is

a. Tactical.
b. Easy
c. Impossible

d. Crucial .

Q66. We must determine the?

a. Intent of the enemy
b. Intent of the surveillance.
c. Intent of the survivals.
d. Content of the enemy.

Q67. We need to go for deep intelligence collection and access a myriad of sources so that slowly the behavioral characteristics are discerned.

a. True
b. False.

Q68. The Early Warning system is more of a proactive-intelligence approach rather than a

a. Reactive-intelligence one.
b. Reputed-intelligence one
c. Repeated-intelligence one
d. None is correct.

Q69. There after the Commander brainstorms with his staff the possible.

a. COAs
b. PIRs
c. CCIRs
d. BOS

Q70. A terrorist attack may more be directed at the Parliament House than a

a. Hall,
b. House
c. Cinema hall
d. Mall

Q71. What grossly sums up the steps in the intelligence cycle.

a. Develop intelligence requirements.
b. Collect information to answer intelligence requirements.
c. Compile analyzed information
d. All are correct.

Q72. If the enemy is an asymmetrical one like the terrorist/insurgent then it has the capability to attack hard targets.

a. True
b. False

Q73. Tracking adversary capabilities is a

a. Criminal process.
b. Crucial process.
c. Continual system.
d. Continual process

Q74. TTPs is stands for.

a. Tactics for Techniques and Procedures.
b. Tactics, Technical and Procedures.
c. Tactics, Techniques and Procurement.
d. Tactics, Techniques and Procedures.

Q75. To properly collect information during war or any situation involving what?

a. Ground troops and the enemy.
b. Enemy.
c. Ground troops.
d. Ground troops and the enemy position.

Q76. We need persons as HUMINT agents with

a. Good interrogation skills,
b. Ability to conduct tactical questioning.
c. Good debriefing skills
d. All are correct.

Q77. For a CI soldiers foreign language ability will be?

a. An asset.
b. A hazard

c. A burden
d. A good chance.

Q78. Collection comprises?

a. 3 main components.
b. 6 main components.
c. 5 main components.
d. 4 main components.

Q79. Command and control, collection platforms, sensors, processing and exploitation and data exfiltration: these are component of collection?

a. True
b. False.

Q80. Intelligence is technically speaking composed of ?

a. Four attributes.
b. Four activities.
c. Four systems
d. Five attributes.

Q81. Technically speaking composed attributes?

a. Collection,
b. Anticipation,
c. Transmission and efforts to degrade an enemy's efforts
d. All are correct.

Q82. Counterterrorism collection is more important than the other attributes.

a. True
b. False

Q83. The nature of target influences?

a. Intelligence collection.

b. Intelligence activities.
c. Intelligence collision.
d. Intelligence correction.

Q84. SIGINT stands for?

a. Sign intelligence.
b. Single intelligence
c. Signals intelligence.
d. Signals information.

Q85. NSA stands for?

a. National Scientist Agency.
b. National System Agency.
c. Nation Security Agency
d. National Security Agency.

Q86. COMINT stands for communications intelligence.

a. True
b. False.

Q87. ELINT stands for?

a. Electronic intelligence.
b. Electrical intelligence.
c. Emergency intelligence.
d. Electronic information.

Q88. FISINT stands for foreign instrumental signals intelligence.

a. True
b. False.

Q89. IMINT stands for Imagery intelligence.

a. True
b. False.

Q90. HUMINT stands for?

a. Human-source intelligence.
b. Human intelligence.
c. Human-sight intelligence.
d. Human-source internet.

Q91. Special reconnaissance (SR) is conducted by

a. Units of highly trained military personnel.
b. Military units of highly trained small personnel.
c. Small units of highly trained military personnel.
d. Small units of general trained military personnel.

Q92. Special reconnaissance (SR) is distinct from

a. Commander operations.
b. Military operations.
c. Commando activities.
d. Commando operations.

Q93. Open-source information is publicly available information appearing in print or electronic form.

a. True
b. False.

Q94. Open-source information takes information from?

a. Radio, television,
b. Newspapers, journals,
c. The Internet, commercial databases,
d. All are correct.

Q95. How many of finished intelligence are available to the consumer.

a. Five categories.
b. Four categories.
c. Six categories.
d. Three categories.

Q96. What are the categories of Finished Intelligence?

a. **Current intelligence**
b. **Estimative intelligence**
c. **Warning intelligence**

d. **All are correct.**

Q97. Which categories i addresses day-to-day events?

a. Current intelligence
b. Estimative intelligence
c. Warning intelligence
d. Research intelligence

Q98. DIA is stands for Directorate for Intelligence Production.

a. True.
b. False.

Q99. NGO is stands for

a. Non-governmental orphan.
b. Non-governmental organization.
c. Non-governmental social organization.
d. Non-governmental private organization

Q100. One of the most commonly and increasingly modified weapon of the insurgent is the IED.

a. True
b. False.

Q101. The HUMINT collector represents?

a. A high-density, high-demand asset.
b. A low-density, low-demand asset
c. A high-density, low-demand asset.
d. A low-density, high-demand asset.

Q102. This is particularly true in an information environment saturated with un-vetted information.

a. True
b. False.

Q103. HUMINT is not the most versatile and powerful information collection discipline.

a. True
b. False.

Q104. Special Forces efforts to stop the Taliban in Afghanistan at the beginning of OEF in late.

a. 2001
b. 2006
c. 2010
d. 2000

Q105. The two disciplines of most use in obtaining actionable intelligence against asymmetric warfare targets are?

a. HUMINT and FISINT
b. HUMINT and ELINT
c. SIGINT T and ELINT
d. HUMINT and SIGINT.

Q106. Which Army used HUMINT almost extensively for actionable intelligence during the Battle?

a. The US Army.
b. The French Army.
c. The Canadian Army.
d. The Indian Army.

Q107. What are the criteria while choosing the source for HUMINT.

a. Placement,
b. Access.
c. Motivation
d. All are correct.

Q108. The source can be self-motivated or the HUMINT operator can motivate him—in the latter case he should be susceptible to motivation, monetary or ideological.

a. True.
b. False.

Q109. There are how many components within HUMINT operations:

a. Four

b. Five
c. Three
d. Two

Q110. Components within HUMINT operations:

a. Plan,
b. Prepare,
c. Execute and Assess.
d. All are correct.

Q111. Mission duration must be carefully understood with all allowances for possible emergencies and the unexpected.

a. True
b. False

Q112. What is the actual collection activity phase where information is collected for HUMINT?

a. Plan,
b. Prepare,
c. Execute
d. Assess

Q113. How many main categories for HUMINT collection?

a. Seven
b. Five
c. Four
d. Eight

Q114. CEE stands for?

a. Captured enemy equipment.
b. Computerized enemy equipment.
c. Critical enemy equipment
d. Central enemy equipment.

Q115. Interrogation is an essential part of the intelligence process.

a. True

b. False.

Q116. SCO stands for?

a. Human source contact operations.
b. Human resource contact operations
c. Human source critical operations.
d. None is correct.

Q117. MDMP stands for military decision-making process.

a. True
b. False.

Q118. DOCEX method may proceed with false information falling into the hands of the enemy.

a. True.
b. False.

Q119. CEE operations are also part of the FISINT collection process.

a. True
b. False

Q120. Commanders that conduct HUMINT operations take responsibility for :

a. Constituting task organizations
b. Assigning missions
c. Execution of the mission
d. All are correct.

Q121. Commanders must understand and know the enemy, his organization, his ISR capability.

a. True
b. False.

Q122. ACE is stands for

a. Analysis & Control Element.
b. Analysis & Critical Element.
c. Analysis & Central Element.

d. None is correct.

Q123. ACT is stands for Analysis Control Team.

a. True.
b. False.

Q124. TEB is stands for?

a. Technical Exploitation Battalion.
b. Tactical Exploitation Battalion.
c. Tactical Exploitation Battlefield.
d. None is correct.

Q125. HUMINT activities ensure technical control and deconfliction.

a. True.
b. False.

Q126. Every soldier is a

a. Sensor.
b. Remote
c. Monitor
d. VDO eye.

Q127. Soldiers can conduct TQ when they are:

a. Manning a check post/roadblock
b. Occupying an OP
c. On a patrolling mission
d. All are correct.

Q128. Analysis is a continuous process.

a. True
b. False.

Q129. The collector should be aware of enemy's

a. Counterintelligence agents.
b. Counterintelligence threat
c. Armed agents
d. All agents.

Q130. . Once trust is established, it becomes easier to extract information and the source may be more willing to provide additional information.

- **a. True**
- **b. False.**

Q131. Soldiers would not only be empowered to protect themselves with equipment and weapons, but be empowered to protect the intelligence information in their minds- one of the greatest assets to the unit.

- **a. True**
- **b. False**

Q132. Neurolinguistics is a

- **a. Behavioral model.**
- **b. Behavioral communication model.**
- **c. Biological communication model.**
- **d. Natural communication model.**

Q133. HUMINT is considered the.

- **a. Eye for any intelligence operation.**
- **b. Backbone for any intelligence operation.**
- **c. Backhoe for any intelligence operation.**
- **d. Backing for any intelligence operation.**

Q134. The screening of human sources is the first step of the FISINT collection.

- **a. True**
- **b. False.**

Q135. Several ways may be used to enter the operation area and their mission is to

- **a. Avoid direct combat.**
- **b. Avoid direct contact.**
- **c. Avoid direct control.**
- **d. Avoid direct conflict.**

Q136. To extract vital information, the method of torture seems to be the first option.

a. True.
b. False.

Q137. Which country prisoners committed suicide when captured in WWII ?

a. The Germanise prisoners
b. The Japanese prisoners
c. The US prisoners
d. The Indian prisoners

Q138. Screening is not an information collection technique.

a. true
b. False.

Q139. One very important point to be noted here is that screening may have to be executed in a very short span of time.

a. True.
b. False.

Q140. In screening operations the target is usually the permanent and transitory population in the AO such as.

a. Refugees,
b. Locals, EPWs
c. Other detainees.
d. All are correct.

Q141. Tactical screening is conducted during combat.

a. True
b. False.

Q142. CI operatives are interested in persons who :

a. Have no identification documents.
b. Have excessive or modified identification documents.

c. Possess unexplainable large amounts of cash or valuables.
d. All are correct.

Q143. At this point the civilian or military detainee should be initially questioned as to his name, rank, unit, job type, why he is here.

a. True.
b. False.

Q144. Any items seized from them including documents are also tagged and bagged.

a. True.
b. False.

Q145. The source is assigned a screening code as follows: Cooperation level: B means:

a. Responds very well to questioning.

b. Responds hesitatingly to questioning.

c. Responds very poor to questioning.

d. None is correct.

Q146. The source is assigned a screening code as follows Knowledge ability level: 3 means:

a. Appear to have all information.

b. Does not appear to have any information

c. B is correct.

d. None is correct.

Q147. The screener may have to make a rapid ''prescreen'' in order to filter out the individuals who have no information.

a. True.

b. False.

Q148. Debriefing and interrogation are the two basic types of interviews.

a. True.

b. False.

Q149. Elements which must be collected at interviews.

a. **HUMINT collection requirements which are urgent**
b. **The EPW/detainee serial number who is to be analyzed**
c. **The questioning time and location.**
d. **All are correct.**

Q150. Strong judgment needs to be carried out whether to be dominant or use psychological pressures

a. **True.**
b. **False.**

Q151. The prisoner may drop his guard after he is made comfortable and given a hearty beer.

a. **This would actually occur due to drowsiness.**
b. **This would actually occur due to sleepiness.**
c. **This would actually occur due to friendly atmosphere.**
d. **None is correct.**

Q152. It is formal in nature to meet in an apartment space but informal to meet in an office.

a. **True.**
b. **False.**

Q153. Incentives may play a vital role in the

a. **Extraction of information.**
b. **Extraction of knowledge.**
c. **Knowledge of information.**
d. **None is correct.**

Q154. BSC is stands for?

a. **Behavioural Science Consultant.**
b. **Behavioural Scientific Consultant.**
c. **Behavioural Science Consumer.**
d. **Best Science Consultant.**

Q155. The tentative technique must be selected keeping in mind.

a. **3 primary factors.**

b. 4 primary factors.
c. 2 primary factors.
d. 4 primary factors.

Q156. Over friendliness and loss of control of the interrogation must also be avoided.

a. True.
b. False.

Q157. Such subjects must be passed on to the senior interrogators when the juniors have already carried out their limited interview.

a. True.
b. False.

Q158. For a reluctant subject, the intelligence interrogation must assume the tempo like

a. Riding a cycle.
b. Riding a horse.
c. Riding a car.
d. Riding a motorcycle.

Q159. Which parts have been determined as the standard lines of procedure.

a. Detention and arrest
b. Preliminary interview and questioning
c. Intensive examinations
d. All are correct.

Q160. The commander's PIR and SIR demand to know if?

a. The enemy will fire.
b. The enemy will bombing.
c. The enemy will move.
d. The enemy will attack.

Q161. Every operation is initiated as per plan.

a. True.
b. False.

Q162. Make sure that the ops officer understands

- **a. All intelligence platforms available.**
- **b. All platforms available.**
- **c. All interrogation platforms available**
- **d. All intermediate platforms available.**

Q163. Militarized and non-militarized strategies are part of the asymmetric warfare process.

- **a. True.**
- **b. False.**

Q164. Asymmetric warfare does not engage in traditional.

- **a. Force-on-force engagements.**
- **b. Face-to-face engagements.**
- **c. Force-on-force fighting.**
- **d. Force-on-force direct contact.**

Q165. The ultimate goal of an insurgency is to politically amputate the working power for control of all.

- **a. True.**
- **b. False.**

Q166. A proper understanding of the operational environment helps in.

- **a. Making the right decision in deploying proper resources and combat forces.**
- **b. Making the right decision in deploying proper levels of solders.**
- **c. Making the right decision in deploying proper levels of arms.**
- **d. None is correct.**

Q167. What are basically the violent activities that insurgents can choose to utilize?

- **a. Terrorist,**
- **b. Guerilla,**
- **c. Conventional tactics.**

d. All are correct.

Q168. Non-military courses of action such as

a. Kidnapping, Political demonstrations
b. Hostage taking, infiltration and subversion,
c. Propaganda and seizure actions.
d. All are correct.

Q169. An intelligence officer can gather intelligence from a variety of channels.

a. True.
b. False.

Home Made Explosives Part 2

1. Aluminum Powder may look:

a. Whitish

b. Silver

c. Gray or black

d. Both a & b

e. All of the above

ANSWER: e.

2. Aluminum Power vapors can be explosive.

a. True

b. False

ANSWER: a.

3. Some commercial uses for Aluminum Powder are:

a. Paints

b. Pyrotechnics

c. First-aid cold packs

d. Both a & b

e. All of the above

ANSWER: d.

4. In small quantities (less than 5 gallons) Ammonium Nitrate may be stored in glass or plastic containers; however in larger quantities (more than 5 gallons), it should be contained in:

a. Steel drums

b. Wooden barrels

c. Plastic or paper bags

d. None of the above / plastic containers only

ANSWER: c.

5. Some of the key identifiers for Ammonium Nitrate are:

a. Crystalline or powder that is colorless or yellow & odorless

b. Spherical pellets, granular, crystalline or powder that is colorless or white & odorless

c. Spherical pellets, granular, crystalline or powder that can be gray, black or white & odorless

d. Spherical pellets, granular, crystalline or powder that is colorless or white, with an acrid/ sour odor

ANSWER: b.

6. Some of hazards of Ammonium Nitrate are:

a. Eye, skin, respiratory irritant

b. Should not be near chemicals rich in oxygen

c. By itself it can be explosive

d. Both a. & c.

e. Both a. & b.

ANSWER: d.

7. Ammonium Nitrate can be found in products purchased from:

a. Agricultural supply stores, chemical supply stores, first aid supplies

b. Agricultural supply stores, beauty supply stores, first aid supplies

c. Beauty supply stores, chemical supply stores, first aid supplies

d. Chemical supply stores, first aid supplies, health food stores

ANSWER: a.

8. Some key identifiers for Citric Acid are:

a. Crystalline, white or colorless, acrid/sour odor

b. Power (fine), silver or white, odorless

c. Crystalline, white or colorless, odorless

d. Power (fine), silver or white, acrid/sour odor

ANSWER: c.

9. Other names for Citric Acid can be:

a. Hydrogen Nitrate & citric salt

b. Hydrogen Citrate & sour salt

c. Hydrogen Dioxide & sour salt

d. None of the above

ANSWER: b.

10. One of the commercial uses for Citric Acid is as a food additive.

a. True

b. False

ANSWER: a.

11. Ethylene Glycol is also known as:

a. Glycol of Ethyl

b. Ethanediol

c. Glycoethyl

d. Monoethyl Glycol

ANSWER: b.

12. Large quantities (more than 5 gallons) of Ethylene Glycol will more than likely be found stored in:

a. Large glass containers

b. Large steel containers

c. Both a. & b.

d. None of the above / should be stored in small quantities only

ANSWER: b.

13. Ethylene Glycol should ideally be stored in a warm, oxygen rich environment to stabilize its nature.

a. True

b. False

ANSWER: b.

14. Some of the commercial uses of Ethylene Glycol include:

a. Antifreeze

b. Commercial explosives

c. Both a. & b.

d. None known

ANSWER: c.

15. Hexamine can come in a crystalline or solid white tablet form and:

a. Is odorless

b. Has a slight fish odor

c. Has an acrid, sour odor

d. Has a slight ammonia like odor

ANSWER: d.

16. Large quantities of Hexamine are usually stored in:

a. Woven bags

b. Plastic bags

c. Steel containers

d. Plastic containers

ANSWER: a.

17. Hexamine is also known as:

a. Hexanitrate

b. Hexamethylene

c. Methenamine

d. None of the above

ANSWER: c.

18. Hexamine should not be stored near peroxides, or chemicals rich in oxygen.

a. True

b. False

ANSWER: b.

19. Because of its various commercial uses, Hexamine can be found in products sold in:

a. Agricultural supply stores

b. Camping & army surplus stores

c. Chemical stores

d. Both a. & c.

e. Both b. & c.

f. All of the above

ANSWER: e.

20. Hydrochloric Acid is most commonly know to be found in liquid form, but in its purest state may also be found in a solid tablet form.

a. True

b. False

ANSWER: b.

21. Some examples of equipment that would be likely in the presence of large quantities of Hydrochloric Acid would be:

a. Grinders, respirators, acid resistant aprons, impermeable gloves, fume hoods

b. Blenders, respirators, acid resistant aprons, fume hoods

c. Protective face/eyewear, impermeable gloves, respirators, fume hoods

d. Grinders, Pyrex containers, acid resistant aprons, protective face/eyewear

ANSWER: c.

22. Hydrochloric Acid should not be stored near anything except other acids.

a. True

b. False

ANSWER: a.

23. Some commercial uses for Hydrochloric Acid are:

a. Paint remover

b. Beauty supply products

c. Manufacture of plastics and some chemicals

d. All of the above

ANSWER: c.

24. Hydrogen Peroxide is also known as:

a. Hydroxide

b. Dihydrogen Dioxide

c. Hydrogen Dioxide

d. None of the above

ANSWER: b.

25. Some key identifiers for Hydrogen Peroxide are:

a. Clear, colorless liquid, odorless

b. Slightly whitish/milky liquid, odorless

c. Light/pale blue liquid, with a slightly pungent, caustic odor

d. Clear, colorless liquid, with a slightly pungent, caustic odor

ANSWER: d.

26. Select where the highest concentration of Hydrogen Peroxide can be obtained:

a. Internet

b. Chemical supply stores

c. Beauty supply stores

d. Drug stores

ANSWER: b.

27. Magnesium Powder can come in the following form:

a. Solid

b. Spherical pellets

c. Powder

d. Both a. & c.

e. All of the above

ANSWER: d.

28. Small quantities of Magnesium Powder may be stored in:

a. Plastic & steel containers

b. Steel containers

c. Plastic containers

d. Plastic or paper bags

ANSWER: a.

29. Magnesium Powder should not be stored in direct sunlight as it could cause the release of flammable gasses.

a. True

b. False

ANSWER: b.

30. With regards to the known hazards of Methyl Ethyl Ketone, it should be remembered that the vapor:

a. May be present in adjacent areas

b. Can be explosive

c. May cause drowsiness and dizziness

d. Both a. & c.

e. All of the above

ANSWER: e.

31. One especially caustic solution that Methyl Ethyl Ketone should be kept away from is:

a. Acid

b. Lye

c. Hydrogen Peroxide

d. None of the above

ANSWER: b.

32. A couple of commercial uses for Methyl Ethyl Ketone are:

a. Wax remover and paint thinners

b. Manufacture of engines and cars

c. Dynamite and pyrotechnics

d. Paint removers & plastics manufacture

ANSWER: d.

33. Nitric Acid has the darkest hue (color), when:

a. Its concentration level is high

b. Its concentration is low

c. When it is exposed to heat or direct sunlight

d. None of the above / colorless

ANSWER: a.

34. Skin exposed to Nitric Acid will turn:

a. White

b. Black

c. Yellow

d. Red

ANSWER: c.

35. Two additional names Nitric Acid is known as are:

a. Aqua Fortis & Azotic Nitrate

b. Aqua Nitrate & Azotic Fortis

c. Hydrogen Nitrate & Aqua Acid

d. Aqua Fortis & Azotic Acid

ANSWER: d.

36. Inhalation of Nitric Acid can be fatal.

a. True

b. False

ANSWER: a.

37. A weapon of choice in many parts of Asia and the Middle East use __________ as a means for disfiguring women.

a. Hydrochloric acid

b. Sulfuric acid

c. Nitric acid

d. All of the above

ANSWER: d.

38. The commercial uses of Nitric Acid vary widely; from rocket propellant, to fertilizer/explosives manufacture, to beauty supply products.

a. True

b. False

ANSWER: b.

39. Some of the key identifiers for Nitro Methane are that it is:

a. Liquid, clear colorless to light yellow or greenish yellow, pungent / sour odor

b. Liquid, colorless, fruity disagreeable odor

c. Liquid, colorless, sweet, minty, acetone-like agreeable odor

d. Liquid, light to dark brown color, odorless

ANSWER: b.

40. Large quantities of Nitro Methane can be kept in glass, metal or plastic containers.

a. True

b. False

ANSWER: b.

41. Some of the hazards of Nitro Methane are:

a. It can be explosive in hot confined areas

b. Extremely flammable vapors, flammable, and susceptible to explosion

c. Dizziness, vomiting, weakness & fall in blood pressure

d. Both a. & b.

e. All of the above

ANSWER: e.

42. One example of a commercial use for Nitro Methane is:

a. Dynamite

b. Beauty supply products

c. Industrial solvent

d. Paint remover

ANSWER: c.

43. Potassium Chlorate is a:

a. White, odorless liquid

b. White, odorless crystalline or powder

c. White, acrid or sour odor, crystalline or powder

d. White, acrid or sour odor liquid

ANSWER: b.

44. Potassium Chlorate is also known as:

a. Chlorate of Potassium

b. Chlorate of Potash

c. Potash Chlorate

d. Potassium Oxynitrate

ANSWER: b.

45. Below are some examples of places where Potassium Chlorate could be sourced. Which one is not?

a. Agricultural supply stores

b. Beauty supply stores

c. Chemical supply stores

d. Hardware supply stores

ANSWER: b.

46. Potassium Permanganate can come in a solid or crystalline, is odorless, violet or purple in color, & will stain most anything, including the skin which it will stain ________?

a. Purple

b. Blue

c. Brown

d. It will not affect skin

ANSWER: c.

47. Potassium Permanganate stands out as different in that although it has certain hazards, i.e. should not be near metals, acids, fuels, peroxides and combustibles, when it come to safe handling, the most that is required is a well ventilated area (open windows, doors and fans).

a. True

b. False

ANSWER: False

48. Three main types of locations that Potassium Permanganate can be acquired at are:

a. Agricultural, chemical & pool supply stores

b. Agricultural, chemical & first aid supply stores

c. Aquarium, chemical & pool supply stores

d. Aquarium, agricultural & pool supply stores

ANSWER: c.

49. Sodium Chlorate is used in these commercial purposes:

a. Fertilizer

b. Pesticides

c. Plastic Manufacture

d. None of the above

e. All of the above

ANSWER: d.

50. Some key identifiers for Sulfur are:

a. Granular, white, odorless

b. Powder (chalky), colorless, smells like rotten eggs when heated

c. Powder (chalky), yellow, odorless

d. Tablet form, white until ground, then yellowish, smells like rotten eggs

ANSWER: c.

51. Which is NOT an example of a commercial use for Sulfur?

a. Fertilizer

b. Food additive

c. Matches

d. Soil additive

ANSWER: b.

52. Sulfur, if combined with chemicals rich in oxygen could be used to create a ________ HME:

a. Ammonium Nitrate Mixtures

b. Dynamite

c. Water gels

d. Flash powders

ANSWER: d.

53. Sulfuric Acid is also known as:

a. Oleam

b. Vitriol

c. Hydrogen Sulfur

d. None of the above

ANSWER: b.

54. Sulfuric Acid is very corrosive, as well as a severe irritant to eyes, skin and respiratory systems, and therefore, should be stored near chemicals rich in oxygen, but away from caustic solutions such as lye.

a. True

b. False

ANSWER: b.

55. An example of a commercial use for Sulfuric Acid is:

a. Drain pipe cleaners

b. Automotive batteries

c. Polymer manufacture

d. Both a. & c.

e. All of the above

ANSWER: e.

56. Sulfuric Acid can be used to make the following HME:

a. EDGN

b. TATP

c. MEKP

d. Both b. & c.

e. All of the above

ANSWER: e.

57. Urea can come in crystalline, granular or powder form and has the following odor:

a. None

b. Metallic like

c. Ammonia like

d. All of the above (each form differs)

ANSWER: c.

58. Some hazards of Urea are that it can be an eye, skin and respiratory irritant; however, in cream form it can be used as a moisturizer for dry, cracked, calloused & rough skin.

a. True

b. False

ANSWER: a.

59. Grinders are used to reduce the granule size of solid components. An example would be:

a. Mortar / pestle

b. Handheld electric coffee grinder

c. Commercial grade coffee grinder

d. Ball mill

e. Both b. & c.

f. All of the above

ANSWER: f.

60. Grinders are commonly used in the production of which HME?

a. Ammonium Nitrate Mixtures

b. Black Powder

c. Chlorate / Perchlorate Mixtures

d. All of the above

ANSWER: d.

61. Ice baths cool mixtures that generate heat. An example of an ice bath would be:

a. Ice with salted water

b. Dry ice with acetone

c. Bath water

d. Both a. & b.

e. All of the above

ANSWER: e.

62. Ice baths are commonly used in the production of this HME:

a. TATP

b. HMTD

c. MEKP

d. Both b. & c.

e. All of the above

ANSWER: e.

63. Distillers concentrate chemical components with low-level heat, and therefore, require complex scientific equipment and not improvised or household items as some other process methods can get away with.

a. True

b. False

ANSWER: b.

64. Filters are used to separate the solids from the liquids and are commonly used in the HME production of:

a. HMTD

b. TATP

c. Hydrogen Peroxide Mixtures

d. Urea Nitrate

e. All of the above

ANSWER: e.

65. There are various hazards associated to the handling of the chemicals we have discussed such as eye, skin & respiratory irritants, severe burns etc., that can only heighten during the production of HMEs; therefore a telltale indicator that HMEs are in fact being produced will be the presence of safety equipment such as masks, goggles, face shields,

protective clothing and vents.

a. True

b. False

ANSWER: b.

Home Made Explosives

1. Which of the following is NOT an example of a homemade explosive?

a. Ammonium Nitrate Mixtures

b. Chlorate/Perchlorate Mixtures

c. Syntax Peroxide Mixtures

d. Triacetone Triperoxide

ANSWER: c.

2. Which of the following is NOT a chemical component?

a. Ammonium Nitrate

b. Cellulose Acetate

c. Hexamine

d. Nitric Acid

ANSWER: b.

3. Binders are materials that are used to hold certain explosive mixtures together. Which of the following is NOT an example of such a material?

a. Carnauba Wax

b. Duct Tape

c. Grease

d. Vaseline

ANSWER: b.

4. In order to readily enable you to determine if you are dealing with a homemade explosive(s) lab, it is imperative you memorize the hard & fast rules of what to look for.

a. True

b. False

ANSWER: b.

5. If, in a suspected explosives lab, you notice finer, more granular product in the presence of Pyrex or scientific glassware, filters, acid-resistant skin protection & ice water baths, which of the following should be furthered reviewed for information?

a. Ammonium Nitrate

b. Black Powder

c. Chlorate/Perchlorate Mixtures

d. Urea Nitrate

ANSWER: d.

6. Below are examples of equipment that would suggest safety measures are being implemented. Select the item that doesn’t reflect this:

a. Impermeable Gloves

b. Dust Masks

c. Protective Eyewear

d. Blenders

ANSWER: d.

7. If you notice predominantly liquid components in a suspected lab, along with scientific glassware, safety glasses, acid-resistant skin protection etc. Which of these following would you review information on?

a. Ammonium Nitrate

b. EGDN

c. HMTD

d. Urea Nitrate

e. All of the above

ANSWER: b.

8. One example of an Ammonium Nitrate Mixture would be:

a. Ammonium Nitrate & Confectionery Icing

b. Ammonium Nitrate & Coffee

c. Ammonium Nitrate & Vegetable Oil

d. Ammonium Nitrate & Citric Acid

ANSWER: a.

9. One hazard of Ammonium Nitrate is that it can be explosive in hot, confined areas.

a. True

b. False

ANSWER: a.

10. Black Powder can appear in the following hues:

a. Gray

b. Dark Blue

c. Black

d. Both a. & c.

e. All of the above

ANSWER: d.

11. Some commercial uses of Black Powder are:

a. Fuses

b. Pyrotechnics

c. Gunpowder

d. Both a. & c.

e. All of the above

ANSWER: e.

12. Potassium Nitrate can be found in which of the following:

a. Shampoo

b. Cooking oil

c. Food Preservatives

d. Anti-bacterial Hand Soap

ANSWER: c.

13. A key identifier of Chlorate / Perchlorate Mixtures is:

a. A sugary sweet odor

b. That it is odorless

c. A dead fish smell

d. A fuel odor

ANSWER: b.

14. One of the chemical components found in Chlorate / Perchlorate Mixtures is:

a. Petroleum Jelly

b. Ethylene Glycol

c. Nitric Acid

d. Sulfuric Acid

ANSWER: a.

15. Key identifiers of Ethylene Glycol Dinitrate (EGDN) are that it is an oily, viscous liquid that can range from colorless to dark yellow and is odorless.

a. True

b. False

ANSWER: a.

16. Colorless to white product found with solids settled at the bottom of a container and stored in a refrigerator or freezer may be:

a. Ammonium Nitrate Mixtures

b. Clorate / Perchlorate Mixtures

c. Hexamethylene Triperoxide Diamene (HMTD)

d. Methyl Ethyl Ketone Peroxide (MEKP)

ANSWER: c.

17. If found, Hexamethylene Triperoxide Diamene (HMTD), should be stored near metals to ensure stability of the product.

a. True

b. False

ANSWER: b.

18. Hexamethylene Triperoxide Diamene (HMTD), can be made by combining chemical components found in such items as:

a. Nail polish remover, bleaching agent, nitric acid

b. Paint remover, hair products, sulfuric acid

c. Hair products, cumin, racing car fuel

d. Camp stove fuel tablets, hair products, water softener

ANSWER: d.

19. Select the key identifiers for Hydrogen Peroxide Mixtures.

a. Liquid or semi liquid gel, mixture color varies with additives, slightly pungent caustic odor

b. Liquid or semi liquid gel, colorless to white, odorless

c. Oily, viscous liquid, colorless to dark yellow, odorless

d. Powdery substance, finer than flour, gray or black in color, dead fish odor

ANSWER: a.

20. Methyl Ethyl Ketone Peroxide (MEKP) is also known as:

a. Ethylene Dinitrate

b. Hexamine

c. Luberisol DDM

d. Mother of Satan

ANSWER: c.

21. Hazards of Methyl Ethyl Ketone Peroxide (MEKP) are:

a. Extremely sensitive to impact, friction, static spark & heat; should not be near metals

b. Extremely sensitive to impact, friction, static spark & heat; should not be near sulfuric acid

c. Large quantities can self-heat and ignite if in sunlight or elevated room temperatures

d. Large quantities can become unstable and ignite if kept in cooler room temperatures

ANSWER: b.

22. Some key identifiers for Triacetone Triperoxide (TATP) are:

a. Flour like appearance, solids settle on top of the container, fruity or vinegar smell

b. Sugar like appearance, solids settle at the bottom of the container, fruity or vinegar smell

c. Crystals, colorless to white in appearance, solids settle at the bottom of the container, odorless

d. Sugar like appearance, solids settle at the bottom of the container, odorless

ANSWER: b.

23. The chemical components that make up Triacetone Triperoxide (TATP) are:

a. Acetone, Acid, Hydrogen Peroxide

b. Methyl Ethyl Ketone, Acid, Hydrogen Peroxide

c. Acetone, Nitromethane, Hydrogen Peroxide

d. Hydrogen Peroxide, Acetone, Ethanol

ANSWER: a.

24. One of the commercial uses for Triacetone Triperoxide (TATP) is:

a. Blasting Agent (also know as ANFO)

b. Dynamite

c. Flash powders: Fireworks

d. None known

ANSWER: d.

25. Urea Nitrate is also known as:

a. Acidogen Nitrate

b. Gunpowder

c. Luberisol DDM

d. Mother of Satan

e. None of the above

ANSWER: a.

26. Urea Nitrate is unique in that additives will not alter the physical appearance of its color.

a. True

b. False

ANSWER: b.

27. Commercial uses for Urea Nitrate include:

a. Blasting Agent (also know as ANFO)

b. Dynamite

c. Hydroponics

d. None known

e. Both a. & c.

ANSWER: d

28. Urea is found in:

a. Cumin

b. Fertilizer

c. Hair products

d. Nail polish remover

ANSWER: b.

29. Equipment used for the purpose of mixing Urea Nitrate is:

a. Blenders, grinders, distillers, ice bath

b. Glassware, distillers, blenders, filters

c. Glassware, mixers, ice bath, filters

d. Grinders, mixers, plastic containers, filters

ANSWER: c.

30. The chemical components that make up Urea Nitrate are such that the mixture requires refrigeration.

a. True

b. False

ANSWER: b.

31. One of the key identifiers of Acetone is that is has a sweet flowery or perfume like odor, much like nail polish remover.

a. True

b. False

ANSWER: a.

32. Large quantities of Acetone may be kept in:

a. Large wooden kegs 5 to 55 gallons

b. Large plastic drums from 10 to 50 gallons

c. Large metal cans or drums from 5 to 55 gallons

d. Large quantities cannot be stored; may self-heat & ignite

ANSWER: c.

33. Acetone vapors can cause drowsiness, dizziness, and numbness in hands and feet.

a. True

b. False

ANSWER: a.

34. Acetone is readily accessible to anyone, through the purchase of products sold at:

a. Beauty supply stores

b. Chemical supply stores

c. Drug stores

d. Both a. & c.

e. All of the above

ANSWER: e.

Terrorism Threat AT Officer Training

1. The following is DOD's definition of terrorism:

"The calculated use of violence or threat of violence to inculcate fear; intended to coerce or intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological."

a. True

b. False

ANSWER: a.

2. When looking at a geographical area, what factors must you consider when determining the threat?

a. Are there any terrorist groups in that geographical area?

b. Are they violent?

c. What tactics, weapons, & types of attacks are they know for?

d. How do they operate?

e. How active are they?

f. All of the above

ANSWER: f.

3. When conducting a terrorism threat assessment one must include a terrorist profile. A typical terrorist profile is: male, 20's, single, urban, well educated and middle to upper class.

a. True

b. False

c. Not enough information to answer

ANSWER: a.

4. During a possible terrorism threat which of the following are possible terrorist tactics?

a. Beheadings

b. Bombings

c. Sieges & occupations

d. Kidnapping

e. None of the above

f. All of the above

ANSWER: f.

5. In the target selection phase of a terrorism threat, what needs to be considered?

a. Target of opportunity

b. Recognition target

c. Retaliation target

d. Both a. & b.

ANSWER: d.

6. In the DOD’s increasing terrorism threat level chart, the second level of threat is identified as “significant” and by the colour orange.

a. True

b. False

ANSWER: b.

7. When conducting a terrorism threat analysis based on the DOD's terrorism threat level chart, one must consider the following:

a. History / existence

b. Capability / intentions

c. Faction / cause

d. Last known attack proxemics

e. Both a. & b.

ANSWER: e.

8. In order to "fill in the gaps", in the terrorism threat analysis picture, local initiative is needed. Fusing local asset information with threat intelligence helps to create a full threat analysis.

a. True

b. False

ANSWER: a.

9. When conducting a full terrorism threat assessment local initiative is needed to fill the gaps in the threat assessment picture. The following are examples of local information channels:

a. Local authorities

b. Local businesses

c. Media

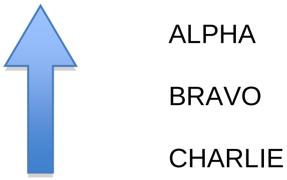
d. Local citizens

e. None of the above

f. All of the above

ANSWER: f.

10. In terms of a terrorism threat, the following is the correct Force Protection Condition sequence:



ALPHA

BRAVO

CHARLIE

a. True

b. False

ANSWER: b.

11. Force Protection Condition, or FPCON Normal, is best described as:

a. A terrorist attack is imminent

b. No indication of probable terrorist attack

c. Best information received indicates terrorist attack is probable

d. Condition white

ANSWER: b.

12. When in FPCON Normal, one would expect to see a normal security posture to the terrorism threat level:

a. True

b. False

ANSWER: a.

13. Force Protection Condition FPCON Alpha is best described as:

a. An increased general threat of possible activity & violence, the nature of which could is unpredictable.

b. An attack is imminent on personnel and facilities

c. Real time information suggests violence

d. An attack is not probable based on information received

ANSWER: a.

14. Force Protection Condition FPCON Bravo is best described as:

a. When an increased or more predictable threat of terrorist activity exists

b. An attack is imminent on personnel and facilities

c. Must be capable of being maintained

d. Both a. & c.

e. None of the above

ANSWER: d.

15. It is a standard operating procedure, that when in FPCON Bravo, extra precaution is appropriate to deter terrorist planning:

a. True

b. False

ANSWER: a.

16. You should expect to see closer inspections of vehicles and deliveries, as well as ID checks & a greater presence of guards on your installation during FPCON Bravo.

a. True

b. False

ANSWER: a.

17. FPCON Charlie is best described as:

a. When an attack has occurred & rigorous security is required

b. When an incident occurs or intelligence is received indicating some sort of terrorist action or targeting against personnel or facilities is likely

c. Nothing indicates that an installation is targeted

d. General conditions suggest possible violence

ANSWER: b.

18. During FPCON Charlie one would expect rigorous efforts to inspect vehicles & facilities & you may be required to inspect vehicles & facilities, as well as be required to participate in special guard duties.

a. True

b. False

ANSWER: a.

19. When a terrorist attack has occurred, or when intelligence has been received that indicates terrorist action against a specific location is imminent, the Force Protection Condition is known as FPCON Delta.

a. True

b. False

ANSWER: a.

20. When FPCON Delta exists, one can expect:

a. Additional security measures are implemented which delay & interrupt normal routines

b. Expect rigorous efforts to conduct further inspections on vehicles & installations

c. Evidence of a terrorist attack in the planning - such as surveillance or local source reports

d. None of the above

e. All of the above

ANSWER: a.

21. When considering your security measures during a terrorist threat, it is essential operating procedure to implement random security measures in conjunction with the Force Protection Condition.

a. True

b. False

ANSWER: a.

22. When developing a comprehensive, anti-terrorism program, one must ensure the following components are present:

- **Threat Assessment**
- **Vulnerability Assessment**
- **AT Plan**
- **AT Program Review**
- **Practical Exercises**
- **Training**

a. True

b. False

c. Not enough information to answer

ANSWER: a.

23. When planning self protective measures during a terrorist threat, on should:

a. Be prepared for unexpected events

b. Overcome routines

c. Always divulge your information to several individuals so they can reach you during an incident

d. Stay within the boundaries of daily routines

e. Both a. & b.

f. Both c. & d.

ANSWER: e.

24. During a terrorist threat, one should maintain a low profile & overcome routines, as well as varying routes & times to & from work.

a. True

b. False

ANSWER: a.

25. During a terrorist threat, one should consider the following self-protective measures:

a. Be alert & aware of changes in the security atmosphere

b. When possible stay indoors & avoid public venues

c. When in public, look for larger crowds & stay with them when moving

d. Avoid public disputes or confrontations & report any trouble to the proper authorities

e. Both a. & d.

f. Both b. & c.

ANSWER: e.

Bomb Threat Management

1. A bomb threat could be a warning or simply a hoax. If upon search you locate a suspicious package or “bomb” and you’re *certain* it is a hoax, (or a training exercise), then you can safely pick up the package/bomb, bring it in, & advise your superior that you safely located the item.

a. True

b. False

ANSWER: b.

2. If a bomb threat is received and search reveals nothing out of the ordinary, you can safely conclude that the call was simply a hoax & relax your guard – business as usual.

a. True

b. False

ANSWER: b.

3. Types of bombers are broken down into 3 different categories – suicidal, amateur & professional.

a. True

b. False

ANSWER: b.

4. Of the various types of categorized bombers, the least worrisome is the amateur bomber.

a. True

b. False

ANSWER: b.

5. Bombers are generally referred to as falling under what main categories:

a. Amateur

b. Professional

c. Psychopathic

d. Suicidal

e. a., b. & d.

f. All of the above

ANSWER: f.

6. Examples of *typical* motivators for bombers would be:

a. Emotional release / revenge

b. Ideological / recognition

c. Experimental / vandalism

d. Both a. & b.

e. All of the above

ANSWER: e.

7. Bomb threats would normally be handled:

a. Internally by a company CEO, or kept within the confines of a household

b. EMS

c. Local Law Enforcement or Private Security

d. By the person who received the call

e. All of the above

ANSWER: c.

8. There are general guidelines for the handling of a bomb threat scenario. If you know of a bomb threat, or are the receiver of a bomb threat you should be sure to:

a. Try to obtain answers to a checklist questions as quickly as possible so you can pass the information on to authorities

b. Ensure to show emotion to the caller as a means of humanizing the situation

c. Ensure that you do not ask the caller if they placed the bomb

d. Ask the caller when the bomb is going to explode

e. All of the above

ANSWER: d.

9. Showing emotion over the phone when you are the receiver of a bomb threat can humanize the situation, and 50% of the time could thwart the intended plot.

a. True

b. False

ANSWER: b.

10. Which of the following question(s) should not be asked if you are the receiver of a bomb threat call?

a. When is the bomb going to explode?

b. Where is it located now?

c. What kind of a bomb is it & what does it look like?

d. Did you place the bomb?

e. Both b. & c.

f. All should the above should be asked

ANSWER: f.

11. If you are the receiver of a bomb threat call, ensure that you concentrate on obtaining answers to the general guideline questions & don’t become distracted or unfocused in the task by background noise during the call.

a. True

b. False

ANSWER: b.

12. In additional to obtaining answers to the checklist of questions you should have if you are the recipient of a bomb threat call, you should also be sure to try and determine:

a. Race

b. Sex

c. Age

d. Background Noise

e. Choice a., b. & c.

f. All of the above

ANSWER: f.

13. Everyone that could potentially be assigned the task of conducting a search for a bomb or suspicious package, should, if they happen upon either of these:

a. Ensure they well versed in the handling of varied bombs types

b. Ensure they are properly geared up in a bomb suit prior to conducting the search

c. Leave the handling of such items to EOD or bomb personnel only

d. Both b. & c.

ANSWER: c.

14. When faced with a bomb threat, there are decision-making guidelines that should be considered. Some examples are:

a. Race of the caller?

b. Age of the caller?

c. Sex of the caller?

d. All of the above

e. None of the above

ANSWER: e.

15. When faced with a bomb threat, there are certain decision-making guidelines that should be considered. Some examples are:

a. How tight is the security at the target?

b. What is the targets’ previous experience?

c. What is the current climate for terrorist or radical activity?

d. All of the above

e. None of the above

ANSWER: d.

16. The intended “target” of a bomb threat is generally the biggest unknown.

a. True

b. False

ANSWER: b.

17. The intended time to detonate is generally the biggest unknown for a bomb threat.

a. True

b. False

ANSWER: a.

18. Not knowing when a bomb is set to detonate, is of particularly less concern to:

a. Those in the surrounding perimeter of the bomb

b. Those in the immediate area of the bomb itself

c. Those in Law Enforcement

d. All of the above

ANSWER: b.

19. Standard operating procedures for bomb threat management should include who will notify facility personnel & how they will be notified.

a. True

b. False

ANSWER: a.

20. History has taught us that they are several common placement locations for bombs to be set. Which of the following is not a common location?

a. Behind bushes

b. Outside stairs

c. Lobby Areas

d. Restrooms, especially Men's

ANSWER: d.

21. Some xamples of planning issues that could hinder action to deal with bomb threats would be:

a. Time & Money

b. Training & effort spent on planning

c. Current information; intelligence

d. Both a. & b.

e. All of the above

ANSWER: e.

22. There are two evacuation options – evacuation or no evacuation.

a. True

b. False

ANSWER: b.

23. There are three evacuation options – evacuation, partial evacuation or no evacuation.

a. True

b. False

ANSWER: a.

24. Evacuation procedure processes should include:

a. A primary evacuation route

b. A secondary evacuation route

c. Assembly areas – both primary & secondary

d. Windows & doors should be left open

e. a., b. & c.

f. All of the above

ANSWER: f.

25. Unlike fire drill / evacuation procedures where “floor wardens” are assigned, in the case of a bomb threat time is of the essence and therefore no such “wardens” or leaders are necessary.

a. True

b. False

ANSWER: b.

26. Some key responsibilities of Evacuation Leaders during a bomb threat evacuation are:

a. To ensure all window & doors are left open

b. To know the primary & secondary evacuation routes, as well as the primary and secondary assembly areas

c. Provide accountability for all persons in their evacuation zones

d. To screen the evacuation routes for secondary devices

e. a., b. and d.

f. b., c. & d.

ANSWER: f.

27. In order to maximize everyone’s safety, where the bomb is located (i.e. briefcase, van, large truck), should determine whether or not the distance for the evacuation assembly area(s) should be widened in case of detonation.

a. True

b. False

ANSWER: a.

28. In the case of evacuation and a known location of a potential bomb, the following distance for evacuation safety should be:

Small box	**-**	**985 feet or 300 meters**
Briefcase	**-**	**1123 feet or 342 meters**
Small car	**-**	**1500 feet or 457 meters**
Large car	**-**	**1750 feet or 534 meters**
Van	**-**	**2750 feet or 838 meters**
Large Truck	**-**	**5000 feet or 1534 meters**

a. True

b. False

ANSWER: b.

29. With regards to evacuation scene safety, there are several guidelines that should be adhered to. Which of the following is NOT a recommended guideline?

a. Avoid puddles of liquid

b. Wear PPE

c. Stay down wind/hill if possible

d. Do not move suspicious objects

ANSWER: c.

30. With regards to Establishing Security & Control, in the event that a bomb has detonated, it is important to be empathetic to the victims and evacuees. One way to demonstrate this is by waiting a min. of 24 hours prior to establishing a perimeter, setting up a command post etc., as this will only add to the stress of those around.

a. True

b. False

ANSWER: b.

31. If a blast has occurred, some general guidelines to follow in regards to general scene

response include:

a. Establish a perimeter, which may be up to a 900-foot radius around the blast crater

b. Establish a command post

c. Safety sweep the area immediately surrounding the command post & within the perimeter for secondary devices

d. Both b. & c.

e. All of the above

ANSWER: e.

32. When exercising scene safety, it is important to:

a. Request add'l resources & personnel to mitigate identified hazards

b. Use tools and PPE appropriate to the tasks being dealt with

c. Mark hazard areas clearly and designate safety zones to receive victims & evacuees

d. Both a. & b.

e. All of the above

ANSWER: e.

33. An example of an additional resource to request when dealing with a site where a blast has occurred is:

a. Bomb technicians

b. Building inspectors

c. Representatives from utility companies such as gas, water, electric

d. Both a. & c.

e. All of the above

ANSWER: e.

34. One of the most important aspects when it comes to scene safety is to allow full access to the scene – the more eyes the better!

a. True

b. False

ANSWER: b.

35. With regards to scene safety control, it is important to keep track of your people. You should have full knowledge of not only the number of people at the scene, but also be further aware of the number of individuals working in hazards, as well as non-hazard areas.

a. True

b. False

ANSWER: a.

36. If a blast occurs, time is of the essence to deal with evacuating individuals from the blast area as well as dealing with victims that have been injured. Which of the following is NOT a priority at this time?

a. Initiate rescues of severely injured and/or trapped individuals

b. Preform triage

c. Remove fatalities

d. Treat life-threatening injuries

e. Evacuate ambulatory victims

ANSWER: c.

37. There are jurisdictional rights that take precedence for certain agencies, against which a bomb threat may be received directly or indirectly; because of the umbrella under which certain properties may fall. These specific agencies are:

a. BATF

b. FBI

c. Postal Service

d. Both a. & b.

e. All of the above

ANSWER: e.

38. FBI has jurisdiction in situations involving:

a. Bomb threats or offenses against property leased, used, or owned by the US Gov't

b. Bomb threats or offenses against property leased, used, or owned by the Treasury Dept.

c. Bomb threats or offenses against property leased, used, or owned by Postal Service

d. Both a. & b.

e. All of the above

ANSWER: a.

39. BATF has jurisdiction in situations involving:

a. Bomb threats or offenses against property leased, used, or owned by the US Gov't

b. Bomb threats or offenses against property leased, used, or owned by the Treasury Dept.

c. Bomb threats or offenses against property leased, used, or owned by Postal Service

d. None of the above

ANSWER: b.

40. Postal Service has jurisdiction in situations involving:

a. Bomb threats or offenses against property leased, used, or owned by the US Gov't

b. Bomb threats or offenses against property leased, used, or owned by the Treasury Dept.

c. Bomb threats or offenses against property leased, used, or owned by Postal Service

d. Both b. & c.

ANSWER: c.

41. A first responder called in to assist with a bomb threat scenario is likely to be requested to assist at the following type of scene:

a. Pre-detonation

b. Post-detonation

c. Searches

d. Continuing incident

e. All of the above

ANSWER: e.

42. In the case of possession of explosives while in or on the properties leased, used, or owned by all three of the following agencies, BATF, FBI or Postal Service, jurisdiction falls solely under the BATF.

a. True

b. False

ANSWER: b.

43. In the case of possession of explosives while in or on the properties leased, used, or owned by all three of the following agencies, BATF, FBI or Postal Service, jurisdiction falls solely under the FBI.

a. True

b. False

ANSWER: b.

44. Pre-detonation scenes may include:

a. Bomb threats

b. Suspicious items

c. Confirmed devices

d. Both b. & c.

e. All of the above

ANSWER: e.

45. The main concerns with regards to establishing scene security when a device or a suspicious item has been found are:

a. Deny access to the scene

b. Establish an evacuation distance

c. Establish a hard perimeter & begin evacuations

d. All of the above

e. None of the above

ANSWER: d.

46. No matter which type of incident occurs, things such as time (until detonation occurs), distance (evacuation distances), & shielding are universal things to consider. When it comes to distance, the most important thing to remember is time is of the essence therefore calculating the closest, safety distance to steer evacuees to is the most ideal.

a. True

b. False

ANSWER: b.

47. When a suspicious item or bomb is found, the most important thing to do immediately is to quickly move the suspicious item or bomb far away from people. It is much faster to move an item/bomb than it is to move a group of people.

a. True

b. False

ANSWER: b.

48. When evacuating individuals from a device that may or may not have detonated, it is important to move them quickly to safe areas. Again, time is of the essence, therefore the speed and distance at which you people is more important than hesitating and delaying the haste in which you move by worrying about secondary devices that may or may not be present.

a. True

b. False

ANSWER: b.

49. Once a suspicious item has been identified as a confirmed device, the device may then be handled or moved by:

a. Building maintenance

b. Law Enforcement / Private Security

c. First responders

d. Bomb technicians

e. All of the above

ANSWER: e.

50. Once a suspicious item has been identified as a confirmed device, shielding from the device must take place. The most important thing to remember here is:

a. More is always better – as much distance away the better

b. Structural differences (brick vs. cinder block vs. wood)

c. The size / type of the device

d. Both a. & b.

e. All of the above

ANSWER: d.

51. Safety of the public & of the bomb tech is always of utmost importance when dealing with a device. Also import to consider is the "safety" of the evidence. Two examples of this are, counter-charges & contamination.

a. True

b. False

ANSWER: a.

52. Post-detonation scenes will vary depending on the type of device used. A very small homemade device may cause little to no structural damage, whereas larger devices can cause major structural damage and mass confusion. Regardless of the damage caused, one must always keep in mind that rescue, recovery & fire suppression efforts will need room to do their job.

a. True

b. False

ANSWER: a.

53. While rescue, recovery & fire suppression efforts are underway, there is a possibility that these efforts may alter the scene and contaminate evidence to the point that it is altered or destroyed. At all costs, it is most important to preserve the evidence above all else.

a. True

b. False

ANSWER: b.

Anti Terrorism Accreditation Board
www.ATABonline.info

"Establishing a Safe Standard for Responders to Terrorist Incidents"

December 24, 2018

To whom it may concern:

The Anti Terrorism Accreditation Board was established in 2002 to standardize and provide a high standard of training to terrorism responders worldwide. ATAB has certified over 15,900 terrorism responders around the world. ATAB has provided training to over 98,000 military and law enforcement terrorism and first responders. ATAB was contracted by the U.S. Department of Defense to provide training for military members during the war in Iraq in the areas of Intelligence, Military Police, Special Operations and EOD. ATAB requested Mr. Mazumdar to assist us with this task.

Mr. Keshav Mazumdar, CMAS has been affiliated with the Anti Terrorism Accreditation Board (ATAB) since 2009. He earned his Certified Anti-terrorism Specialist Certification CAS on the 24th of April 2009 and his CMAS or Certified Master Anti-Terrorism Specialist certification on the 14th of August 2009. His ATAB ID number is 097265. Mr. Mazumdar was appointed Sr. Vice President of training committees on 3 May 2012. His responsibilities included the development of training materials to be utilized in the ATAB training of U.S. Military members in the Global War on Terror.

After extensive ATAB training and his completion of the S2 Safety and Intelligence Institute Tampa Florida which i got on 03/27/2011 bearing registration number A7949976535G Mr. Mazumdar was given Authorization by the Board of Directors of ATAB to provide training on behalf of ATAB and issue continuing education hours in the areas of intelligence/counterintelligence and antiterrorism and all of the ATAB areas of study.

With the change in U.S. Government requirements for private training of government employees ATAB was required to establish an independent online testing facility in order to provide training and maintain the integrity of the examinations. In 2013 Mr. Mazumdar established the ATAB War College and developed online capabilities for students to study and complete examinations while deployed to combat zones or to Navel Vessels.

In the time that I have known Mr. Mazumdar I have found him to be a true professional of the highest ethics. Mr. Mazumdar has been responsible for the training and coordination of 1000's of students for the last 9 years. In that time, we have only had one complaint and after reviewing the training records it was obvious that the complaining student had not completed the study materials and had not successfully passed the exam.

Mr. Mazumdar has developed complete training courses in Anti-Terrorism and Intelligence that have been utilized in training of U.S. Military members as well as responders from Canada, England, South and Latin America.

If you have any questions you may reach me at keithflannigan@atabonline.org or at 703-880-5212.

Professionally Submitted

J. Keith Flannigan

J. Keith Flannigan, PhD, CMAS
Certification Chairman
Board of Directors ATAB